The 5G-AKA Authentication Protocol Privacy (Technical Report)

ADRIEN KOUTSOS, LSV, CNRS, ENS Paris-Saclay, Université Paris-Saclay

We study the 5G-AKA authentication protocol described in the 5G mobile communication standards. This version of AKA tries to achieve a better privacy than the 3G and 4G versions through the use of asymmetric randomized encryption. Nonetheless, we show that except for the IMSI-catcher attack, all known attacks against 5G-AKA privacy still apply.

Next, we modify the 5G-AKA protocol to prevent these attacks, while satisfying 5G-AKA efficiency constraints as much as possible. We then formally prove that our protocol is σ-unlinkable. This is a new security notion, which allows for a fine-grained quantification of a protocol privacy. Our security proof is carried out in the Bana-Comon indistinguishability logic. We also prove mutual authentication as a secondary result.

CCS Concepts: • **Security and privacy → Formal security models**; **Privacy-preserving protocols**; *Mobile and wireless security*.

Additional Key Words and Phrases: AKA, Unlinkability, Privacy, Formal Methods.

ACM Reference Format:
Adrien Koutsos. 2019. The 5G-AKA Authentication Protocol Privacy (Technical Report). 1, 1 (July 2019), 141 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Mobile communication technologies are widely used for voice, text and Internet access. These technologies allow a subscriber's device, typically a mobile phone, to connect wirelessly to an antenna, and from there to its service provider. The two most recent generations of mobile communication standards, the 3G and 4G standards, have been designed by the 3GPP consortium. The *fifth generation* (5G) of mobile communication standards is being finalized, and drafts are now available [38]. These standards describe protocols that aim at providing security guarantees to the subscribers and service providers. One of the most important such protocol is the *Authentication and Key Agreement* (AKA) protocol, which allows a subscriber and its service provider to establish a shared secret key in an authenticated fashion. There are different variants of the AKA protocol, one for each generation.

In the 3G and 4G-AKA protocols, the subscriber and its service provider share a long term secret key. The subscriber stores this key in a cryptographic chip, the *Universal Subscriber Identity Module* (*USIM*), which also performs all the cryptographic computations. Because of the *USIM* limited computational power, the protocols only use symmetric key cryptography without any pseudo-random number generation on the subscriber side. Therefore the subscriber does not use a random challenge to prevent replay attacks, but instead relies on a sequence number SQN. Since the sequence number has to be tracked by the subscriber and its service provider, the AKA protocols are stateful.

Because a user could be easily tracked through its mobile phone, it is important that the AKA protocols provide privacy guarantees. The 3G and 4G-AKA protocols try to do that using temporary identities. While this provides some privacy against a *passive adversary*, this is not enough against an *active adversary*. Indeed, these protocols allow an antenna to ask for a user permanent identity

Author's address: Adrien Koutsos, adrien.koutsos@lsv.fr, LSV, CNRS, ENS Paris-Saclay, Université Paris-Saclay.

2019. XXXX-XXXX/2019/7-ART $15.00
https://doi.org/10.1145/1122445.1122456

when it does not know its temporary identity (e.g. in roaming situations). This mechanism is abused by IMSI-catchers [37] to collect the permanent identities of all mobile devices in range.

The IMSI-catcher attack is not the only known attack against the privacy of the AKA protocols. In [15], the authors show how an attacker can obtain the least significant bits of a subscriber's sequence number, which allows the attacker to monitor the user's activity. The authors of [4] describe a linkability attack against the 3G-AKA protocol. This attack is similar to the attack on the French e-passport [3], and relies on the fact that 3G-AKA protocol uses different error messages if the authentication failed because of a bad Mac or because a de-synchronization occurred.

The 5G standards include changes to the AKA protocol to improve its privacy guarantees. In 5G-AKA, a user never sends its permanent identity in plain-text. Instead, it encrypts it using a *randomized asymmetric encryption* with its service provider public key. While this prevents the IMSI-catcher attack, this is not sufficient to get unlinkability. Indeed, the attacks from [4, 15] against the 3G and 4G-AKA protocols still apply. Moreover, the authors of [22] proposed an attack against a variant of the AKA protocol introduced in [4], which uses the fact that an encrypted identity can be replayed. It turns out that their attack also applies to 5G-AKA.

Objectives. Our goal is to improve the privacy of 5G-AKA while satisfying its design and efficiency constraints. In particular, our protocol should be as efficient as the 5G-AKA protocol, have a similar communication complexity and rely on the same cryptographic primitives. Moreover, we want strong guarantees on the privacy provided by our protocol.

Formal Methods. Formal methods are the best way to get a strong confidence in the security provided by a protocol. They have been successfully applied to prove the security of crucial protocols, such as Signal [30] and TLS [12, 21]. There exist several approaches to formally prove a protocol security.

In the *symbolic* or *Dolev-Yao* (DY) model, protocols are modeled as members of a formal process algebra [1]. In this model, the attacker controls the network: he reads all messages and he can forge new messages using capabilities granted to him through a fixed set of rules. While security in this model can be automated (e.g. [13, 18, 20, 33]), it offers limited guarantees: we only prove security against an attacker that has the designated capabilities.

The *computational model* is more realistic. The attacker also controls the network, but is not limited by a fixed set of rules. Instead, the attacker is any Probabilistic Polynomial-time Turing Machine (PPTM for short). Security proofs in this model are typically sequences of game transformations [36] between a game stating the protocol security and cryptographic hypotheses. This model offers strong security guarantees, but proof automation is much harder. For instance, CryptoVerif [14] cannot prove the security of stateful cryptographic protocols (such as the AKA protocols).

There is a third model, the *Bana-Comon* model for equivalence properties [8, 9], also known as the Computationally Complete Symbolic Attacker model. This is a first-order logic, in which messages as represented by terms. But instead of specifying the adversary by what he can do, as in the Dolev-Yao model, the adversary is defined negatively by what he *cannot do*, using a set of first-order axioms Ax. These axioms may reflect structural properties of the logic, implementation assumptions on the primitives (e.g. functional correctness), or cryptographic hypotheses on the primitives. We require that these axioms are computationally valid, under some cryptographic assumptions. Then, given a protocol and a security property, we can compute a formula ψ expressing the security of the protocol. Showing the unsatisfiability of the conjunction of the axioms Ax and the negation of ψ entails the security of the protocol. Indeed, we know that there exists no adversary that can simultaneously satisfy the axioms Ax and break the security property. Since our axioms are computationally valid, we deduce that the security property ψ holds in all computational models: the protocol is secure.

This model has several advantages over the Dolev-Yao and the computational models. First, it gives strong security guarantees, as security in the Bana-Comon model implies computational security. Second, this model is simpler than the computational model: there is no probabilities and no security games, only first-order formulas. Third, it does not allow for *implicit assumptions*. For example, if the security of a protocol relies on the fact that the first projection of a nonce can (almost) never be confused with an agent's name, then we need to add an axiom stating that this is the case. Otherwise, the security proof cannot be completed. Proving a protocol in the Bana-Comon model requires to make precise and *explicit* assumptions on the protocol implementation. Finally, it is well-suited to analyse stateful protocol, such as the AKA protocols.

A inherent drawback of the Bana-Comon approach is that it is only valid for protocols with a finite number of sessions: we may only consider protocols with no unbounded replication. Still, it is possible to show that a protocol is secure for any *constant but arbitrarily large* number of sessions. E.g. if ψ_n is a formula encoding the security of n sessions of a protocol, then it is sufficient to show that for every n, $\mathsf{Ax} \wedge \neg\psi_n$ is unsatisfiable. Typically, such a proof is done by induction over n (this is the approach we use in this paper). Note that security for any constant number of sessions does not imply security for a number of sessions that depends on the security parameter. Nonetheless, most attacks do not require polynomially-many sessions.

Related Works on the AKA Protocol. There are several formal analysis of AKA protocols in the symbolic models. In [18], the authors use the Deepsec tool to prove unlinkability of the protocol for three sessions. In [4] and [39], the authors use Proverif to prove unlinkability of AKA variants for, respectively, three sessions and an unbounded number of sessions. In these three works, the authors abstracted away several key features of the protocol. Because Deepsec and Proverif do not support the xor operator, they replaced it with a symmetric encryption. Moreover, sequence numbers are modeled by nonces in [4] and [18]. While [39] models the sequence number update, they assume it is always incremented by one, which is incorrect. Finally, none of these works modeled the re-synchronization or the temporary identity mechanisms. Because of these inaccuracies in their models, they all miss attacks.

In [10], the authors use the Tamarin prover to analyse multiple properties of 5G-AKA. For each property, they either find a proof, or exhibit an attack. To our knowledge, this is the most precise symbolic analysis of an AKA protocol. For example, they correctly model the xor and the re-synchronization mechanisms, and they represent sequence numbers as integers (which makes their model stateful). Still, they decided not to include the temporary identity mechanism. Using this model, they successfully rediscover the linkability attack from [4].

We are aware of two analysis of AKA protocols in the computational model. In [22], the authors present a significantly modified version of AKA, called PRIV-AKA, and claim it is unlinkable. However, we discovered a linkability attack against the protocol, which falsifies the authors claim. In [31], the authors study the 4G-AKA protocol *without its first message*. They show that this reduced protocol satisfies a form of anonymity (which is weaker than unlinkability). Because they consider a weak privacy property for a reduced protocol, they fail to capture the linkability attacks from the literature.

Related Works Using the Bana-Comon Model. Several protocols have been analyzed using the Bana-Comon equivalence model. In [6], the authors design axioms for several cryptographic hypothesis: asymmetric encryption (ind-cca$_1$ and ind-cca$_2$), signatures (euf-cma) and for the Decisional Diffie-Hellman assumption. With these axioms, they prove that the Diffie-Hellman key-exchange provides real-or-random secrecy [2] of the shared key. They also prove several properties of the NSL protocol, including authentication and real-or-random secrecy of the shared nonces.

In [19], the authors analyze the privacy of two RFID authentication protocols, KCL [29] and LAK [32]. To do this, they had to design axioms for the xor operator and for hash functions, in particular for the for the Collision Resistance and Pseudo-Random Function cryptographic assumptions. Remark that the Bana-Comon model can handle the xor operator without difficulties, contrary to the symbolic model [5].

In [34], the authors design a prove secure a key wrapping API. Interestingly, their proof is modular in the choice of the symmetric encryption used in the wrapping mechanism: the authors design intermediate axioms for the wrapping mechanism, prove the security of the wrapping API using these axioms, and show that both *randomized* and *deterministic* symmetric encryption schemes satisfy the intermediate axioms. This is a nice benefit of the Bana-Comon approach.

Finally, in [7], the authors analyze the vote privacy of the FOO voting protocol [23]. First, they design axioms for blind signatures [17]. Second, they found new attacks on the privacy of the FOO protocol, when the candidate identities or the messages signatures are of different lengths. These are typical examples of implicit implementation assumptions that can be found using the Bana-Comon approach. Then, under the proper assumptions, they prove that the FOO protocol provides vote privacy.

Contributions. Our contributions are:

- We study the privacy of the 5G-AKA protocol described in the 3GPP draft [38]. Thanks to the introduction of asymmetric encryption, the 5G version of AKA is not vulnerable to the IMSI-catcher attack. However, we show that the linkability attacks from [4, 15, 22] against older versions of AKA still apply to 5G-AKA.
- We present a new linkability attack against PRIV-AKA, a significantly modified version of the AKA protocol introduced and claimed unlinkable in [22]. This attack exploits the fact that, in PRIV-AKA, a message can be delayed to yield a state update later in the execution of the protocol, where it can be detected.
- We propose the AKA$^+$ protocol, which is a modified version of 5G-AKA with better privacy guarantees and satisfying the same design and efficiency constraints.
- We introduce a new privacy property, called σ-unlinkability, inspired from [27] and Vaudenay's Strong Privacy [40]. Our property is parametric and allows us to have a fine-grained quantification of a protocol privacy.
- We formally prove that AKA$^+$ satisfies the σ-unlinkability property in the Bana-Comon model. Our proof is for any number of agents and sessions that are not related to the security parameter. We also show that AKA$^+$ provides mutual authentication.

Outline. In Section 2 and 3 we describe the 5G-AKA protocol and the known linkability attacks against it. We present the AKA$^+$ protocol in Section 4, and we define the σ-unlinkability property in Section 5. We recall the Bana-Comon model in Section 6, and show how we model the AKA$^+$ protocol using it in Section 7. We describe some of the axioms we use in this paper in Section 8. We state and sketch the proofs of the mutual authentication and σ-unlinkability of AKA$^+$ in Section 9, and we conclude in Section 10. The full proofs are in Appendix.

2 THE 5G-AKA PROTOCOL

We present the 5G-AKA protocol described in the 3GPP standards [38]. This is a three-party authentication protocol between:

- The *User Equipment* (*UE*). This is the subscriber's physical device using the mobile communication network (e.g. a mobile phone). Each *UE* contains a cryptographic chip, the *Universal Subscriber Identity Module* (*USIM*), which stores the user confidential material (e.g. secret keys).

- The *Home Network* (*HN*), which is the subscriber's service provider. It maintains a database with the necessary data to authenticate its subscribers.
- The *Serving Network* (*SN*). It controls the base station (the antenna) the *UE* is communicating with through a wireless channel.

If the *HN* has a base station nearby the *UE*, then the *HN* and the *SN* are the same entity. But this is not always the case (e.g. in roaming situations). When no base station from the user's *HN* are in range, the *UE* uses another network's base station.

The *UE* and its corresponding *HN* share some confidential key material and the *Subscription Permanent Identifier* (SUPI), which uniquely identifies the *UE*. The *SN* does not have access to the secret key material. It follows that all cryptographic computations are performed by the *HN*, and sent to the *SN* through a secure channel. The *SN* also forwards all the information it gets from the *UE* to the *HN*. But the *UE* permanent identity is not kept hidden from the *SN*: after a successful authentication, the *HN* sends the SUPI to the *SN*. This is not technically needed, but is done for legal reasons. Indeed, the *SN* needs to know whom it is serving to be able to answer to *Lawful Interception* requests.

Therefore, privacy requires to trust both the *HN* and the *SN*. Since, in addition, they communicate through a secure channel, we decided to model them as a single entity and we include the *SN* inside the *HN*. A description of the protocol with three distinct parties can be found in [10].

2.1 Description of the Protocol

The 5G standard proposes two authentication protocols, EAP-AKA′ and 5G-AKA. Since their differences are not relevant for privacy, we only describe the 5G-AKA protocol.

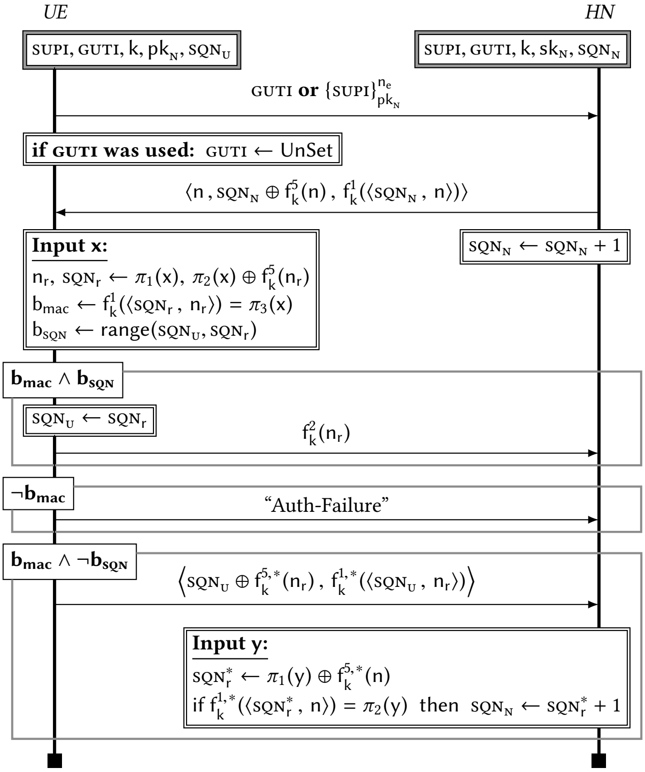
Cryptographic Primitives. As in the 3G and 4G variants, the 5G-AKA protocol uses several keyed cryptographic one-way functions: $\mathsf{f}^1 - \mathsf{f}^5$, $\mathsf{f}^{1,*}$ and $\mathsf{f}^{5,*}$. These functions are used both for integrity and confidentiality, and take as input a long term secret key k (which is different for each subscriber).

A major novelty in the 5G version of AKA is the introduction of an asymmetric randomized encryption $\{\cdot\}_{\mathsf{pk}}^{\mathsf{n_e}}$. Here pk is the public key, and $\mathsf{n_e}$ is the encryption randomness. Previous versions of AKA did not use asymmetric encryption because the *USIM*, which is a cryptographic micro-processor, had no randomness generation capabilities. The asymmetric encryption is used to conceal the identity of the *UE*, by sending $\{\textsc{supi}\}_{\mathsf{pk}}^{\mathsf{n_e}}$ instead of transmitting the SUPI in clear (as in 3G and 4G-AKA).

Temporary Identities. After a successful run of the protocol, the *HN* may issue a temporary identity, a *Globally Unique Temporary Identifier* (GUTI), to the *UE*. Each GUTI can be used in *at most one session* to replace the encrypted identity $\{\textsc{supi}\}_{\mathsf{pk}}^{\mathsf{n_e}}$. It is renewed after each use. Using a GUTI allows to avoid computing the asymmetric encryption. This saves a pseudo-random number generation and the expensive computation of an asymmetric encryption.

Sequence Numbers. The 5G-AKA protocol prevents replay attacks using a sequence number SQN instead of a random challenge. This sequence number is included in the messages, incremented after each successful run of the protocol, and must be tracked and updated by the *UE* and the *HN*. As it may get de-synchronized (e.g. because a message is lost), there are two versions of it: the *UE* sequence number $\textsc{sqn}_\textsc{u}$, and the *HN* sequence number $\textsc{sqn}_\textsc{n}$.

State. The *UE* and *HN* share the *UE* identity SUPI, a long-term symmetric secret key k, a sequence number $\textsc{sqn}_\textsc{u}$ and the *HN* public key $\mathsf{pk}_\textsc{n}$. The *UE* also stores in GUTI the value of the last temporary identity assigned to it (if there is one). Finally, the *HN* stores the secret key $\mathsf{sk}_\textsc{n}$ corresponding to $\mathsf{pk}_\textsc{n}$, its version $\textsc{sqn}_\textsc{n}$ of every *UE*'s sequence number and a mapping between GUTIs and SUPIs.


UE
HN
$\textsc{supi}, \textsc{guti}, \mathsf{k}, \mathsf{pk}_{\mathsf{N}}, \textsc{sqn}_{\mathsf{U}}$
$\textsc{supi}, \textsc{guti}, \mathsf{k}, \mathsf{sk}_{\mathsf{N}}, \textsc{sqn}_{\mathsf{N}}$
$\textsc{guti}$ **or** $\{\textsc{supi}\}^{\mathsf{n_e}}_{\mathsf{pk_N}}$
if $\textsc{guti}$ **was used:** $\textsc{guti} \leftarrow \mathsf{UnSet}$
$\langle \mathsf{n}, \textsc{sqn}_{\mathsf{N}} \oplus \mathsf{f}^5_{\mathsf{k}}(\mathsf{n}), \mathsf{f}^1_{\mathsf{k}}(\langle \textsc{sqn}_{\mathsf{N}}, \mathsf{n} \rangle) \rangle$
Input x:
$\mathsf{n_r}, \textsc{sqn}_{\mathsf{r}} \leftarrow \pi_1(\mathsf{x}), \pi_2(\mathsf{x}) \oplus \mathsf{f}^5_{\mathsf{k}}(\mathsf{n_r})$
$\mathsf{b_{mac}} \leftarrow \mathsf{f}^1_{\mathsf{k}}(\langle \textsc{sqn}_{\mathsf{r}}, \mathsf{n_r} \rangle) = \pi_3(\mathsf{x})$
$\mathsf{b}_{\textsc{sqn}} \leftarrow \mathsf{range}(\textsc{sqn}_{\mathsf{U}}, \textsc{sqn}_{\mathsf{r}})$
$\textsc{sqn}_{\mathsf{N}} \leftarrow \textsc{sqn}_{\mathsf{N}} + 1$
$\mathbf{b_{mac}} \wedge \mathbf{b}_{\textsc{sqn}}$
$\textsc{sqn}_{\mathsf{U}} \leftarrow \textsc{sqn}_{\mathsf{r}}$
$\mathsf{f}^2_{\mathsf{k}}(\mathsf{n_r})$
$\neg \mathbf{b_{mac}}$
"Auth-Failure"
$\mathbf{b_{mac}} \wedge \neg \mathbf{b}_{\textsc{sqn}}$
$\left\langle \textsc{sqn}_{\mathsf{U}} \oplus \mathsf{f}^{5,*}_{\mathsf{k}}(\mathsf{n_r}), \mathsf{f}^{1,*}_{\mathsf{k}}(\langle \textsc{sqn}_{\mathsf{U}}, \mathsf{n_r} \rangle) \right\rangle$
Input y:
$\textsc{sqn}^*_{\mathsf{r}} \leftarrow \pi_1(\mathsf{y}) \oplus \mathsf{f}^{5,*}_{\mathsf{k}}(\mathsf{n})$
if $\mathsf{f}^{1,*}_{\mathsf{k}}(\langle \textsc{sqn}^*_{\mathsf{r}}, \mathsf{n} \rangle) = \pi_2(\mathsf{y})$ then $\textsc{sqn}_{\mathsf{N}} \leftarrow \textsc{sqn}^*_{\mathsf{r}} + 1$

Conventions: ← denotes assignments, and has a lower priority than the test =.

Fig. 1. The 5G-AKA Protocol

Authentication Protocol. The 5G-AKA protocol is represented in Figure 1. We now describe an honest execution of the protocol. First, the *UE* initiates the protocol by identifying itself to the *HN*, which it can do in two different ways:

- It can send a temporary identity GUTI, if one was assigned to it. After sending the GUTI, the *UE* sets it to UnSet to ensure that it will not be used more than once. Otherwise, it would allow an adversary to link sessions together.
- It can send its concealed permanent identity $\{\textsc{supi}\}^{\mathsf{n_e}}_{\mathsf{pk_N}}$, using the *HN* public key $\mathsf{pk_N}$ and a fresh randomness $\mathsf{n_e}$.

Upon reception of an identifying message, the *HN* retrieves the permanent identity SUPI: if it received a temporary identity GUTI, this is done through a database look-up; and if a concealed permanent identity was used, it uses $\mathsf{sk_N}$ to decrypt it. It can then recover $\textsc{sqn}_{\mathsf{N}}$ and the key k associated to the identity SUPI from its memory. The *HN* then generates a fresh nonce n. It masks the sequence number $\textsc{sqn}_{\mathsf{N}}$ by xoring it with $\mathsf{f}^5_{\mathsf{k}}(\mathsf{n})$, and mac the message by computing $\mathsf{f}^1_{\mathsf{k}}(\langle \textsc{sqn}_{\mathsf{N}}, \mathsf{n} \rangle)$. It then sends the message $\langle \mathsf{n}, \textsc{sqn}_{\mathsf{N}} \oplus \mathsf{f}^5_{\mathsf{k}}(\mathsf{n}), \mathsf{f}^1_{\mathsf{k}}(\langle \textsc{sqn}_{\mathsf{N}}, \mathsf{n} \rangle) \rangle$.

When receiving this message, the *UE* computes $\mathsf{f}^5_{\mathsf{k}}(\mathsf{n})$. With it, it unmasks $\textsc{sqn}_{\mathsf{N}}$ and checks the authenticity of the message by re-computing $\mathsf{f}^1_{\mathsf{k}}(\langle \textsc{sqn}_{\mathsf{N}}, \mathsf{n} \rangle)$ and verifying that it is equal to the

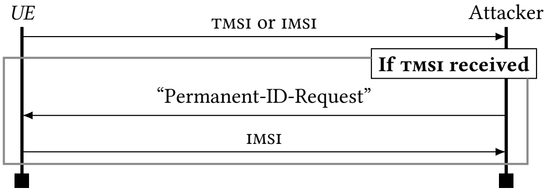


Fig. 2. An IMSI-Catcher Attack

third component of the message. It also checks whether SQN_N and SQN_U are in range[1]. If both checks succeed, the *UE* sets SQN_U to SQN_N, which prevents this message from being accepted again. It then sends $f^2_k(n)$ to prove to *HN* the knowledge of k. If the authenticity check fails, an "Auth-Failure" message is sent. Finally, if the authenticity check succeeds but the range check fails, *UE* starts the re-synchronization sub-protocol, which we describe below.

Re-synchronization. The re-synchronization protocol allows the *HN* to obtain the current value of SQN_U. First, the *UE* masks SQN_U by xoring it with $f^{5,*}_k(n)$, mac the message using $f^{1,*}_k(\langle \text{SQN}_U , n\rangle)$ and sends the pair $\langle \text{SQN}_U \oplus f^{5,*}_k(n) , f^{1,*}_k(\langle \text{SQN}_U , n\rangle)\rangle$. When receiving this message, the *HN* unmasks SQN_U and checks the mac. If the authentication test is successful, *HN* sets the value of SQN_N to $\text{SQN}_U + 1$. This ensures that *HN* first message in the next session of the protocol is in the correct range.

GUTI Assignment. There is a final component of the protocol which is not described in Figure 1 (as it is not used in the privacy attacks we present later). After a successful run of the protocol, the *HN* generates a new temporary identity GUTI and links it to the *UE*'s permanent identity in its database. Then, it sends the concealed fresh GUTI to the *UE*. The sub-protocol used to send a fresh GUTI is not used in the privacy attacks we present in the next session. Therefore, we omit its description.

3 UNLINKABILITY ATTACKS AGAINST 5G-AKA

We present in this section several attacks against AKA that appeared in the literature. All these attacks but one (the IMSI-catcher attack) carry over to 5G-AKA. Moreover, several fixes of the 3G and 4G versions of AKA have been proposed. We discuss the two most relevant fixes, the first by Arapinis et al. [4], and the second by Fouque et al. [22].

None of these fixes are satisfactory. The modified AKA protocol given in [4] has been shown flawed in [22]. The authors of [22] then propose their own protocol, called PRIV-AKA, and claim it is unlinkable (they only provide a proof sketch). While analyzing the PRIV-AKA protocol, we discovered an attack allowing to permanently de-synchronize the *UE* and the *HN*. Since a de-synchronized *UE* can be easily tracked (after being de-synchronized, the *UE* rejects all further messages), our attack is also an unlinkability attack. This is in direct contradiction with the security property claimed in [22]. This is a novel attack that never appeared in the literature.

3.1 IMSI-Catcher Attack

All the older versions of AKA (4G and earlier) are vulnerable to the IMSI-catcher attack [37]. This attack simply relies on the fact that, in these versions of AKA, the permanent identity (called the *International Mobile Subscriber Identity* or IMSI in the 4G specifications) is not encrypted but sent in plain-text. Moreover, even if a temporary identity is used (a *Temporary Mobile Subscriber Identity* or

[1] The specification is loose: it only requires that $\text{SQN}_U < \text{SQN}_N \leq \text{SQN}_U + C$, where C is some constant chosen by the *HN*.

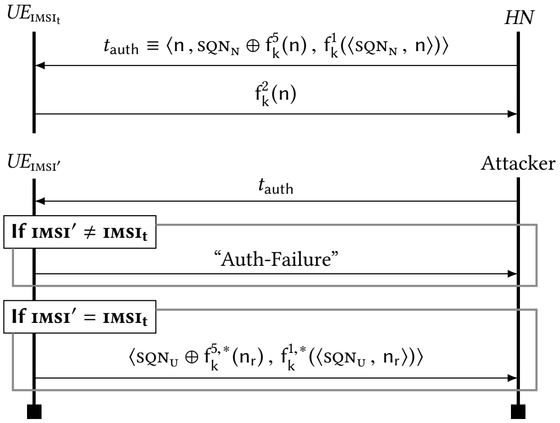

UE_{IMSI_t}
HN
$t_{\text{auth}} \equiv \langle \mathsf{n}, \text{SQN}_\text{N} \oplus \mathsf{f}^5_\mathsf{k}(\mathsf{n}), \mathsf{f}^1_\mathsf{k}(\langle \text{SQN}_\text{N}, \mathsf{n}\rangle)\rangle$
$\mathsf{f}^2_\mathsf{k}(\mathsf{n})$
$UE_{\text{IMSI}'}$
Attacker
t_{auth}
If $\text{IMSI}' \neq \text{IMSI}_t$
"Auth-Failure"
If $\text{IMSI}' = \text{IMSI}_t$
$\langle \text{SQN}_\text{U} \oplus \mathsf{f}^{5,*}_\mathsf{k}(\mathsf{n}_r), \mathsf{f}^{1,*}_\mathsf{k}(\langle \text{SQN}_\text{U}, \mathsf{n}_r\rangle)\rangle$

Fig. 3. The Failure Message Attack by [4].

TMSI), an attacker can simply send a Permanent-ID-Request message to obtain the *UE*'s permanent identity. The attack is depicted in Figure 2.

This necessitates an active attacker with its own base station. At the time, this required specialized hardware, and was believed to be too expensive. This is no longer the case, and can be done for a few hundreds dollars (see [35]).

3.2 The Failure Message Attack

In [4], Arapinis et al. propose to use an asymmetric encryption to protect against the IMSI-catcher attack: each *UE* carries the public-key of its corresponding *HN*, and uses it to encrypt its permanent identity. This is basically the solution that was adopted by 3GPP for the 5G version of AKA. Interestingly, they show that this is not enough to ensure privacy, and give a linkability attack that does not rely on the identification message sent by *UE*. While their attack is against the 3G-AKA protocol, it is applicable to the 5G-AKA protocol.

The Attack. The attack is depicted in Figure 3, and works in two phases. First, the adversary eavesdrops a successful run of the protocol between the *HN* and the target *UE* with identity IMSI_t, and stores the authentication message t_{auth} sent by *HN*. In a second phase, the attacker $\mathcal{A}$ tries to determine whether a *UE* with identity IMSI' is the initial *UE* (i.e. whether $\text{IMSI}' = \text{IMSI}_t$). To do this, $\mathcal{A}$ initiates a new session of the protocol and replays the message t_{auth}. If $\text{IMSI}' \neq \text{IMSI}_t$, then the mac test fails, and $UE_{\text{IMSI}'}$ answers "Auth-Failure". If $\text{IMSI}' = \text{IMSI}_t$, then the mac test succeeds but the range test fails, and $UE_{\text{IMSI}'}$ sends a re-synchronization message.

The adversary can distinguish between the two messages, and therefore knows if it is interacting with the original or a different *UE*. Moreover, the second phase of the attack can be repeated every time the adversary wants to check for the presence of the tracked user IMSI_t in its vicinity.

Proposed Fix. To protect against the failure message attack, the authors of [4] propose that the *UE* encrypts both error message using the public key pk_N of the *HN*, making them indistinguishable. To the adversary, there is no distinctions between an authentication and a de-synchronization failure. The fixed AKA protocol, *without the identifying message* $\{\text{IMSI}\}^{n_e}_{pk_N}$, was formally checked in the symbolic model using the PROVERIF tool. Because this message was omitted in the model, an attack was missed. We present this attack in the next section.

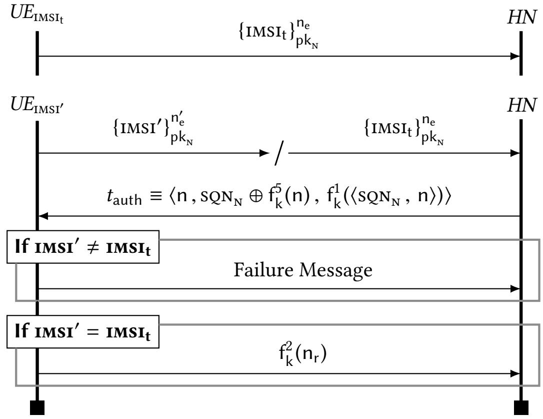

UE_{IMSI_t}
HN
$\{\text{IMSI}_t\}^{n_e}_{pk_N}$
$UE_{\text{IMSI}'}$
HN
$\{\text{IMSI}'\}^{n'_e}_{pk_N}$
$\{\text{IMSI}_t\}^{n_e}_{pk_N}$
$t_{\text{auth}} \equiv \langle n, \text{SQN}_N \oplus f^5_k(n), f^1_k(\langle \text{SQN}_N, n \rangle)\rangle$
If $\text{IMSI}' \neq \text{IMSI}_t$
Failure Message
If $\text{IMSI}' = \text{IMSI}_t$
$f^2_k(n_r)$

Fig. 4. The Encrypted IMSI Replay Attack by [22].

3.3 The Encrypted IMSI Replay Attack

In [22], Fouque et al. give an attack against the fixed AKA proposed by Arapinis et al. in [4]. Their attack, described in Figure 4, uses the fact the identifying message $\{\text{IMSI}_t\}^{n_e}_{pk_N}$ in the proposed AKA protocol by Arapinis et al. can be replayed.

In a first phase, the attacker $\mathcal{A}$ eavesdrops and stores the identifying message $\{\text{IMSI}_t\}^{n_e}_{pk_N}$ of an honest session between the user UE_{IMSI_t} it wants to track and the *HN*. Then, every time $\mathcal{A}$ wants to determine whether some user $UE_{\text{IMSI}'}$ is the tracked user UE_{IMSI_t}, it intercepts the identifying message $\{\text{IMSI}'\}^{n'_e}_{pk_N}$ sent by $UE_{\text{IMSI}'}$, and replaces it with the stored message $\{\text{IMSI}_t\}^{n_e}_{pk_N}$. Finally, $\mathcal{A}$ lets the protocol continue without further tampering. We have two possible outcomes:

- If $\text{IMSI}' \neq \text{IMSI}_t$ then the message t_{auth} sent by *HN* is mac-ed using the wrong key, and the *UE* rejects the message. Hence the attacker observes a failure message.
- If $\text{IMSI}' = \text{IMSI}_t$ then t_{auth} is accepted by $UE_{\text{IMSI}'}$, and the attacker observes a success message.

Therefore the attacker knows if it is interacting with $UE(\text{IMSI}_t)$ or not, which breaks unlinkability.

3.4 Attack Against The PRIV-AKA Protocol

The authors of [22] then propose the PRIV-AKA protocol, which is a significantly modified version of AKA. The authors claim that their protocol achieves authentication and client unlinkability. But we discovered a de-synchronization attack: it is possible to permanently de-synchronize the *UE* and the *HN*. Our attack uses the fact that in PRIV-AKA, the *HN* sequence number is incremented only upon reception of the confirmation message from the *UE*. Therefore, by intercepting the last message from the *UE*, we can prevent the *HN* from incrementing its sequence number. We now describe the attack.

We run a session of the protocol, but we intercept the last message and store it for latter use. Note that the *HN*'s session is not closed. At that point, the *UE* and the *HN* are de-synchronized by one. We re-synchronize them by running a full session of the protocol. We then re-iterate the steps described above: we run a session of the protocol, prevent the last message from arriving at the *HN*, and then run a full session of the protocol to re-synchronize the *HN* and the *UE*. Now the *UE* and the *HN* are synchronized, and we have two stored messages, one for each uncompleted session. We then send the two messages to the corresponding *HN* sessions, which accept them and increment the sequence number. In the end, it is incremented by *two*.

The problem is that the *UE* and the *HN* cannot recover from a de-synchronization by two. We believe that this was missed by the authors of [22].[2] Remark that this attack is also an unlinkability attack. To attack some user UE_{IMSI}'s privacy, we permanently de-synchronize it. Then each time UE_{IMSI} tries to run the PRIV-AKA protocol, it will abort, which allows the adversary to track it.

Remark 1. Our attack requires that the *HN* does not close the first session when we execute the second session. At the end of the attack, before sending the two stored messages, there are two *HN* sessions simultaneously opened for the same *UE*. If the *HN* closes any un-finished sessions when starting a new session with the same *UE*, our attack does not work.

But this make another unlinkability attack possible. Indeed, closing a session because of some later session between the *HN* and the same *UE* reveals a link between the two sessions. We describe the attack. First, we start a session i between a user UE_{A} and the *HN*, but we intercept and store the last message t_{A} from the user. Then, we let the *HN* run a full session with some user UE_{X}. Finally, we complete the initial session i by sending the stored message t_{A} to the *HN*. Here, we have two cases. If $\mathrm{X} = \mathrm{A}$, then the *HN* closed the first session when it completed the second. Hence it rejects t_{A}. If $\mathrm{X} \neq \mathrm{A}$, then the first session is still opened, and it accepts t_{A}.

Closing a session may leak information to the adversary. Protocols which aim at providing unlinkability must explicit when sessions can safely be closed. By default, we assume a session stays open. In a real implementation, a timeout *tied to the session* (and not the user identity) could be used to avoid keeping sessions opened forever. ◇

3.5 Sequence Numbers and Unlinkability

We conjecture that it is not possible to achieve functionality (i.e. honest sessions eventually succeed), authentication and unlinkability at the same time when using a sequence number based protocol with no random number generation capabilities in the *UE* side. We briefly explain our intuition.

In any sequence number based protocol, the agents may become de-synchronized because they cannot know if their last message has been received.[3] Furthermore, the attacker can cause de-synchronization by blocking messages. The problem is that we have contradictory requirements. On the one hand, to ensure authentication, an agent must reject a replayed message. On the other hand, in order to guarantee unlinkability, an honest agent has to behave the same way when receiving a message from a synchronized agent or from a de-synchronized agent. Since functionality requires that a message from a synchronized agent is accepted, it follows that a message from a de-synchronized agent must be accepted. Intuitively, it seems to us that an honest agent cannot distinguish between a protocol message which is being replayed and an honest protocol message from a de-synchronized agent. It follows that a replayed message should be both rejected and accepted, which is a contradiction.

This is only a conjecture. We do not have a formal statement, or a proof. Actually, it is unclear how to formally define the set of protocols that rely on sequence numbers to achieve authentication. Note however that all requirements can be satisfied simultaneously if we allow *both* parties to generate random challenges in each session (in AKA, only *HN* uses a random challenge). Examples of challenge based unlinkable authentication protocols can be found in [28].

4 THE AKA$^+$ PROTOCOL

We now describe our principal contribution, which is the design of the AKA$^+$ protocol. This is a fixed version of the 5G-AKA protocol offering some form of privacy against an *active* attacker. First,

[2] "the two sequence numbers may become desynchronized by one step [...]. Further desynchronization is prevented [...]" (p. 266 [22])

[3] Indeed, in an asynchronous communication system one never knows if the last message has been received.

we explicit the efficiency and design constraints. We then describe the AKA$^+$ protocol, and explain how we designed this protocol from 5G-AKA by fixing all the previously described attacks. As we mentioned before, we think unlinkability cannot be achieved under these constraints. Nonetheless, our protocol satisfies some weaker notion of unlinkability that we call σ-unlinkability. This is a new security property that we introduce. Finally, we will show a subtle attack, and explain how we fine-tuned AKA$^+$ to prevent it.

4.1 Efficiency and Design Constraints

We now explicit the protocol design constraints. These constraints are necessary for an efficient, in-expensive to implement and backward compatible protocol. Observe that, in a mobile setting, it is very important to avoid expensive computations as they quickly drain the *UE*'s battery.

Communication Complexity. In 5G-AKA, authentication is achieved using only three messages: two messages are sent by the *UE*, and one by the *HN*. We want our protocol to have a similar communication complexity. While we did not manage to use only three messages in all scenarios, our protocol achieves authentication in less than four messages.

Cryptographic primitives. We recall that all cryptographic primitives are computed in the *USIM*, where they are implemented in hardware. It follows that using more primitives in the *UE* would make the *USIM* more voluminous and expensive. Hence we restrict AKA$^+$ to the cryptographic primitives used in 5G-AKA: we use only symmetric keyed one-way functions and asymmetric encryption. Notice that the *USIM* cannot do asymmetric *decryption.* As in 5G-AKA, we use some in-expensive functions, e.g. xor, pairs, by-one increments and boolean tests. We believe that relying on the same cryptographic primitives helps ensuring backward compatibility, and would simplify the protocol deployment.

Random Number Generation. In 5G-AKA, the *UE* generates at most one nonce per session, which is used to randomize the asymmetric encryption. Moreover, if the *UE* was assigned a GUTI in the previous session then there is no random number generation. Remark that when the *UE* and the *HN* are de-synchronized, the authentication fails and the *UE* sends a re-synchronization message. Since the session fails, no fresh GUTI is assigned to the *UE*. Hence, the next session of the protocol has to conceal the SUPI using $\{\text{SUPI}\}_{\mathsf{pk}_{\mathsf{N}}}^{\mathsf{n}_{\mathsf{e}}}$, which requires a random number generation. Therefore, we constrain our protocol to use at most one random number generation by the *UE* per session, and only if no GUTI has been assigned or if the *UE* and the *HN* have been de-synchronized.

Summary. We summarize the constraints for AKA$^+$:

- It must use at most four messages per sessions.
- The *UE* may use only keyed one-way functions and asymmetric *encryption.* The *HN* may use these functions, plus asymmetric *decryption.*
- The *UE* may generate at most one random number per session, and only if no GUTI is available, or if re-synchronization with the *HN* is necessary.

4.2 Key Ideas

In this section, we present the two key ideas used in the design of the AKA$^+$ protocol.

Postponed Re-Synchronization Message. We recall that whenever the *UE* and the *HN* are de-synchronized, the authentication fails and the *UE* sends a re-synchronization message. The problem is that this message can be distinguished from a mac failure message, which allows the attack presented in Section 3.2. Since the session fails, no GUTI is assigned to the *UE*, and the next session will use the asymmetric encryption to conceal the SUPI. The first key idea is to piggy-back on the

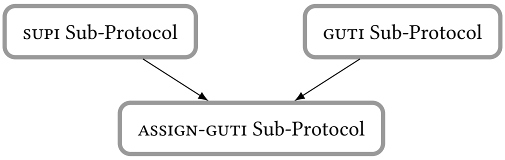


Fig. 5. General Architecture of the AKA$^+$ Protocol

randomized encryption of the *next session* to send a concealed re-synchronization message. More precisely, we replace the message $\{\textsc{supi}\}^{n_e}_{pk_N}$ by $\{\langle \textsc{supi}, \textsc{sqn}_U \rangle\}^{n_e}_{pk_N}$. This has several advantages:

- We can remove the re-synchronization message that lead to the unlinkability attack presented in Section 3.2. In AKA$^+$, whenever the mac check or the range check fails, the same failure message is sent.
- This does not require more random number generation by the *UE*, since a random number is already being generated to conceal the SUPI in the next session.

The 3GPP technical specification (see [38], Annex C) requires that the asymmetric encryption used in the 5G-AKA protocol is the ECIES encryption scheme, which is an hybrid encryption scheme. Hybrid encryption schemes use a randomized asymmetric encryption to conceal a temporary key. This key is then used to encrypt the message using a symmetric encryption, which is in-expensive. Hence encrypting the pair $\langle \textsc{supi}, \textsc{sqn}_U \rangle$ is almost as fast as encrypting only SUPI, and requires the *UE* to generate the same amount of randomness.

HN Challenge Before Identification. To prevent the Encrypted IMSI Replay Attack of Section 3.3, we add a random challenge n from the *HN*. The *UE* initiates the protocol by requesting a challenge without identifying itself. When requested, the *HN* generates and sends a fresh challenge n to the *UE*, which includes it in its response by mac-ing it with the SUPI using a symmetric one-way function Mac^1 with key k^{ID}_m. The *UE* response is now:

$$\Big\langle \{\langle \textsc{supi}, \textsc{sqn}_U \rangle\}^{n_e}_{pk_N}, \mathsf{Mac}^1_{k^{\mathrm{ID}}_m}(\langle \{\langle \textsc{supi}, \textsc{sqn}_U \rangle\}^{n_e}_{pk_N}, n \rangle) \Big\rangle$$

This challenge is only needed when the encrypted permanent identity is used. If the *UE* uses a temporary identity GUTI, then we do not need to use a random challenge. Indeed, temporary identities can only be used once before being discarded, and are therefore not subject to replay attacks. By consequence we split the protocol in two sub-protocols:

- The SUPI sub-protocol uses a random challenge from the *HN*, encrypts the permanent identity and allows to re-synchronize the *UE* and the *HN*.
- The GUTI sub-protocol is initiated by the *UE* using a temporary identity.

In the SUPI sub-protocol, the *UE*'s answer includes the challenge. We use this to save one message: the last confirmation step from the *UE* is not needed, and is removed. The resulting sub-protocol has four messages. Observe that the GUTI sub-protocol is faster, since it uses only three messages.

4.3 Architecture and States

Instead of a monolithic protocol, we have three sub-protocols: the SUPI and GUTI sub-protocols, which handle authentication; and the ASSIGN-GUTI sub-protocol, which is run after authentication has been achieved and assigns a fresh temporary identity to the *UE*. A full session of the AKA$^+$ protocol comprises a session of the SUPI or GUTI sub-protocols, followed by a session of the ASSIGN-GUTI sub-protocol. This is graphically depicted in Figure 5.

Since the GUTI sub-protocol uses only three messages and does not require the *UE* to generate a random number or compute an asymmetric encryption, it is faster than the SUPI sub-protocol. By consequence, the *UE* should always use the GUTI sub-protocol if it has a temporary identity available.

The *HN* runs concurrently an arbitrary number of sessions, but a subscriber cannot run more than one session at the same time. Of course, sessions from *different* subscribers may be concurrently running. We associate a unique integer, the session number, to every session, and we use *HN*(j) and $UE_{\mathrm{ID}}(j)$ to refer to the j-th session of, respectively, the *HN* and the *UE* with identity ID.

One-Way Functions. We separate functions that are used only for confidentiality from functions that are also used for integrity. We have two confidentiality functions f and f^{r}, which use the key k, and five integrity functions Mac^1– Mac^5, which use the key $\mathsf{k_m}$. We require that f and f^{r} (resp. Mac^1– Mac^5) satisfy jointly the PRF assumption. This is a new assumption, which requires that these functions are *simultaneously* computationally indistinguishable from random functions.

Definition 1 (Jointly PRF Functions). Let $H_1(\cdot,\cdot),\dots,H_n(\cdot,\cdot)$ be a finite family of keyed hash functions from $\{0,1\}^* \times \{0,1\}^\eta$ to $\{0,1\}^\eta$. The functions $H_1,\dots,H_n$ are *Jointly Pseudo Random Functions* if, for any PPTM adversary $\mathcal{A}$ with access to oracles $\mathcal{O}_{f_1},\dots,\mathcal{O}_{f_n}$:

$$|\mathbf{Pr}(k : \mathcal{A}^{\mathcal{O}_{H_1(\cdot,k)},\dots,\mathcal{O}_{H_n(\cdot,k)}}(1^\eta) = 1) - \mathbf{Pr}(g_1,\dots,g_n : \mathcal{A}^{\mathcal{O}_{g_1(\cdot)},\dots,\mathcal{O}_{g_n(\cdot)}}(1^\eta) = 1)|$$

is negligible, where:

- k is drawn uniformly in $\{0,1\}^\eta$.
- $g_1,\dots,g_n$ are drawn uniformly in the set of all functions from $\{0,1\}^*$ to $\{0,1\}^\eta$.

Observe that if $H_1,\dots,H_n$ are jointly PRF then, in particular, every individual H_i is a PRF.

Remark 2. While this is a non-usual assumption, it is simple to build a set of functions $H_1,\dots,H_n$ which are jointly PRF from a single PRF H. First, let $(\mathsf{tag}_i(\cdot))_{1\le i\le n}$ be a set of tagging functions. We require that these functions are unambiguous, i.e. for all bit-strings u, v and $i \neq j$ we must have $\mathsf{tag}_i(u) \neq \mathsf{tag}_j(v)$. Then for every $1 \le i \le n$, we let $H_i(x,y) = H(\mathsf{tag}_i(x), y)$. It is straightforward to show that if H is a PRF then $H_1,\dots,H_n$ are jointly PRF. ◇

UE Persistent State. Each UE_{ID} with identity ID has a state $\mathsf{state}_{\mathrm{U}}^{\mathrm{ID}}$ persistent across sessions. It contains the following immutable values: the permanent identity SUPI = ID, the confidentiality key k^{ID}, the integrity key $\mathsf{k}_{\mathsf{m}}^{\mathrm{ID}}$ and the *HN*'s public key pk_{N}. The states also contain mutable values: the sequence number $\mathrm{SQN}_{\mathrm{U}}$, the temporary identity $\mathrm{GUTI}_{\mathrm{U}}$ and the boolean $\mathsf{valid\text{-}guti}_{\mathrm{U}}$. We have $\mathsf{valid\text{-}guti}_{\mathrm{U}} = \mathsf{false}$ whenever no valid temporary identity is assigned to the *UE*. Finally, there are mutable values that are not persistent across sessions. E.g. $\mathsf{b\text{-}auth}_{\mathrm{U}}$ stores *HN*'s random challenge, and $\mathsf{e\text{-}auth}_{\mathrm{U}}$ stores *HN*'s random challenge *when the authentication is successful.*

HN Persistent State. The *HN* state $\mathsf{state}_{\mathrm{N}}$ contains the secret key sk_{N} corresponding to the public key pk_{N}. Also, for every subscriber with identity ID, it stores the keys k^{ID} and $\mathsf{k}_{\mathsf{m}}^{\mathrm{ID}}$, the permanent identity SUPI = ID, the *HN* version of the sequence number $\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}$ and the temporary identity $\mathrm{GUTI}_{\mathrm{N}}^{\mathrm{ID}}$. It stores in $\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}$ the random challenge of the last session that was either a successful SUPI session which modified the sequence number, or a GUTI session which authenticated ID. This is used to detect and prevent some subtle attacks, which we present later. Finally, every session *HN*(j) stores in $\mathsf{b\text{-}auth}_{\mathrm{N}}^{j}$ the identity claimed by the *UE*, and in $\mathsf{e\text{-}auth}_{\mathrm{N}}^{j}$ the identity of the *UE* it authenticated.

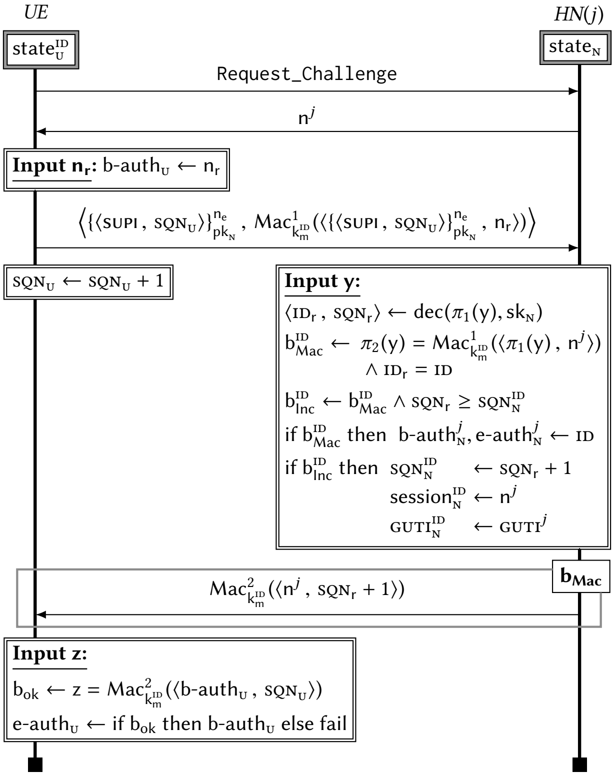

UE
HN(j)
$\mathsf{state}_{\mathrm{U}}^{\mathrm{ID}}$
$\mathsf{state}_{\mathrm{N}}$
Request_Challenge
n^j
Input $\mathbf{n_r}$: $\mathsf{b\text{-}auth}_{\mathrm{U}} \leftarrow \mathsf{n_r}$
$\left\langle \{\langle \mathrm{SUPI}\,,\ \mathrm{SQN}_{\mathrm{U}}\rangle\}^{\mathsf{n_e}}_{\mathsf{pk_N}}\,,\ \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\mathrm{ID}}}(\langle \{\langle \mathrm{SUPI}\,,\ \mathrm{SQN}_{\mathrm{U}}\rangle\}^{\mathsf{n_e}}_{\mathsf{pk_N}}\,,\ \mathsf{n_r}\rangle)\right\rangle$
$\mathrm{SQN}_{\mathrm{U}} \leftarrow \mathrm{SQN}_{\mathrm{U}} + 1$
Input y:
$\langle \mathrm{ID_r}\,,\ \mathrm{SQN_r}\rangle \leftarrow \mathsf{dec}(\pi_1(\mathsf{y}), \mathsf{sk_N})$
$\mathsf{b}^{\mathrm{ID}}_{\mathsf{Mac}} \leftarrow \pi_2(\mathsf{y}) = \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\mathrm{ID}}}(\langle \pi_1(\mathsf{y})\,,\ \mathsf{n}^j\rangle)$
$\wedge\ \mathrm{ID_r} = \mathrm{ID}$
$\mathsf{b}^{\mathrm{ID}}_{\mathsf{Inc}} \leftarrow \mathsf{b}^{\mathrm{ID}}_{\mathsf{Mac}} \wedge \mathrm{SQN_r} \geq \mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}$
if $\mathsf{b}^{\mathrm{ID}}_{\mathsf{Mac}}$ then $\mathsf{b\text{-}auth}^j_{\mathrm{N}}, \mathsf{e\text{-}auth}^j_{\mathrm{N}} \leftarrow \mathrm{ID}$
if $\mathsf{b}^{\mathrm{ID}}_{\mathsf{Inc}}$ then $\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}} \leftarrow \mathrm{SQN_r} + 1$
$\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}} \leftarrow \mathsf{n}^j$
$\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}} \leftarrow \mathrm{GUTI}^j$
$\mathbf{b_{Mac}}$
$\mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\mathrm{ID}}}(\langle \mathsf{n}^j\,,\ \mathrm{SQN_r} + 1\rangle)$
Input z:
$\mathsf{b_{ok}} \leftarrow \mathsf{z} = \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\mathrm{ID}}}(\langle \mathsf{b\text{-}auth}_{\mathrm{U}}\,,\ \mathrm{SQN}_{\mathrm{U}}\rangle)$
$\mathsf{e\text{-}auth}_{\mathrm{U}} \leftarrow$ if $\mathsf{b_{ok}}$ then $\mathsf{b\text{-}auth}_{\mathrm{U}}$ else fail

Fig. 6. The SUPI Sub-Protocol of the AKA$^+$ Protocol

4.4 The SUPI, GUTI and ASSIGN-GUTI Sub-Protocols

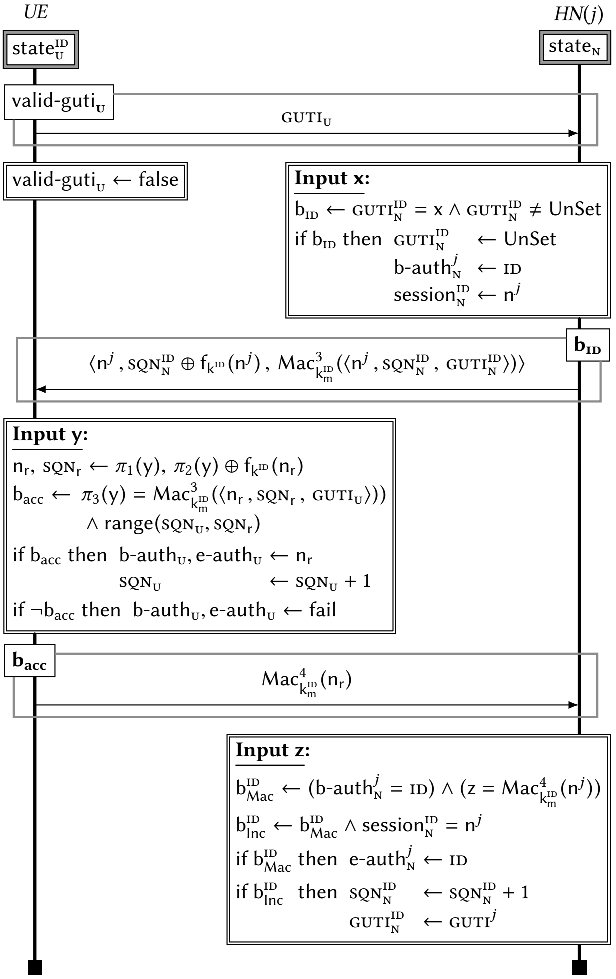
We describe honest executions of the three sub-protocols of the AKA$^+$ protocol. An honest execution is an execution where the adversary dutifully forwards the messages without tampering. Each execution is between a *UE* and *HN*(j).

The SUPI Sub-Protocol. This protocol uses the *UE*'s permanent identity, re-synchronizes the *UE* and the *HN* and is expensive to run. The protocol is sketched in Figure 6.

The *UE* initiates the protocol by requesting a challenge from the network. When asked, *HN*(j) sends a fresh challenge n^j. After receiving n^j, the *UE* stores it in $\mathsf{b\text{-}auth}_{\mathrm{U}}$, and answers with the encryption of its permanent identity together with the current value of its sequence number, using the *HN* public key $\mathsf{pk_N}$. It also includes the mac of this encryption and of the challenge, which yields the message:

$$\left\langle \{\langle \mathrm{SUPI}\,,\ \mathrm{SQN}_{\mathrm{U}}\rangle\}^{\mathsf{n_e}}_{\mathsf{pk_N}}\,,\ \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\mathrm{ID}}}(\langle \{\langle \mathrm{SUPI}\,,\ \mathrm{SQN}_{\mathrm{U}}\rangle\}^{\mathsf{n_e}}_{\mathsf{pk_N}}\,,\ \mathsf{n}^j\rangle)\right\rangle$$

Then the *UE* increments its sequence number by one. When it gets this message, the *HN* retrieves the pair $\langle \mathrm{SUPI}\,,\ \mathrm{SQN}_{\mathrm{U}}\rangle$ by decrypting the encryption using its secret key $\mathsf{sk_N}$. For every identity ID, it checks if $\mathrm{SUPI} = \mathrm{ID}$ and if the mac is correct. If this is the case, *HN* authenticated ID, and it stores ID in $\mathsf{b\text{-}auth}^j_{\mathrm{N}}$ and $\mathsf{e\text{-}auth}^j_{\mathrm{N}}$. After having authenticated ID, *HN* checks whether the sequence number $\mathrm{SQN}_{\mathrm{U}}$ it received is greater than or equal to $\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}$. If this holds, it sets $\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}$ to $\mathrm{SQN}_{\mathrm{U}} + 1$, stores n^j in $\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}$, generates a fresh temporary identity GUTI^j and stores it into $\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}$. This additional



UE
HN(*j*)
$\mathrm{state}_{\mathrm{U}}^{\mathrm{ID}}$
$\mathrm{state}_{\mathrm{N}}$
$\text{valid-guti}_{\mathrm{U}}$
$\mathrm{GUTI}_{\mathrm{U}}$
$\text{valid-guti}_{\mathrm{U}} \leftarrow \text{false}$
Input x:
$b_{\mathrm{ID}} \leftarrow \mathrm{GUTI}_{\mathrm{N}}^{\mathrm{ID}} = x \wedge \mathrm{GUTI}_{\mathrm{N}}^{\mathrm{ID}} \neq \mathrm{UnSet}$
if b_{ID} then $\mathrm{GUTI}_{\mathrm{N}}^{\mathrm{ID}} \leftarrow \mathrm{UnSet}$
$\text{b-auth}_{\mathrm{N}}^{j} \leftarrow \mathrm{ID}$
$\mathrm{session}_{\mathrm{N}}^{\mathrm{ID}} \leftarrow n^{j}$
$\mathbf{b_{ID}}$
$\langle n^{j}, \mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}} \oplus f_{k^{\mathrm{ID}}}(n^{j}), \mathrm{Mac}^{3}_{k_m^{\mathrm{ID}}}(\langle n^{j}, \mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}, \mathrm{GUTI}_{\mathrm{N}}^{\mathrm{ID}}\rangle)\rangle$
Input y:
$n_r, \mathrm{SQN}_r \leftarrow \pi_1(y), \pi_2(y) \oplus f_{k^{\mathrm{ID}}}(n_r)$
$b_{acc} \leftarrow \pi_3(y) = \mathrm{Mac}^{3}_{k_m^{\mathrm{ID}}}(\langle n_r, \mathrm{SQN}_r, \mathrm{GUTI}_{\mathrm{U}}\rangle)$
$\wedge\ \mathrm{range}(\mathrm{SQN}_{\mathrm{U}}, \mathrm{SQN}_r)$
if b_{acc} then $\text{b-auth}_{\mathrm{U}}, \text{e-auth}_{\mathrm{U}} \leftarrow n_r$
$\mathrm{SQN}_{\mathrm{U}} \leftarrow \mathrm{SQN}_{\mathrm{U}} + 1$
if $\neg b_{acc}$ then $\text{b-auth}_{\mathrm{U}}, \text{e-auth}_{\mathrm{U}} \leftarrow \text{fail}$
$\mathbf{b_{acc}}$
$\mathrm{Mac}^{4}_{k_m^{\mathrm{ID}}}(n_r)$
Input z:
$b_{\mathrm{Mac}}^{\mathrm{ID}} \leftarrow (\text{b-auth}_{\mathrm{N}}^{j} = \mathrm{ID}) \wedge (z = \mathrm{Mac}^{4}_{k_m^{\mathrm{ID}}}(n^{j}))$
$b_{\mathrm{Inc}}^{\mathrm{ID}} \leftarrow b_{\mathrm{Mac}}^{\mathrm{ID}} \wedge \mathrm{session}_{\mathrm{N}}^{\mathrm{ID}} = n^{j}$
if $b_{\mathrm{Mac}}^{\mathrm{ID}}$ then $\text{e-auth}_{\mathrm{N}}^{j} \leftarrow \mathrm{ID}$
if $b_{\mathrm{Inc}}^{\mathrm{ID}}$ then $\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}} \leftarrow \mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}} + 1$
$\mathrm{GUTI}_{\mathrm{N}}^{\mathrm{ID}} \leftarrow \mathrm{GUTI}^{j}$

Fig. 7. The GUTI Sub-Protocol of the AKA^{+} Protocol

check ensures that the *HN* sequence number is always increasing, which is a crucial property of the protocol.

If the *HN* authenticated ID, it sends a confirmation message $\mathrm{Mac}^{2}_{k_m^{\mathrm{ID}}}(\langle n^{j}, \mathrm{SQN}_{\mathrm{U}} + 1\rangle)$ to the *UE*. This message is sent even if the received sequence number $\mathrm{SQN}_{\mathrm{U}}$ is smaller than $\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}$. When receiving the confirmation message, if the mac is valid then the *UE* authenticated the *HN*, and it stores in $\text{e-auth}_{\mathrm{U}}$ the initial random challenge (which it keeps in $\text{b-auth}_{\mathrm{U}}$). If the mac test fails, it stores in $\text{e-auth}_{\mathrm{U}}$ the special value fail.

The GUTI Sub-Protocol. This protocol uses the *UE*'s temporary identity, requires synchronization to succeed and is inexpensive. The protocol is sketched in Figure 7.

When $\text{valid-guti}_{\mathrm{U}}$ is true, the *UE* can initiate the protocol by sending its temporary identity $\mathrm{GUTI}_{\mathrm{U}}$. The *UE* then sets $\text{valid-guti}_{\mathrm{U}}$ to false to guarantee that this temporary identity is not used again. When receiving a temporary identity x, *HN* looks if there is an ID such that $\mathrm{GUTI}_{\mathrm{N}}^{\mathrm{ID}}$ is equal to x and is not UnSet. If the temporary identity belongs to ID, it sets $\mathrm{GUTI}_{\mathrm{N}}^{\mathrm{ID}}$ to UnSet and stores ID

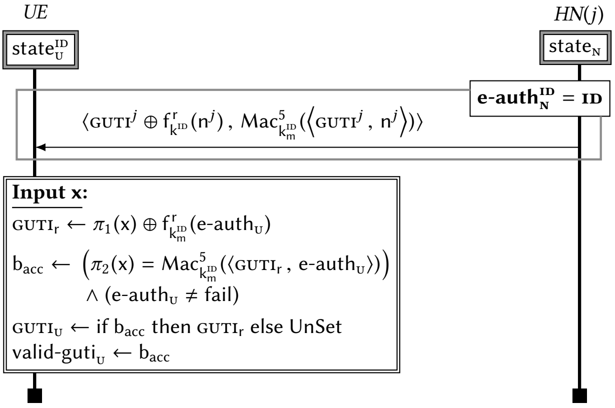

UE
HN(j)
$\mathsf{state}_{\mathrm{U}}^{\mathrm{ID}}$
$\mathsf{state}_{\mathrm{N}}$
$\textbf{e-auth}_{\mathbf{N}}^{\mathbf{ID}} = \mathbf{ID}$
$\langle \textsc{guti}^j \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\textsc{id}}}(\mathsf{n}^j)\,,\ \mathsf{Mac}^5_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \textsc{guti}^j\,,\ \mathsf{n}^j\rangle)\rangle$
Input x:
$\textsc{guti}_{\mathsf{r}} \leftarrow \pi_1(\mathsf{x}) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\mathsf{e\text{-}auth}_{\mathrm{U}})$
$\mathsf{b}_{\mathsf{acc}} \leftarrow \big(\pi_2(\mathsf{x}) = \mathsf{Mac}^5_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \textsc{guti}_{\mathsf{r}}\,,\ \mathsf{e\text{-}auth}_{\mathrm{U}}\rangle)\big)$
$\wedge\ (\mathsf{e\text{-}auth}_{\mathrm{U}} \neq \mathsf{fail})$
$\textsc{guti}_{\mathrm{U}} \leftarrow \mathsf{if}\ \mathsf{b}_{\mathsf{acc}}\ \mathsf{then}\ \textsc{guti}_{\mathsf{r}}\ \mathsf{else}\ \mathsf{UnSet}$
$\mathsf{valid\text{-}guti}_{\mathrm{U}} \leftarrow \mathsf{b}_{\mathsf{acc}}$

Fig. 8. The ASSIGN-GUTI Sub-Protocol of the AKA$^+$ Protocol

in $\mathsf{b\text{-}auth}_{\mathrm{N}}^j$. Then it generates a random challenge n^j, stores it in $\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}$, and sends it to the *UE*, together with the xor of the sequence number $\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}$ with $\mathsf{f}_{\mathsf{k}^{\textsc{id}}}(\mathsf{n}^j)$, and a mac:

$$\left\langle \mathsf{n}^j\,,\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}} \oplus \mathsf{f}_{\mathsf{k}^{\textsc{id}}}(\mathsf{n}^j)\,,\ \mathsf{Mac}^3_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \mathsf{n}^j\,,\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}\,,\ \textsc{guti}_{\mathrm{N}}^{\mathrm{ID}}\rangle)\right\rangle$$

When it receives this message, the *UE* retrieves the challenge n^j at the beginning of the message, computes $\mathsf{f}_{\mathsf{k}^{\textsc{id}}}(\mathsf{n}^j)$ and uses this value to unconceal the sequence number $\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}$. It then computes $\mathsf{Mac}^3_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \mathsf{n}^j\,,\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}\,,\ \textsc{guti}_{\mathrm{U}}\rangle)$ and compares it to the mac received from the network. If the macs are not equal, or if the range check $\mathsf{range}(\textsc{sqn}_{\mathrm{U}}, \textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$ fails, it puts fail into $\mathsf{b\text{-}auth}_{\mathrm{U}}$ and $\mathsf{e\text{-}auth}_{\mathrm{U}}$ to record that the authentication was not successful. If both tests succeed, it stores in $\mathsf{b\text{-}auth}_{\mathrm{U}}$ and $\mathsf{e\text{-}auth}_{\mathrm{U}}$ the random challenge, increments $\textsc{sqn}_{\mathrm{U}}$ by one and sends the confirmation message $\mathsf{Mac}^4_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\mathsf{n}^j)$. When receiving this message, the *HN* verifies that the mac is correct. If this is the case then the *HN* authenticated the *UE*, and stores $\textsc{id}$ into $\mathsf{e\text{-}auth}_{\mathrm{N}}^{\mathrm{ID}}$. Then, *HN* checks whether $\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}$ is still equal to the challenge n^j stored in it at the beginning of the session. If this is true, the *HN* increments $\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}$ by one, generates a fresh temporary identity $\textsc{guti}^j$ and stores it into $\textsc{guti}_{\mathrm{N}}^{\mathrm{ID}}$.

The ASSIGN-GUTI Sub-Protocol. The ASSIGN-GUTI sub-protocol is run after a successful authentication, regardless of the authentication sub-protocol used. It assigns a fresh temporary identity to the *UE* to allow the next AKA$^+$ session to run the faster GUTI sub-protocol. It is depicted in Figure 8.

The *HN* conceals the temporary identity $\textsc{guti}^j$ generated by the authentication sub-protocol by xoring it with $\mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\textsc{id}}}(\mathsf{n}^j)$, and macs it. When receiving this message, *UE* unconceals the temporary identity $\textsc{guti}_{\mathrm{N}}^{\mathrm{ID}}$ by xoring its first component with $\mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\mathsf{e\text{-}auth}_{\mathrm{U}})$ (since $\mathsf{e\text{-}auth}_{\mathrm{U}}$ contains the *HN*'s challenge after authentication). Then *UE* checks that the mac is correct and that the authentication was successful. If it is the case, it stores $\textsc{guti}_{\mathrm{N}}^{\mathrm{ID}}$ in $\textsc{guti}_{\mathrm{U}}$ and sets $\mathsf{valid\text{-}guti}_{\mathrm{U}}$ to true.

5 UNLINKABILITY

We now define our notion of unlinkability, which is inspired from [27] and Vaudenay's privacy [40].

Definition. The property is defined by a game in which an adversary tries to link together some subscriber's sessions. The adversary is a PPTM which interacts, through oracles, with N different subscribers with identities $\textsc{id}_1, \ldots, \textsc{id}_N$, and with the *HN*. The adversary cannot use a subscriber's permanent identity to refer to it, as it may not know it. Instead, we associate a virtual handler vh to any subscriber currently running a session of the protocol. We maintain a list l_{free} of all subscribers that are ready to start a session. We now describe the oracles O_b:

- `StartSession()`: starts a new *HN* session and returns its session number j.
- $\mathsf{SendHN}(m, j)$ (resp. $\mathsf{SendUE}(m, \mathsf{vh})$): sends the message m to *HN*(j) (resp. the *UE* associated with vh), and returns *HN*(j) (resp. vh) answer.
- $\mathsf{ResultHN}(j)$ (resp. $\mathsf{ResultUE}(\mathsf{vh})$): returns true if *HN*(j) (resp. the *UE* associated with vh) has made a successful authentication.
- $\mathsf{DrawUE}(\textsc{id}_{i_0}, \textsc{id}_{i_1})$: checks that $\textsc{id}_{i_0}$ and $\textsc{id}_{i_1}$ are both in l_{free}. If that is the case, returns a new virtual handler pointing to $\textsc{id}_{i_b}$, depending on an internal secret bit b. Then, it removes $\textsc{id}_{i_0}$ and $\textsc{id}_{i_1}$ from l_{free}.
- $\mathsf{FreeUE}(\mathsf{vh})$: makes the virtual handler vh no longer valid, and adds back to l_{free} the two identities that were removed when the virtual handler was created.

A function is negligible if and only if it is asymptotically smaller than the inverse of any polynomial. An adversary $\mathcal{A}$ interacting with O_b is winning the q-unlinkability game if: $\mathcal{A}$ makes less than q calls to the oracles; and it can guess the value of the internal bit b with a probability better than 1/2 by a non-negligible margin, i.e. if the following quantity is non negligible in η:

$$\left|2 \times \mathbf{Pr}\left(b : \mathcal{A}^{O_b}(1^\eta) = b\right) - 1\right|$$

A protocol is q-unlinkable if there are no winning adversaries against the q-unlinkability game.

Corruption. In [27, 40], the adversary is allowed to corrupt some tags using a `Corrupt` oracle. Several classes of adversary are defined by restricting its access to the corruption oracle. A *strong* adversary has unrestricted access, a *destructive* adversary can no longer use a tag after corrupting it (it is destroyed), a *forward* adversary can only follow a `Corrupt` call by further `Corrupt` calls, and finally a *weak* adversary cannot use `Corrupt` at all. A protocol is C unlinkable if no adversary in C can win the unlinkability game. Clearly, we have the following relations:

$$\textit{strong} \;\Rightarrow\; \textit{destructive} \;\Rightarrow\; \textit{forward} \;\Rightarrow\; \textit{weak}$$

The 5G-AKA protocol does not provide forward secrecy: indeed, obtaining the long-term secret of a *UE* allows to decrypt all its past messages. By consequence, the best we can hope for is *weak* unlinkability. Since such adversaries cannot call `Corrupt`, we removed the oracle.

Wide Adversary. Remark that the adversary knows if the protocol was successful or not using the `ResultUE` and `ResultHN` oracles (such an adversary is called *wide* in Vaudenay's terminology [40]). Indeed, in an authenticated key agreement protocol, this information is always available to the adversary: if the key exchange succeeds then it is followed by another protocol using the newly established key; while if it fails then either a new key-exchange session is initiated, or no message is sent. Hence the adversary knows if the key exchange was successful by passive monitoring.

5.1 σ-Unlinkability

In accord with our conjecture in Section 3.5, the AKA$^+$ protocol is not unlinkable. Indeed, an adversary $\mathcal{A}$ can easily win the linkability game. First, $\mathcal{A}$ ensures that $\textsc{id}_{\text{A}}$ and $\textsc{id}_{\text{B}}$ have a valid temporary identity assigned: $\mathcal{A}$ calls $\mathsf{DrawUE}(\textsc{id}_{\text{A}}, \textsc{id}_{\text{A}})$ to obtain a virtual handler for $\textsc{id}_{\text{A}}$, and runs a SUPI and ASSIGN-GUTI sessions between $\textsc{id}_{\text{A}}$ and the *HN* with no interruptions. This assigns a temporary identity to $\textsc{id}_{\text{A}}$. We use the same procedure for $\textsc{id}_{\text{B}}$.

Then, $\mathcal{A}$ executes the attack described in Figure 9. It starts a GUTI session with $\textsc{id}_{\text{A}}$, and intercepts the last message. At that point, $\textsc{id}_{\text{A}}$ no longer has a temporary identity, while $\textsc{id}_{\text{B}}$ still does. Then, it calls $\mathsf{DrawUE}(\textsc{id}_{\text{A}}, \textsc{id}_{\text{B}})$, which returns a virtual handler vh to $\textsc{id}_{\text{A}}$ or $\textsc{id}_{\text{B}}$. The attacker then start a new GUTI session with vh. If vh is a handler for $\textsc{id}_{\text{A}}$, the *UE* returns NoGuti. If vh aliases $\textsc{id}_{\text{B}}$, the

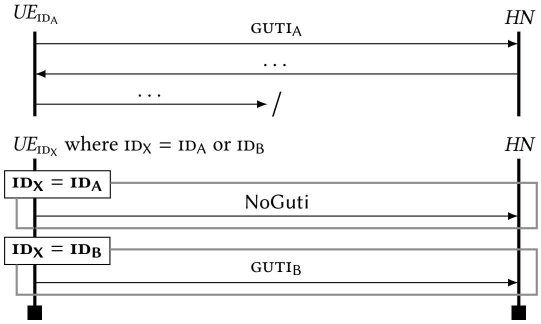

UE_{ID_A}
HN
GUTI_A
...
...
UE_{ID_X} where $\text{ID}_\text{X} = \text{ID}_\text{A}$ or ID_B
HN
$\mathbf{ID_X = ID_A}$
NoGuti
$\mathbf{ID_X = ID_B}$
GUTI_B

Fig. 9. Consecutive GUTI Sessions of AKA$^+$ Are Not Unlinkable.

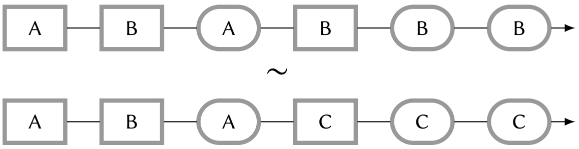


Fig. 10. Two indistinguishable executions. Square (resp. round) nodes are executions of the SUPI (resp. GUTI) protocol. Each time the SUPI protocol is used, we can change the subscriber's identity.

UE returns the temporary identity GUTI_A. The adversary $\mathcal{A}$ can distinguish between these two cases, and therefore wins the game.

σ-Unlinkability. To prevent this, we want to forbid DrawUE to be called on de-synchronized subscribers. We do this by modifying the state of the user chosen by DrawUE. We let σ be an update on the state of the subscribers. We then define the oracle $\mathtt{DrawUE}_\sigma(\text{ID}_{i_0}, \text{ID}_{i_1})$: it checks that ID_A and ID_B are both free, then *applies the update* σ to ID_{i_b}'s state, and returns a new virtual handler pointing to ID_{i_b}. The (q, σ)-unlinkability game is the q-unlinkability game in which we replace DrawUE with $\mathtt{DrawUE}_\sigma$. A protocol is (q, σ)-unlinkable if and only if there is no winning adversary against the (q, σ)-unlinkability game. Finally, a protocol is σ-unlinkable if it is (q, σ)-unlinkable for any q.

Application to AKA$^+$. The privacy guarantees given by the σ-unlinkability property depend on the choice of σ. The idea is to choose a σ that allows to establish privacy in *some scenarios* of the standard unlinkability game.[4]

We illustrate this on the AKA$^+$ protocol. Let $\sigma_{\mathsf{ul}} = \mathsf{valid\text{-}guti}_{\mathsf{U}} \mapsto \mathsf{false}$ be the function that makes the *UE*'s temporary identity not valid. This simulates the fact that the GUTI has been used and is no longer available. If the *UE*'s temporary identity is not valid, then it can only run the SUPI sub-protocol. Hence, if the AKA$^+$ protocol is σ_{ul}-unlinkable, then no adversary can distinguish between a normal execution and an execution where we change the identity of a subscriber each time it runs the SUPI sub-protocol. We give in Figure 10 an example of such a scenario. We now state informally our main result:

THEOREM (*INFORMAL*). *The AKA$^+$ protocol is σ_{ul}-unlinkable for an arbitrary number of agents and sessions when the asymmetric encryption $\{\_\}_{\_}^{\_}$ is IND-CCA$_1$ secure and f and f^r (resp. $Mac^1 - Mac^5$) satisfy jointly the PRF assumption.*

[4] Remark that when σ is the empty state update, the σ-unlinkability and unlinkability properties coincide.

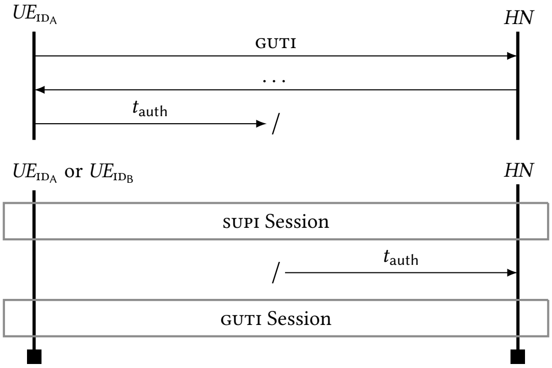


Fig. 11. A Subtle Attack Against The $\text{AKA}^{+}_{\text{no-inc}}$ Protocol

This result is shown later. The intuition is that no adversary can distinguish between two sessions of the SUPI protocol. Moreover, the SUPI protocol has two important properties. First, it re-synchronizes the user with the *HN*, which prevents the attacker from using any prior de-synchronization. Second, the AKA^{+} protocol is designed in such a way that no message sent by the *UE* before a successful SUPI session can modify the *HN*'s state after the SUPI session. Therefore, any time the SUPI protocol is run, we get a "clean slate" and we can change the subscriber's identity. Note that we have a trade-off between efficiency and privacy: the SUPI protocol is more expensive to run, but provides more privacy.

5.2 A Subtle Attack

We now explain what is the role of $\text{session}^{\text{ID}}_{\text{N}}$, and how it prevents a subtle attack against the σ_{ul}-unlinkability of AKA^{+}. We let $\text{AKA}^{+}_{\text{no-inc}}$ be the AKA^{+} protocol where we modify the GUTI sub-protocol we described in Figure 7: in the state update of the *HN*'s last input, we remove the check $\text{session}^{\text{ID}}_{\text{N}} = \mathsf{n}^{j}$ (i.e. $\mathsf{b}^{\text{ID}}_{\text{Inc}} = \mathsf{b}^{\text{ID}}_{\text{Mac}}$). The attack is described in Figure 11.

First, we run a session of the GUTI sub-protocol between UE_{ID_A} and the *HN*, but we do not forward the last message t_{auth} to the *HN*. We then call $\mathtt{DrawUE}_{\sigma_{\text{ul}}}(\text{ID}_A, \text{ID}_B)$, which returns a virtual handler vh to ID_A or ID_B. We run a full session using the SUPI sub-protocol with vh, and then send the message t_{auth} to the *HN*. We can check that, because we removed the condition $\text{session}^{\text{ID}}_{\text{N}} = \mathsf{n}^{j}$ from $\mathsf{b}^{\text{ID}}_{\text{Inc}}$, this message causes the *HN* to increment $\text{SQN}^{\text{ID}_A}_{\text{N}}$ by one. At that point, UE_{ID_A} is de-synchronized but UE_{ID_B} is synchronized. Finally, we run a session of the GUTI sub-protocol. The session has two possible outcomes: if vh aliases to A then it fails, while if vh aliases to B, it succeeds. This leads to an attack.

When we removed the condition $\text{session}^{\text{ID}}_{\text{N}} = \mathsf{n}^{j}$, we broke the "clean slate" property of the SUPI sub-protocol: we can use a message from a session that started *before* the SUPI session to modify the state *after* the SUPI session. $\text{session}^{\text{ID}}_{\text{N}}$ allows to detect whether another session has been executed since the current session started, and to prevent the update of the sequence number when this is the case.

6 THE BANA-COMON LOGIC

To prove that the AKA^{+} protocol is σ_{ul}-unlinkable, we use the Bana-Comon model introduced in [9]. This is a sorted first-order logic, in which terms represent messages of the protocol sent over the network. For example, the term $\langle \mathsf{A}\, ,\, \mathsf{n} \rangle$ represents a message which comprises two parts: an agent name A (which is a constant function symbol), and a name n (taken in the set of names $\mathcal{N}$), representing a random uniform sampling in $\{0,1\}^\eta$ (where η is the security parameter). A key idea in the logic is to use special adversarial function symbols $g_0, g_1, \dots \in \mathcal{G}$ to represent the adversary's inputs. Morally, these function symbols are uninterpreted, which allows to model the fact that the adversary can do any polynomial-time computation. These adversarial function symbols receive as input the current knowledge of the adversary ϕ (the frame), which is simply the sequence of all messages sent over the network since the protocol started (since messages are modeled by terms, ϕ is a sequence of terms). For example, $g(\langle \mathsf{A}\,,\ \mathsf{n}\rangle)$ represents anything the adversary can compute after having intercepted the message $\langle \mathsf{A}\,,\ \mathsf{n}\rangle$. More generally, if ϕ is the current frame, then $g(\phi)$ represents any message that can be computed by the adversary at that point of the protocol execution.

In order to be able to represent messages of the protocol by terms, the control-flow of the protocol needs to be internalized in the logic. This is done by encoding tests of the protocol agents by boolean terms, and branching using the if_then_else_ function symbol. For example, imagine a protocol where some agent A behaves as follows: first A wait for a message from the network; then, after receiving a message x, A checks whether this message is equal to some secret value secret; if this is the case, A outputs its identity $\textsc{id}_\mathsf{A}$, otherwise it outputs an constant error message Error. This is modeled by the term:

$$\mathsf{if}\ \mathsf{eq}(g(\phi), \mathsf{secret})\ \mathsf{then}\ \textsc{id}_\mathsf{A}\ \mathsf{else}\ \mathsf{Error} \tag{1}$$

where $\mathsf{eq}(\_,\_)$ is a function symbol representing the equality check, $\textsc{id}_\mathsf{A}$ and Error are constant function symbols and, we recall, $g(\phi)$ is a term representing the input from the network.

Formulas of the logic are built using the usual Boolean connectives and FO quantifiers, and a single predicate, $\sim$, which stands for indistinguishability. Given two protocols P and Q, we can build a ground formula $\vec{u}_P \sim \vec{u}_Q$ stating that P is indistinguishable from Q, where $\vec{u}_P$ (resp. $\vec{u}_Q$) is a sequence of terms representing the messages sent over the network during the execution of P (resp. Q).

The semantics of the logic is the usual first-order semantics: each sort is interpreted as a domain and function symbols and predicates are interpreted as, respectively, functions and subsets of the appropriate domains. Still, since we want to interpret sequences of terms representing executions of protocols, we are particularly interested in *computational models*, in which terms are interpreted as *probabilistic polynomial-time Turing machines* (PPTMs), and $\sim$ is interpreted as computational indistinguishability.

Axioms. Of course, any non-trivial protocol will not be secure in any computational model $\mathcal{M}_c$. E.g., any real-world protocol is probably not secure if the encryption function symbol is interpreted as the function that always returns the plain-text. By consequence, we are going to show that a protocol is secure in some class of models. We do this by restricting the models that have to be considered using axioms Ax, where an axiom is a formula of the logic stating something that the adversary *cannot* do. Then, if we can prove that the conjunction $\mathsf{Ax} \wedge \vec{u}_P \not\sim \vec{u}_Q$ of the axioms Ax and the negation of the security property $\vec{u}_P \not\sim \vec{u}_Q$ is unsatisfiable, we know that the protocols P and Q are indistinguishable in any computational model satisfying the axioms Ax.

6.1 Syntax and Semantics

We now quickly recall the syntax and semantics of the logic.

Signature. This is a sorted logic with two sorts, term and bool, with bool $\subseteq$ term. We assume a set of function symbols $\mathcal{F}$, the *signature*. Every function symbols $f \in \mathcal{F}$ has an arity $\mathsf{arity}(f) = n \in \mathbb{N}$, and a type $\mathsf{type}(f) \in \{\mathsf{term} \times \mathsf{bool}\}^{n+1}$. We let $f : s_1 \times \dots \times s_n \to s$ denote the fact that $\mathsf{type}(f) = (s_1, \dots, s_n, s)$.

The signature $\mathcal{F}$ contains a countable set of *adversarial* function symbols $\mathcal{G}$, which represent the adversary inputs, and a set of protocol function symbols, which are used in the protocol description.

Example 1. We give the main function symbols used in the AKA$^+$ protocol: a constant function symbols $\textsc{id}_\mathsf{A}$ for the user A's identity, the public/private key functions $\mathsf{pk}(\_), \mathsf{sk}(\_)$, asymmetric encryption and decryption $\{\_\}^{\_}_{\_}$, $\mathsf{dec}(\_,\_)$, the pair and triplet $\langle \_\,,\,\_ \rangle$ and $\langle \_\,,\_\,,\,\_ \rangle$, projections π_1, π_2, π_3, the xor $\_ \oplus \_$, the equality and greater-than tests $\mathsf{eq}(\_,\_)$ and $\mathsf{geq}(\_,\_)$, the successor $\_ + 1$, $\mathsf{if\_then\_else\_}$, true, false, the error messages $\mathsf{UnknownId}$, error and the length $\mathsf{len}(\_)$.
We give their types below:

$$\mathsf{UnknownId}, \mathsf{error}, \textsc{id}_\mathsf{A} \;:\rightarrow \mathsf{term} \qquad\qquad \mathsf{eq}(\_,\_), \mathsf{geq}(\_,\_) \;:\; \mathsf{term}^2 \rightarrow \mathsf{bool}$$

$$\{\_\}^{\_}_{\_}, \langle \_\,,\_\,,\,\_ \rangle \;:\; \mathsf{term}^3 \rightarrow \mathsf{term} \qquad\qquad \mathsf{true}, \mathsf{false} :\rightarrow \mathsf{bool}$$

$$\mathsf{len}(\_), \mathsf{pk}(\_),\ \mathsf{sk}(\_),\ \pi_1(\_),\ \pi_2(\_),\ \pi_3(\_), (\_ + 1) \;:\; \mathsf{term} \rightarrow \mathsf{term}$$

$$\mathsf{dec}(\_,\_), \langle \_\,,\,\_ \rangle, \_ \oplus \_ \;:\; \mathsf{term}^2 \rightarrow \mathsf{term} \qquad\qquad \mathsf{if\_then\_else\_} \;:\; \mathsf{bool} \times \mathsf{term}^2 \rightarrow \mathsf{term}$$

The public/private key pair take as argument the random seed used in the key generation. Corresponding public/private keys are keys with the same random, e.g. the public key $\mathsf{pk}(\mathsf{n})$ corresponds to the private key $\mathsf{sk}(\mathsf{n})$. The asymmetric encryption takes the encryption randomness as an extra parameter: $\{\textsc{id}_\mathsf{A}\}^{\mathsf{n_e}}_{\mathsf{pk_N}}$ is the encryption of $\textsc{id}_\mathsf{A}$ using public key $\mathsf{pk_N}$ and randomness $\mathsf{n_e}$. ◇

Terms. Terms are built using function symbols in $\mathcal{F}$, names in $\mathcal{N}$ (representing random samplings) and variables in $\mathcal{X}$. Names are always of sort term and every variables comes with a sort. For any subset $\mathcal{S}$ of $\mathcal{F}$, $\mathcal{N}$ and $\mathcal{X}$, we let $\mathcal{T}(\mathcal{S})$ be the set of terms built upon $\mathcal{S}$ (we require that terms are well-typed). Given a term t, the type of t is its larger type, where bool is smaller than term.

Example 2. To give an example of a term, we re-use the example in (1). The term:

$$\mathsf{if}\ \mathsf{eq}(g(\phi), \mathsf{secret})\ \mathsf{then}\ \textsc{id}_\mathsf{A}\ \mathsf{else}\ \mathsf{Error}$$

can be used to model the output of an agent that checks if its input $g(\phi)$ is equal to a secret value secret (which can be a constant function symbol, a name in $\mathcal{N}$, or a more complex term). If this is the case, the agent outputs its identity $\textsc{id}_\mathsf{A}$, and otherwise it sends an error message Error. ◇

Formulas. For every integer n, we have one predicate symbol $\sim_n$ of arity $2n$, which represents equivalence between two vectors of terms of length n. We use an infix notation for $\sim_n$, and omit n when not relevant. Formulas are built using the usual Boolean connectives and FO quantifiers.

Example 3. For example, the formula:

$$\mathsf{if}\ g()\ \mathsf{then}\ \mathsf{n}_0\ \mathsf{else}\ \mathsf{n}_1 \sim \mathsf{n}$$

states that sampling from n_0 or n_1, depending on the branch chosen by the adversarial function $g()$, is equivalent to sampling from a single name n. ◇

Semantics. We use the classical semantics using first-order models: every sort is interpreted by some domain and function symbols and predicates are interpreted as, respectively, functions of the appropriate domains and relations on these domains. Then, given such a model $\mathcal{M}$, we define the validity of a formula ϕ in $\mathcal{M}$ as usual, and we write $\mathcal{M} \models \phi$ whenever ϕ holds in $\mathcal{M}$.

We focus on a particular class of models, called the *computational models* (see [9] for a formal definition). In a computational model $\mathcal{M}_\mathsf{c}$, terms are interpreted in the set of PPTMs equipped with a working tape and two random tapes ρ_1, ρ_2. The tape ρ_1 is used for the protocol random values, while ρ_2 is for the adversary's random samplings. The adversary cannot access directly the random tape ρ_1, although it may obtain part of ρ_1 through the protocol messages. A key feature is to let the interpretation of an adversarial function g be *any* PPTM, which soundly models an attacker *arbitrary probabilistic polynomial time computation.* Moreover, the predicates $\sim_n$ are interpreted using *computational indistinguishability* $\approx$. Two families of distributions of bit-string sequences $(m_\eta)_\eta$ and $(m'_\eta)_\eta$, indexed by η, are indistinguishable if and only if for every PPTM $\mathcal{A}$ with random tape ρ_2, the following quantity is negligible in η:

$$\left|\mathbf{Pr}(\rho_1, \rho_2 :\ \mathcal{A}(m_\eta(\rho_1, \rho_2), \rho_2) = 1) - \mathbf{Pr}(\rho_1, \rho_2 :\ \mathcal{A}(m'_\eta(\rho_1, \rho_2), \rho_2) = 1)\right|$$

Axioms. We describe most of the axioms used to prove that the AKA$^+$ protocol is secure later. Still, as an example, we give three simple structural axioms, Refl, Sym and Trans, which are valid in any computational model and states that indistinguishability is an equivalence relation:

$$\frac{}{\vec{u} \sim \vec{u}}\ \mathsf{Refl} \qquad\qquad \frac{\vec{v} \sim \vec{u}}{\vec{u} \sim \vec{v}}\ \mathsf{Sym} \qquad\qquad \frac{\vec{u} \sim \vec{w} \qquad \vec{w} \sim \vec{v}}{\vec{u} \sim \vec{v}}\ \mathsf{Trans}$$

7 MODELING

In this section, we explain how we model the σ_{ul}-unlinkability of the AKA$^+$ protocol using the Bana-Comon logic. To improve readability, protocol descriptions often omit some details: e.g., in Section 4, we sometimes omitted the description of the error messages. In other words, the AKA$^+$ protocol presented in Section 4 is *under-specified.* The failure message attack of [4] demonstrates that such details may be crucial for security. Therefore, before proving the AKA$^+$ protocol's security, we need to fully formalize it, and to make all assumptions explicit. Similarly, the σ-unlinkability property presented in Section 5.1 is only defined informally using a game.

Therefore, to formally define the protocol, we choose to describe it directly in the BC logic. Then, the assumptions on the protocol can be directly expressed in the logic using axioms. This is simpler than describing the protocol and the assumptions as interactive Turing machines and properties of these machines, and then translating them. We also define the σ_{ul}-unlinkability property in the BC logic, as the unsatisfiability of a set of formulas, one for each trace of the protocol execution.

7.1 The AKA$^+$ Protocol Action Trace

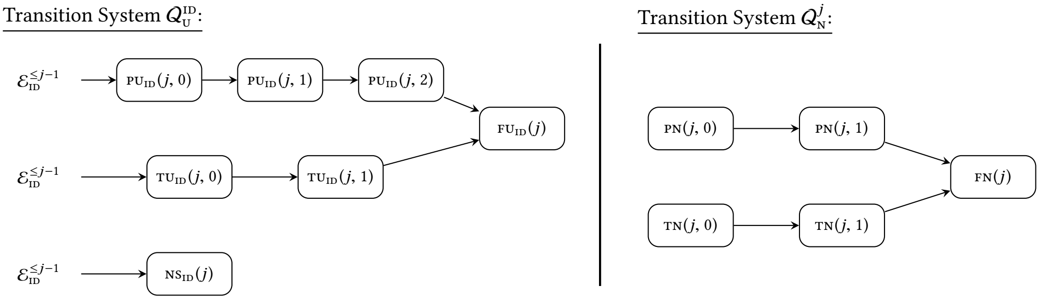
We let $\mathcal{S}_{\mathsf{id}}^{\omega}$ be a countable set of zero-arity function symbols, which are used to represent identities. We are going to define the AKA^+_N protocol, which is the AKA$^+$ protocol on N identities $\mathcal{S}_{\mathsf{id}} = \{\textsc{id}_1, \dots, \textsc{id}_N\}$.

Symbolic State. For every identity $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$, we use several variables to represent $UE_{\textsc{id}}$'s state. E.g. $\textsc{sqn}_{\textsc{u}}^{\textsc{id}}$ and $\textsc{guti}_{\textsc{u}}^{\textsc{id}}$ store, respectively, $UE_{\textsc{id}}$'s sequence number and temporary identity. Similarly, we have variables for HN's state, e.g. $\textsc{sqn}_{\textsc{n}}^{\textsc{id}}$. We let Vars_σ be the set of variables used in AKA^+_N:

$$\mathsf{Vars}_\sigma \;=\; \bigcup_{\substack{\textsc{a} \in \{\textsc{u},\textsc{n}\} \\ j \in \mathbb{N},\, \textsc{id} \in \mathcal{S}_{\mathsf{id}}}} \left\{ \begin{array}{l} \textsc{sqn}_{\textsc{a}}^{\textsc{id}}, \textsc{guti}_{\textsc{a}}^{\textsc{id}}, \mathsf{e\text{-}auth}_{\textsc{u}}^{\textsc{id}}, \mathsf{b\text{-}auth}_{\textsc{u}}^{\textsc{id}}, \mathsf{e\text{-}auth}_{\textsc{n}}^{j} \\ \mathsf{b\text{-}auth}_{\textsc{n}}^{j}, \mathsf{s\text{-}valid\text{-}guti}_{\textsc{u}}^{\textsc{id}}, \mathsf{valid\text{-}guti}_{\textsc{u}}^{\textsc{id}}, \mathsf{session}_{\textsc{n}}^{\textsc{id}} \end{array} \right\}$$

A symbolic state σ is a mapping from Vars_σ to terms. Intuitively, $\sigma(\mathrm{x})$ is a term representing (the distribution of) the value of x.

Example 4. To avoid confusion with the semantic equality $=$, we use $\equiv$ to denote syntactic equality between terms. We can express the fact that $\textsc{guti}_{\textsc{u}}^{\textsc{id}}$ is unset in a symbolic state σ by having $\sigma(\textsc{guti}_{\textsc{u}}^{\textsc{id}}) \equiv \mathsf{UnSet}$. Also, given a state σ, we can state that σ' is the state σ in which we


Transition System $Q_{\mathrm{U}}^{\mathrm{ID}}$:
$\mathcal{E}_{\mathrm{ID}}^{\leq j-1}$
$\mathrm{PU}_{\mathrm{ID}}(j,0)$
$\mathrm{PU}_{\mathrm{ID}}(j,1)$
$\mathrm{PU}_{\mathrm{ID}}(j,2)$
$\mathrm{FU}_{\mathrm{ID}}(j)$
$\mathcal{E}_{\mathrm{ID}}^{\leq j-1}$
$\mathrm{TU}_{\mathrm{ID}}(j,0)$
$\mathrm{TU}_{\mathrm{ID}}(j,1)$
$\mathcal{E}_{\mathrm{ID}}^{\leq j-1}$
$\mathrm{NS}_{\mathrm{ID}}(j)$
Transition System Q_{N}^{j}:
$\mathrm{PN}(j,0)$
$\mathrm{PN}(j,1)$
$\mathrm{FN}(j)$
$\mathrm{TN}(j,0)$
$\mathrm{TN}(j,1)$

Convention: where $\mathcal{E}_{\mathrm{ID}}^{\leq j} = \{\mathrm{PU}_{\mathrm{ID}}(j_0,i), \mathrm{TU}_{\mathrm{ID}}(j_0,i), \mathrm{FU}_{\mathrm{ID}}(j_0), \mathrm{NS}_{\mathrm{ID}}(j_0) \mid j_0 \leq j\}$, the initial states of $Q_{\mathrm{U}}^{\mathrm{ID}}$ are $\mathrm{PU}_{\mathrm{ID}}(0,0)$ and $\mathrm{TU}_{\mathrm{ID}}(0,0)$, and the initial states of Q_{N}^{j} are $\mathrm{PN}(j,0)$ and $\mathrm{TN}(j,0)$. Every state of $Q_{\mathrm{U}}^{\mathrm{ID}}$ and Q_{N}^{j} is final.

Fig. 12. The Transition Systems Used to Define Valid Action Traces.

incremented $\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}$ as follows:

$$\forall \mathsf{x} \in \mathsf{Vars}_{\sigma},\ \sigma'(\mathsf{x}) \ \equiv \ \begin{cases} \sigma(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) + 1 & \text{if } \mathsf{x} = \mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}} \\ \sigma(\mathsf{x}) & \text{otherwise} \end{cases} \qquad \diamond$$

Action Labels. In the $(q, \sigma_{\mathsf{ul}})$-unlinkability game, the adversary chooses dynamically which oracle it wants to call. This is not convenient to use in proofs, as we do not know statically the i-th action of the adversary. We prefer an alternative point-of-view, in which the trace of oracle calls is fixed. Then, there are no winning adversaries against the σ_{ul}-unlinkability game with a fixed trace of oracle calls if the adversary's interactions with the oracles when $b = 0$ are indistinguishable from the interactions with the oracles when $b = 1$.

For every set of identities $\mathcal{S}_{\mathsf{id}}$, we use the following action labels $\mathcal{L}$ to represent symbolic calls to the $(q, \sigma_{\mathsf{ul}})$-unlinkability oracles:

- $\mathrm{NS}_{\mathrm{ID}}(j)$ represents a call to $\mathsf{DrawUE}_{\sigma_{\mathsf{ul}}}(\mathrm{ID}, \_)$ when $b = 0$ or $\mathsf{DrawUE}_{\sigma_{\mathsf{ul}}}(\_, \mathrm{ID})$ when $b = 1$.
- $\mathrm{PU}_{\mathrm{ID}}(j,i)$ (resp. $\mathrm{TU}_{\mathrm{ID}}(j,i)$) is the i-th user message in the session $\mathit{UE}_{\mathrm{ID}}(j)$ of the SUPI (resp. GUTI) sub-protocol.
- $\mathrm{FU}_{\mathrm{ID}}(j)$ is the only user message in the session $\mathit{UE}_{\mathrm{ID}}(j)$ of the ASSIGN-GUTI sub-protocol.
- $\mathrm{PN}(j,i)$ (resp. $\mathrm{TN}(j,i)$) is the i-th network message in the session $\mathit{HN}(j)$ of the SUPI (resp. GUTI) sub-protocol.
- $\mathrm{FN}(j)$ is the only network message in the session $\mathit{HN}(j)$ of the ASSIGN-GUTI sub-protocol.

The remaining oracle calls either have no outputs and do not modify the state (e.g. `StartSession`), or can be simulated using the oracles above. E.g., since the *HN* sends an error message whenever the protocol is not successful, the output of `ResultHN` can be deduced from the protocol messages.

Valid Action Traces. An *action trace* τ is a finite sequence of action labels. Remark that some sequences of actions do not correspond to a valid execution of the protocol. E.g. since the session $\mathit{UE}_{\mathrm{ID}}(j)$ cannot execute both the SUPI and the GUTI protocols, a *valid action trace* cannot contain both $\mathrm{PU}_{\mathrm{ID}}(j, \_)$ and $\mathrm{TU}_{\mathrm{ID}}(j, \_)$. Similarly, the *HN*'s second message in the SUPI protocol cannot be sent before the first message, hence $\mathrm{PN}(j,1)$ cannot appear before $\mathrm{PN}(j,0)$ in τ. This motivate the definition of *valid action traces.*

Definition 2. Let $(Q_{\mathrm{U}}^{\textsc{id}})_{\textsc{id}\in\mathcal{S}_{\mathsf{id}}}$ and $(Q_{\mathrm{N}}^{j})_{j\in\mathbb{N}}$ be the transition systems in Figure 12. A trace $\tau = \mathsf{ai}_0,\dots,\mathsf{ai}_n$ is a *valid* action trace of the protocol AKA^+_N if and only if τ is an interleaving of the words $w_{\textsc{id}_1},\dots,w_{\textsc{id}_N}, w_{\mathrm{N}}^0,\dots,w_{\mathrm{N}}^l,\dots$ where:

- for every $1 \leq j \leq N$, $w_{\textsc{id}_j}$ is a run of $Q_{\mathrm{U}}^{\textsc{id}_j}$.
- for every $j \in \mathbb{N}$, w_{N}^j is a run of Q_{N}^j.

Example 5. We give valid action traces corresponding to the honest execution of AKA^+_N between $UE_{\textsc{id}}(i)$ and $HN(j)$. If the $\textsc{supi}$ protocol is used, we have the trace $\tau_{\textsc{supi}}^{i,j}(\textsc{id})$:

$$\textsc{pu}_{\textsc{id}}(i,0),\ \textsc{pn}(j,0), \textsc{pu}_{\textsc{id}}(i,1), \textsc{pn}(j,1), \textsc{pu}_{\textsc{id}}(i,2), \textsc{fn}(j), \textsc{fu}_{\textsc{id}}(i)$$

And if the $\textsc{guti}$ sub-protocol is used, the trace $\tau_{\textsc{guti}}^{i,j}(\textsc{id})$:

$$\textsc{tu}_{\textsc{id}}(i,0), \textsc{tn}(j,0), \textsc{tu}_{\textsc{id}}(i,1), \textsc{tn}(j,1), \textsc{fn}(j), \textsc{fu}_{\textsc{id}}(i)$$

Which such notations, the left trace τ_l of the attack described in Figure 11, in which the adversary only interacts with A, is:

$$\textsc{tu}_{\mathrm{A}}(0,0), \textsc{tn}(0,0), \textsc{tu}_{\mathrm{A}}(0,1), \tau_{\textsc{supi}}^{1,1}(\mathrm{A}), \textsc{tn}(0,1), \tau_{\textsc{guti}}^{2,2}(\mathrm{A})$$

Similarly, we can give the right trace τ_r in which the adversary interacts with A and B:

$$\textsc{tu}_{\mathrm{A}}(0,0), \textsc{tn}(0,0), \textsc{tu}_{\mathrm{A}}(0,1), \tau_{\textsc{supi}}^{0,1}(\mathrm{B}), \textsc{tn}(0,1), \tau_{\textsc{guti}}^{1,2}(\mathrm{B}) \qquad \diamond$$

7.2 The AKA$^+$ Protocol Symbolic Outputs and State Updates

We define, for every action label ai, the term representing the output observed by the adversary when ai is executed. Since the protocol is stateful, this term is a function of the prefix trace of actions executed since the beginning. We define by mutual induction, for any symbolic trace $\tau = \tau_0, \mathsf{ai}$ whose last action is ai:

- The term t_τ representing the last message observed during the execution of τ.
- The symbolic state σ_τ representing the state after the execution of τ.
- The frame ϕ_τ representing the sequence of all messages observed during the execution of τ.

Some syntactic sugar: we let $\sigma_\tau^{\mathsf{in}} \equiv \sigma_{\tau_0}$ be the symbolic state before the execution of the last action; and $\phi_\tau^{\mathsf{in}} \equiv \phi_{\tau_0}$ be the sequence of all messages observed during the execution of τ, except for the last message.

The frame ϕ_τ is simply the frame ϕ_τ^{in} extended with t_τ, i.e. $\phi_\tau \equiv \phi_\tau^{\mathsf{in}}, t_\tau$. When executing an action ai, only a subset of the symbolic state is modified. For example, if the adversary interacts with $UE_{\textsc{id}}$ then the state of the *HN* and of all the other users is unchanged. Therefore instead of defining σ_τ, we define the *symbolic state update* $\sigma_\tau^{\mathsf{up}}$, which is a *partial* function from Vars_σ to terms. Then σ_τ is the function:

$$\sigma_\tau(\mathsf{x}) \equiv \begin{cases} \sigma_\tau^{\mathsf{in}}(\mathsf{x}) & \text{if } \mathsf{x} \notin \mathsf{dom}(\sigma_\tau^{\mathsf{up}}) \\ \sigma_\tau^{\mathsf{up}}(\mathsf{x}) & \text{if } \mathsf{x} \in \mathsf{dom}(\sigma_\tau^{\mathsf{up}}) \end{cases}$$

where dom gives the domain of a function.

We start by giving the initial frame ϕ_ϵ and initial symbolic state.

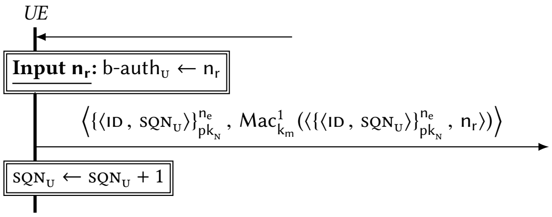
Definition 3. The initial frame of the AKA$^+$ protocol is $\phi_\epsilon \equiv \mathsf{pk}_{\mathrm{N}}$, and its initial symbolic state σ_ϵ is the function from Vars_σ to terms defined by having, for every $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$ and $j \in \mathbb{N}$:

$$\sigma_\epsilon(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}}) \equiv \mathsf{sqn\text{-}init}_{\mathrm{U}}^{\textsc{id}} \qquad \sigma_\epsilon(\textsc{sqn}_{\mathrm{N}}^{\textsc{id}}) \equiv \mathsf{sqn\text{-}init}_{\mathrm{N}}^{\textsc{id}} \qquad \sigma_\epsilon(\textsc{guti}_{\mathrm{X}}^{\textsc{id}}) \equiv \mathsf{UnSet} \qquad \sigma_\epsilon(\mathsf{e\text{-}auth}_{\mathrm{U}}^{\textsc{id}}) \equiv \mathsf{fail}$$

$$\sigma_\epsilon(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\textsc{id}}) \equiv \mathsf{fail} \qquad \sigma_\epsilon(\mathsf{e\text{-}auth}_{\mathrm{N}}^{j}) \equiv \mathsf{fail} \qquad \sigma_\epsilon(\mathsf{b\text{-}auth}_{\mathrm{N}}^{j}) \equiv \mathsf{fail} \qquad \sigma_\epsilon(\mathsf{s\text{-}valid\text{-}guti}_{\mathrm{U}}^{\textsc{id}}) \equiv \mathsf{false}$$

$$\sigma_\epsilon(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\textsc{id}}) \equiv \mathsf{false} \qquad \sigma_\epsilon(\mathsf{session}_{\mathrm{N}}^{\textsc{id}}) \equiv \mathsf{UnSet}$$

Now, for every action trace τ, we have to define t_τ and $\sigma_\tau^{\mathsf{up}}$ using ϕ_τ^{in} and $\sigma_\tau^{\mathsf{in}}$. As an example, we describe the second message and state update of the session $UE_{\textsc{id}}(j)$ for the SUPI sub-protocol, which corresponds to the action $\mathsf{ai} = \textsc{pu}_{\textsc{id}}(j, 1)$. We recall the relevant part of Figure 6:


UE
Input $\mathsf{n_r}$: $\mathsf{b\text{-}auth_U} \leftarrow \mathsf{n_r}$
$\left\langle \{\langle \textsc{id}, \textsc{sqn}_U\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e}}, \mathsf{Mac}_{\mathsf{k_m}}^1(\langle \{\langle \textsc{id}, \textsc{sqn}_U\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e}}, \mathsf{n_r}\rangle) \right\rangle$
$\textsc{sqn}_U \leftarrow \textsc{sqn}_U + 1$

First, we build a term representing the asymmetric encryption of the pair containing the UE's permanent identity ID and its sequence number. The permanent identity ID is simply represented using a constant function symbol ID, and $UE_{\textsc{id}}$'s sequence number is stored in the variable $\textsc{sqn}_U^{\textsc{id}}$, and can be retrieved from the symbolic state $\sigma_\tau^{\mathsf{in}}$ using $\sigma_\tau^{\mathsf{in}}(\textsc{sqn}_U^{\textsc{id}})$. Finally, we use the asymmetric encryption function symbol to build the term:

$$t_\tau^{\mathsf{enc}} \equiv \{\langle \textsc{id}, \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_U^{\textsc{id}})\rangle\}_{\mathsf{pk_N}}^{\mathsf{n}_e^j}$$

Notice that the encryption is randomized using a nonce n_e^j, and that the freshness of the randomness is guaranteed by indexing the nonce with the session number j. Finally, we can give t_τ and $\sigma_\tau^{\mathsf{up}}$:

$$t_\tau \equiv \left\langle t_\tau^{\mathsf{enc}}, \mathsf{Mac}_{\mathsf{k_m^{\textsc{id}}}}^1(\langle t_\tau^{\mathsf{enc}}, g(\phi_\tau^{\mathsf{in}})\rangle)\right\rangle \qquad \sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \textsc{sqn}_U^{\textsc{id}} \mapsto \mathsf{suc}(\sigma_\tau^{\mathsf{in}}(\textsc{sqn}_U^{\textsc{id}})) & \mathsf{e\text{-}auth}_U^{\textsc{id}} \mapsto \mathsf{fail} \\ \mathsf{b\text{-}auth}_U^{\textsc{id}} \mapsto g(\phi_\tau^{\mathsf{in}}) & \textsc{guti}_U^{\textsc{id}} \mapsto \mathsf{UnSet} \\ \mathsf{valid\text{-}guti}_U^{\textsc{id}} \mapsto \mathsf{false} & \end{cases}$$

Remark that we omitted some state updates in the description of the protocol in Figure 6. For example, $UE_{\textsc{id}}$ temporary identity $\textsc{guti}_U^{\textsc{id}}$ is reset when starting the SUPI sub-protocol. In the Bana-Comon model, these details are made explicit.

The description of t_τ and $\sigma_\tau^{\mathsf{up}}$ for the other actions can be found in Figure 13 and Figure 14. Observe that we describe one more message for the SUPI and GUTI protocols than in Section 4. This is because we added one message ($\textsc{pu}_{\textsc{id}}(j, 2)$ for SUPI and $\textsc{tn}(j, 1)$ for GUTI) for proof purposes, to simulate the `ResultUE` and `ResultHN` oracles. Also, notice that in the GUTI protocol, when HN receives an unassigned GUTI, it sends a decoy message to a special dummy identity $\textsc{id}_{\mathsf{dum}}$.

7.3 Modeling σ-Unlinkability

We associate, to any execution of the $(q, \sigma_{\mathsf{ul}})$-unlinkability game with a fixed trace of oracle calls, a pair of action traces (τ_l, τ_r), which corresponds to the adversary's interactions with the oracles when b is, respectively, 0 and 1. We do this as follows:

- First, we consider a valid action trace τ on a set of identities $\mathcal{S}_{\mathsf{vh}}$, seen as virtual handlers. The trace τ is the sequence of oracle calls as seen by the adversary.
- We consider a mapping θ_l which associates, to every virtual handler in $\mathcal{S}_{\mathsf{vh}}$, an identity in $\mathcal{S}_{\mathsf{id}}$, where $\mathcal{S}_{\mathsf{id}} = \{\textsc{id}_1, \ldots, \textsc{id}_N\}$. This mapping must check that new virtual handlers are associated to identities in l_{free}: for every identity $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$, this mapping must be such that, at any point in τ, there is at most one virtual handler which is alive and mapped to ID by θ_l. Similarly, we consider a mapping θ_r for the right side.
- Finally, we let τ_l be the action trace obtained from τ by replacing the virtual handler by the corresponding concrete identities using θ_l, and re-numbering the session numbers. We define similarly τ_l using θ_r. Then $\mathcal{R}_{\mathsf{ul}}^N$ contains the pair of action trace (τ_l, τ_r).

We define what it means for the AKA_N^+ protocol to be is σ_{ul}-unlinkable.

Case $\mathsf{ai} = \textsc{ns}_{\textsc{id}}(j)$. $\sigma_\tau^{\mathsf{up}} \equiv \mathsf{valid\text{-}guti}_{\textsc{u}}^{\textsc{id}} \mapsto \mathsf{false}$

Case $\mathsf{ai} = \textsc{pu}_{\textsc{id}}(j, 0)$. $t_\tau \equiv \texttt{Request\_Challenge}$

Case $\mathsf{ai} = \textsc{pn}(j, 0)$. $t_\tau \equiv \mathsf{n}^j$

Case $\mathsf{ai} = \textsc{pu}_{\textsc{id}}(j, 1)$. Let $t_\tau^{\mathsf{enc}} \equiv \{\langle \textsc{id}\,,\, \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\textsc{n}}}^{\mathsf{n}_{\mathsf{e}}^{j}}$, then:

$$t_\tau \equiv \langle t_\tau^{\mathsf{enc}}\,,\, \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle t_\tau^{\mathsf{enc}}\,,\, g(\phi_\tau^{\mathsf{in}})\rangle)\rangle$$

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \textsc{sqn}_{\textsc{u}}^{\textsc{id}} \mapsto \mathsf{suc}(\sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})) & \mathsf{e\text{-}auth}_{\textsc{u}}^{\textsc{id}} \mapsto \mathsf{fail} \qquad \mathsf{valid\text{-}guti}_{\textsc{u}}^{\textsc{id}} \mapsto \mathsf{false} \\ \mathsf{b\text{-}auth}_{\textsc{u}}^{\textsc{id}} \mapsto g(\phi_\tau^{\mathsf{in}}) & \textsc{guti}_{\textsc{u}}^{\textsc{id}} \mapsto \mathsf{UnSet} \end{cases}$$

Case $\mathsf{ai} = \textsc{pn}(j, 1)$. Let $t_{\mathsf{dec}} \equiv \mathsf{dec}(\pi_1(g(\phi_\tau^{\mathsf{in}})), \mathsf{sk}_{\textsc{n}})$, and let:

$$\mathsf{accept}_\tau^{\textsc{id}_i} \equiv \mathsf{eq}(\pi_2(g(\phi_\tau^{\mathsf{in}})), \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}_i}}(\langle \pi_1(g(\phi_\tau^{\mathsf{in}}))\,,\, \mathsf{n}^j\rangle)) \;\wedge\; \mathsf{eq}(\pi_1(t_{\mathsf{dec}}), \textsc{id}_i)$$

$$\mathsf{inc\text{-}accept}_\tau^{\textsc{id}_i} \equiv \mathsf{accept}_\tau^{\textsc{id}_i} \wedge \mathsf{geq}(\pi_2(t_{\mathsf{dec}}), \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}_i}))$$

$$\begin{aligned} t_\tau \equiv\ & \text{if } \mathsf{accept}_\tau^{\textsc{id}_1} \text{ then } \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}_1}}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\pi_2(t_{\mathsf{dec}}))\rangle) \\ & \text{else if } \mathsf{accept}_\tau^{\textsc{id}_2} \text{ then } \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}_2}}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\pi_2(t_{\mathsf{dec}}))\rangle) \\ & \quad\ldots \\ & \text{else } \mathsf{UnknownId} \end{aligned}$$

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \mathsf{session}_{\textsc{n}}^{\textsc{id}_i} \mapsto \text{if } \mathsf{inc\text{-}accept}_\tau^{\textsc{id}_i} \text{ then } \mathsf{n}^j \text{ else } \mathsf{session}_{\textsc{n}}^{\textsc{id}_i} \\ \textsc{guti}_{\textsc{n}}^{\textsc{id}_i} \mapsto \text{if } \mathsf{inc\text{-}accept}_\tau^{\textsc{id}_i} \text{ then } \textsc{guti}^j \text{ else } \sigma_\tau^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}_i}) \\ \textsc{sqn}_{\textsc{n}}^{\textsc{id}_i} \mapsto \text{if } \mathsf{inc\text{-}accept}_\tau^{\textsc{id}_i} \text{ then } \mathsf{suc}(\pi_2(t_{\mathsf{dec}})) \text{ else } \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}_i}) \\ \mathsf{b\text{-}auth}_{\textsc{n}}^{j}, \mathsf{e\text{-}auth}_{\textsc{n}}^{j} \mapsto \text{if } \mathsf{accept}_\tau^{\textsc{id}_1} \text{ then } \textsc{id}_1 \\ \qquad\qquad \text{else if } \mathsf{accept}_\tau^{\textsc{id}_2} \text{ then } \textsc{id}_2 \\ \qquad\qquad\quad \ldots \\ \qquad\qquad \text{else } \mathsf{UnknownId} \end{cases}$$

Case $\mathsf{ai} = \textsc{pu}_{\textsc{id}}(j, 2)$. Let $\mathsf{accept}_\tau^{\textsc{id}} \equiv \mathsf{eq}(g(\phi_\tau^{\mathsf{in}}), \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle \sigma_\tau^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\textsc{u}}^{\textsc{id}})\,,\, \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})\rangle))$, then:

$$t_\tau \equiv \text{if } \mathsf{accept}_\tau^{\textsc{id}} \text{ then } \mathsf{ok} \text{ else } \mathsf{error}$$

$$\sigma_\tau^{\mathsf{up}} \equiv \mathsf{e\text{-}auth}_{\textsc{u}}^{\textsc{id}} \mapsto \text{if } \mathsf{accept}_\tau^{\textsc{id}} \text{ then } \sigma_\tau^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\textsc{u}}^{\textsc{id}}) \text{ else } \mathsf{fail}$$

Case $\mathsf{ai} = \textsc{fn}(j)$. Let $\mathsf{msg}_\tau^{\textsc{id}_i} \equiv \langle \textsc{guti}^j \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\textsc{id}_i}}(\mathsf{n}^j)\,,\, \mathsf{Mac}^5_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}_i}}(\langle \textsc{guti}^j\,,\, \mathsf{n}^j\rangle)\rangle$, then:

$$\begin{aligned} t_\tau \equiv\ & \text{if } \mathsf{eq}(\sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\textsc{n}}^{j}), \textsc{id}_1) \text{ then } \mathsf{msg}_\tau^{\textsc{id}_1} \\ & \text{else if } \mathsf{eq}(\sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\textsc{n}}^{j}), \textsc{id}_2) \text{ then } \mathsf{msg}_\tau^{\textsc{id}_2} \\ & \quad\ldots \\ & \text{else } \mathsf{UnknownId} \end{aligned}$$

Case $\mathsf{ai} = \textsc{fu}_{\textsc{id}}(j)$. Let $t_{\textsc{guti}} \equiv \pi_1(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\textsc{id}}}(\sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\textsc{u}}^{\textsc{id}}))$, then:

$$\mathsf{accept}_\tau^{\textsc{id}} \equiv \mathsf{eq}(\pi_2(g(\phi_\tau^{\mathsf{in}})), \mathsf{Mac}^5_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle t_{\textsc{guti}}\,,\, \sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\textsc{u}}^{\textsc{id}})\rangle)) \;\wedge\; \neg\mathsf{eq}(\sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\textsc{u}}^{\textsc{id}}), \mathsf{fail})$$

$$t_\tau \equiv \text{if } \mathsf{accept}_\tau^{\textsc{id}} \text{ then } \mathsf{ok} \text{ else } \mathsf{error}$$

$$\sigma_\tau^{\mathsf{up}} \equiv \left\{ \mathsf{valid\text{-}guti}_{\textsc{u}}^{\textsc{id}} \mapsto \mathsf{accept}_\tau^{\textsc{id}} \qquad \textsc{guti}_{\textsc{u}}^{\textsc{id}} \mapsto \text{if } \mathsf{accept}_\tau^{\textsc{id}} \text{ then } t_{\textsc{guti}} \text{ else } \mathsf{UnSet} \right.$$

Convention: For every $j \in \mathbb{N}$, $\textsc{guti}^j \in \mathcal{N}$.

Fig. 13. The Symbolic Terms and States for $\textsc{ns}_{\textsc{id}}(j)$ and the SUPI and ASSIGN-GUTI Sub-Protocols.

Case $\underline{\text{ai} = \textsc{tu}_{\textsc{id}}(j, 0).}$

$$t_\tau \equiv \text{if } \sigma_\tau^{\text{in}}(\text{valid-guti}_{\textsc{u}}^{\textsc{id}}) \text{ then } \sigma_\tau^{\text{in}}(\textsc{guti}_{\textsc{u}}^{\textsc{id}}) \text{ else NoGuti}$$

$$\sigma_\tau^{\text{up}} \equiv \begin{cases} \text{valid-guti}_{\textsc{u}}^{\textsc{id}} \mapsto \text{false} & \text{e-auth}_{\textsc{u}}^{\textsc{id}} \mapsto \text{fail} \\ \text{s-valid-guti}_{\textsc{u}}^{\textsc{id}} \mapsto \sigma_\tau^{\text{in}}(\text{valid-guti}_{\textsc{u}}^{\textsc{id}}) & \text{b-auth}_{\textsc{u}}^{\textsc{id}} \mapsto \text{fail} \end{cases}$$

Case $\underline{\text{ai} = \textsc{tn}(j, 0).}$ Let $t_\oplus^{\textsc{id}_i} \equiv \sigma_\tau^{\text{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}_i}) \oplus \mathsf{f}_{\mathsf{k}^{\textsc{id}_i}}(\mathsf{n}^j)$, then:

$$\begin{aligned} \text{msg}_\tau^{\textsc{id}_i} &\equiv \langle \mathsf{n}^j, t_\oplus^{\textsc{id}_i}, \text{Mac}^3_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}_i}}(\langle \mathsf{n}^j, \sigma_\tau^{\text{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}_i}), \sigma_\tau^{\text{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}_i})\rangle)\rangle \\ \text{accept}_\tau^{\textsc{id}_i} &\equiv \text{eq}(\sigma_\tau^{\text{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}_i}), g(\phi_\tau^{\text{in}})) \wedge \neg\text{eq}(\sigma_\tau^{\text{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}_i}), \text{UnSet}) \\ t_\tau &\equiv \text{if accept}_\tau^{\textsc{id}_1} \text{ then msg}_\tau^{\textsc{id}_1} \\ &\quad\ \text{else if accept}_\tau^{\textsc{id}_2} \text{ then msg}_\tau^{\textsc{id}_2} \\ &\qquad\quad \ldots \\ &\quad\ \text{else msg}_\tau^{\textsc{id}_{\text{dum}}} \end{aligned}$$

$$\sigma_\tau^{\text{up}} \equiv \begin{cases} \textsc{guti}_{\textsc{n}}^{\textsc{id}_i} \mapsto \text{if accept}_\tau^{\textsc{id}_i} \text{ then UnSet else } \sigma_\tau^{\text{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}_i}) \\ \text{session}_{\textsc{n}}^{\textsc{id}_i} \mapsto \text{if accept}_\tau^{\textsc{id}_i} \text{ then } \mathsf{n}^j \text{ else } \sigma_\tau^{\text{in}}(\text{session}_{\textsc{n}}^{\textsc{id}_i}) \\ \text{b-auth}_{\textsc{n}}^{j} \mapsto \text{if accept}_\tau^{\textsc{id}_1} \text{ then } \textsc{id}_1 \\ \qquad\qquad\quad \text{else if accept}_\tau^{\textsc{id}_2} \text{ then } \textsc{id}_2 \\ \qquad\qquad\qquad\quad \ldots \\ \qquad\qquad\quad \text{else UnknownId} \end{cases}$$

Case $\underline{\text{ai} = \textsc{tu}_{\textsc{id}}(j, 1).}$ Let $t_{\textsc{sqn}} \equiv \pi_2(g(\phi_\tau^{\text{in}})) \oplus \mathsf{f}_{\mathsf{k}^{\textsc{id}}}(\pi_1(g(\phi_\tau^{\text{in}})))$, then:

$$\text{accept}_\tau^{\textsc{id}} \equiv \begin{array}{l} \quad\ \text{eq}(\pi_3(g(\phi_\tau^{\text{in}})), \text{Mac}^3_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle \pi_1(g(\phi_\tau^{\text{in}})), t_{\textsc{sqn}}, \sigma_\tau^{\text{in}}(\textsc{guti}_{\textsc{u}}^{\textsc{id}})\rangle)) \\ \wedge\ \sigma_\tau^{\text{in}}(\text{s-valid-guti}_{\textsc{u}}^{\textsc{id}}) \ \wedge\ \text{range}(\sigma_\tau^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}), t_{\textsc{sqn}}) \end{array}$$

$$t_\tau \equiv \text{if accept}_\tau^{\textsc{id}} \text{ then Mac}^4_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\pi_1(g(\phi_\tau^{\text{in}}))) \text{ else error}$$

$$\sigma_\tau^{\text{up}} \equiv \begin{cases} \text{b-auth}_{\textsc{u}}^{\textsc{id}}, \text{e-auth}_{\textsc{u}}^{\textsc{id}} \mapsto \text{if accept}_\tau^{\textsc{id}} \text{ then } \pi_1(g(\phi_\tau^{\text{in}})) \text{ else fail} \\ \textsc{sqn}_{\textsc{u}}^{\textsc{id}} \mapsto \text{if accept}_\tau^{\textsc{id}} \text{ then suc}(\sigma_\tau^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})) \text{ else } \sigma_\tau^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) \end{cases}$$

Case $\underline{\text{ai} = \textsc{tn}(j, 1).}$

$$\begin{aligned} \text{accept}_\tau^{\textsc{id}_i} &\equiv \text{eq}(g(\phi_\tau^{\text{in}}), \text{Mac}^4_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}_i}}(\mathsf{n}^j)) \wedge \text{eq}(\sigma_\tau^{\text{in}}(\text{b-auth}_{\textsc{n}}^{j}), \textsc{id}_i) \\ \text{inc-accept}_\tau^{\textsc{id}_i} &\equiv \text{accept}_\tau^{\textsc{id}_i} \wedge \text{eq}(\sigma_\tau^{\text{in}}(\text{session}_{\textsc{n}}^{\textsc{id}_i}), \mathsf{n}^j) \\ t_\tau &\equiv \text{if } \textstyle\bigvee_i \text{accept}_\tau^{\textsc{id}_i} \text{ then ok else error} \end{aligned}$$

$$\sigma_\tau^{\text{up}} \equiv \begin{cases} \textsc{sqn}_{\textsc{n}}^{\textsc{id}_i} \mapsto \text{if inc-accept}_\tau^{\textsc{id}_i} \text{ then suc}(\sigma_\tau^{\text{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}_i})) \\ \qquad\qquad\qquad\qquad\qquad\qquad\quad \text{else } \sigma_\tau^{\text{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}_i}) \\ \textsc{guti}_{\textsc{n}}^{\textsc{id}_i} \mapsto \text{if inc-accept}_\tau^{\textsc{id}_i} \text{ then } \textsc{guti}^j \text{ else } \sigma_\tau^{\text{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}_i}) \\ \text{e-auth}_{\textsc{n}}^{j} \mapsto \text{if accept}_\tau^{\textsc{id}_1} \text{ then } \textsc{id}_1 \\ \qquad\qquad\quad \text{else if accept}_\tau^{\textsc{id}_2} \text{ then } \textsc{id}_2 \\ \qquad\qquad\qquad\quad \ldots \\ \qquad\qquad\quad \text{else UnknownId} \end{cases}$$

Convention: For every $j \in \mathbb{N}$, $\textsc{guti}^j \in \mathcal{N}$.

Fig. 14. The Symbolic Terms and States the GUTI Sub-Protocol.

Definition 4. The protocol AKA^+_N is σ_{ul}-unlinkable in any computational model satisfying the axioms Ax if, for every $(\tau_l, \tau_r) \in \mathcal{R}^N_{\text{ul}}$, we can derive $\phi_{\tau_l} \sim \phi_{\tau_r}$ using Ax.

Proposition 1. *$\mathcal{R}^N_{ul}$ is reflexive, symmetric and transitive. Moreover, for every $\tau \in support(\mathcal{R}^N_{ul})$, τ is a valid action trace of AKA^+_N.*

Proof. We show this by induction over the valid action trace τ_{vh}, on virtual identities $\mathcal{S}_{\text{vh}}$, used to define τ. We omit the details. ■

Most Anonymised Trace. Given an action trace $\tau \in \text{support}(\mathcal{R}^N_{\text{ul}})$, there is a particular and unique action trace $\underline{\tau}$ which is the "most anonymised trace" corresponding to τ. Intuitively, $\underline{\tau}$ is the trace τ where we changed a user identity every time we could (i.e. every time $\textsc{ns}_{\textsc{id}}(\_)$ appears). This is useful to prove that the AKA^+ protocol is σ_{ul}-unlinkable, as it reduces the number of cases we have to consider: we only need to show that we can derive $\phi_\tau \sim \phi_{\underline{\tau}}$ for every $\tau \in \text{support}(\mathcal{R}^N_{\text{ul}})$.

There is a small difficulty here: the number if identities in $\underline{\tau}$ is not the same than in τ. Therefore, on the right side we need to consider an execution of the AKA^+ protocol with more identities. More precisely, since the number of identities in $\underline{\tau}$ is upper-bounded by $|\mathcal{S}_{\text{id}}| \times |\tau| = N \times |\tau|$, it is sufficient to prove that for every $\tau \in \text{support}(\mathcal{R}^N_{\text{ul}})$, for every $\underline{N} \geq N \times |\tau|$, there exists a derivation of:

$$\phi_\tau^{\text{AKA}^+_N} \sim \phi_{\underline{\tau}}^{\text{AKA}^+_{\underline{N}}} \tag{2}$$

To do this, we consider a countable subset $\mathcal{S}_{\text{bid}} = \{\mathsf{A}_i \mid i \in \mathbb{N}\}$ of $\mathcal{S}^\omega_{\text{id}}$. The set $\mathcal{S}_{\text{bid}}$ is a set of base identities. Then, for every base identity A_i, we have copies $\mathsf{A}_i = \mathsf{A}_{i,1}, \dots, \mathsf{A}_{i,C}, \dots$ of A_i. The first copy $\mathsf{A}_{i,1}$ is always A_i, and all the copies are distinct function symbols. Moreover, for every $(i, j) \neq (i', j')$, the function symbols $\mathsf{A}_{i,j}$ and $\mathsf{A}_{i',j'}$ are distinct.

Definition 5. Given an identity $\mathsf{A}_{b,c}$, we let $\text{fresh-id}(\mathsf{A}_{b,c}) = \mathsf{A}_{b,c+1}$, and given a base identity $\mathsf{A}_{b,1}$ we let $\text{copies-id}_C(\mathsf{A}_{b,1}) = \{\mathsf{A}_{b,i} \mid 1 \leq i \leq C\}$. We require that all these identities are distinct:

$$\mathcal{S}^\omega_{\text{id}} = \biguplus_{i,j \in \mathbb{N}} \{\mathsf{A}_{i,j}\}$$

where $\uplus$ denotes the disjoint union.

A *basic action trace* is an action trace using only base identities $\{\mathsf{A}_{b,1} \mid b \in \mathbb{N}\}$.

Definition 6. An action trace τ is *basic* if it only uses network action labels and user action labels $\mathsf{X}_{\textsc{id}}(\_)$ where $\textsc{id}$ is a base identity, i.e. $\textsc{id} \in \mathcal{S}_{\text{bid}}$.

For every basic action trace τ, we let $\underline{\tau}$ be the most anonymised action trace corresponding to τ.

Definition 7. For every basic action trace τ, we let $\underline{\tau}$ be the action trace obtained from τ by replacing, each time we encounter an action $\textsc{ns}_{\textsc{id}}(j)$, all subsequent actions with agent $\textsc{id}$ by actions with agent $\text{fresh-id}(\textsc{id})$:

$$\underline{\tau} = \begin{cases} \textsc{ns}_{\nu\textsc{id}}(j), \underline{\tau_0[\nu\textsc{id}/\textsc{id}]} & \text{when } \tau = \textsc{ns}_{\textsc{id}}(j), \tau_0 \text{ and } \nu\textsc{id} = \text{fresh-id}(\textsc{id}) \\ \text{ai}, \underline{\tau_0} & \text{when } \tau = \text{ai}, \tau_0 \text{ and ai} \notin \{\textsc{ns}_{\textsc{id}}(j) \mid \textsc{id} \in \mathcal{S}_{\text{id}}, j \in \mathbb{N}\} \end{cases}$$

Proposition 2. *If τ is a valid basic action trace on identities $\mathcal{S}_{id}$ then $\underline{\tau}$ is a valid action trace using less than $|\mathcal{S}_{id}| \times |\tau|$ distinct identities.*

Proof. The proof is straightforward by induction over τ. ■

We can check that for every $(\tau_l, \tau_r) \in \mathcal{R}^N_{\text{ul}}$ we have $\underline{\tau_l} = \underline{\tau_r}$. Moreover, $\sim$ is a transitive relation. Therefore, instead of proving that for every $\mathcal{R}^N_{\text{ul}}(\tau_l, \tau_r)$ the formula in (2) using Ax, it is sufficient to show that for every $\tau \in \text{support}(\mathcal{R}^N_{\text{ul}})$, there exists a derivation of:

$$\phi_\tau^{\text{AKA}^+_N} \sim \phi_{\underline{\tau}}^{\text{AKA}^+_{\underline{N}}} \tag{3}$$

where $\underline{N}$ is larger than the number of distinct identities used in $\underline{\tau}$. Formally:

Proposition 3. *Let Ax be a set of axioms including Trans and Sym. The AKA^+_N protocol is σ_{ul}-unlinkable in any computational model satisfying some axioms Ax if for every $\tau \in$ support$(\mathcal{R}^N_{ul})$, for every $\underline{N} \geq N \times |\tau|$, there is a derivation using Ax of* (3).

Proof. Let $(\tau_l, \tau_r) \in \mathcal{R}^N_{\mathrm{ul}}$. Using Proposition 2, we know that $\underline{\tau_l}$ and $\underline{\tau_r}$ are valid action traces of $\mathrm{AKA}^+_{\underline{N}}$. Since $\underline{\tau_l} = \underline{\tau_r}$, and using the transitivity and symmetry axioms Trans and Sym, we get the wanted derivation:

$$\frac{\phi_{\tau_l}^{\mathrm{AKA}^+_N} \sim \phi_{\underline{\tau_l}}^{\mathrm{AKA}^+_{\underline{N}}} \qquad \phi_{\underline{\tau_r}}^{\mathrm{AKA}^+_{\underline{N}}} \sim \phi_{\tau_r}^{\mathrm{AKA}^+_N}}{\phi_{\tau_l}^{\mathrm{AKA}^+_N} \sim \phi_{\tau_r}^{\mathrm{AKA}^+_N}}\ (\text{Trans} + \text{Sym})^*$$

■

8 AXIOMS

Using Proposition 3, we know that to prove that the AKA^+_N protocol is σ_{ul}-unlinkable, we only need to give a derivation of (3) for every $\tau \in \mathrm{support}(\mathcal{R}^N_{\mathrm{ul}})$ and $\underline{N} \geq N \times |\tau|$, using the set of inference rules Ax. Moreover, we need the axioms Ax to be valid in any computational model where the asymmetric encryption $\{\_\}^{\_}_{\_}$ is IND-CCA$_1$ secure and f and f^{r} (resp. Mac^1– Mac^5) satisfy jointly the PRF assumption.

The AKA^+_N protocol described in Section 4 is under-specified. E.g., we never specified how the $\langle \_ , \_ \rangle$ function should be implemented. Instead of giving a complex specification of the protocol, we are going to put requirements on AKA^+_N implementations through the set of axioms Ax. Then, if we can derive (3) using Ax, we know that any implementation of AKA^+_N satisfying Ax is secure.

Our axioms are of two kinds. First, we have *structural axioms*, which are properties that are valid in any computational model. By consequence, such axioms can always be safely added. For example, we already gave axioms stating that $\sim$ is an equivalence relation. Second, we have *implementation axioms*, which reflect implementation assumptions on the protocol functions. For example, we can declare that different identity symbols are never equal by having an axiom $\mathsf{eq}(\mathrm{ID}_1, \mathrm{ID}_2) \sim \mathsf{false}$ for every $\mathrm{ID}_1 \not\equiv \mathrm{ID}_2$. For space reasons, we only describe a few of them here (the full set of axioms Ax is given in Section A and Section B).

8.1 Structural Axioms

Almost all the axioms in this subsection have been introduced in the literature, see [6, 9, 19].

Equality Axioms. If $\mathsf{eq}(s, t) \sim \mathsf{true}$ holds in any computational model then we know that the interpretations of s and t are always equal except for a negligible number of samplings. Hence all properties of equality hold: this relation is symmetric, reflexive, transitive and closed under function applications. Moreover, we can replace any occurrence of s by t in a formula without changing its semantics with respect to computational indistinguishability. We let $s = t$ be the shorthand for $\mathsf{eq}(s, t) \sim \mathsf{true}$, and $s \neq t$ for $\mathsf{eq}(s, t) \sim \mathsf{false}$, and we introduce the axioms:

$$\frac{}{u = u}\ \text{=-refl} \qquad \frac{v = u}{u = v}\ \text{=-sym} \qquad \frac{u = w \qquad w = v}{u = v}\ \text{=-trans}$$

$$\frac{u_0 = v_0 \qquad \ldots \qquad u_n = v_n}{f(u_0, \ldots, u_n) = f(v_0, \ldots, v_n)}\ \text{=-subst} \quad (f \in \mathcal{F}) \qquad \frac{\vec{u}, t \sim \vec{v} \qquad s = t}{\vec{u}, s \sim \vec{v}}\ \text{Equ}$$

We use = to specify functional properties of the function symbols. For example, the following rules reflects properties of the if_then_else_, of the pair and of the encryption function symbols:

$$\text{if } b \text{ then } x \text{ else } x = x \qquad \pi_i(\langle x_1 , x_2 \rangle) = x_i \text{ for } i \in \{1, 2\} \qquad \mathsf{dec}(\{x\}^z_{\mathsf{pk}(y)}, \mathsf{sk}(y)) = x$$

Other Structural Axioms. As an example, we present three simple structural axioms. The full set of structural axioms is given in Section A.1.

$$\frac{\vec{u}_1, \vec{v}_1 \sim \vec{u}_2, \vec{v}_2}{f(\vec{u}_1), \vec{v}_1 \sim f(\vec{u}_2), \vec{v}_2}\ \mathsf{FA} \qquad \frac{\vec{u}, \mathsf{n} \sim \vec{v} \qquad \mathsf{len}(t) = \mathsf{len}(\mathsf{n})}{\vec{u}, t \oplus \mathsf{n} \sim \vec{v}}\ \oplus\text{-ind} \quad \text{when } \mathsf{n} \notin \mathsf{st}(\vec{u}, \vec{v}, t)$$

The axiom FA states that to show that two function applications are indistinguishable, it is sufficient to show that their arguments are indistinguishable. The $\oplus$-ind axioms states that the xor of a term t and an uniform random value n is indistinguishable from an uniform random value, as long as t and n are independent and of the same length. The fact that t and n are independent is checked by requiring that n does not appear in t in the syntactic side-condition $\mathsf{n} \notin \mathsf{st}(\vec{u}, \vec{v}, t)$ (therefore this is an infinite schema of ground axioms).

8.2 Cryptographic Assumptions and Axioms

It is well-known that if H is a PRF then H is unforgeable against an adversary with oracle access to H, and that no adversary can efficiently find collision for H. Similarly, we can show that if $\mathsf{H}, \mathsf{H}_1, \dots, \mathsf{H}_l$ are jointly PRF, then no adversary can forge a mac of H, even if it has oracle access to $\mathsf{H}, \mathsf{H}_1, \dots, \mathsf{H}_l$ (the same holds for the collision-resistance property). In the next two sub-sections, we explain how cryptographic hypothesis on hash functions are translated in the logic, by giving axioms for the unforgeability and collision-resistance properties. We only give axioms for the standard assumptions, as the axioms for the joint assumptions are straightforward to obtain from them (the joint axioms can be found in Section B.8).

Before starting, we introduce some notations used in side-conditions of cryptographic axioms.

Definition 8. For every ground terms $\vec{u}, \vec{v}$, we let $\mathsf{fresh}(\vec{u}; \vec{v})$ holds if and only if no term in $\vec{v}$ is a subterm of a term in $\vec{v}$, i.e. $\{u \mid u \in \vec{u}\} \cap \mathsf{st}(\vec{v}) = \emptyset$.

Definition 9. Let $s, \vec{u}$ be ground terms and $C_{\vec{x},\cdot}$ be a context with one distinguished hole variable $\cdot$ such that the hole variable $\cdot$ appears exactly once in $C_{\vec{x},\cdot}$. We let $s \sqsubseteq_{C_{\vec{x},\cdot}} \vec{u}$ holds whenever s appears in $\vec{u}$ only in subterms of the form $C[\vec{w}, s]$. Formally:

$$\forall u \in \vec{u}, \forall p \in \mathsf{pos}(u), u_{|p} \equiv s \rightarrow \exists \vec{w} \in \mathcal{T}(\mathcal{F}, \mathcal{N}), \exists q \in \mathsf{pos}(u) \text{ s.t. } q \leq p \wedge u_{|q} \equiv C[\vec{w}, s]$$

Given n contexts $C_1, \dots, C_n$, we let $s \sqsubseteq_{C_1,\dots,C_n} \vec{u}$ if and only if for all $1 \leq i \leq n$, $s \sqsubseteq_{C_i} \vec{u}$.

Example 6. Two examples:

- $\mathsf{n} \sqsubseteq_{\mathsf{pk}(\cdot),\mathsf{sk}(\cdot)} \vec{u}$ states that the nonce n appears only in terms of the form pk(n) or sk(n) in $\vec{u}$.
- $\mathsf{sk}(\mathsf{n}) \sqsubseteq_{\mathsf{dec}(\_,\cdot)} \vec{u}$ states that the secret key sk(n) appears only in decryption position in $\vec{u}$. ◇

8.3 The CR-HK Axioms

A hash function $\mathsf{H}(\cdot, \mathsf{k})$ is collision-resistant if no polynomial-time adversary can find distinct messages having the same image by $\mathsf{H}(\cdot, \mathsf{k})$. Formally:

Definition 10 (CR-HK [26]). A hash function H is said to be *collision resistant under hidden-key attacks* iff for any PPTM $\mathcal{A}$ with oracle access to the keyed hash function, the following quantity:

$$\mathbf{Pr}\left(\mathsf{k} : \mathcal{A}^{\mathcal{O}_{\mathsf{H}(\cdot,\mathsf{k})}}(1^\eta) = \langle m_1\,,\, m_2 \rangle, m_1 \neq m_2 \text{ and } \mathsf{H}(m_1, \mathsf{k}) = \mathsf{H}(m_2, \mathsf{k})\right)$$

is negligible, where k is drawn uniformly at random in $\{0, 1\}^\eta$.

We translate this game in the logic as follows:

Definition 11. We let CR be the set of axioms:

$$\frac{}{\mathsf{H}(m_1, \mathsf{k}) \doteq \mathsf{H}(m_2, \mathsf{k}) \ \rightarrow\ m_1 \doteq m_2}\ \text{CR} \qquad \text{when } \mathsf{k} \sqsubseteq_{\mathsf{H}(\_,\cdot)} m_1, m_2$$

where $u \doteq v$ denotes the term $\mathsf{eq}(u, v)$, using an infix notation. Note that a different axiom for collision-resistence already appear in the literature, in [19]. We believe the axioms we presented above are simpler, and easier to use.

Remark 3. We need the implication here, we cannot simply state that, when the terms m_1 and m_2 are distinct, we have:

$$(\mathsf{H}(m_1, \mathsf{k}) \doteq \mathsf{H}(m_2, \mathsf{k})) = \mathsf{false} \tag{4}$$

For instance, take $m_1 = g(u)$ and $m_2 = g(u')$ where u, u' are distinct and g is an attacker's function symbol. Then, even though m_1 and m_2 are syntactically distinct, the function symbol g can be interpreted, e.g., as a function that discards its argument and always return the same value. In such a case, the interpretations of m_1 and m_2 are identical, and the formula in (4) is not valid. ◇

PROPOSITION 4. *The* CR *axioms are valid in any computational model where the function symbol H is interpreted as a* CR-HK *keyed hash function.*

PROOF. The proof is given in Section B.3. ■

8.4 EUF-MAC Axioms

A Mac schema is a pair $(\mathsf{Mac}\_(\_), \mathsf{Verify}(\_,\_,\_))$ where Mac creates symmetric signatures of messages, and Verify checks that some message has a valid signature. For every η, they must satisfy the following soundness relation:

$$\forall k \in \{0,1\}^{\eta}, \forall m \in \{0,1\}^{*}.\ \mathsf{Verify}(m, \mathsf{Mac}_{\mathsf{k}}(m), \mathsf{k}) = \mathsf{true}$$

Moreover, $\mathsf{Mac}_{\mathsf{k}}(\cdot)$ must be computationally unforgeable, even when letting the adversary have access to a Mac oracle $\mathcal{O}_{\mathsf{Mac}_{\mathsf{k}}(\cdot)}$. To successively forge a Mac, the adversary must find a pair (m, σ) such that $\mathsf{Verify}(m, \sigma, \mathsf{k})$ and m was never queried to the oracle $\mathcal{O}_{\mathsf{Mac}_{\mathsf{k}}(\cdot)}$. Formally:

Definition 12. A Mac schema (Mac, Verify) is *unforgeable against chosen-message attacks* (EUF-CMA) iff for every PPTM $\mathcal{A}$, the following quantity:

$$\mathbf{Pr}\Big(\mathsf{k} : \mathcal{A}^{\mathcal{O}_{\mathsf{Mac}_{\mathsf{k}}(\cdot)}}(1^{\eta}) = \langle m\,,\ \sigma\rangle\,, m \text{ not queried to } \mathcal{O}_{\mathsf{Mac}_{\mathsf{k}}(\cdot)} \text{ and } \mathsf{Verify}(m, \sigma, \mathsf{k})\Big)$$

is negligible, where k is drawn uniformly at random in $\{0,1\}^{\eta}$.

We explain how we translate this cryptographic assumption in the logic. Given two terms m, s where m is a message and s is a (candidate) forgery of a Mac of m, if s is a valid forgery (i.e. $\mathsf{Verify}(m, s, \mathsf{k})$ holds) then s must be a honestly generated Mac. Moreover, the set of honest Macs is simply the set of all subterms of m and s which are of the form $\mathsf{Mac}_{\mathsf{k}}(\_)$. This motivates the following definition:

Definition 13. We let $\text{set-mac}_{\mathsf{k}}(u)$ be the set of Maced terms, using key k, in u:

$$\text{set-mac}_{\mathsf{k}}(u) = \Big\{m \mid \mathsf{Mac}_{\mathsf{k}}(m) \in \mathsf{st}(u)\Big\}$$

We can now give the EUF-MAC axioms:

Definition 14. We let EUF-MAC be the set of axioms:

$$\frac{}{\mathsf{Verify}(m, s, \mathsf{k}) \ \rightarrow\ \bigvee_{u \in S} s \doteq \mathsf{Mac}_{\mathsf{k}}(u)}\ \text{EUF-MAC} \qquad \text{when} \begin{cases} \mathsf{k} \sqsubseteq_{\mathsf{Mac}.(\_)} s, m \\ S = \text{set-mac}_{\mathsf{k}}(s, m) \end{cases}$$

PROPOSITION 5. *The* EUF-MAC *axioms are valid in any computational model where (Mac, Verify) is interpreted as an* EUF-CMA *secure function.*

PROOF. The proof is given in Section B.4. ■

9 SECURITY OF THE AKA$^+$ PROTOCOL

We now state the authentication and σ_{ul}-unlinkability lemmas, and sketch the proofs. The full proofs are given later, in Sections D, E and F.

9.1 Mutual Authentication of the AKA$^+$ Protocol

Authentication is modeled by a correspondence property [41] of the form “in any execution, if event A occurs, then event B occurred”. This can be translated in the BC indistinguishability logic.

Authentication of the User by the Network. AKA$^+$ guarantees authentication of the user by the network if in any execution, if $HN(j)$ believes it authenticated UE_{ID}, then UE_{ID} stated earlier that it had initiated the protocol with $HN(j)$.

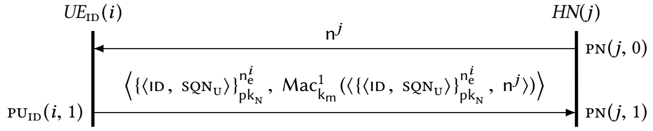
We recall that $\text{e-auth}_{\text{N}}^{j}$ stores the identity of the UE authenticated by $HN(j)$, and that UE_{ID} stores in $\text{b-auth}_{\text{U}}^{\text{ID}}$ the random challenge it received. Moreover, the session $HN(j)$ is uniquely identified by its random challenge n^j. Therefore, authentication of the user by the network is modeled by stating that, for any valid action trace τ, if $\sigma_\tau(\text{e-auth}_{\text{N}}^{j}) \doteq \text{ID}$ then there exists some prefix τ' of τ such that $\sigma_{\tau'}(\text{b-auth}_{\text{U}}^{\text{ID}}) \doteq \mathsf{n}^j$. Let $\preceq$ be the prefix ordering on action traces, then:

Lemma 1. *For every valid trace τ on $\mathcal{S}_{id}$, $\text{ID} \in \mathcal{S}_{id}$ and $j \in \mathbb{N}$, we have:*

$$\sigma_\tau(\textit{e-auth}_{N}^{j}) \doteq \textit{ID} \;\rightarrow\; \bigvee\nolimits_{\tau' \preceq \tau} \; \sigma_{\tau'}(\textit{b-auth}_{U}^{ID}) \doteq n^j$$

The key ingredients to show this lemma are *necessary conditions* for a message to be accepted by the network. Basically, a message can be accepted only if it was honestly generated by a subscriber. These necessary conditions rely on the unforgeability and collision-resistance of $(\mathsf{Mac}^j)_{1 \le j \le 5}$.

Necessary Acceptance Conditions. Using the EUF-MAC^j and CR^j axioms, we can find necessary conditions for a message to be accepted. We illustrate this on the HN's second message in the SUPI sub-protocol. We depict the beginning of the execution between session $UE_{\text{ID}}(i)$ and session $HN(j)$:


$UE_{\text{ID}}(i)$
$HN(j)$
n^j
$\text{PN}(j, 0)$
$\left\langle \{\langle \text{ID}, \text{SQN}_{\text{U}} \rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{i}}, \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}}^{1}(\langle \{\langle \text{ID}, \text{SQN}_{\text{U}} \rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{i}}, \mathsf{n}^j \rangle) \right\rangle$
$\text{PU}_{\text{ID}}(i, 1)$
$\text{PN}(j, 1)$

We then prove that if a message is accepted by $HN(j)$ as coming from UE_{ID}, then the first component of this message must have been honestly generated by a session of UE_{ID}. Moreover, we know that this session received the challenge n^j.

Lemma 2. *Let $\text{ID} \in \mathcal{S}_{id}$ and τ be a valid trace on $\mathcal{S}_{id}$ ending with $\text{PN}(j, 1)$. Then:*

$$\text{accept}_{\tau}^{ID} \rightarrow \bigvee_{\tau_1 = \_, PU_{ID}(\_, 1) \preceq \tau} \Big(\pi_1(g(\phi_\tau^{in})) \doteq t_{\tau_1}^{enc} \wedge g(\phi_{\tau_1}^{in}) \doteq n^j \Big)$$

Proof sktech. Let t_{dec} be the term $\text{dec}(\pi_1(g(\phi_\tau^{\text{in}})), \mathsf{sk}_{\text{N}})$. Then $HN(j)$ accepts the last message iff the following test succeeds:

$$\underline{\pi_2(g(\phi_\tau^{\text{in}})) \doteq \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^{1}(\langle \pi_1(g(\phi_\tau^{\text{in}})), \mathsf{n}^j \rangle)} \wedge \pi_1(t_{\text{dec}}) \doteq \text{ID}$$

By applying EUF-MAC to the underlined part above[5], we know that if the test holds then $\pi_2(g(\phi_\tau^{\text{in}}))$ is equal to one of the honest $\mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^{1}$ subterms of $\pi_2(g(\phi_\tau^{\text{in}}))$, which are the terms:

[5] Remark that in the AKA$^+$ protocol, $\mathsf{Verify}(m, s, \mathsf{k}_{\mathsf{m}}^{\text{ID}}) \equiv s \doteq \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^{1}(m)$

$$\left(\mathsf{Mac}^1_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle t^{\mathsf{enc}}_{\tau_1}\,,\, g(\phi^{\mathsf{in}}_{\tau_1})\rangle)\right)_{\tau_1 = \_, \textsc{pu}_{\textsc{id}}(\_,1) \prec \tau} \quad (5) \qquad \left(\mathsf{Mac}^1_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \pi_1(g(\phi^{\mathsf{in}}_{\tau_1}))\,,\, \mathsf{n}^{j_1}\rangle)\right)_{\tau_1 = \_, \textsc{pn}(j_1,1) \prec \tau} \quad (6)$$

Where $\prec$ is the strict version of $\preceq$. We know that $\textsc{pn}(j, 1)$ cannot appear twice in τ. Hence for every $\tau_1 = \_, \textsc{pn}(j_1, 1) \prec \tau$, we know that $j_1 \neq j$. Since distinct nonces are never equal, except for a negligible number of samplings, we derive that $\mathsf{eq}(\mathsf{n}^{j_1}, \mathsf{n}^j) \doteq \mathsf{false}$. Using an axiom stating that the pair is injective and the $\textsc{cr}^1$ axiom, we can show that $\pi_2(g(\phi^{\mathsf{in}}_\tau))$ cannot by equal to one of the terms in (6). Finally, for every $\tau_1 = \_, \textsc{pu}_{\textsc{id}}(\_, 1) \prec \tau$, using $\textsc{cr}^1$ and the pair injectivity, we derive that:

$$\left(\mathsf{Mac}^1_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \pi_1(g(\phi^{\mathsf{in}}_{\tau}))\,,\, \mathsf{n}^{j}\rangle) \doteq \mathsf{Mac}^1_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle t^{\mathsf{enc}}_{\tau_1}\,,\, g(\phi^{\mathsf{in}}_{\tau_1})\rangle)\right) \rightarrow \pi_1(g(\phi^{\mathsf{in}}_{\tau})) \doteq t^{\mathsf{enc}}_{\tau_1} \wedge \mathsf{n}^j \doteq g(\phi^{\mathsf{in}}_{\tau_1}) \qquad \blacksquare$$

We prove a similar lemma for $\textsc{tn}(j, 1)$. Lemma 1's proof is straightforward using these two properties.

Authentication of the Network by the User. The AKA$^+$ protocol also provides authentication of the network by the user. That is, in any execution, if $UE_{\textsc{id}}$ believes it authenticated session $HN(j)$ then $HN(j)$ stated that it had initiated the protocol with $UE_{\textsc{id}}$. Formally:

Lemma 3. *For every valid trace τ on $\mathcal{S}_{id}$, $\textsc{id} \in \mathcal{S}_{id}$ and $j \in \mathbb{N}$, we have:*

$$\sigma_\tau(\textit{e-auth}^{\textsc{id}}_U) \doteq n^j \;\rightarrow\; \bigvee_{\tau' \preceq \tau} \sigma_{\tau'}(\textit{b-auth}^j_N) \doteq \textsc{id}$$

This is shown using the same techniques than for Lemma 1.

9.2 σ-Unlinkability of the AKA$^+$ Protocol

Lemma 2 gives a necessary condition for a message to be accepted by $\textsc{pn}(j, 1)$ as coming from $\textsc{id}$. We can actually go further, and show that a message is accepted by $\textsc{pn}(j, 1)$ as coming from $\textsc{id}$ *if and only if* it was honestly generated by a session of $UE_{\textsc{id}}$ which received the challenge n^j.

Lemma 4. *Let $\textsc{id} \in \mathcal{S}_{id}$ and τ be a valid trace ending with $\textsc{pn}(j, 1)$. There exists a derivation of:*

$$\mathsf{accept}^{\textsc{id}}_\tau \leftrightarrow \bigvee_{\tau_1 = \_, \textsc{pu}_{\textsc{id}}(\_,1) \preceq \tau} \left(g(\phi^{in}_\tau) \doteq t_{\tau_1} \wedge g(\phi^{in}_{\tau_1}) \doteq n^j \right)$$

We prove similar lemmas for most actions of the AKA$^+$ protocol. Basically, these lemmas state that a message is accepted if and only if it is part of an honest execution of the protocol between $UE_{\textsc{id}}$ and HN. This allow us to replace each acceptance conditional $\mathsf{accept}^{\textsc{id}}_\tau$ by a disjunction over all possible honest partial transcripts of the protocol.

We now state the σ_{ul}-unlinkability lemma:

Lemma 5. *AKA^+_N is σ_{ul}-unlinkable in any computational model satisfying the axioms Ax.*

Proof sktech. Using Proposition 3, we only need to show that for every valid basic action trace τ, there exists a derivation of $\phi_\tau \sim \phi_{\underline{\tau}}$ (where the left frame is a frame of the AKA^+_N protocol, and the right frame of the $\text{AKA}^+_{\underline{N}}$ protocol for $\underline{N}$ large enough). The full proof is long and technical, and is by induction on τ. Take a valid action trace τ, we assume by induction that there is a derivation of $\phi^{\mathsf{in}}_\tau \sim \phi^{\mathsf{in}}_{\underline{\tau}}$. We want to build a derivation of $\phi^{\mathsf{in}}_\tau, t_{\underline{\tau}} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, t_{\underline{\tau}}$ using the inference rules in Ax.

First, we rewrite t_τ using acceptance characterization lemmas, such as Lemma 4. This replaces each $\mathsf{accept}^{\textsc{id}}_\tau$ by a case disjunction over all honest executions *on the left side*. Similarly, we rewrite $t_{\underline{\tau}}$ as a case disjunction over honest executions *on the right side*. Our goal is then to find a matching between left and right transcripts such that matched transcripts are indistinguishable. If a left and right transcript correspond to the same trace of oracle calls, this is easy. But since the left and right traces of oracle calls may differ, this is not always possible. E.g., some left transcript may not have a corresponding right transcript. When this happens, we have two possibilities: instead of a one-to-one match we build a many-to-one match, e.g. matching a left transcript to several right transcripts; or we show that some transcripts always result in a failure of the protocol. Showing the latter is complicated, as it requires to precisely track the possible values of $\text{SQN}_{\text{U}}^{\text{ID}}$ and $\text{SQN}_{\text{N}}^{\text{ID}}$ across multiple sessions of the protocol to prove that some transcripts always yield a de-synchronization between UE_{ID} and HN. ■

10 CONCLUSION

We studied the privacy provided by the 5G-AKA authentication protocol. While this protocol is not vulnerable to IMSI catchers, we showed that several privacy attacks from the literature apply to it. We also discovered a novel desynchronization attack against PRIV-AKA, a modified version of AKA, even though it had been claimed secure.

We then proposed the AKA$^+$ protocol. This is a fixed version of 5G-AKA, which is both efficient and has improved privacy guarantees. To study AKA$^+$'s privacy, we defined the σ-unlinkability property. This is a new parametric privacy property, which requires the prover to establish privacy only for a subset of the standard unlinkability game scenarios. Finally, we formally proved that AKA$^+$ provides mutual authentication and σ_{ul}-unlinkability for any number of agents and sessions. Our proof is carried out in the Bana-Comon model, which is well-suited to the formal analysis of stateful protocols.

REFERENCES

[1] M. Abadi, B. Blanchet, and C. Fournet. The applied pi calculus: Mobile values, new names, and secure communication. *J. ACM*, 65(1):1:1–1:41, 2018.

[2] M. Abdalla, P. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. In *Public Key Cryptography*, volume 3386 of *Lecture Notes in Computer Science*, pages 65–84. Springer, 2005.

[3] M. Arapinis, T. Chothia, E. Ritter, and M. Ryan. Analysing unlinkability and anonymity using the applied pi calculus. In *Proceedings of the 23rd IEEE Computer Security Foundations Symposium, CSF 2010*, pages 107–121. IEEE Computer Society, 2010.

[4] M. Arapinis, L. I. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar. New privacy issues in mobile telephony: fix and verification. In *the ACM Conference on Computer and Communications Security, CCS'12*, pages 205–216. ACM, 2012.

[5] M. Backes and B. Pfitzmann. Limits of the cryptographic realization of dolev-yao-style XOR. In *ESORICS*, volume 3679 of *Lecture Notes in Computer Science*, pages 178–196. Springer, 2005.

[6] G. Bana and R. Chadha. Verification methods for the computationally complete symbolic attacker based on indistinguishability. *IACR Cryptology ePrint Archive*, 2016:69, 2016.

[7] G. Bana, R. Chadha, and A. K. Eeralla. Formal analysis of vote privacy using computationally complete symbolic attacker. In *ESORICS (2)*, volume 11099 of *LNCS*, pages 350–372. Springer, 2018.

[8] G. Bana and H. Comon-Lundh. Towards unconditional soundness: Computationally complete symbolic attacker. In *Principles of Security and Trust, 2012*, volume 7215 of *LNCS*, pages 189–208. Springer, 2012.

[9] G. Bana and H. Comon-Lundh. A computationally complete symbolic attacker for equivalence properties. In *2014 ACM Conference on Computer and Communications Security, CCS '14*, pages 609–620. ACM, 2014.

[10] D. A. Basin, J. Dreier, L. Hirschi, S. Radomirovi'c, R. Sasse, and V. Stettler. A formal analysis of 5G authentication. In *the ACM Conference on Computer and Communications Security, CCS'18*. ACM, 2018.

[11] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *CRYPTO*, volume 1462 of *LNCS*, pages 26–45. Springer, 1998.

[12] K. Bhargavan, C. Fournet, and M. Kohlweiss. mitls: Verifying protocol implementations against real-world attacks. *IEEE Security & Privacy*, 14(6):18–25, 2016.

[13] B. Blanchet. *ProVerif: Cryptographic protocols verifier in the formal model.* available at http://proseccco.gforge..inria.fr/personal/bblanchet/proverif/.

[14] B. Blanchet. A computationally sound mechanized prover for security protocols. *IEEE Trans. Dependable Sec. Comput.*, 5(4):193–207, 2008.

[15] R. Borgaonkar, L. Hirshi, S. Park, A. Shaik, A. Martin, and J.-P. Seifert. New adventures in spying 3G & 4G users: Locate, track, monitor, 2017. Briefing at BlackHat USA 2017.

[16] C. Chang and R. C. T. Lee. *Symbolic logic and mechanical theorem proving*. Computer science classics. Academic Press, 1973.

[17] D. Chaum. Blind signatures for untraceable payments. In *CRYPTO*, pages 199–203. Plenum Press, New York, 1982.

[18] V. Cheval, S. Kremer, and I. Rakotonirina. DEEPSEC: deciding equivalence properties in security protocols theory and practice. In *2018 IEEE Symposium on Security and Privacy, SP 2018*, pages 529–546. IEEE, 2018.

[19] H. Comon and A. Koutsos. Formal computational unlinkability proofs of RFID protocols. In *30th Computer Security Foundations Symposium, 2017*, pages 100–114. IEEE Computer Society, 2017.

[20] V. Cortier, N. Grimm, J. Lallemand, and M. Maffei. A type system for privacy properties. In *ACM Conference on Computer and Communications Security, CCS'17*, pages 409–423. ACM, 2017.

[21] C. Cremers, M. Horvat, J. Hoyland, S. Scott, and T. van der Merwe. A comprehensive symbolic analysis of TLS 1.3. In *ACM Conference on Computer and Communications Security, CCS'17*, pages 1773–1788. ACM, 2017.

[22] P. Fouque, C. Onete, and B. Richard. Achieving better privacy for the 3gpp AKA protocol. *PoPETs*, 2016(4):255–275, 2016.

[23] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In *AUSCRYPT*, volume 718 of *Lecture Notes in Computer Science*, pages 244–251. Springer, 1992.

[24] O. Goldreich. *The Foundations of Cryptography - Volume 1, Basic Techniques*. Cambridge University Press, 2001.

[25] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. *J. ACM*, 33(4):792–807, 1986.

[26] S. Goldwasser and M. Bellare. Lecture notes on cryptography, 2001.

[27] J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel. A new RFID privacy model. In *ESORICS*, volume 6879 of *Lecture Notes in Computer Science*, pages 568–587. Springer, 2011.

[28] L. Hirschi, D. Baelde, and S. Delaune. A method for verifying privacy-type properties: The unbounded case. In *IEEE Symposium on Security and Privacy, SP 2016*, pages 564–581. IEEE Computer Society, 2016.

[29] I. J. Kim, E. Y. Choi, and D. H. Lee. Secure mobile RFID system against privacy and security problems. In *Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2007. SECPerU 2007. Third International Workshop on*, pages 67–72, July 2007.

[30] N. Kobeissi, K. Bhargavan, and B. Blanchet. Automated verification for secure messaging protocols and their implementations: A symbolic and computational approach. In *2017 IEEE European Symposium on Security and Privacy, EuroS&P*, pages 435–450. IEEE, 2017.

[31] M. Lee, N. P. Smart, B. Warinschi, and G. J. Watson. Anonymity guarantees of the UMTS/LTE authentication and connection protocol. *Int. J. Inf. Sec.*, 13(6):513–527, 2014.

[32] S. Lee, T. Asano, and K. Kim. RFID mutual authentication scheme based on synchronized secret information. In *Symposium on cryptography and information security*, 2006.

[33] S. Meier, B. Schmidt, C. Cremers, and D. Basin. The tamarin prover for the symbolic analysis of security protocols. In *25th International Conference on Computer Aided Verification, CAV'13*, pages 696–701. Springer-Verlag, 2013.

[34] G. Scerri and R. Stanley-Oakes. Analysis of key wrapping apis: Generic policies, computational security. In *IEEE 29th Computer Security Foundations Symposium, CSF 2016, Lisbon, Portugal, June 27 - July 1, 2016*, pages 281–295. IEEE Computer Society, 2016.

[35] A. Shaik, J. Seifert, R. Borgaonkar, N. Asokan, and V. Niemi. Practical attacks against privacy and availability in 4g/lte mobile communication systems. In *23rd Annual Network and Distributed System Security Symposium, NDSS*. The Internet Society, 2016.

[36] V. Shoup. Sequences of games: a tool for taming complexity in security proofs. *IACR Cryptology ePrint Archive*, 2004:332, 2004. https://eprint.iacr.org/2004/332.

[37] D. Strobel. IMSI catcher. *Ruhr-Universität Bochum, Seminar Work*, 2007.

[38] TS 33.501: Security architecture and procedures for 5G system, September 2018.

[39] F. van den Broek, R. Verdult, and J. de Ruiter. Defeating IMSI catchers. In *ACM Conference on Computer and Communications Security, CCS'15*, pages 340–351. ACM, 2015.

[40] S. Vaudenay. On privacy models for RFID. In *ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security*, LNCS, pages 68–87. Springer, 2007.

[41] T. Y. C. Woo and S. S. Lam. A semantic model for authentication protocols. In *Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy*, pages 178–194, May 1993.

Contents

A ADDITIONAL AXIOMS

A.1 Structural Axioms

Equality Axioms. The equality axioms are given in Figure 15. Most of these axioms deal with the if_then_else_ function symbols: E_1 contains the functional properties of the equality test; E_2 contains the homomorphism and simplification rules of the if_then_else_; and E_3 allows to change the order in which conditional tests are performed.

Other Structural Axioms. The rest of the structural axioms can be found in Figure 16. These axioms are generic, and can be re-used to analyse a different protocol. We informally describe them:

- Perm allows to change the terms order, using the same permutation π on both sides of $\sim$.

$$\frac{u_{\pi(1)}, \dots, u_{\pi(n)} \sim v_{\pi(1)}, \dots, v_{\pi(n)}}{u_1, \dots, u_n \sim v_1, \dots, v_n}\ \textsf{Perm}$$

- Restr is a strengthening axiom, stating that to prove that $\vec{u} \sim \vec{v}$, it is sufficient to show the stronger property $\vec{u}, s \sim \vec{v}, t$.

$$\frac{\vec{u}, s \sim \vec{v}, t}{\vec{u} \sim \vec{v}}\ \textsf{Restr}$$

$$\mathsf{E}_1 \;:\quad \mathsf{eq}(x,x) = \mathsf{true}$$

$$\mathsf{E}_2 \;:\; \begin{cases} f(\vec{u}, \text{if } b \text{ then } x \text{ else } y, \vec{v}) = \text{if } b \text{ then } f(\vec{u}, x, \vec{v}) \text{ else } f(\vec{u}, y, \vec{v}) \\ \text{if } b \text{ then } x \text{ else } x = x \\ \text{if true then } x \text{ else } y = x \\ \text{if false then } x \text{ else } y = y \\ \text{if } b \text{ then (if } b \text{ then } x \text{ else } y) \text{ else } z = \text{if } b \text{ then } x \text{ else } z \\ \text{if } b \text{ then } x \text{ else (if } b \text{ then } y \text{ else } z) = \text{if } b \text{ then } x \text{ else } z \end{cases}$$

$$\mathsf{E}_3 \;:\; \begin{cases} \text{if } b \text{ then (if } a \text{ then } x \text{ else } y) \text{ else } z = \text{if } a \text{ then (if } b \text{ then } x \text{ else } z) \text{ else (if } b \text{ then } y \text{ else } z) \\ \text{if } b \text{ then } x \text{ else (if } a \text{ then } y \text{ else } z) = \text{if } a \text{ then (if } b \text{ then } x \text{ else } y) \text{ else (if } b \text{ then } x \text{ else } z) \end{cases}$$

Fig. 15. Equality Axioms $\mathsf{E}_1, \mathsf{E}_2, \mathsf{E}_3$.

$$\frac{}{u = u}\ \text{=-refl} \qquad \frac{v = u}{u = v}\ \text{=-sym} \qquad \frac{u = w \qquad w = v}{u = v}\ \text{=-trans} \qquad \frac{u_0 = v_0 \qquad \dots \qquad u_n = v_n}{f(u_0, \dots, u_n) = f(v_0, \dots, v_n)}\ \text{=-subst}$$

$$\frac{\vec{u}, t \sim \vec{v} \qquad s = t}{\vec{u}, s \sim \vec{v}}\ \mathsf{Equ} \qquad \frac{u_{\pi(1)}, \dots, u_{\pi(n)} \sim v_{\pi(1)}, \dots, v_{\pi(n)}}{u_1, \dots, u_n \sim v_1, \dots, v_n}\ \mathsf{Perm} \qquad \frac{\vec{u}, s \sim \vec{v}, t}{\vec{u} \sim \vec{v}}\ \mathsf{Restr}$$

$$\frac{\vec{u}_1, \vec{v}_1 \sim \vec{u}_1, \vec{v}_2}{f(\vec{u}_1), \vec{v}_1 \sim f(\vec{u}_2), \vec{v}_2}\ \mathsf{FA} \qquad \frac{\vec{u}, s \sim \vec{v}, t}{\vec{u}, s, s \sim \vec{v}, t, t}\ \mathsf{Dup} \qquad \frac{}{\vec{u} \sim \vec{u}}\ \mathsf{Refl} \qquad \frac{\vec{v} \sim \vec{u}}{\vec{u} \sim \vec{v}}\ \mathsf{Sym}$$

$$\frac{\vec{u} \sim \vec{w} \qquad \vec{w} \sim \vec{v}}{\vec{u} \sim \vec{v}}\ \mathsf{Trans} \qquad \frac{\vec{u} \sim \vec{v}}{\vec{u}, \mathsf{n} \sim \vec{v}, \mathsf{n}'}\ \mathsf{Fresh} \quad \text{when } \mathsf{n} \notin \mathsf{st}(\vec{u}) \text{ and } \mathsf{n}' \notin \mathsf{st}(\vec{v})$$

$$\frac{}{\mathsf{eq}(t, \mathsf{n}) = \mathsf{false}}\ \text{=-ind} \quad \text{when } \mathsf{n} \notin \mathsf{st}(t) \qquad \frac{\vec{u}, \mathsf{n} \sim \vec{v} \qquad \mathsf{len}(t) = \mathsf{len}(\mathsf{n})}{\vec{u}, t \oplus \mathsf{n} \sim \vec{v}}\ \oplus\text{-ind} \quad \text{when } \mathsf{n} \notin \mathsf{st}(\vec{u}, \vec{v}, t)$$

$$\frac{\vec{u}, C\,[\text{if } \mathsf{eq}(s,t) \text{ then } C_0[t] \text{ else } w] \sim \vec{v}}{\vec{u}, C\,[\text{if } \mathsf{eq}(s,t) \text{ then } C_0[s] \text{ else } w] \sim \vec{v}}\ \mathsf{IFT} \qquad \frac{\vec{w}, b, (u_i)_i \sim \vec{w}', b', (u'_i)_i \qquad \vec{w}, b, (v_i)_i \sim \vec{w}', b', (v'_i)_i}{\vec{w}, (\text{if } b \text{ then } u_i \text{ else } v_i)_i \sim \vec{w}', (\text{if } b' \text{ then } u'_i \text{ else } v'_i)_i}\ \mathsf{CS}$$

Conventions: π is a permutation of $\{1, \dots, n\}$ and $f \in \mathcal{F}$.

Fig. 16. Some Structural Axioms.

- The function application axiom FA states that to prove that two images (by $f \in \mathcal{F}$) are indistinguishable, it is sufficient to show that the arguments are indistinguishable.

$$\frac{\vec{u}_1, \vec{v}_1 \sim \vec{u}_1, \vec{v}_2}{f(\vec{u}_1), \vec{v}_1 \sim f(\vec{u}_2), \vec{v}_2}\ \mathsf{FA}$$

- Dup states that giving twice the same value to an adversary is equivalent to giving it only once.

$$\frac{\vec{u}, s \sim \vec{v}, t}{\vec{u}, s, s \sim \vec{v}, t, t}\ \mathsf{Dup}$$

- Fresh states that giving a value uniformly sampled at random and independent from the rest of the distribution is useless. We guarantee that n is independent from $\vec{u}$ by requiring that n

does not appear in $\vec{u}$'s subterms (and similarly for n' and $\vec{v}$). By consequence, this is not a universally quantified axiom. Instead, this is a recursive infinite set of axioms, one for each *ground* formula satisfying the side-condition.

$$\frac{\vec{u} \sim \vec{v}}{\vec{u}, \mathsf{n} \sim \vec{v}, \mathsf{n}'}\ \mathsf{Fresh} \quad \text{when } \mathsf{n} \notin \mathsf{st}(\vec{u}) \text{ and } \mathsf{n}' \notin \mathsf{st}(\vec{v})$$

- =-ind is a axiom schema stating that, if t is independent from a uniform random sampling n, then t is never equal to n, except for a negligible number of samplings.

$$\frac{}{\mathsf{eq}(t, \mathsf{n}) = \mathsf{false}}\ =\text{-}\mathsf{ind} \quad \text{when } \mathsf{n} \notin \mathsf{st}(t)$$

- The $\oplus$-ind axioms states that the xor of a term t and an uniform random value n is indistinguishable from an uniform random value, as long as t and n are independent and of the same length. The fact that t and n are independent is checked by requiring that n does not appear in t in the syntactic side-condition $\mathsf{n} \notin \mathsf{st}(\vec{u}, \vec{v}, t)$ (therefore this is an infinite schema of ground axioms).

$$\frac{\vec{u}, \mathsf{n} \sim \vec{v} \qquad \mathsf{len}(t) = \mathsf{len}(\mathsf{n})}{\vec{u}, t \oplus \mathsf{n} \sim \vec{v}}\ \oplus\text{-}\mathsf{ind} \quad \text{when } \mathsf{n} \notin \mathsf{st}(\vec{u}, \vec{v}, t)$$

- The IFT axioms allows to replace a term s by a term t if it appears in the then branch of a $\mathsf{eq}(s, t)$ conditional. Again, this is an axiom schema.

$$\frac{\vec{u}, C\,[\mathsf{if}\ \mathsf{eq}(s, t)\ \mathsf{then}\ C_0[t]\ \mathsf{else}\ w] \sim \vec{v}}{\vec{u}, C\,[\mathsf{if}\ \mathsf{eq}(s, t)\ \mathsf{then}\ C_0[s]\ \mathsf{else}\ w] \sim \vec{v}}\ \mathsf{IFT}$$

- The CS axioms states that in order to show that:

$$\mathsf{if}\ b\ \mathsf{then}\ u\ \mathsf{else}\ v \sim \mathsf{if}\ b'\ \mathsf{then}\ u'\ \mathsf{else}\ v'$$

  it is sufficient to show that the then branches and the else branches are indistinguishable, *when giving to the adversary the value of the conditional* (i.e. b on the left and b' on the right). We can do better, by considering simultaneously several terms starting with the same conditional. We also allow some terms $\vec{w}$ and $\vec{w}\,'$ on the left and right to stay untouched.

$$\frac{\vec{w}, b, (u_i)_i \sim \vec{w}\,', b', (u_i')_i \qquad \vec{w}, b, (v_i)_i \sim \vec{w}\,', b', (v_i')_i}{\vec{w}, (\mathsf{if}\ b\ \mathsf{then}\ u_i\ \mathsf{else}\ v_i)_i \sim \vec{w}\,', (\mathsf{if}\ b'\ \mathsf{then}\ u_i'\ \mathsf{else}\ v_i')_i}\ \mathsf{CS}$$

Remark 4. In the CS axioms, we need to give the conditional b to the adversary. For example, assume that that $\mathcal{F}_\mathsf{p}$ contains two constant function symbols one and zero. Then, in every computational model $\mathcal{M}_\mathsf{c}$:

$$\mathcal{M}_\mathsf{c} \models \mathsf{zero} \sim \mathsf{zero} \qquad\qquad \mathcal{M}_\mathsf{c} \models \mathsf{one} \sim \mathsf{one}$$

But if $\mathcal{M}_\mathsf{c}$ is such that zero's interpretation is different from one's interpretation, then:

$$\mathcal{M}_\mathsf{c} \not\models \mathsf{if}\ \mathsf{true}\ \mathsf{then}\ \mathsf{zero}\ \mathsf{else}\ \mathsf{one} \sim \mathsf{if}\ \mathsf{false}\ \mathsf{then}\ \mathsf{zero}\ \mathsf{else}\ \mathsf{one} \qquad \diamond$$

The conjunction of the equality axioms in Figure 15 and the axioms in Figure 16 form the set of structural axioms $\mathsf{Ax}_\mathsf{struct}$.

Definition 15. We let $\mathsf{Ax}_\mathsf{struct}$ be the union of sets of axioms in Figure 15 and Figure 16.

Structural axioms are valid in all computational models.

Proposition 6. *The axioms $\mathsf{Ax}_{\mathsf{struct}}$ are valid in all computational models.*

Proof. The proof is straightforward, and can be found in the literature [6, 9, 19]. ■

A.2 Implementation Axioms

Implementation axioms are axioms that are not valid in any computational model. When studying the security of a protocol, implementation axioms are what allow the prover to put *requirements* on the protocol concrete implementations. For example, we can require that the first projection of a pair is equal to the first element of the pair, or that distinct constant function symbols representing agents names are never equal. Then, if we can show that the conjunction of the structural axioms, the implementation axioms and the negation of the security property hold, we know that the protocol is secure in any computational model where the implementation axioms hold.

We now define the set of implementation axioms $\mathsf{Ax}_{\mathsf{impl}}$ we use to prove that the AKA$^+$ protocol provides mutual authentication and σ_{ul}-unlinkability. Some of these axioms are general, and can be re-used (e.g. boolean axioms), while other axioms are specific to the AKA$^+$ protocol (e.g. sequence number axioms).

Booleans. We use the following functions symbols to represent boolean operations:

$$\mathsf{and}, \mathsf{or}, \mathsf{imply}, \mathsf{equiv} \;:\; \mathsf{bool}^2 \to \mathsf{bool} \qquad\qquad \mathsf{neg} \;:\; \mathsf{bool} \to \mathsf{bool}$$

We also add an axiom to link the if_then_else_ function symbol with the boolean function symbols whenever the then and else branches are of sort bool:

$$\mathsf{if}\ a\ \mathsf{then}\ b\ \mathsf{else}\ c = \mathsf{or}\left(\mathsf{and}(a, b), \mathsf{and}(\mathsf{neg}(a), c)\right) \tag{7}$$

where a, b and c are variables of sort bool. Instead of adding multiple axioms allowing to reason on terms with boolean function symbols, we use a single axiom schema stating that if two terms, seen as formulas in first-order logic with equality, are equivalent, then they are equal:

$$\frac{t_\phi \text{ and } t_\psi \text{ are encoding of } \phi \text{ and } \psi \qquad \phi \Leftrightarrow \psi \text{ valid in } \textsc{fo}(=)}{t_\phi = t_\psi} \tag{8}$$

Again, this is a recursive schema of ground axioms: t_ϕ and t_ψ are ground terms.

Example 7. For example, we can obtain De Morgan's laws:

$$\mathsf{neg}(\mathsf{and}(a, b)) = \mathsf{or}(\mathsf{neg}(a), \mathsf{neg}(b)) \qquad\qquad \mathsf{neg}(\mathsf{or}(a, b)) = \mathsf{and}(\mathsf{neg}(a), \mathsf{neg}(b))$$

If we consider first-order logic with equality and injectivity of the pair function symbols, we obtain:

$$\mathsf{imply}\left(\mathsf{neg}(\mathsf{eq}(\langle u\,,\ v\rangle\,, \langle s\,,\ t\rangle)), \mathsf{or}(\mathsf{neg}(\mathsf{eq}(u, s)), \mathsf{neg}(\mathsf{eq}(v, t)))\right) = \mathsf{true} \qquad \diamond$$

This allow to push part of the reasoning outside the Bana-Comon logic, into some standard logic, without having to fix the way we reason in the outer logic: the proof that ϕ and ψ are equivalent takes place in the meta-logic. In practice, we use a logic with more axioms than $\textsc{fo}(=)$. For example, in the study of the AKA protocol, we will need to do reasoning about conjunctions of inequalities between integer sequence numbers, for which we need, e.g., properties of orderings. We define the set of axioms $\mathsf{Ax}_{\mathsf{bool}}$:

Definition 16. $\mathsf{Ax}_{\mathsf{bool}}$ is the conjunction of the axioms in (7) and (8).

Notations. The prefix notation for boolean terms is cumbersome to use. Therefore, we introduce infix notations for and, or, imply, equiv, neg, eq:

$$\dot\wedge,\ \dot\vee,\ \dot\rightarrow,\ \dot\leftrightarrow,\ \dot\neg,\ \doteq$$

We use the usual precedence, e.g. $a \mathrel{\dot\vee} b \mathrel{\dot\wedge} c$ is $a \mathrel{\dot\vee} (b \mathrel{\dot\wedge} c)$. For every boolean term b, when there is no confusion, we write b instead of $b \sim \mathsf{true}$.

While it may seems that we need to be careful not to confuse $\doteq$ and $=$, this is actually not the case. Indeed, the formula $a \doteq b$ is, by definition, the formula $\mathsf{eq}(a, b) \sim \mathsf{true}$, which is also the formula $a = b$. Moreover, the following two rules are admissible using the axioms in Figure 15 and 16:

$$\frac{a \doteq b}{(a \doteq b) \doteq \mathsf{true}} \qquad\qquad \frac{(a \doteq b) \doteq \mathsf{true}}{a \doteq b}$$

We give the derivations below:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{a \doteq b}{a \doteq b \sim \mathsf{true}}}{(a \doteq b), \mathsf{true} \sim \mathsf{true}, \mathsf{true}}\;\mathsf{FA}}{(a \doteq b) \doteq \mathsf{true} \sim \mathsf{true} \doteq \mathsf{true}}\;\mathsf{FA} \qquad \dfrac{}{(\mathsf{true} \doteq \mathsf{true}) = \mathsf{true}}\;\text{=-refl}}{(a \doteq b) \doteq \mathsf{true} \sim \mathsf{true}}\;\mathsf{Equ}}{(a \doteq b) \doteq \mathsf{true}}$$

$$\dfrac{\dfrac{\dfrac{}{\mathsf{true} \sim \mathsf{true}}\;\mathsf{Refl} \qquad (a \doteq b) \doteq \mathsf{true}}{a \doteq b \sim \mathsf{true}}\;\mathsf{Equ}}{a \doteq b}$$

Constants. We define the set of constants $\mathcal{S}_{\mathsf{cst}}$, which contains the set of identities $\mathcal{S}_{\mathsf{id}}^{\omega}$, the integers 0 and 1, and the special values UnknownId, fail, defaut and error. This set does not include all the constants of the AKA^{+}, but only the ones whose interpretations must be distinct (this is enforced by an axiom below).

Definition 17. We define the set $\mathcal{S}_{\mathsf{cst}}$ of constant function symbols:

$$\mathcal{S}_{\mathsf{cst}} \;:=\; \mathcal{S}_{\mathsf{id}}^{\omega} \cup \{\mathsf{UnSet}, \mathsf{UnknownId}, \mathsf{fail}, \mathsf{defaut}, \mathsf{error}, 0, 1\}$$

Axioms. The set of implementation axioms is given in Figure 17. We quickly describe them:

- The set of axioms $\mathsf{Ax}_{\mathsf{fun}}$ contains the functional correctness properties of the protocol function symbols. For example, the following rules state that the i-th projection of a pair is the i-th element of the pair, and that the decryption with the correct key of a cipher-text is equal to the message in plain-text:

  $$\pi_i(\langle x_1\,,\,x_2\rangle) = x_i \text{ for } i \in \{1, 2\} \qquad\qquad \mathsf{dec}(\{x\}^{z}_{\mathsf{pk}(y)}, \mathsf{sk}(y)) = x$$

  The following axioms state that the $\oplus$ and 0 function symbols satisfies the the usual ACUN (associativity, commutativity, unit and nilpotence) properties of the bit-string xor:

  $$x \oplus (y \oplus z) = (x \oplus y) \oplus z \qquad x \oplus y = y \oplus x \qquad 0 \oplus x = x \qquad x \oplus x = 0$$

- The set $\mathsf{Ax}_{\mathsf{eq}}$ contains the dis-equality axioms require that all the elements of $\mathcal{S}_{\mathsf{cst}}$ must be interpreted by distinct bit-strings:

  $$\dfrac{}{\mathsf{eq}(\mathsf{A}, \mathsf{B}) = \mathsf{false}}\;\neq\text{-Const} \qquad \text{for every } \mathsf{A}, \mathsf{B} \in \mathcal{S}_{\mathsf{cst}} \text{ s.t. } \mathsf{A} \not\equiv \mathsf{B}$$

- $\mathsf{Ax}_{\mathsf{len}}$ is the set of implementation axioms on the length function len(_). In particular, all identities in $\mathcal{S}_{\mathsf{id}}^{\omega}$ must have the same lengths, and not be of length 0. Similarly, sequence numbers must have the same lengths. There are also some axioms to reason on lengths, e.g.:

  $$\frac{\mathsf{len}(u) = \mathsf{len}(s) \qquad \mathsf{len}(v) = \mathsf{len}(t)}{\mathsf{len}(\langle u\,,\,v\rangle) = \mathsf{len}(\langle s\,,\,t\rangle)} \qquad \frac{\mathsf{len}(u) \neq 0}{\mathsf{len}(\langle u\,,\,v\rangle) \neq 0} \qquad \frac{\mathsf{len}(v) \neq 0}{\mathsf{len}(\langle u\,,\,v\rangle) \neq 0}$$

- *The set Ax_{fun} of functional correctness axioms:*

$$\pi_i(\langle x_1, x_2\rangle) = x_i \text{ for } i \in \{1,2\} \qquad \pi_i(\langle x_1\,, x_2\,,\, x_3\rangle) = x_i \text{ for } i \in \{1,2,3\} \qquad \mathsf{dec}(\{x\}^z_{\mathsf{pk}(y)}, \mathsf{sk}(y)) = x$$

$$x \oplus (y \oplus z) = (x \oplus y) \oplus z \qquad x \oplus y = y \oplus x \qquad 0 \oplus x = x \qquad x \oplus x = 0$$

- *The set Ax_{eq} of dis-equality axioms:*

$$\frac{}{\mathsf{eq}(\mathsf{A},\mathsf{B}) = \mathsf{false}}\ \neq\text{-Const} \quad \begin{array}{l}\text{for every } \mathsf{A},\mathsf{B} \in \mathcal{S}_{\mathsf{cst}}\\ \text{s.t. } \mathsf{A} \not\equiv \mathsf{B}\end{array}$$

- *The set Ax_{len} of length axioms:*

$$\frac{\mathsf{len}(u) = \mathsf{len}(s) \qquad \mathsf{len}(v) = \mathsf{len}(t)}{\mathsf{len}(\langle u\,,\,v\rangle) = \mathsf{len}(\langle s\,,\,t\rangle)} \qquad \frac{}{\mathsf{len}(\textsc{id}_1) = \mathsf{len}(\textsc{id}_2)} \ \text{ for every } \textsc{id}_1, \textsc{id}_2 \in \mathcal{S}^{\omega}_{\mathsf{id}}$$

$$\frac{}{\mathsf{len}(\mathsf{suc}(\mathsf{sqn\text{-}init}^{\textsc{id}}_{\textsc{u}})) = \mathsf{len}(\mathsf{sqn\text{-}init}^{\textsc{id}}_{\textsc{u}})} \ \text{ for every } \textsc{id} \in \mathcal{S}^{\omega}_{\mathsf{id}}$$

$$\frac{}{\mathsf{len}(\mathsf{sqn\text{-}init}^{\textsc{id}_1}_{\textsc{u}}) = \mathsf{len}(\mathsf{sqn\text{-}init}^{\textsc{id}_2}_{\textsc{u}})} \ \text{ for every } \textsc{id}_1, \textsc{id}_2 \in \mathcal{S}^{\omega}_{\mathsf{id}}$$

$$\frac{}{\mathsf{len}(\mathsf{sqn\text{-}init}^{\textsc{id}}_{\textsc{u}}) = \mathsf{len}(\mathsf{n})} \ \text{ for every } \textsc{id} \in \mathcal{S}^{\omega}_{\mathsf{id}}, \mathsf{n} \in \mathcal{N} \qquad \frac{}{\mathsf{len}(0^x) = x} \qquad \frac{}{\mathsf{len}(1^x) = x}$$

$$\frac{}{\mathsf{len}(\mathsf{x}) \neq 0} \ \text{ when } \mathsf{x} \in \mathcal{S}_{\mathsf{cst}} \qquad \frac{\mathsf{len}(u) \neq 0}{\mathsf{len}(\langle u\,,\,v\rangle) \neq 0} \qquad \frac{\mathsf{len}(v) \neq 0}{\mathsf{len}(\langle u\,,\,v\rangle) \neq 0}$$

$$\frac{A \neq B \qquad \mathsf{len}(A) \neq 0 \qquad x \neq 0}{A^x \neq B^y}\ \mathsf{l\text{-}neq}$$

- *The set Ax_{inj} of injectivity axioms:*

$$\frac{}{\neg\mathsf{eq}(u,s) \wedge \mathsf{eq}(\langle u\,,\,v\rangle\,, \langle s\,,\,t\rangle) = \mathsf{false}}\ \mathsf{EQInj}(\langle\cdot\,,\,\_\rangle)$$

$$\frac{}{\neg\mathsf{eq}(v,t) \wedge \mathsf{eq}(\langle u\,,\,v\rangle\,, \langle s\,,\,t\rangle) = \mathsf{false}}\ \mathsf{EQInj}(\langle\_\,,\,\cdot\rangle)$$

$$\frac{}{\neg\mathsf{eq}(u,v) \wedge \mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{v\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}) = \mathsf{false}}\ \mathsf{EQInj}(\{\cdot\}^{\_}_{\_})$$

- *The set Ax_{SQN} of sequence number axioms:*

$$\frac{}{\mathsf{range}(u,v) = \mathsf{eq}(u,v)} \qquad \frac{}{\mathsf{suc}(u) = u + 1}$$

$$\frac{}{\mathsf{geq}(\mathsf{sqn\text{-}init}^{\textsc{id}}_{\textsc{u}}, \mathsf{sqn\text{-}init}^{\textsc{id}}_{\textsc{n}})}\ \textsc{sqn}\text{-ini} \quad \text{for every } \textsc{id} \in \mathcal{S}^{\omega}_{\mathsf{id}}$$

$$\frac{}{\phi[\vec{u}] = \mathsf{true}} \quad \begin{array}{l}\text{when } \vec{u} \text{ are ground terms}\\ \text{and } \mathrm{Th}(\mathbb{Z}, 0, 1, +, -, =, \leq) \models \phi[\vec{x}\,]\end{array}$$

Fig. 17. The Set of Axiom $\mathsf{Ax_{impl}} = \mathsf{Ax_{fun}} \cup \mathsf{Ax_{eq}} \cup \mathsf{Ax_{len}} \cup \mathsf{Ax_{inj}} \cup \mathsf{Ax_{SQN}}$.

- The set $\mathsf{Ax_{inj}}$ contains injectivity axioms for the pair and encryption. For example, for the pair, we have the left injectivity axioms:

$$\frac{}{\neg\mathsf{eq}(u,s) \wedge \mathsf{eq}(\langle u\,,\,v\rangle\,, \langle s\,,\,t\rangle) = \mathsf{false}}\ \mathsf{EQInj}(\langle\cdot\,,\,\_\rangle)$$

- The set $\mathsf{Ax}_{\textsc{sqn}}$ contains sequence numbers axioms. In particular, it requires that:
  - The range and successor functions are, resp., an equality check and a by-one increment:

$$\frac{}{\mathsf{range}(u,v) = \mathsf{eq}(u,v)} \qquad\qquad \frac{}{\mathsf{suc}(u) = u + 1}$$

  - Initially, the *HN* sequence number is no larger than the *UE* sequence number.

$$\frac{}{\mathsf{geq}(\mathsf{sqn\text{-}init}_{\mathrm{U}}^{\mathrm{ID}}, \mathsf{sqn\text{-}init}_{\mathrm{N}}^{\mathrm{ID}})}\ \textsc{sqn}\text{-ini} \qquad \text{for every } \textsc{id} \in \mathcal{S}_{\mathsf{id}}^{\omega}$$

  - For any term $\phi[]$ encoding of a boolean formula, if $\phi[\vec{u}]$ is valid in the first-order theory $\mathrm{Th}(\mathbb{Z}, 0, 1, +, -, =, \leq)$ then $\phi[\vec{u}] = \mathsf{true}$ is a valid axiom.

$$\frac{}{\phi[\vec{u}] = \mathsf{true}} \qquad \text{when } \vec{u} \text{ are ground termsand } \mathrm{Th}(\mathbb{Z}, 0, 1, +, -, =, \leq) \models \phi[\vec{x}\,]$$

We now define the set of axioms $\mathsf{Ax}_{\mathsf{impl}}$.

Definition 18. $\mathsf{Ax}_{\mathsf{impl}}$ is the union of the boolean axioms $\mathsf{Ax}_{\mathsf{bool}}$ and of axioms given in Figure 17.

B ADDITIONAL CRYPTOGRAPHIC AXIOMS

B.1 The CCA$_1$ Axioms

We informally recall the IND-CCA$_2$ game (for Indistinguishability against Chosen Ciphertexts Attacks, see [11]). First, the challenger computes a public/private key pair $(\mathsf{pk}(\mathsf{n}), \mathsf{sk}(\mathsf{n}))$ (using a nonce n of length η uniformly sampled), and sends $\mathsf{pk}(\mathsf{n})$ to the attacker. The adversary has access to two oracles:

- A left-right oracle $\mathcal{O}_{\mathsf{LR}}^{b}(\mathsf{n})$ that takes two messages m_0, m_1 of the same length as input and returns $\{m_b\}_{\mathsf{pk}(\mathsf{n})}^{\mathsf{n}_r}$, where b is an internal random bit uniformly drawn at the beginning by the challenger and n_r is a fresh nonce.
- A decryption oracle $\mathcal{O}_{\mathsf{dec}}(\mathsf{n})$ that, given m, returns $\mathsf{dec}(m, \mathsf{sk}(\mathsf{n}))$ if m was not submitted to the $\mathcal{O}_{\mathsf{LR}}$ oracle yet, and length of m zeros otherwise.

Remark that the two oracles have a shared memory. The advantage $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CCA}_2}(\eta)$ of an adversary $\mathcal{A}$ against this game is the probability for $\mathcal{A}$ to guess the bit b:

$$\Big|\ \mathbf{Pr}\Big(\mathsf{n} : \mathcal{A}^{\mathcal{O}_{\mathsf{LR}}^{1}(\mathsf{n}), \mathcal{O}_{\mathsf{dec}}(\mathsf{n})}(1^{\eta}) = 1\Big) - \mathbf{Pr}\Big(\mathsf{n} : \mathcal{A}^{\mathcal{O}_{\mathsf{LR}}^{0}(\mathsf{n}), \mathcal{O}_{\mathsf{dec}}(\mathsf{n})}(1^{\eta}) = 1\Big)\ \Big|$$

An encryption scheme is IND-CCA$_2$ if the advantage $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CCA}_2}(\eta)$ of any adversary $\mathcal{A}$ is negligible in η. The IND-CCA$_1$ game is the restriction of this game where the adversary cannot call $\mathcal{O}_{\mathsf{dec}}$ after having called $\mathcal{O}_{\mathsf{LR}}$. An encryption scheme is IND-CCA$_1$ if $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CCA1}}(\eta)$ is negligible for any adversary $\mathcal{A}$.

The CCA$_1^s$ Axioms. We define first a set of axioms CCA$_1^s$:

Definition 19. We let CCA$_1^s$ be the set of axioms:

$$\frac{\mathsf{len}(s) = \mathsf{len}(t)}{\vec{u}, \{s\}_{\mathsf{pk}(\mathsf{n})}^{\mathsf{n_e}} \sim \vec{u}, \{t\}_{\mathsf{pk}(\mathsf{n})}^{\mathsf{n_e}}}\ \mathrm{CCA}_1^s \qquad \text{when } \begin{cases} \mathsf{fresh}(\mathsf{n_e}; \vec{u}, s, t) \\ \mathsf{n} \sqsubseteq_{\mathsf{pk}(\cdot), \mathsf{sk}(\cdot)} \vec{u}, s, t \ \wedge\ \mathsf{sk}(\mathsf{n}) \sqsubseteq_{\mathsf{dec}(\_, \cdot)} \vec{u}, s, t \end{cases}$$

This set of axioms CCA$_1^s$ is very similar to the one used in [9]. The only difference is that in [9], the length equality requirement is not a premise of the axiom. Instead, if the length are not equal they return a error message. We found our version of the axiom simpler to use.

We have the following soundness property:

PROPOSITION 7. *The CCA$_1^s$ axioms are valid in any computational model where $(\{\}, dec, pk, sk)$ is interpreted as an IND-CCA$_1$ secure encryption scheme.*

Proof. The proof is by contradiction, and is given below.

We assume that there is a computational model $\mathcal{M}_c$ where the encryption scheme is IND-CCA$_1$ secure, and such that there is an instance $\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{t\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}$ of the axioms CCA$_1^s$ which is not valid. We deduce that there exists an attacker $\mathcal{A}$ that can distinguish between the left and right terms, i.e. the following quantity is non-negligible:

$$\left|\mathbf{Pr}\Big(\rho_1, \rho_2 : \mathcal{A}(1^\eta, [\![\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c}, \rho_2) = 1\Big) - \mathbf{Pr}\Big(\rho_1, \rho_2 : \mathcal{A}(1^\eta, [\![\vec{u}, \{t\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c}, \rho_2) = 1\Big)\right| \qquad (9)$$

where $[\![\vec{t}\,]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c}\mathsf{n_e}$ is the interpretation of $\vec{t}$ in $\mathcal{M}_c$, using the random tapes ρ_1, ρ_2 and security parameter η. We refer the reader to [9] for a formal definition.

Using $\mathcal{A}$, we can build an adversary $\mathcal{B}$ with a non-negligible advantage against the IND-CCA$_1$ game. First, $\mathcal{B}$ samples a vector of bit-strings $\vec{u}_s, s_s, t_s$ from $[\![\vec{u}, s, t]\!]_{\mathcal{M}_c}$, querying the decryption oracle whenever it needs to compute a subterm of the from $\mathsf{dec}(\_, \mathsf{sk(n)})$. Remark that the syntactic side-conditions:

$$\mathsf{n} \sqsubseteq_{\mathsf{pk}(\cdot),\mathsf{sk}(\cdot)} \vec{u}, s, t \qquad\qquad \mathsf{sk(n)} \sqsubseteq_{\mathsf{dec}(\_,\cdot)} \vec{u}, s, t$$

guarantee that this is always possible. Afterward, $\mathcal{B}$ queries the left-or-right oracle with (s_s, t_s) to get a value a. Here, we need the side-condition $\mathsf{fresh}(\mathsf{n_e}; \vec{u}, s, t)$ to guarantee that the random value $\mathsf{n_e}$ has not been sampled by $\mathcal{B}$. Indeed, the value $\mathsf{n_e}$ is sampled by the challenger, and is not available to $\mathcal{B}$. If the challenger internal bit b is 0 then $\vec{u}_s, a$ has been sampled from $[\![\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}]\!]_{\mathcal{M}_c}$, and if the challenger internal bit is 1 then $\vec{u}_s, a$ has been sampled from $[\![\vec{u}, \{t\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}]\!]_{\mathcal{M}_c}$:

$$\vec{u}_s, a \xleftarrow{\$} \begin{cases} [\![\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}]\!]_{\mathcal{M}_c} & \text{if } b = 0 \\ [\![\vec{u}, \{t\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}]\!]_{\mathcal{M}_c} & \text{if } b = 1 \end{cases}$$

Finally, $\mathcal{B}$ returns $\mathcal{A}(\vec{u}_s, a)$. It is easy to check that the advantage of $\mathcal{B}$ against the IND-CCA$_1$ game is exactly the advantage of $\mathcal{A}$ against $\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{t\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}$ This advantage is the quantity in (9), which we assumed non-negligible. Hence $\mathcal{B}$ is winning against the IND-CCA$_1$ game. Contradiction. ∎

The CCA$_1$ *Axioms.* We define the axioms CCA$_1$, which are more convenient to use than CCA$_1^s$. Basically, CCA$_1$ is the axiom CCA$_1^s$ where we applied transitivity to have different terms $\vec{u}, \vec{v}$ on each side.

Definition 20. We let CCA$_1$ be the set of axioms:

$$\frac{\vec{u}, \mathsf{len}(s) \sim \vec{v}, \mathsf{len}(t)}{\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{t\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}}\ \text{CCA}_1 \qquad \text{when} \begin{cases} \mathsf{fresh}(\mathsf{n_e}, \mathsf{n'_e}; \vec{u}, \vec{v}, s, t) \\ \vec{u} \equiv \mathsf{pk(n)}, \_ \ \wedge\ \vec{v} \equiv \mathsf{pk(n')}, \_ \\ \mathsf{n} \sqsubseteq_{\mathsf{pk}(\cdot),\mathsf{sk}(\cdot)} \vec{u}, s \ \wedge\ \mathsf{sk(n)} \sqsubseteq_{\mathsf{dec}(\_,\cdot)} \vec{u}, s \\ \mathsf{n'} \sqsubseteq_{\mathsf{pk}(\cdot),\mathsf{sk}(\cdot)} \vec{v}, t \ \wedge\ \mathsf{sk(n')} \sqsubseteq_{\mathsf{dec}(\_,\cdot)} \vec{v}, t \end{cases}$$

We have the following soundness theorem:

Proposition 8. *The* CCA$_1$ *axioms are valid in any computational model where* $(\{\}, dec, pk, sk)$ *is interpreted as an* IND-CCA$_1$ *secure encryption scheme.*

Proof. We are going to give a direct derivation of the axioms CCA$_1$, using rules that are valid in all computational models where $(\{\}, \mathsf{dec}, \mathsf{pk}, \mathsf{sk})$ is interpreted as an IND-CCA$_1$ secure encryption scheme. The derivation mostly rely on the Trans and the CCA$_1^s$ axioms. First, we use transitivity to split the goal $\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{t\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}$ into three sub-goals, by replacing the plain-texts with zeros:

$$\overbrace{\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \mathrlap{\underbrace{\phantom{\vec{u}, \{\mathbf{0}(\mathsf{len}(s))\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{\mathbf{0}(\mathsf{len}(t))\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}}}}\vec{u}, \{\mathbf{0}(\mathsf{len}(s))\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}} \sim \overbrace{\vec{v}, \{\mathbf{0}(\mathsf{len}(t))\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}} \sim \vec{v}, \{t\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}}$$

We deal with the left and right sub-goals using the CCA^s_1 axioms. We deal with the length equality constraint of the CCA^s_1 axioms using the axioms:

$$\mathsf{len}(t) = \mathsf{len}(\mathbf{0}(\mathsf{len}(t))) \qquad\qquad \mathsf{len}(s) = \mathsf{len}(\mathbf{0}(\mathsf{len}(s)))$$

which are valid in any computational model, using the fact that len interpretation is fixed. Finally, for the middle sub-goal, we deconstruct the terms using the FA rule and then apply Dup and Fresh. Putting everything together:

$$\dfrac{\dfrac{\dfrac{}{\mathsf{len}(s) = \mathsf{len}(\mathbf{0}(\mathsf{len}(s)))}}{\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{u}, \{\mathbf{0}(\mathsf{len}(s))\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}}\ \text{CCA}^s_1 \qquad \boxed{\vec{u}, \{\mathbf{0}(\mathsf{len}(s))\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{t\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}}}{\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{t\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}}\ \text{Trans}$$

$$\dfrac{\boxed{\vec{u}, \{\mathbf{0}(\mathsf{len}(s))\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{\mathbf{0}(\mathsf{len}(t))\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}} \qquad \dfrac{\dfrac{}{\mathsf{len}(t) = \mathsf{len}(\mathbf{0}(\mathsf{len}(t)))}}{\vec{v}, \{\mathbf{0}(\mathsf{len}(t))\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}} \sim \vec{v}, \{t\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}}\ \text{CCA}^s_1}{\boxed{\vec{u}, \{\mathbf{0}(\mathsf{len}(s))\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{t\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}}}\ \text{Trans}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vec{u}, \mathsf{len}(s) \sim \vec{v}, \mathsf{len}(t)}}{\vec{u}, \mathsf{len}(s), \mathsf{n_e} \sim \vec{v}, \mathsf{len}(t), \mathsf{n'_e}}\ \text{Fresh}}{\vec{u}, \mathsf{len}(s), \mathsf{pk(n)}, \mathsf{n_e} \sim \vec{v}, \mathsf{len}(t), \mathsf{pk(n')}, \mathsf{n'_e}}\ \text{Dup}}{\boxed{\vec{u}, \{\mathbf{0}(\mathsf{len}(s))\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{\mathbf{0}(\mathsf{len}(t))\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}}}\ \text{FA}^3$$

■

B.2 PRF Axioms

We now present the axioms we designed for keyed hash functions satisfying the *Pseudo Random Function* (PRF) assumption. Informally, a keyed hash function $\mathsf{H}(\cdot, \mathsf{k})$ is a PRF if its outputs are computationally indistinguishable from the outputs of a random function. Formally:

Definition 21 (PRF [24, 25]). Let $\mathsf{H}(\cdot,\cdot) : \{0,1\}^* \times \{0,1\}^\eta \rightarrow \{0,1\}^\eta$ be a keyed hash functions. The function H is a *Pseudo Random Function* iff, for any PPTM adversary $\mathcal{A}$ with access to an oracle $\mathcal{O}_f$:

$$|\mathbf{Pr}(k :\ \mathcal{A}^{\mathcal{O}_{\mathsf{H}(\cdot,k)}}(1^\eta) = 1) - \mathbf{Pr}(g :\ \mathcal{A}^{\mathcal{O}_{g(\cdot)}}(1^\eta) = 1)|$$

is negligible, where:

- k is drawn uniformly in $\{0,1\}^\eta$.
- g is drawn uniformly in the set of all functions from $\{0,1\}^*$ to $\{0,1\}^\eta$.

Here are the axioms:

Definition 22. We let PRF be the set of axioms:

$$\frac{}{\begin{array}{l} \vec{u}, \text{if } \dot{\bigvee}_{i\in I}\, m \doteq m_i \text{ then } \mathbf{0} \text{ else } \mathsf{H}(m,\mathsf{k}) \\ \sim\ \vec{u}, \text{if } \dot{\bigvee}_{i\in I}\, m \doteq m_i \text{ then } \mathbf{0} \text{ else } \mathsf{n} \end{array}} \qquad \text{when } \begin{cases} \mathsf{fresh}(\mathsf{n};\vec{u},m) \\ \mathsf{k} \sqsubseteq_{\mathsf{H}(\_,\cdot)} \vec{u}, m \\ \{m_i \mid i \in I\} = \{u \mid \mathsf{H}(u,\mathsf{k}) \in \mathsf{st}(\vec{u},m)\} \end{cases}$$

PROPOSITION 9. *The* PRF *axioms are valid in any computational model where H is interpreted as a* PRF *function.*

PROOF. Consider a computational model $\mathcal{M}_{\mathrm{c}}^0$ where H is interpreted as a PRF function, and an instance of the axiom schema which is not valid in $\mathcal{M}_{\mathrm{c}}^0$:

$$\frac{}{\begin{array}{l} \vec{u}, \text{if } \dot{\bigvee}_{i\in I}\, m \doteq m_i \text{ then } \mathbf{0} \text{ else } \mathsf{H}(m,\mathsf{k}) \\ \sim\ \vec{u}, \text{if } \dot{\bigvee}_{i\in I}\, m \doteq m_i \text{ then } \mathbf{0} \text{ else } \mathsf{n} \end{array}}$$

Let $\vec{h} \equiv (\mathsf{H}(m_i,\mathsf{k}))_{i\in I}$ and $\vec{v}[], b[]$ be contexts such that $\vec{v}[\vec{h}] \equiv \vec{u}$, $b[\vec{h}] \equiv \bigvee_{i\in I} \mathsf{eq}(m, m_i)$ and such that $\mathsf{k} \notin \mathsf{st}(\vec{v}, b)$. To get a contradiction, we just have to show that:

$$\mathbf{Pr}\Big(\rho_1,\rho_2 : \mathcal{A}\Big([\![\vec{v}[\vec{h}], [b[\vec{h}]]\mathsf{H}(m,\mathsf{k})]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_{\mathrm{c}}^0}\Big) = 1\Big) \approx \mathbf{Pr}\Big(\rho_1,\rho_2 : \mathcal{A}\Big([\![\vec{v}[\vec{h}], [b[\vec{h}]]\mathsf{n}]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_{\mathrm{c}}^0}\Big) = 1\Big) \qquad (10)$$

Let $\mathcal{M}_{\mathrm{c}}$ be an extension of $\mathcal{M}_{\mathrm{c}}^0$ where we added two function symbols $g, g' \in \mathcal{F}_{\mathrm{p}}$ which are interpreted as random functions. Observe that $\mathcal{M}_{\mathrm{c}}$ is not a computational model, because we require that function in $\mathcal{F}_{\mathrm{p}}$ are interpreted as *deterministic* polynomial-time functions. Still, $\mathcal{M}_{\mathrm{c}}$ is a first-order model. Moreover, $\mathcal{M}_{\mathrm{c}}$ and $\mathcal{M}_{\mathrm{c}}^0$'s interpretations coincide on terms which do not use g and g'. Hence, to prove (10) it is sufficient to show that:

$$\mathbf{Pr}\Big(\rho_1,\rho_2 : \mathcal{A}\Big([\![\vec{v}[\vec{h}], [b[\vec{h}]]\mathsf{H}(m,\mathsf{k})]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_{\mathrm{c}}}\Big) = 1\Big) \approx \mathbf{Pr}\Big(\rho_1,\rho_2 : \mathcal{A}\Big([\![\vec{v}[\vec{h}], [b[\vec{h}]]\mathsf{n}]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_{\mathrm{c}}}\Big) = 1\Big) \qquad (11)$$

Let $\vec{r} \equiv (g(m_i))_{i\in I}$. It is straightforward to check that, thanks to the PRF assumption of H, we can replace all subterms of the form $H(\mathsf{x},\mathsf{k})$ by $g(\mathsf{x})$ on the left:

$$\mathbf{Pr}\Big(\rho_1,\rho_2 : \mathcal{A}\Big([\![\vec{v}[\vec{h}], [b[\vec{h}]]\mathsf{H}(m,\mathsf{k})]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_{\mathrm{c}}}\Big) = 1\Big) \approx \mathbf{Pr}\Big(\rho_1,\rho_2 : \mathcal{A}\Big([\![\vec{v}[\vec{r}\,], [b[\vec{r}\,]]g(m)]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_{\mathrm{c}}}\Big) = 1\Big)$$

Moreover, using the fact that the subterm $g(m)$ is guarded by $b[\vec{r}\,]$, we know that, except for a negligible number of samplings, m is never queried to the random function g, except once, in $[b[\vec{r}\,]]g(m)$. It follows that we can safely replace the last call to $g(m)$ by a call to $g'(m)$, which yields:

$$\mathbf{Pr}\Big(\rho_1,\rho_2 : \mathcal{A}\Big([\![\vec{v}[\vec{r}\,], [b[\vec{r}\,]]g(m)]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_{\mathrm{c}}}\Big) = 1\Big) \approx \mathbf{Pr}\Big(\rho_1,\rho_2 : \mathcal{A}\Big([\![\vec{v}[\vec{r}\,], [b[\vec{r}\,]]g'(m)]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_{\mathrm{c}}}\Big) = 1\Big)$$

Now, using again the PRF property of H, we know that:

$$\mathbf{Pr}\Big(\rho_1,\rho_2 : \mathcal{A}\Big([\![\vec{v}[\vec{r}\,], [b[\vec{r}\,]]g'(m)]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_{\mathrm{c}}}\Big) = 1\Big) \approx \mathbf{Pr}\Big(\rho_1,\rho_2 : \mathcal{A}\Big([\![\vec{v}[\vec{h}], [b[\vec{h}]]g'(m)]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_{\mathrm{c}}}\Big) = 1\Big)$$

Finally, since g' appears only once in $\vec{v}[\vec{h}], [b[\vec{h}]]g'(m)$, we can replace $g'(m)$ by a fresh nonce. Hence:

$$\mathbf{Pr}\Big(\rho_1,\rho_2 : \mathcal{A}\Big([\![\vec{v}[\vec{h}], [b[\vec{h}]]g'(m)]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_{\mathrm{c}}}\Big) = 1\Big) \approx \mathbf{Pr}\Big(\rho_1,\rho_2 : \mathcal{A}\Big([\![\vec{v}[\vec{h}], [b[\vec{h}]]\mathsf{n}]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_{\mathrm{c}}}\Big) = 1\Big)$$

Which concludes the proof of (11). ■

Remark 5. If we have a valid instance of PRF:

$$\frac{}{\begin{array}{l} \vec{u}, \text{if } \dot{\bigvee}_{i\in I}\, m \doteq m_i \text{ then } \mathbf{0} \text{ else } \mathsf{H}(m,\mathsf{k}) \\ \sim\ \vec{u}, \text{if } \dot{\bigvee}_{i\in I}\, m \doteq m_i \text{ then } \mathbf{0} \text{ else } \mathsf{n} \end{array}}\ \textsc{prf}$$

then, using transitivity, we know that:

$$\dfrac{\dfrac{}{\begin{array}{l}\vec{u}, \text{if } \dot{\bigvee}_{i\in I}\, m \doteq m_i \text{ then } \mathbf{0} \text{ else } \mathsf{H}(m,\mathsf{k}) \\ \sim\ \vec{u}, \text{if } \dot{\bigvee}_{i\in I}\, m \doteq m_i \text{ then } \mathbf{0} \text{ else } \mathsf{n}\end{array}}\,\textsc{prf} \qquad \vec{u}, \text{if } \dot{\bigvee}_{i\in I}\, m \doteq m_i \text{ then } \mathbf{0} \text{ else } \mathsf{n} \sim \vec{v}}{\vec{u}, \text{if } \dot{\bigvee}_{i\in I}\, m \doteq m_i \text{ then } \mathbf{0} \text{ else } \mathsf{H}(m,\mathsf{k}) \sim \vec{v}}\,\text{Trans}$$

Therefore the following axiom schema is admissible using $\textsc{prf}$ and the transitivity axiom Trans:

$$\dfrac{\vec{u}, \text{if } \dot{\bigvee}_{i\in I}\, m \doteq m_i \text{ then } \mathbf{0} \text{ else } \mathsf{n} \sim \vec{v}}{\vec{u}, \text{if } \dot{\bigvee}_{i\in I}\, m \doteq m_i \text{ then } \mathbf{0} \text{ else } \mathsf{H}(m,\mathsf{k}) \sim \vec{v}}\,\textsc{prf} \quad \text{when} \begin{cases} \mathsf{fresh}(\mathsf{n}; \vec{u}, m) \\ \mathsf{k} \sqsubseteq_{\mathsf{H}(\_,\cdot)} \vec{u}, m \\ \{m_i \mid i \in I\} = \{u \mid \mathsf{H}(u,\mathsf{k}) \in \mathsf{st}(\vec{u}, m)\} \end{cases}$$

We will prefer the axiom schema above over the axiom schema given in Definition 22. By a notation abuse, we also refer to the above axioms as $\textsc{prf}$. ◇

B.3 Proof of Proposition 4

Proof. Let b be the following boolean term:

$$\mathsf{H}(m_1,\mathsf{k}) \doteq \mathsf{H}(m_2,\mathsf{k}) \ \dot{\rightarrow}\ m_1 \doteq m_2$$

Let $\mathcal{M}_c$ be a computational model such that H is interpreted by as collision-resistant keyed hash function, and assume that there exists an adversary $\mathcal{A}$ such that:

$$\left|\mathbf{Pr}\left(\rho_1,\rho_2 \ :\ \mathcal{A}(1^\eta, [\![b]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c}, \rho_2)\right) - \mathbf{Pr}\left(\rho_1,\rho_2 \ :\ \mathcal{A}(1^\eta, [\![\mathsf{true}]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c}, \rho_2)\right)\right|$$

is non-negligible. Since b is a boolean term, $[\![b]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} \in \{0,1\}$, hence the existence of $\mathcal{A}$ is equivalent to:

$$\mathbf{Pr}\left(\rho_1,\rho_2 \ :\ [\![b]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} = 0\right) \text{ is non-negligible} \tag{12}$$

We are going to define an adversary $\mathcal{B}$ against the $\textsc{cr-hk}$ game. Since the only occurrences of k in m_1 and m_2 are as second argument of H, the adversary $\mathcal{B}$ can sample two value a_1 and b_2 from, respectively, $[\![m_1]\!]_{\mathcal{M}_c}$ and $[\![m_2]\!]_{\mathcal{M}_c}$ (names different from k are uniformly sampled by $\mathcal{B}$, and subterms of the form $\mathsf{H}(u,\mathsf{k})$ are computed by calling the hash oracle). The adversary $\mathcal{B}$ returns $\langle a_1\,,\, a_2\rangle$. Then:

$$\begin{aligned} & \mathbf{Pr}\left(\mathsf{k} \ :\ \mathcal{B}^{\mathcal{O}_{\mathsf{H}(\cdot,\mathsf{k})}}(1^\eta) = \langle x_1\,,\, x_2\rangle, x_1 \neq x_2 \text{ and } \mathsf{H}(x_1,\mathsf{k}) = \mathsf{H}(x_2,\mathsf{k})\right) \\ = \ & \mathbf{Pr}\left(\rho_1,\rho_2 \ :\ [\![m_1]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} \neq [\![m_2]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} \wedge [\![\mathsf{H}(m_1,\mathsf{k})]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} = [\![\mathsf{H}(m_2,\mathsf{k})]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c}\right) \\ = \ & \mathbf{Pr}\left(\rho_1,\rho_2 \ :\ \neg\left([\![\mathsf{H}(m_1,\mathsf{k})]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} = [\![\mathsf{H}(m_2,\mathsf{k})]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} \rightarrow [\![m_1]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} = [\![m_2]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c}\right)\right) \\ = \ & \mathbf{Pr}\left(\rho_1,\rho_2 \ :\ \neg[\![\mathsf{H}(m_1,\mathsf{k}) \doteq \mathsf{H}(m_2,\mathsf{k}) \ \dot{\rightarrow}\ m_1 \doteq m_2]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c}\right) \\ = \ & \mathbf{Pr}\left(\rho_1,\rho_2 \ :\ [\![\mathsf{H}(m_1,\mathsf{k}) \doteq \mathsf{H}(m_2,\mathsf{k}) \ \dot{\rightarrow}\ m_1 \doteq m_2]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} = 0\right) \end{aligned}$$

which by hypothesis (12) is non-negligible. ■

B.4 Proof of Proposition 5

Proof. We assume that there is a computational model $\mathcal{M}_c$ where $(\mathsf{Mac}, \mathsf{Verify})$ is interpreted as an $\textsc{euf-cma}$ secure function. Moreover, we assume that there is an instance:

$$\dfrac{}{\mathsf{Verify}(m,s,\mathsf{k}) \ \dot{\rightarrow}\ \dot{\bigvee}_{u\in S}\, s \doteq \mathsf{Mac}_{\mathsf{k}}(u)}\,\textsc{euf-mac}$$

of the EUF-MAC axioms which is not valid in $\mathcal{M}_c$, where $S = \text{set-mac}_k(s, m)$. Therefore we know that the following quantity is non-negligible:

$$\mathbf{Pr}\left(\rho_1, \rho_2 \;:\; [\![\mathsf{Verify}(m, s, \mathsf{k})]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} \wedge \neg[\![\dot{\bigvee}_{u \in S}\, s \doteq \mathsf{Mac}_{\mathsf{k}}(u)]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c}\right)$$

Or, equivalently, the following quantity is non-negligible:

$$\mathbf{Pr}\left(\rho_1, \rho_2 \;:\; [\![\mathsf{Verify}(m, s, \mathsf{k})]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} \wedge \bigwedge_{u \in S}[\![s]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} \neq [\![\mathsf{Mac}_{\mathsf{k}}(u)]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c}\right) \tag{13}$$

Using $\mathcal{M}_c$, we can build a adversary $\mathcal{A}$ against the EUF-CMA game. The adversary $\mathcal{A}$ simply samples two values a_s, a_m from $[\![s]\!]_{\mathcal{M}_c}$ and $[\![m]\!]_{\mathcal{M}_c}$, by sampling all the subterms of s and m in a bottom-up fashion. The adversary calls the Mac oracle $\mathcal{O}_{\mathsf{Mac}_{\mathsf{k}}(\cdot)}$ whenever he needs to sample a value from a subterm of the form $\mathsf{Mac}_{\mathsf{k}}(\_)$. Remark that the side-condition $\mathsf{k} \sqsubseteq_{\mathsf{Mac}.(\_)} s, m$ ensures that this is always possible. Then $\mathcal{A}$ returns a_s, a_m. One can check that the advantage of $\mathcal{A}$ against the EUF-CMA game is exactly the quantity (13). It follows that $\mathcal{A}$ has a non-negligible probability of winning the game. Contradiction. ■

B.5 Additional Unforgeability Axioms

P-EUF-MAC$_s$ Axioms. We can refine the unforgeability axioms EUF-MAC using a finite partition of the outcomes, which is quite useful in proofs.

Definition 23. A finite family of conditionals $(b_i)_{i \in I}$ is a valid CS partition under some axioms Ax if the following formula is valid in every computational model satisfying the axioms Ax:

$$\left(\dot{\bigvee}_i\, b_i \mathrel{\dot{\wedge}} \dot{\bigwedge}_{i \neq j}\, b_i \mathrel{\dot{\neq}} b_j\right) = \mathsf{true}$$

Definition 24. For every terms b, t, we let $[b]t$ be the term if b then t else defaut, where defaut is a constant function symbol of types term and bool.

We can have a more precise axiom, by considering a valid CS partition $(b_i)_{i \in I}$ and applying the EUF-MAC axiom once for each element of the partition.

Definition 25. We let P-EUF-MAC$_s$ be the set of axioms:

$$\frac{}{\mathsf{Verify}(m, s, \mathsf{k}) \mathrel{\dot{\to}} \dot{\bigvee_{i \in I}}\, b_i \mathrel{\dot{\wedge}} \dot{\bigvee_{u \in S_i}}\, s \doteq \mathsf{Mac}_{\mathsf{k}}(u)} \quad \text{when} \begin{cases} \mathsf{k} \sqsubseteq_{\mathsf{Mac}.(\_)} s, m \\ (b_i)_{i \in I} \text{ is a valid CS partition} \\ \text{There exists } (s_i, m_i)_{i \in I} \text{ s.t. for every } i \in I \\ \qquad [b_i]s_i = [b_i]s \wedge [b_i]m_i = [b_i]m \\ \qquad S_i = \text{set-mac}_{\mathsf{k}}(s_i, m_i) \end{cases}$$

Proposition 10. *The P-EUF-MAC$_s$ axioms are valid in any computational model where (Mac, Verify) is interpreted as an EUF-CMA secure function.*

Proof. To show this, we prove that the P-EUF-MAC$_s$ axioms are a logical consequences of the axioms EUF-MAC and the axioms in Figure 15 and 16. The proof is pretty straightforward:

$$\begin{aligned} \mathsf{Verify}(m, s, \mathsf{k}) &\to \dot{\bigvee_{i \in I}}\, b_i \mathrel{\dot{\wedge}} \mathsf{Verify}(m, s, \mathsf{k}) && \text{(Since } (b_i)_{i \in I} \text{ is a valid CS partition)} \\ &\mathrel{\dot{\to}} \dot{\bigvee_{i \in I}}\, b_i \mathrel{\dot{\wedge}} \mathsf{Verify}(m_i, s_i, \mathsf{k}) && \text{(Since } [b_i]s_i = [b_i]s \text{ and } [b_i]m_i = [b_i]m) \end{aligned}$$

$$\begin{aligned}
&\dot{\rightarrow} \quad \dot{\bigvee_{i \in I}} b_i \mathrel{\dot{\wedge}} \dot{\bigvee_{u \in S_i}} s_i \doteq \mathsf{Mac}_{\mathsf{k}}(u) && \text{(Using EUF-MAC for every } i \in I\text{)}\\
&\dot{\rightarrow} \quad \dot{\bigvee_{i \in I}} b_i \mathrel{\dot{\wedge}} \dot{\bigvee_{u \in S_i}} s \doteq \mathsf{Mac}_{\mathsf{k}}(u) && \blacksquare
\end{aligned}$$

P-EUF-MAC Axioms. We can further refine the unforgeability axioms, by noticing that Macs appearing only in boolean conditionals can be ignored. For this, we let strict-st(u) be the set of subterms of u appearing outside u's conditionals. The definition is by structural induction on u.

Definition 26. For every u, we let strict-st(u) be the set of subterms of u appearing outside conditionals:

$$\begin{aligned}
\text{strict-st}(\text{if } b \text{ then } u \text{ else } v) &= \{\text{if } b \text{ then } u \text{ else } v\} \cup \text{strict-st}(u) \cup \text{strict-st}(v)\\
\text{strict-st}(f(\vec{u})) &= \{f(\vec{u})\} \cup \textstyle\bigcup_{u \in \vec{u}} \text{strict-st}(u) \qquad (\forall f \in \mathcal{F} \backslash \{\text{if\_then\_else\_}\})
\end{aligned}$$

We define the set of strict Mac subterms of a term u:

Definition 27. We let strict-set-mac$_{\mathsf{k}}(u)$ be the set of mac-ed terms under key k in u appearing outside a conditional:

$$\text{strict-set-mac}_{\mathsf{k}}(u) = \{m \mid \mathsf{Mac}_{\mathsf{k}}(m) \in \text{strict-st}(u)\}$$

We give the axioms:

Definition 28. We let P-EUF-MAC be the set of axioms:

$$\frac{}{\mathsf{Verify}(m, s, \mathsf{k}) \ \dot{\rightarrow} \ \dot{\bigvee}_{i \in I} b_i \mathrel{\dot{\wedge}} \bigvee_{u \in S_i} s \doteq \mathsf{Mac}_{\mathsf{k}}(u)} \quad \text{when} \begin{cases} \mathsf{k} \sqsubseteq_{\mathsf{Mac}_{\cdot}(\_)} s, m \\ (b_i)_{i \in I} \text{ is a valid CS partition} \\ \exists (s_i, m_i)_{i \in I} \text{ s.t. for every } i \in I \\ \qquad [b_i] s_i = [b_i] s \wedge [b_i] m_i = [b_i] m \\ \qquad S_i = \text{strict-set-mac}_{\mathsf{k}}(s_i, m_i) \end{cases}$$

Proposition 11. *The P-EUF-MAC axioms are valid in any computational model where (Mac, Verify) is interpreted as an EUF-CMA secure function.*

Proof. First, we are going to show that the following axioms are a logical consequences of the axioms EUF-MAC and the structural axioms $\mathsf{Ax}_{\mathsf{struct}}$.

$$\frac{}{\mathsf{Verify}(m, s, \mathsf{k}) \ \dot{\rightarrow} \ \bigvee_{u \in S} s \doteq \mathsf{Mac}_{\mathsf{k}}(u)} \quad \text{when} \begin{cases} \mathsf{k} \sqsubseteq_{\mathsf{Mac}_{\cdot}(\_)} s, m \\ S \equiv \text{strict-set-mac}_{\mathsf{k}}(s, m) \end{cases} \tag{14}$$

Assuming the axioms above are valid, it is easy to conclude by repeating the proof of Proposition 10, using the axioms above instead of EUF-MAC.

To show that the axioms in (14) are admissible, we are going to pull out all conditionals using the properties of the if_then_else_ function symbols. This yields a term of the form $C[\vec{\beta} \diamond \vec{e}]$ where the terms $\vec{e}$ are of the form Verify(u', s', k). Then, we apply the EUF-MAC axioms to every $e \in \vec{e}$. Finally, we rewrite back the conditionals. To be able to do this last step, we need, when we pulled out the conditionals, to remember which conditional appeared where. We do this by replacing a conditional b with either true$_b$ or false$_b$, where the lower-script b is a label that we attach to the term.

This motivates the following definition: for every boolean term b, we let $\mathsf{Val}_b = \{\mathsf{true}_b, \mathsf{false}_b\}$. We extend this to vector of conditionals by having $\mathsf{Val}_{u_0,\dots,u_l} = \mathsf{Val}_{u_0} \times \cdots \times \mathsf{Val}_{u_l}$. Basically, for every vector of conditionals $\vec{\beta}$, choosing a vector of terms $\vec{v} \in \mathsf{Val}_{\vec{\beta}}$ correspond to choosing a valuation of $\vec{\beta}$.

We start showing the validity of (14). Let $\vec{\beta}$ be the set of conditionals appearing in s, m, and C be an if-context such that:

$$\mathsf{Verify}(m, s, \mathsf{k}) \leftrightarrow C\left[\vec{\beta} \diamond \left(\mathsf{Verify}(m[\vec{v}/\vec{\beta}], s[\vec{v}/\vec{\beta}], \mathsf{k})\right)_{\vec{v} \in \mathsf{Val}_{\vec{\beta}}}\right]$$

where $t[\vec{u}/\vec{v}]$ denotes the substitution of every occurrence of $\vec{v}$ by $\vec{u}$ in t. For every $\vec{v} \in \mathsf{Val}_{\vec{\beta}}$, let $S_{\vec{v}} = \text{set-mac}_{\mathsf{k}}(s[\vec{v}/\vec{\beta}], m[\vec{v}/\vec{\beta}])$. By applying EUF-MAC to every $\mathsf{Verify}(m[\vec{v}/\vec{\beta}], s[\vec{v}/\vec{\beta}], \mathsf{k})$ we get:

$$\mathsf{Verify}(m, s, \mathsf{k}) \mathrel{\dot{\rightarrow}} C\left[\vec{\beta} \diamond \left(\dot{\bigvee}_{u \in S_{\vec{v}}} s[\vec{v}/\vec{\beta}] \doteq \mathsf{Mac}_{\mathsf{k}}(u)\right)_{\vec{v} \in \mathsf{Val}_{\vec{\beta}}}\right]$$

Since any conditional of $s[\vec{v}/\vec{\beta}]$ or $m[\vec{v}/\vec{\beta}]$ is of the form true_x or false_x for some label x, we know that:

$$S_{\vec{v}} = \text{set-mac}_{\mathsf{k}}(s[\vec{v}/\vec{\beta}], m[\vec{v}/\vec{\beta}]) = \text{strict-set-mac}_{\mathsf{k}}(s[\vec{v}/\vec{\beta}], m[\vec{v}/\vec{\beta}])$$

Moreover, we can check that:

$$\text{strict-set-mac}_{\mathsf{k}}(s[\vec{v}/\vec{\beta}], m[\vec{v}/\vec{\beta}]) = (\text{strict-set-mac}_{\mathsf{k}}(s, m))\,[\vec{v}/\vec{\beta}]$$

Let $S = \text{strict-set-mac}_{\mathsf{k}}(s, m)$, we just showed that $S_{\vec{v}} = S[\vec{v}/\vec{\beta}]$. Hence:

$$\begin{aligned} C\left[\vec{\beta} \diamond \left(\dot{\bigvee}_{u \in S_{\vec{v}}} s[\vec{v}/\vec{\beta}] \doteq \mathsf{Mac}_{\mathsf{k}}(u)\right)_{\vec{v} \in \mathsf{Val}_{\vec{\beta}}}\right] &\mathrel{\dot{\rightarrow}} C\left[\vec{\beta} \diamond \left(\dot{\bigvee}_{u \in S[\vec{v}/\vec{\beta}]} s[\vec{v}/\vec{\beta}] \doteq \mathsf{Mac}_{\mathsf{k}}(u)\right)_{\vec{v} \in \mathsf{Val}_{\vec{\beta}}}\right] \\ &\mathrel{\dot{\rightarrow}} C\left[\vec{\beta} \diamond \left(\left(\dot{\bigvee}_{u \in S} s \doteq \mathsf{Mac}_{\mathsf{k}}(u)\right)[\vec{v}/\vec{\beta}]\right)_{\vec{v} \in \mathsf{Val}_{\vec{\beta}}}\right] \\ &\mathrel{\dot{\rightarrow}} \dot{\bigvee_{u \in S}} s \doteq \mathsf{Mac}_{\mathsf{k}}(u) \end{aligned}$$

■

CR-KEY$_{\neq}$ Axioms. Finally, we have an axiom stating that two macs generated with distinct random keys cannot be equal.

Definition 29. We let CR-KEY$_{\neq}$ be the set of axioms:

$$\frac{}{\mathsf{Mac}_{\mathsf{k}}(u) \doteq \mathsf{Mac}_{\mathsf{k}'}(v) \mathrel{\dot{\rightarrow}} \mathsf{false}} \quad \text{when} \begin{cases} \mathsf{k}, \mathsf{k}' \sqsubseteq_{\mathsf{Mac}_{\cdot}(\_)} u, v \\ \mathsf{k}, \mathsf{k}' \in \mathcal{N}, \mathsf{k} \not\equiv \mathsf{k}' \end{cases}$$

Proposition 12. *The CR-KEY$_{\neq}$ axioms are valid in any computational model where (Mac, Verify) is interpreted as an EUF-CMA secure function.*

Proof. Assume that there exists a computational model $\mathcal{M}_{\mathrm{c}}$ and an instance:

$$\frac{}{\mathsf{Mac}_{\mathsf{k}}(u) \doteq \mathsf{Mac}_{\mathsf{k}'}(v) \mathrel{\dot{\rightarrow}} \mathsf{false}}$$

of the CR-KEY$_{\neq}$ axioms which is not valid in $\mathcal{M}_{\mathrm{c}}$. Then we know that $[\![\mathsf{Mac}_{\mathsf{k}}(u)]\!]$ and $[\![\mathsf{Mac}_{\mathsf{k}'}(v)]\!]$ coincide on a non-negligible number of samplings. We are going to build an adversary $\mathcal{A}$ against the unforgeability game. Basically, the collision is either $([\![u]\!], [\![\mathsf{Mac}_{\mathsf{k}'}(v)]\!])$ or $([\![v]\!], [\![\mathsf{Mac}_{\mathsf{k}}(u)]\!])$. As usual, the adversary works by doing a bottom-up sampling of all the subterms of $(u, \mathsf{Mac}_{\mathsf{k}'}(v))$ or $(v, \mathsf{Mac}_{\mathsf{k}}(u))$, using the mac oracle $\mathcal{O}_{\mathsf{Mac}_{\mathsf{k}}(\cdot)}$ in the former case, and $\mathcal{O}_{\mathsf{Mac}_{\mathsf{k}'}(\cdot)}$ in the latter.

There is a small difficulty though. E.g., consider the case where we try to sample a pair $(e_u, e_{\mathsf{Mac}_{\mathsf{k}'}(v)})$ from $([\![u]\!], [\![\mathsf{Mac}_{\mathsf{k}'}(v)]\!])$. During the sampling, the adversary may need to call the $\mathcal{O}_{\mathsf{Mac}_{\mathsf{k}}(\cdot)}$ oracle to sample an element e_w from $[\![w]\!]$, where w is such that $\mathsf{Mac}_{\mathsf{k}}(w)$ is a subterm of u. The problem is that if $e_u = e_w$ then we do not have a collision, as a collision must not have been submitted to the mac oracle. Besides, since we have not sampled e_u yet (we need to sample e_w before), we cannot check that $e_u \neq e_w$ before calling the oracle.

To avoid this problem, we *randomly guess*, at the beginning of the attack, which terms of $\text{set-mac}_{\mathsf{k}}(u, v)$ are going to be equal to u, and which terms of $\text{set-mac}_{\mathsf{k}'}(u, v)$ are going to be equal to v, and refuse to submit them to the oracle. We describe quickly the attacker:

- First, we guess uniformly at random the equalities in $\text{set-mac}_{\mathsf{k}}(u, v)$ and $\text{set-mac}_{\mathsf{k}'}(u, v)$.
- Then we toss a coin b, to decide if we try to sample from the distribution $([\![u]\!], [\![\mathsf{Mac}_{\mathsf{k}'}(v)]\!])$ or $([\![v]\!], [\![\mathsf{Mac}_{\mathsf{k}}(u)]\!])$. In the former case we use the mac oracle $\mathcal{O}_{\mathsf{Mac}_{\mathsf{k}}(\cdot)}$ and we sample from $\mathsf{Mac}_{\mathsf{k}'}(\cdot)$ directly (by sampling the key k'). In the latter case, we use the oracle $\mathcal{O}_{\mathsf{Mac}_{\mathsf{k}'}(\cdot)}$, and we sample from $\mathsf{Mac}_{\mathsf{k}'}(\cdot)$ directly.
- During the sampling process, we pick a subterm of $u, \mathsf{Mac}_{\mathsf{k}'}(v)$ or $v, \mathsf{Mac}_{\mathsf{k}}(u)$ (depending on the initial coin toss b) that has not been sampled yet, and that we can safely sample from, modulo the equalities we guessed. If $b = 0$, we can sample from a subterm if it is not $\mathsf{Mac}_{\mathsf{k}}(u)$, and if we did not guess that it is equal to $\mathsf{Mac}_{\mathsf{k}}(u)$. If $b = 1$, we have the same condition with v instead of u. If no such subterm exists, we abort.
- We output the candidate collision sampled from $([\![u]\!], [\![\mathsf{Mac}_{\mathsf{k}'}(v)]\!])$ or $([\![v]\!], [\![\mathsf{Mac}_{\mathsf{k}}(u)]\!])$ (depending on b), modulo the guessed equalities, as soon as possible.

To conclude, we need to prove that we have a non-negligible probability of building a collision. Consider the event on random tapes ρ_1, ρ_2:

$$\mathsf{Coll} \;:\; \left\{\rho_1, \rho_2 \mid [\![\mathsf{Mac}_{\mathsf{k}}(u)]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c} = [\![\mathsf{Mac}_{\mathsf{k}'}(v)]\!]^{\eta,\rho_1,\rho_2}_{\mathcal{M}_c}\right\}$$

We know that Coll is of non-negligible measure. We let $E_=$ be the event:

$$E_= \;:\; \text{we correctly guessed the equalities between} \begin{cases} \text{set-mac}_{\mathsf{k}}(u, v) \text{ and } u \\ \text{set-mac}_{\mathsf{k}'}(u, v) \text{ and } v \end{cases}$$

Since there are finitely many possible equalities, we have a non-negligible property of guessing correctly. Assuming $E_=$, we claim that the attacker has a probability greater than one-half *not to abort*. Indeed, assume that the adversary aborts during the attack. W.l.o.g. we assume that $b = 0$ (the other case is symmetrical). The attacker aborts only if he already sampled from $[\![u]\!]$, and did not sample from $[\![v]\!]$ yet (since he outputs an attack as soon as possible). Therefore, we know that the random tapes ρ_1, ρ_2 are such that we can sample from $[\![u]\!]$ without sampling from $[\![v]\!]$, and by consequence without computing $\mathsf{Mac}_{\mathsf{k}'}(v)$. It follows that, if $b = 1$, the adversary does not abort and successfully build a collision. Since b is drawn uniformly at random (and independently from all the other random samplings), the probability of aborting conditioned on $E_=$ and Coll is at least one half. ■

B.6 Joint Cryptographic Assumptions

In the previous sections, we presented axioms for the CR-HK, EUF-MAC and PRF cryptographic assumptions. Unfortunately, we cannot use these axioms for AKA$^+$, as the hash functions of this protocol share the same secret key. Instead, we define variants of our cryptographic axioms for families of hash functions which are *jointly* CR-HK, EUF-MAC or PRF.

The functions $H, H_1, \ldots, H_l$ are jointly CR-HK if no adversary can build a collision for $H(\cdot, \mathsf{k_m})$, even if it has oracle access to $H(\cdot, \mathsf{k_m}), H_1(\cdot, \mathsf{k_m}), \ldots, H_l(\cdot, \mathsf{k_m})$.

Definition 30. A function H is CR-HK secure with a key jointly used by $H_1, \ldots, H_l$ if for every PPTM $\mathcal{A}$, the following quantity is negligible in η:

$$\mathbf{Pr}\Big(\mathsf{k_m} : (m_1, m_2) \leftarrow \mathcal{A}^{\mathcal{O}_{H(\cdot,\mathsf{k_m})}, \mathcal{O}_{H_1(\cdot,\mathsf{k_m})}, \ldots, \mathcal{O}_{H_l(\cdot,\mathsf{k_m})}}(1^\eta), m_1 \neq m_2 \text{ and } H(m_1, \mathsf{k_m}) = H(m_2, \mathsf{k_m})\Big)$$

where $\mathsf{k_m}$ is drawn uniformly in $\{0,1\}^\eta$.

Similarly, the functions $H, H_1, \ldots, H_l$ are jointly EUF-MAC if no adversary can forge a mac of $H(\cdot, \mathsf{k_m})$, even if it has oracle access to $H(\cdot, \mathsf{k_m}), H_1(\cdot, \mathsf{k_m}), \ldots, H_l(\cdot, \mathsf{k_m})$.

Definition 31. A function H is EUF-MAC secure with a key jointly used by $H_1, \ldots, H_l$ if for every PPTM $\mathcal{A}$, the following quantity is negligible in η:

$$\mathbf{Pr}\Big(\mathsf{k_m} : (m, \sigma) \leftarrow \mathcal{A}^{O_{H(\cdot,\mathsf{k_m})}, O_{H_1(\cdot,\mathsf{k_m})}, \ldots, O_{H_l(\cdot,\mathsf{k_m})}}(1^\eta), m \text{ not queried to } O_{H(\cdot,\mathsf{k_m})} \text{ and } \sigma = H(m, \mathsf{k_m})\Big)$$

where $\mathsf{k_m}$ is drawn uniformly in $\{0,1\}^\eta$.

Finally, the functions $H, H_1, \ldots, H_l$ are jointly PRF if they are simultaneously computationally indistinguishable from random functions $g, g_1, \ldots, g_l$.

Definition 32. Let $H_1(\cdot,\cdot), \ldots, H_n(\cdot,\cdot)$ be a finite family of keyed hash functions from $\{0,1\}^* \times \{0,1\}^\eta$ to $\{0,1\}^\eta$. The functions $H_1, \ldots, H_n$ are *Jointly Pseudo Random Functions* if, for any PPTM adversary $\mathcal{A}$ with access to oracles $O_{f_1}, \ldots, O_{f_n}$:

$$|\mathbf{Pr}(k : \mathcal{A}^{O_{H_1(\cdot,k)}, \ldots, O_{H_n(\cdot,k)}}(1^\eta) = 1) - \mathbf{Pr}(g_1, \ldots, g_n : \mathcal{A}^{O_{g_1(\cdot)}, \ldots, O_{g_n(\cdot)}}(1^\eta) = 1)|$$

is negligible, where:

- k is drawn uniformly in $\{0,1\}^\eta$.
- $g_1, \ldots, g_n$ are drawn uniformly in the set of all functions from $\{0,1\}^*$ to $\{0,1\}^\eta$.

B.7 Relations Among Cryptographic Assumptions

It is well known that we have the following relation between the standard cryptographic assumptions:

$$\text{PRF} \Rightarrow \text{EUF-MAC} \Rightarrow \text{CR-HK}$$

These relations have a joint version counterpart, which we prove below:

$$\textit{Joint}\ \text{PRF} \Rightarrow \textit{Joint}\ \text{EUF-MAC} \Rightarrow \textit{Joint}\ \text{CR-HK}$$

PROPOSITION 13. *If the functions $H, H_1, \ldots, H_l$ are jointly PRF then H is EUF-MAC secure with a key jointly used by $H_1, \ldots, H_l$.*

PROOF. The proof is almost the same than the proof showing that if a function H is a PRF then H is EUF-MAC secure, and is by reduction. If H is not EUF-MAC secure with a key jointly used by $H_1, \ldots, H_l$ then there exists an adversary $\mathcal{A}$ winning the corresponding game with a non-negligible probability. It is simple to build from $\mathcal{A}$ an adversary $\mathcal{B}$ against the joint PRF property of $H, H_1, \ldots, H_l$.

First, $\mathcal{B}$ runs the adversary $\mathcal{A}$, forwarding and logging its oracle calls. Eventually, $\mathcal{A}$ returns a pair (m, σ). Then, $\mathcal{B}$ queries the first oracle on m, which returns a value σ'. Finally, $\mathcal{B}$ returns 1 if and only if $\mathcal{A}$ never queried the first oracle on m and $\sigma' = \sigma$. Then:

- If $\mathcal{B}$ is interacting with the oracles $O_{H(\cdot,\mathsf{k_m})}, O_{H_1(\cdot,\mathsf{k_m})}, \ldots, O_{H_l(\cdot,\mathsf{k_m})}$, its probability of returning 1 is exactly the advantage of $\mathcal{A}$ against the EUF-MAC game with key jointly used.
- If $\mathcal{B}$ is interacting with the oracles $O_{g(\cdot)}, O_{g_1(\cdot)}, \ldots, O_{g_l(\cdot)}$ where $g, g_1, \ldots, g_l$ are random functions, then its probability of returning 1 is the probability of having $g(m) = \sigma$ knowing that m was never queried to g. Since g is a random function, this is less than $1/2^\eta$.

Since $\mathcal{A}$ has a non-negligible advantage against the EUF-MAC game with key jointly used, we deduce that $\mathcal{B}$ has a non-negligible advantage against the joint PRF game. ■

PROPOSITION 14. *If H is EUF-MAC secure with a key jointly used by $H_1, \ldots, H_l$ then H is CR secure with a key jointly used by $H_1, \ldots, H_l$.*

Proof. Assume that we have an adversary $\mathcal{A}$ against the joint CR-HK game. We are going to build an adversary $\mathcal{B}$ against the joint EUF-MAC game. W.l.o.g. we can assume that:

- $\mathcal{A}$ makes at most $p(\eta)$ calls to the hash oracle for $\mathcal{O}_{\mathsf{H}_1(\cdot,\mathsf{k_m})}$, where p is a polynomial.
- $\mathcal{A}$ never calls the hash oracle $\mathcal{O}_{\mathsf{H}_1(\cdot,\mathsf{k_m})}$ on the same value twice.
- $\mathcal{A}$'s candidate collision pair (m_1, m_2) has been submitted to the oracle $\mathcal{O}_{\mathsf{H}_1(\cdot,\mathsf{k_m})}$. Moreover, m_2 is the last query to the oracle $\mathcal{O}_{\mathsf{H}_1(\cdot,\mathsf{k_m})}$.
- $\mathcal{A}$'s output is a well-formed message only when it is a valid collision pair.

We use $\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}$ to denote the oracles $\mathcal{O}_{\mathsf{H}_1(\cdot,\mathsf{k_m})}, \dots, \mathcal{O}_{\mathsf{H}_l(\cdot,\mathsf{k_m})}$. On input 1^η, the adversary $\mathcal{B}$ does:

- First, it guesses randomly two indices i, j in $[\![1, p(\eta)]\!]$. If $i \geq j$, it aborts.
- Then, it simulates $\mathcal{A}$, forwarding its calls to the oracles $\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}$, with two exceptions:
  - The j-th query u_j to the oracle $\mathcal{O}_{\mathsf{H}_1(\cdot,\mathsf{k_m})}$ is not forwarded. Instead, $\mathcal{B}$ sends to $\mathcal{A}$ the result of the i-th query u_i to the oracle $\mathcal{O}_{\mathsf{H}_1(\cdot,\mathsf{k_m})}$ (i.e. $\mathsf{H}_1(u_i, \mathsf{k_m})$).
  - If there is a $j+1$-th query to $\mathcal{O}_{\mathsf{H}_1(\cdot,\mathsf{k_m})}$, $\mathcal{B}$ aborts.
- Finally, $\mathcal{B}$ gets a pair (m_1, m_2) from $\mathcal{A}$. It checks whether $m_1 = u_i$ and $m_2 = u_j$. If not, it aborts. Otherwise, it returns $(u_j, \mathsf{H}_1(u_i, \mathsf{k_m}))$.

The probability of $\mathcal{B}$ winning the game is exactly the probability of $\mathcal{B}$ winning the game and not aborting. Moreover, if $\mathcal{B}$ does not abort, $\mathcal{A}$ output a pair (m_1, m_2) which it believes is a valid collision. Therefore $\mathcal{B}$ wins if and only if (m_1, m_2) is a valid collision. We use ρ_1 for $\mathcal{B}$ random tape, and ρ_2 for $\mathcal{A}$ random tape.[6] Then we can lower-bound the probability that $\mathcal{B}$ wins as follows:

$$\begin{aligned}
&\mathbf{Pr}\Big(\rho_1, \rho_2, \mathsf{k_m} \;:\; \mathcal{B}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_1, \rho_2) \text{ wins}\Big)\\
=\;& \mathbf{Pr}\Big(\rho_1, \rho_2, \mathsf{k_m} \;:\; \mathcal{B}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_1, \rho_2) \text{ wins} \wedge \neg\mathrm{abort}(\mathcal{B})\Big)\\
=\;& \mathbf{Pr}\Big(\rho_1, \rho_2, \mathsf{k_m} \;:\; (m_1, m_2) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathcal{B}}(\rho_1,\mathsf{k_m})}(\rho_2) \wedge \mathsf{H}_1(m_1, \mathsf{k_m}) = \mathsf{H}_1(m_2, \mathsf{k_m}) \wedge \neg\mathrm{abort}(\mathcal{B})\Big)\\
\geq\;& \mathbf{Pr}\Big(\rho_1, \rho_2, \mathsf{k_m} \;:\; (m_1, m_2) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathcal{B}}(\rho_1,\mathsf{k_m})}(\rho_2) \wedge \mathsf{H}_1(m_1, \mathsf{k_m}) = \mathsf{H}_1(m_2, \mathsf{k_m}) \wedge \neg\mathrm{abort}(\mathcal{B})\\
&\qquad\qquad\qquad \mid \mathcal{A}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_2) \text{ wins}\Big) \times \mathbf{Pr}\Big(\rho_2, \mathsf{k_m} : \mathcal{A}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_2) \text{ wins}\Big)
\end{aligned}$$

Knowing that $\mathcal{A}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_2)$ wins, the probability over ρ_2 that $\mathcal{B}$ correctly guessed the index of $\mathcal{A}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_2)$'s query of m_1 to the oracle and the number of $\mathcal{A}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_2)$'s queries is $\frac{1}{p(\eta)^2}$. Hence:

$$\begin{aligned}
\geq\;& \mathbf{Pr}\Big(\rho_1, \rho_2, \mathsf{k_m} \;:\; (m_1, m_2) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathcal{B}}(\rho_1,\mathsf{k_m})}(\rho_2) \wedge \mathsf{H}_1(m_1, \mathsf{k_m}) = \mathsf{H}_1(m_2, \mathsf{k_m}) \wedge \neg\mathrm{abort}(\mathcal{B})\\
&\qquad \mid \mathcal{A}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_2) \text{ wins} \wedge \mathrm{guessed}(\mathcal{B})\Big) \times \mathbf{Pr}\Big(\rho_2, \mathsf{k_m} : \mathcal{A}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_2) \text{ wins}\Big) \times \frac{1}{p(\eta)^2}
\end{aligned}$$

Knowing that $\mathcal{B}$ guessed properly, and that $\mathcal{A}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_2)$ wins, we know that the oracles $\mathcal{O}_{\mathsf{H}}(\mathsf{k_m})$ and $\mathcal{O}_{\mathcal{B}}(\rho_1, \mathsf{k_m})$ have the same outputs on $\mathcal{A}(\rho_2)$'s queries. By consequence:

$$\begin{aligned}
\geq\;& \mathbf{Pr}\Big(\rho_1, \rho_2, \mathsf{k_m} \;:\; (m_1, m_2) \leftarrow \mathcal{A}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_2) \wedge \mathsf{H}_1(m_1, \mathsf{k_m}) = \mathsf{H}_1(m_2, \mathsf{k_m}) \wedge \neg\mathrm{abort}(\mathcal{B})\\
&\qquad \mid \mathcal{A}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_2) \text{ wins} \wedge \mathrm{guessed}(\mathcal{B})\Big) \times \mathbf{Pr}\Big(\rho_2, \mathsf{k_m} : \mathcal{A}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_2) \text{ wins}\Big) \times \frac{1}{p(\eta)^2}
\end{aligned}$$

In that case, we know that $\mathcal{B}$ does not abort and that the game is won. Therefore:

$$\geq\; \mathbf{Pr}\Big(\rho_2, \mathsf{k_m} : \mathcal{A}^{\mathcal{O}_{\vec{\mathsf{H}}(\cdot,\mathsf{k_m})}}(\rho_2) \text{ wins}\Big) \times \frac{1}{p(\eta)^2}$$

Which, by hypothesis, is non-negligible. ■

[6] Of course, $\mathcal{B}$ has access to ρ_2 since it simulates $\mathcal{A}$. But it only uses it for the simulation, not for its own coin tosses.

$$\frac{}{\mathsf{Mac}^{j}_{\mathsf{k_m}}(m_1) = \mathsf{Mac}^{j}_{\mathsf{k_m}}(m_2) \rightarrow m_1 = m_2} \qquad \text{when } \mathsf{k_m} \sqsubseteq_{\mathsf{Mac}^{\cdot}_{\cdot}(\_)} m_1, m_2 \qquad (\textsc{cr}^{j})$$

$$\frac{}{s = \mathsf{Mac}^{j}_{\mathsf{k_m}}(m) \rightarrow \bigvee_{u \in S} s = \mathsf{Mac}^{j}_{\mathsf{k_m}}(u)} \qquad \text{when } \begin{cases} \mathsf{k_m} \sqsubseteq_{\mathsf{Mac}^{\cdot}_{\cdot}(\_)} s, m \\ S = \text{set-mac}^{j}_{\mathsf{k_m}}(s, m) \end{cases} \qquad (\textsc{euf-mac}^{j})$$

$$\frac{}{\begin{array}{l} s = \mathsf{Mac}^{j}_{\mathsf{k_m}}(m) \rightarrow \\ \qquad \displaystyle\bigvee_{i \in I} b_i \wedge \bigvee_{u \in S_i} s = \mathsf{Mac}^{j}_{\mathsf{k_m}}(u) \end{array}} \quad \text{when } \begin{cases} \mathsf{k_m} \sqsubseteq_{\mathsf{Mac}^{\cdot}_{\cdot}(\_)} s, m \\ (b_i)_{i \in I} \text{ is a valid CS partition} \\ \exists (s_i, m_i)_{i \in I} \text{ s.t. } \forall i \in I \\ \quad [b_i]s_i \doteq [b_i]s \wedge [b_i]m_i \doteq [b_i]m \\ \quad S_i = \text{strict-set-mac}^{j}_{\mathsf{k_m}}(s_i, m_i) \end{cases} \qquad (\textsc{p-euf-mac}^{j})$$

$$\frac{}{\mathsf{Mac}^{j}_{\mathsf{k_m}}(u) = \mathsf{Mac}^{j}_{\mathsf{k'_m}}(v) = \mathsf{false}} \qquad \text{when } \begin{cases} \mathsf{k_m}, \mathsf{k'_m} \sqsubseteq_{\mathsf{Mac}^{\cdot}_{\cdot}(\_)} u, v \\ \mathsf{k_m}, \mathsf{k'_m} \in \mathcal{N} \end{cases} \qquad (\textsc{cr-key}^{j}_{\neq})$$

$$\frac{}{\begin{array}{rl} & \vec{u}, \text{if } \bigvee_{i \in I} \mathsf{eq}(m, m_i) \text{ then } 0 \text{ else } \mathsf{Mac}^{j}_{\mathsf{k_m}}(m) \\ \sim & \vec{u}, \text{if } \bigvee_{i \in I} \mathsf{eq}(m, m_i) \text{ then } 0 \text{ else } \mathsf{n} \end{array}} \quad \text{when } \begin{cases} \mathsf{fresh}(\mathsf{n}; \vec{u}, m) \\ \mathsf{k_m} \sqsubseteq_{\mathsf{Mac}^{\cdot}_{\cdot}(\_)} \vec{u}, m \\ \{m_i \mid i \in I\} = \text{set-mac}^{j}_{\mathsf{k_m}}(\vec{u}, m) \end{cases} \qquad (\textsc{prf-mac}^{j})$$

$$\frac{}{\begin{array}{rl} & \vec{u}, \text{if } \bigvee_{i \in I} \mathsf{eq}(m, m_i) \text{ then } 0 \text{ else } g_{\mathsf{k}}(m) \\ \sim & \vec{u}, \text{if } \bigvee_{i \in I} \mathsf{eq}(m, m_i) \text{ then } 0 \text{ else } \mathsf{n} \end{array}} \quad \text{when } \begin{cases} \mathsf{fresh}(\mathsf{n}; \vec{u}, m) \\ \mathsf{k} \sqsubseteq_{\mathsf{f}_{\cdot}(\_), \mathsf{f}^{\mathsf{r}}_{\cdot}(\_)} \vec{u}, m \\ \{m_i \mid i \in I\} = \text{set-prf}^{g}_{\mathsf{k}}(\vec{u}, m) \end{cases} \qquad (\textsc{prf-g})$$

Convention: $1 \leq j \leq 5$ and $g \in \{\mathsf{f}, \mathsf{f}^{\mathsf{r}}\}$.

Fig. 18. Axioms for Joint Cryptographic Assumptions

B.8 Cryptographic Axioms for Joint Assumptions

We translate these games in the logic for the two families of functions $(\mathsf{Mac}^{j})_{1 \leq j \leq 5}$ and $(\mathsf{f}, \mathsf{f}^{\mathsf{r}})$. As expected, these axioms are very similar to the axioms of Section 8.2. First, some definitions.

Definition 33. For every ground term u, we define three set of subterms of u:

- We let $\text{set-mac}^{j}_{\mathsf{k_m}}(u)$ be the set of Mac^{j} terms under key $\mathsf{k_m}$ in u:

$$\text{set-mac}^{j}_{\mathsf{k_m}}(u) = \{m \mid \mathsf{Mac}^{j}_{\mathsf{k_m}}(m) \in \mathsf{st}(u)\}$$

- We let $\text{strict-set-mac}^{j}_{\mathsf{k_m}}(u)$ be the set of mac-ed terms under key $\mathsf{k_m}$ and tag j in u appearing outside a conditional:

$$\text{strict-set-mac}^{j}_{\mathsf{k_m}}(u) = \{m \mid \mathsf{Mac}^{j}_{\mathsf{k_m}}(m) \in \text{strict-st}(u)\}$$

- For every $g \in \{\mathsf{f}, \mathsf{f}^{\mathsf{r}}\}$, we let $\text{set-prf}^{g}_{\mathsf{k}}(u)$ be the set of g terms under key k in u:

$$\text{set-prf}^{g}_{\mathsf{k}}(u) = \{m \mid g_{\mathsf{k}}(m) \in \mathsf{st}(u)\}$$

The axioms are given in Figure 18, and are sound under the appropriate cryptographic assumptions.

Proposition 15. *The axioms in Figure 18 are valid in any computational model where:*

$\textsc{cr}^j$	$(Mac^i)_{1 \leq i \leq 5}$ *are jointly* $\textsc{cr-hk}$
$\textsc{euf-mac}^j$, $\textsc{p-euf-mac}^j$ *and* $\textsc{cr-key}^j_{\neq}$	$(Mac^i)_{1 \leq i \leq 5}$ *are jointly* $\textsc{euf-mac}$
$\textsc{prf-mac}^j$	$(Mac^i)_{1 \leq i \leq 5}$ *are jointly* $\textsc{prf}$
$\textsc{prf}$-f *and* $\textsc{prf}$-f^r	(f, f^r) *are jointly* $\textsc{prf}$

Proof. The proof are exactly the same than in Section 8.2. We omit the details. ■

Remark 6. Similarly to what we observed in Remark 5, the following axiom schema is admissible using $\textsc{prf-mac}^j$ + Trans:

$$\frac{\vec{u}, \mathsf{if}\ \bigvee_{i \in I} \mathsf{eq}(m, m_i)\ \mathsf{then}\ 0\ \mathsf{else}\ \mathsf{n} \sim \vec{v}}{\vec{u}, \mathsf{if}\ \bigvee_{i \in I} \mathsf{eq}(m, m_i)\ \mathsf{then}\ 0\ \mathsf{else}\ \mathsf{Mac}^j_{\mathsf{k_m}}(m) \sim \vec{v}} \quad \text{when} \begin{cases} \mathsf{fresh}(\mathsf{n}; \vec{u}, m) \\ \mathsf{k_m} \sqsubseteq_{\mathsf{Mac}^{\_}_{\cdot}(\_)} \vec{u}, m \\ \{m_i \mid i \in I\} = \mathsf{set\text{-}mac}^j_{\mathsf{k_m}}(\vec{u}, m) \end{cases}$$

By a notation abuse, we refer also to the axiom above as $\textsc{prf-mac}^j$. The same remark applies to $\textsc{prf}$-f and $\textsc{prf}$-f^r. ◇

Definition 34. We let $\mathsf{Ax_{crypto}}$ be the set of cryptographic axioms:

$$\mathsf{Ax_{crypto}} = \textsc{cca}_1 \cup \left(\textsc{prf-mac}^j\right)_{1 \leq j \leq 5} \cup \textsc{prf}\text{-}\mathsf{f} \cup \textsc{prf}\text{-}\mathsf{f}^\mathsf{r} \cup \left(\textsc{euf-mac}^j\right)_{1 \leq j \leq 5} \cup \left(\textsc{cr}^j\right)_{1 \leq j \leq 5}$$

Proposition 16. *The axioms in* $\mathsf{Ax_{crypto}}$ *are valid in any computational model where the asymmetric encryption* $\{\_\}^{\_}_{\_}$ *is* $\textsc{ind-cca}_1$ *secure and* f *and* f^r *(resp.* $Mac^1 - Mac^5$*) are jointly* $\textsc{prf}$.

Proof. For $\textsc{cca}_1$, this is from Propositions 8. For the other axioms, we know using Proposition 13 and Proposition 14 that f and f^r (resp. Mac^1– Mac^5) are jointly $\textsc{euf-mac}$ and $\textsc{cr-hk}$. Therefore we can conclude using Proposition 15. ■

C MODELING AND GHOST VARIABLES

C.1 Axioms and Notations

We now define the set of axioms Ax:

Definition 35. Ax is the set of axioms $\mathsf{Ax} = \mathsf{Ax_{struct}} \cup \mathsf{Ax_{impl}} \cup \mathsf{Ax_{crypto}}$. We recall that:

- $\mathsf{Ax_{struct}}$ is the set of structural axioms, which are given in Figure 15 and Figure 16.
- $\mathsf{Ax_{crypto}}$ is the set of cryptographic axioms in Figure 18, plus the $\textsc{cca}_1$ axiom given in Section B.1.
- $\mathsf{Ax_{impl}}$ is the set of implementation axioms given in Figure 17.

Notations. In the rest of this paper, the set of axioms Ax is fixed, and we stop to specify that we use it: we say that we have a derivation of a formula ϕ to mean that ϕ can be deduced from Ax. Furthermore, we say that ϕ holds when there is a derivation of ϕ.

Moreover, we abuse notations and write $u = v$ instead of $u \doteq v$. We can always disambiguate using the context: if we expect a term, then $u = v$ stands for the term $\mathsf{eq}(u, v)$, whereas if a formula is expected then $u = v$ stands for $\mathsf{eq}(u, v) \sim \mathsf{true}$. We extends this to any boolean term: if b is a boolean term then we say that b holds if we can show that $b \sim \mathsf{true}$ holds. For example, $\sigma_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) \geq \sigma_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$ holds if we can show that $\mathsf{geq}(\sigma_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}), \sigma_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})) \sim \mathsf{true}$.

C.2 Axiom Extensions

We present Extensions of our axioms, and show that they are logical consequences of Ax.

Definition 36. We let Simp denote a sequence of applications of R, FA and Dup, i.e.:

$$\frac{\vec{s} \sim \vec{t}}{\vec{u} \sim \vec{v}}\ \mathsf{Simp} \qquad \text{when} \qquad \frac{\vec{s} \sim \vec{t}}{\vec{u} \sim \vec{v}}\ (R + \mathsf{FA} + \mathsf{Dup})^*$$

Definition 37 (The indep-branch Axioms). Let $\vec{u}, \vec{b}$ be ground terms, $C[]$ an if-context and n, $(\mathsf{n}_i)_{i \in I}$ nonces. If n, $(\mathsf{n}_i)_{i \in I}$ are distinct and such that $\mathsf{fresh}(\mathsf{n}, (\mathsf{n}_i)_{i \in I}; \vec{u}, \vec{b}, C[])$, then the following inference rule is an instance of the indep-branch axiom:

$$\frac{}{\vec{u}, C\left[\vec{b} \diamond (\mathsf{n}_i)_{i \in I}\right] \sim \vec{u}, \mathsf{n}}\ \mathsf{indep\text{-}branch}$$

Proposition 17. *The indep-branch axioms are a consequence of the Ax axioms.*

Proof. To prove this, we first introduce the if-context $C[]$ on the right to match the shape of the left side. We then split the proof using CS, and conclude by applying Fresh. This yields the derivation:

$$\cfrac{\cfrac{\cfrac{}{\forall i \in I, \vec{u}, \vec{b}, \mathsf{n}_i \sim \vec{u}, \vec{b}, \mathsf{n}}\ \mathsf{Fresh}}{\vec{u}, C\left[\vec{b} \diamond (\mathsf{n}_i)_{i \in I}\right] \sim \vec{u}, C\left[\vec{b} \diamond (\mathsf{n})_{i \in I}\right]}\ \mathsf{CS}^*}{\vec{u}, C\left[\vec{b} \diamond (\mathsf{n}_i)_{i \in I}\right] \sim \vec{u}, \mathsf{n}}\ R$$

■

It is often convenient to apply the FA axiom under an if-context C.

Definition 38. Let $\vec{v}, \vec{b}, (u_{i,j})_{i \in I, 1 \le j \le n}, (u'_{i,j})_{i \in I, 1 \le j \le n}$ be ground terms and C an if-context. Then the following inference rule is an instance of the $\mathsf{FA_c}$ axiom:

$$\frac{\vec{v}, \left(C\left[\vec{b} \diamond (u_{i,j})_{i \in I}\right]\right)_{1 \le j \le n} \sim \vec{v}', \left(C\left[\vec{b}' \diamond (u'_{i,j})_{i \in I}\right]\right)_{1 \le j \le n}}{\vec{v}, C\left[\vec{b} \diamond \left(f((u_{i,j})_{1 \le j \le n})\right)_{i \in I}\right] \sim \vec{v}', C\left[\vec{b}' \diamond \left(f((u'_{i,j})_{1 \le j \le n})\right)_{i \in I}\right]}\ \mathsf{FA_c}$$

Proposition 18. *The FA_c axioms are a consequence of the Ax axioms.*

Proof. First, we pull the f function outside of the if-context C using the homomorphism properties of the if_then_else_. Finally we apply the FA axiom. This yields the derivation:

$$\cfrac{\cfrac{\vec{v}, \left(C\left[\vec{b} \diamond (u_{i,j})_{i \in I}\right]\right)_{1 \le j \le n} \sim \vec{v}', \left(C\left[\vec{b}' \diamond (u'_{i,j})_{i \in I}\right]\right)_{1 \le j \le n}}{\vec{v}, f\left(C\left[\vec{b} \diamond (u_{i,j})_{i \in I}\right]\right)_{1 \le j \le n} \sim \vec{v}', f\left(C\left[\vec{b}' \diamond (u'_{i,j})_{i \in I}\right]\right)_{1 \le j \le n}}\ \mathsf{FA}}{\vec{v}, C\left[\vec{b} \diamond \left(f((u_{i,j})_{1 \le j \le n})\right)_{i \in I}\right] \sim \vec{v}', C\left[\vec{b}' \diamond \left(f((u'_{i,j})_{1 \le j \le n})\right)_{i \in I}\right]}\ R$$

■

Finally, the following axioms state that two encryptions with different randomness are almost never equal. This requires that the encrypted messages are not of length zero.

Proposition 19. *For every ground terms u, v, the following axiom is a consequence of the Ax axioms:*

$$\frac{len(u) \doteq len(v) \qquad len(u) \not\doteq 0}{eq(\{u\}^{n_e}_{pk(n)}, \{v\}^{n'_e}_{pk(n)}) \doteq false} \qquad when \begin{cases} n_e \not\equiv n'_e \\ fresh(n_e, n'_e; u, v) \\ n \sqsubseteq_{pk(\cdot), sk(\cdot)} u, v \ \wedge\ sk(n) \sqsubseteq_{dec(\_, \cdot)} u, v \end{cases}$$

Proof. We give directly the derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathsf{pk(n)},\ \{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}},\ \mathsf{len}(v) \sim \mathsf{pk(n)},\ \{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}},\ \mathsf{len}(v)}\;\text{Refl} \qquad \dfrac{\dfrac{}{\mathsf{len}(v) \doteq \mathsf{len}(v)}\;\text{Refl}}{\mathsf{len}(v) \doteq \mathsf{len}(1^{\mathsf{len}(v)})}}{\dfrac{\mathsf{pk(n)},\ \{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}},\ \{v\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}} \sim \mathsf{pk(n)},\ \{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}},\ \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}}{\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}},\ \{v\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}} \sim \{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}},\ \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}}\;\text{Restr}}\;\text{CCA}_1}{\mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}},\ \{v\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}) \doteq \mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}},\ \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}})}\;\text{FA} \qquad \mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}},\ \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}}{\mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}},\ \{v\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}}\;\text{Trans}$$

To show $\mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}$, we use the transitivity axiom again:

$$\dfrac{\begin{array}{l}\mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}) \\ \doteq\ \mathsf{eq}(\{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}})\end{array} \qquad \mathsf{eq}(\{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}}{\mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}}\;\text{Trans}$$

Now, we give the derivation of the left premise:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathsf{pk(n)}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}, \mathsf{len}(u) \sim \mathsf{pk(n)}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}, \mathsf{len}(u)}\;\text{Refl} \qquad \dfrac{\dfrac{}{\mathsf{len}(u) \doteq \mathsf{len}(u)}\;\text{Refl}}{\mathsf{len}(u) \doteq \mathsf{len}(0^{\mathsf{len}(u)})}}{\mathsf{pk(n)}, \{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}\{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}} \sim \mathsf{pk(n)}, \{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}\{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}}\;\text{CCA}_1}{\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}\{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}} \sim \{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}\{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}}\;\text{Restr}}{\mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}) \doteq \mathsf{eq}(\{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}})}\;\text{FA}$$

And finally we prove the right premise $\mathsf{eq}(\{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}$:

$$\dfrac{\dfrac{\dfrac{}{\mathsf{eq}(0,1) \doteq \mathsf{false}}\;\neq\text{-Const} \qquad \dfrac{}{\mathsf{len}(0) \neq 0} \qquad \mathsf{len}(u) \neq 0}{\mathsf{eq}(0^{\mathsf{len}(u)}, 1^{\mathsf{len}(v)}) \doteq \mathsf{false}}\;\text{l-neq}}{\mathsf{eq}(\{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n}'_\mathsf{e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}}\;\mathsf{EQInj}(\{\cdot\}^{-}_{-}) + R$$

■

C.3 Trace Functions

We introduce some useful trace functions.

Definition 39. We define some functions on action traces:

- Given an action trace τ, we let $\prec_\tau$ be the restriction of $\prec$ to the set of strict prefixes of τ, i.e. $\tau_2 \prec_\tau \tau_1$ iff $\tau_2 \prec \tau_1$ and $\tau_1 \prec \tau$.
- We extend $\prec_\tau$ to symbolic actions as follows: we have $\mathsf{ai} \prec_\tau \tau_1$ (resp. $\tau_1 \prec_\tau \mathsf{ai}$) iff there exists τ_2 such that $\mathsf{h}(\tau_2) = \mathsf{ai}$ and $\tau_2 \prec_\tau \tau_1$ (resp. $\tau_1 \prec_\tau \tau_2$).

Definition 40. Given a basic trace τ and a basic identity $\textsc{id} = \mathrm{A}_{i,0}$, we let $\nu_\tau(\textsc{id})$ be the identity $\mathrm{A}_{i,l}$ where l is the number of occurrences of $\textsc{ns}_{\textsc{id}}(\_)$ in τ.

C.4 Ghost Variable

To show that the AKA^+_N protocol is σ_{ul}-unlinkable, we need to know, for every identity $\textsc{id} \in \mathcal{S}_{\text{id}}$, if there was a successful $\textsc{supi}$ session since the last $\textsc{ns}_{\textsc{id}}(\_)$. To do this, we extend the set of variables Vars_σ by adding a ghost variable $\text{sync}^{\textsc{id}}_{\textsc{u}}$ for every $\textsc{id} \in \mathcal{S}_{\text{id}}$. We also extend the symbolic state updates of $\textsc{ns}_{\textsc{id}}(\_)$ and $\textsc{pu}_{\textsc{id}}(j, 2)$ as follows:

- For $\text{ai} = \textsc{ns}_{\textsc{id}}(j)$:

$$\sigma^{\text{up}}_\tau \equiv \begin{cases} \text{valid-guti}^{\textsc{id}}_{\textsc{u}} \mapsto \text{false} \\ \text{sync}^{\textsc{id}}_{\textsc{u}} \mapsto \text{false} \end{cases}$$

- For $\text{ai} = \textsc{pu}_{\textsc{id}}(j, 2)$:

$$\sigma^{\text{up}}_\tau \equiv \begin{cases} \text{e-auth}^{\textsc{id}}_{\textsc{u}} \mapsto \text{if accept}^{\textsc{id}}_\tau \text{ then } \sigma^{\text{in}}_\tau(\text{b-auth}^{\textsc{id}}_{\textsc{u}}) \text{ else fail} \\ \text{sync}^{\textsc{id}}_{\textsc{u}} \mapsto \sigma^{\text{in}}_\tau(\text{sync}^{\textsc{id}}_{\textsc{u}}) \vee \text{accept}^{\textsc{id}}_\tau \end{cases}$$

Remark that the variable $\text{sync}^{\textsc{id}}_{\textsc{u}}$ is read only to update its value. It is not used in the actual protocol. By consequence, the AKA^+_N protocol is σ_{ul}-unlinkable if and only if the extended AKA^+_N protocol is σ_{ul}-unlinkable. We extend the initial symbolic state σ_ϵ by adding $\sigma_\epsilon(\text{sync}^{\textsc{id}}_{\textsc{u}}) \equiv \text{false}$.

D MUTUAL AUTHENTICATION OF THE AKA$^+$ PROTOCOL

We now prove that the AKA$^+$ protocol provides mutual authentication. This section is organized as follows: we state some useful properties and necessary acceptance conditions in Section D.1 (we postpone the proofs of the necessary acceptance conditions to Section D.5); then, we prove authentication of the user by the network in Section D.2, and authentication of the network by the user in Section D.3; finally, we prove that we actually have *injective* authentication of the network by the user in Section D.4.

D.1 Invariants and Necessary Acceptance Conditions

We start by proving some properties of the AKA$^+$ protocol. First, we show that the sequence numbers are always of the same length. This is an easy consequence of the length axioms.

Proposition 20. *For every valid action traces τ, τ' on $\mathcal{S}_{id}$, $\textsc{id}_1, \textsc{id}_2 \in \mathcal{S}_{id}$ and $n \in \mathcal{N}$:*

$$len(\sigma^{in}_\tau(\textsc{sqn}^{\textsc{id}_1}_U)) = len(\sigma^{in}_\tau(\textsc{sqn}^{\textsc{id}_2}_U)) \qquad len(\sigma^{in}_\tau(\textsc{sqn}^{\textsc{id}_1}_U)) = len(\sigma^{in}_{\tau'}(\textsc{sqn}^{\textsc{id}_1}_U))$$

$$len(\sigma^{in}_\tau(\textsc{sqn}^{\textsc{id}_1}_U)) = len(n)$$

Proof. We show only the first equality, as the proofs of the other two equalities are similar. First, we prove by induction over τ that for every $\textsc{id} \in \mathcal{S}_{\text{id}}$, there exists an if-context C, terms $\vec{b}$ and integers $(k_i)_i$ such that:

$$\sigma^{\text{in}}_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) = C[\vec{b} \diamond (\text{suc}^{k_i}(\text{sqn-init}^{\textsc{id}}_{\textsc{u}}))_i)]$$

Therefore, let $C_1, C_2, \vec{b}_1, \vec{b}_2$ and $(k^1_i)_i$, $(k^2_j)_j$ be such that:

$$\sigma^{\text{in}}_\tau(\textsc{sqn}^{\textsc{id}_1}_{\textsc{u}}) = C_1[\vec{b}_1 \diamond (\text{suc}^{k^1_i}(\text{sqn-init}^{\textsc{id}_1}_{\textsc{u}}))_i] \qquad \sigma^{\text{in}}_\tau(\textsc{sqn}^{\textsc{id}_2}_{\textsc{u}})) = C_2[\vec{b}_2 \diamond (\text{suc}^{k^2_j}(\text{sqn-init}^{\textsc{id}_2}_{\textsc{u}}))_j]$$

Using the axioms in Ax_{len}, we show that for every i, i', j, j':

$$\text{len}(\text{suc}^{k^1_i}(\text{sqn-init}^{\textsc{id}_1}_{\textsc{u}})) = \text{len}(\text{suc}^{k^1_{i'}}(\text{sqn-init}^{\textsc{id}_1}_{\textsc{u}})) = \text{len}(\text{suc}^{k^2_j}(\text{sqn-init}^{\textsc{id}_2}_{\textsc{u}})) = \text{len}(\text{suc}^{k^2_{j'}}(\text{sqn-init}^{\textsc{id}_2}_{\textsc{u}}))$$

Therefore, using R we have a derivation of:

$$\text{len}(\sigma^{\text{in}}_\tau(\textsc{sqn}^{\textsc{id}_1}_{\textsc{u}})) = \text{len}(\sigma^{\text{in}}_\tau(\textsc{sqn}^{\textsc{id}_2}_{\textsc{u}}))$$ ■

The following proposition states that $\mathsf{n_N}$ appears only in the *HN* public key $\mathsf{pk}(\mathsf{n_N})$ and secret key $\mathsf{sk}(\mathsf{n_N})$, and that for every $\textsc{id} \in \mathcal{S}_{\mathrm{id}}$, the keys k^{ID} and $\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}$ appear only in key position in Mac^1– Mac^5. These properties will be useful to apply the cryptographic axioms later.

Proposition 21 (Invariant (inv-key)). *For all valid action trace τ on $\mathcal{S}_{id} = \{\textsc{id}_1, \dots, \textsc{id}_N\}$, we have:*

$$\begin{aligned} & n_N \sqsubseteq_{pk(\cdot),sk(\cdot)} \phi_\tau \ \wedge\ sk(n_N) \sqsubseteq_{dec(\_,\cdot)} \phi_\tau \\ \forall 1 \le i \le N, \quad & k_m^{ID_i} \sqsubseteq_{Mac^{\cdot}_{\cdot}(\_)} \phi_\tau \\ \forall 1 \le i \le N, \quad & k^{ID_i} \sqsubseteq_{f_{\cdot}(\_), f^{r}_{\cdot}(\_)} \phi_\tau \end{aligned}$$

Proof. The proof is straightforward by induction on τ. ■

The following proposition states that if a user $\textsc{id}$ has no valid temporary identity at instant τ_2 (i.e. $\sigma_{\tau_2}(\textsc{guti}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{UnSet}$), and if every assign-guti sub-protocol session run by $\textsc{id}$ between the instants τ_2 and τ_i failed (i.e. for every $\tau_1 = \_, \textsc{fu}_{\mathrm{ID}}(j_1)$ such that $\tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i$, we have $\neg\mathsf{accept}^{\mathrm{ID}}_{\tau_1}$), then $\textsc{id}$ does not have a valid temporary identity at instant τ_i (i.e. $\sigma^{\mathsf{in}}_{\tau_i}(\textsc{guti}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{UnSet}$). Formally:

Proposition 22. *For every valid action trace τ on $\mathcal{S}_{id}$, for every $\tau_2 \prec_\tau \tau_i$ and $\textsc{id} \in \mathcal{S}_{id}$, we have:*

$$\sigma_{\tau_2}(GUTI^{ID}_U) = UnSet \wedge \bigwedge_{\substack{\tau_1 = \_, \textsc{fu}_{ID}(j_1) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i}} \neg\mathsf{accept}^{ID}_{\tau_1} \rightarrow \sigma^{in}_{\tau_i}(GUTI^{ID}_U) = UnSet$$

Proof. The proof is straightforward by induction on τ_i. ■

We let session be the (partial) function mapping an action label ai to its network session number j.

Definition 41. We define the partial session function:

$$\mathsf{session}(\mathsf{ai}) = j \text{ when } \mathsf{ai} = \textsc{x}(j, \_) \text{ where } \textsc{x} \in \{\textsc{pn}, \textsc{tn}, \textsc{fn}\}$$

We let $\text{s-started}_j(\tau)$ be the predicate holding exactly on action traces where the j-th session of the network started, i.e. where $\mathsf{session}(\mathsf{ai}) = j$ for some ai appearing in τ.

Definition 42. For every action trace τ, we let $\text{s-started}_j(\tau)$ be true if and only if there exists $\mathsf{ai} \in \tau$ such that $\mathsf{session}(\mathsf{ai}) = j$.

We now describe some properties of AKA$^+$. They are formally defined and shown after.

- The property **(A1)** states that the *HN* challenge n^j cannot appear in the frame ϕ_τ if the session j has not started yet. Formally, if $\neg\text{s-started}_j(\tau)$ then $n^j \notin \mathsf{st}(\phi_\tau)$.
- The properties **(A2)** and **(A3)** give conditions under which some user sequence number has changed.
- **(A4)** expresses the fact that two different users $\textsc{id}_1, \textsc{id}_2$ can never have the same temporary identities on the server side. This is intuitive, as the server samples temporary identities uniformly at random, and should never assign the same identity to two different users.
- **(A5)**, **(A6)** and **(A7)** state that if the network accepts a message, then there is no ambiguity on the sender. That is, for every $\textsc{id}_0 \neq \textsc{id}_1$, we cannot have $\mathsf{accept}^{\mathrm{ID}_0}_\tau$ and $\mathsf{accept}^{\mathrm{ID}_1}_\tau$ simultaneously.
- Finally, **(A8)** says that if the user $\textsc{id}$ believes he authenticated the session j of the network (i.e. $\sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^j$), then it must have received the challenge n^j when he started his current session (i.e. $\sigma^{\mathsf{in}}_\tau(\mathsf{b\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^j$).

Proposition 23. *Let $\tau = \_, ai$ be a valid action trace on $\mathcal{S}_{id}$, then:*

(1) ***(A1)*** *If $\neg$s-started$_j(\tau)$ then $n^j \notin st(\phi_\tau)$.*

(2) **(A2)** *For all* $\tau_0 = \_, \textsc{pu}_{\textsc{id}}(j_0, 2) \leq \tau$ *and* $\tau_1 = \_, \textsc{pu}_{\textsc{id}}(j_1, 2) \leq \tau$, *if* $\tau_0 \neq \tau_1$ *then:*

$$\sigma^{in}_{\tau_0}(\textsc{sqn}^{ID}_U) \neq \sigma^{in}_{\tau_1}(\textsc{sqn}^{ID}_U)$$

(3) **(A3)** *For every* $\tau_0 = \_, \textsc{pu}_{\textsc{id}}(j_0, 2)$, $\tau_1 = \_, \textsc{pu}_{\textsc{id}}(j_1, 1)$ *such that* $\tau_1 \prec_\tau \tau_0$, *if* $j_0 \neq j_1$ *then:*

$$\sigma^{in}_{\tau_0}(\textsc{sqn}^{ID}_U) \neq suc(\sigma^{in}_{\tau_1}(\textsc{sqn}^{ID}_U))$$

(4) **(A4)** *For every* $\textsc{id}_0, \textsc{id}_1 \in \mathcal{S}_{id}$ *such that* $\textsc{id}_0 \neq \textsc{id}_1$*:*

$$\left(\sigma^{in}_\tau(\textsc{guti}^{ID_0}_N) \neq UnSet \wedge \sigma^{in}_\tau(\textsc{guti}^{ID_1}_N) \neq UnSet\right) \rightarrow \sigma^{in}_\tau(\textsc{guti}^{ID_0}_N) \neq \sigma^{in}_\tau(\textsc{guti}^{ID_1}_N)$$

(5) **(A5)**, **(A6)**, **(A7)** *If* $ai = \textsc{pn}(j, 1)$, $\textsc{tn}(j, 0)$ *or* $\textsc{tn}(j, 1)$, *then for every* $\textsc{id}_0 \neq \textsc{id}_1$,

$$\left(\neg\mathrm{accept}^{ID_0}_\tau\right) \vee \left(\neg\mathrm{accept}^{ID_1}_\tau\right)$$

(6) **(A8)** *For every* $\textsc{id} \in \mathcal{S}_{id}, j \in \mathbb{N}$, $\sigma^{in}_\tau(e\text{-}auth^{ID}_U) = n^j \rightarrow \sigma^{in}_\tau(b\text{-}auth^{ID}_U) = n^j$.

Proof. All these properties are simple to show:

- **(A1)** is trivial by induction over τ.
- **(A2)** and **(A3)** both follow from the fact that if $\tau = \_, \textsc{pu}_{\textsc{id}}(j, 1)$ then $\sigma_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) \equiv \mathrm{suc}(\sigma^{\mathrm{in}}_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))$, and therefore $\sigma_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) > \sigma^{\mathrm{in}}_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$.
- **(A5)** and **(A7)** follow easily from the unforgeability axioms EUF-MAC, and the collision resistance axioms $\textsc{cr-key}_{\neq}$.
- To prove **(A4)**, we first observe that for every $\textsc{id} \in \mathcal{S}_{\mathrm{id}}$, we initially have $\sigma_\epsilon(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) \equiv \mathrm{UnSet}$, and that the only value we store in $\textsc{guti}^{\textsc{id}}_{\textsc{n}}$ are UnSet or $\textsc{guti}^i$ for some $i \in \mathbb{N}$. Therefore it is easy to show that for every $\tau_n \prec \tau$:
$$\sigma^{\mathrm{in}}_{\tau_n}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) \neq \mathrm{UnSet} \rightarrow \bigvee_{i \in \mathcal{S}} \sigma^{\mathrm{in}}_{\tau_n}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) = \textsc{guti}^i$$
where $\mathcal{S} \subseteq \mathbb{N}$ is the set of network session number appearing in τ. Moreover, we can only store $\textsc{guti}^i$ in $\textsc{guti}^{\textsc{id}}_{\textsc{n}}$ at $\textsc{pn}(i, 1)$ or $\textsc{tn}(i, 1)$, and by validity τ cannot contain both $\textsc{pn}(i, 1)$ and $\textsc{tn}(i, 1)$. We conclude observing that we cannot have $\mathrm{accept}^{\textsc{id}_0}_{\tau_n}$ and $\mathrm{accept}^{\textsc{id}_1}_{\tau_n}$ if $\tau_n = \_, \textsc{pn}(i, 1)$ or $\_, \textsc{tn}(i, 1)$ using **(A5)** and **(A7)**. The result follows.
- **(A6)** is a consequence of **(A4)**.
- **(A8)** follows from the fact that whenever a new session of the protocol is started, we reset both $\text{b-auth}^{\textsc{id}}_{\textsc{u}}$ and $\text{e-auth}^{\textsc{id}}_{\textsc{u}}$. Then $\text{e-auth}^{\textsc{id}}_{\textsc{u}}$ is either set to fail or to $\text{b-auth}^{\textsc{id}}_{\textsc{u}}$. ■

We can now state and prove our first necessary acceptance conditions.

Lemma 6. *Let* $\tau = \_, ai$ *be a valid action trace on* $\mathcal{S}_{id}$, *then:*

(1) **(Acc1)** *If* $ai = \textsc{pn}(j, 1)$, *then for every* $\textsc{id} \in \mathcal{S}_{id}$*:*

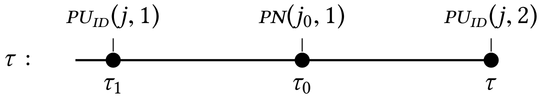
$$\mathrm{accept}^{ID}_\tau \rightarrow \bigvee_{\tau_0 = \_, \textsc{pu}_{\textsc{id}}(j_0, 1) \prec \tau} \left(\pi_1(g(\phi^{in}_\tau)) = \{\left\langle \textsc{id}, \sigma^{in}_{\tau_0}(\textsc{sqn}^{ID}_U)\right\rangle\}^{n^{j_0}_e}_{pk_N} \wedge g(\phi^{in}_{\tau_0}) = n^j\right)$$

(2) **(Acc2)** *If* $ai = \textsc{pu}_{\textsc{id}}(j, 2)$. *Let* $\tau_1 = \_, \textsc{pu}_{\textsc{id}}(j, 1) \prec \tau$. *Then:*

$$\mathrm{accept}^{ID}_\tau \rightarrow \bigvee_{\substack{\tau_0 = \_, \textsc{pn}(j_0, 1) \\ \tau_1 \prec_\tau \tau_0}} \mathrm{accept}^{ID}_{\tau_0} \wedge g(\phi^{in}_{\tau_1}) = n^{j_0} \wedge \pi_1(g(\phi^{in}_{\tau_0})) = \{\langle \textsc{id}, \sigma^{in}_{\tau_1}(\textsc{sqn}^{ID}_U)\rangle\}^{n^j_e}_{pk_N}$$

To help the reader, we graphically represents how the instants τ_1, τ_0 *and* τ *are situated:*[7]

[7] We will often use such pictures in this paper. They are particularly useful when more than two instants are being considered simultaneously. Some conventions: the horizontal line represents the action trace whose name is on the left, before the semi-column (e.g. "τ :" here); instants are represented in their order of appearance at the bottom of the horizontal line; at the top of the line, we indicate (when it is known) the last action of an instant (e.g. here τ_1 ends by $\textsc{pu}_{\textsc{id}}(j, 1)$).



(3) ***(Acc3)*** *If* $ai = \mathrm{TU}_{ID}(j,1)$ *then:*

$$\mathrm{accept}^{ID}_{\tau} \rightarrow \bigvee_{\substack{\tau_0=\_,\mathrm{TN}(j_0,0)\\ \tau_0<\tau}} \left(\begin{array}{l}\mathrm{accept}^{ID}_{\tau_0} \wedge \pi_1(g(\phi^{in}_{\tau})) = n^{j_0} \wedge \pi_2(g(\phi^{in}_{\tau})) = \sigma^{in}_{\tau_0}(\mathrm{SQN}^{ID}_{N}) \oplus f_k(n^{j_0})\\ \wedge\ \sigma^{in}_{\tau}(\mathrm{GUTI}^{ID}_{U}) = \sigma^{in}_{\tau_0}(\mathrm{GUTI}^{ID}_{N})\end{array}\right)$$

(4) ***(Acc4)*** *If* $ai = \mathrm{TN}(j,1)$ *then:*

$$\mathrm{accept}^{ID}_{\tau} \rightarrow \bigvee_{\tau_0=\_,\mathrm{TU}_{ID}(\_,1)<\tau} \mathrm{accept}^{ID}_{\tau_0} \wedge \pi_1(g(\phi^{in}_{\tau_0})) = n^j$$

Proof. The proof of this lemma is given later, in Section D.5. ■

D.2 Authentication of the User by the Network

We now prove that the AKA$^+$ protocol provides authentication of the user by the network. Remark that the lemma below subsumes Lemma 1.

Lemma 7. *For every valid action trace τ on $\mathcal{S}_{id}$, the AKA$^+$ protocol provides authentication of the user by the network:*

$$\forall\, \mathrm{ID} \in \mathcal{S}_{id}, j \in \mathbb{N},\quad \sigma_{\tau}(e\text{-}auth^{j}_{N}) = \mathrm{ID} \rightarrow \bigvee_{\tau' \preceq \tau} \sigma_{\tau'}(b\text{-}auth^{ID}_{U}) = n^j$$

Moreover, if $\tau = \_, \mathrm{TN}(j,1)$ then:

$$\mathrm{accept}^{ID}_{\tau} \rightarrow \bigvee_{\tau_0=\_,\mathrm{TU}_{ID}(\_,1)<\tau} \sigma_{\tau_0}(b\text{-}auth^{ID}_{U}) = n^j$$

Proof. We prove this by induction on τ. First, for $\tau = \epsilon$ we have that for every $\mathrm{ID} \in \mathcal{S}_{\mathrm{id}}$, $\sigma_{\tau}(\text{e-auth}^{j}_{\mathrm{N}}) \equiv \text{fail} \neq \mathrm{ID}$ by axiom $\neq$-Const. Therefore the property holds.

Let $\tau = \_, \text{ai}$. Let $j \in \mathbb{N}$ be a session number. Remark that if $\sigma^{\text{up}}_{\tau}(\text{e-auth}^{j}_{\mathrm{N}}) = \bot$, and if the authentication property holds just before the instant τ, i.e.:

$$\forall \mathrm{ID} \in \mathcal{S}_{\mathrm{id}},\quad \sigma^{\text{in}}_{\tau}(\text{e-auth}^{j}_{\mathrm{N}}) = \mathrm{ID} \rightarrow \bigvee_{\tau'<\tau} \sigma^{\text{in}}_{\tau'}(\text{b-auth}^{\mathrm{ID}}_{\mathrm{U}}) = \text{n}^j$$

then the authentication property for j holds at instant τ. Therefore we only need to consider the action labels $\text{ai} = \mathrm{PN}(j,1)$ and $\text{ai} = \mathrm{TN}(j,1)$.

- **Case ai** $=$ $\mathbf{PN}(j,1)$**:** Let $\mathrm{ID} \in \mathcal{S}_{\mathrm{id}}$. Using $\neq$-Const, we get that $\sigma_{\tau}(\text{e-auth}^{j}_{\mathrm{N}}) = \mathrm{ID} \rightarrow \text{accept}^{\mathrm{ID}}_{\tau}$. Using **(Acc1)** of Proposition 23, we deduce that:

$$\sigma_{\tau}(\text{e-auth}^{j}_{\mathrm{N}}) = \mathrm{ID} \rightarrow \bigvee_{\tau_0=\_,\mathrm{PU}_{\mathrm{ID}}(j_0,1)<\tau} g(\phi^{\text{in}}_{\tau_0}) = \text{n}^j \tag{15}$$

By validity of τ, there exists τ_2 such that $\tau_2 = \_, \mathrm{PN}(j,0) \prec \tau$. Let $\tau_0 \prec_{\tau} \tau_2$, we have $\neg\text{s-started}_j(\tau_0)$. Using **(A1)**, we get that $n^j \not\in \text{st}(\phi^{\text{in}}_{\tau_0})$. It follows from axiom $=$-ind that $g(\phi^{\text{in}}_{\tau_0}) \neq \text{n}^j$. Hence:

$$\bigvee_{\tau_0=\_,\mathrm{PU}_{\mathrm{ID}}(j_0,1)<\tau} g(\phi^{\text{in}}_{\tau_0}) = \text{n}^j \quad\leftrightarrow\quad \bigvee_{\substack{\tau_0=\_,\mathrm{PU}_{\mathrm{ID}}(j_0,1)\\ \tau_2<_{\tau}\tau_0<\tau}} g(\phi^{\text{in}}_{\tau_0}) = \text{n}^j \tag{16}$$

Let τ_0 be such that $\tau_2 \prec_\tau \tau_0 \prec \tau$ and $\tau_0 = \_, \textsc{pu}_{\textsc{id}}(j_0, 1)$. Since $\sigma_{\tau_0}(\mathsf{b\text{-}auth}^{\textsc{id}}_{\textsc{u}}) \equiv g(\phi^{\mathsf{in}}_{\tau_0})$, we have:

$$g(\phi^{\mathsf{in}}_{\tau_0}) = \mathsf{n}^j \rightarrow \sigma_{\tau_0}(\mathsf{b\text{-}auth}^{\textsc{id}}_{\textsc{u}}) = \mathsf{n}^j$$

Hence putting (15) and (16) together, we get:

$$\sigma_\tau(\mathsf{e\text{-}auth}^{j}_{\textsc{n}}) = \textsc{id} \;\rightarrow \bigvee_{\substack{\tau_0 = \_, \textsc{pu}_{\textsc{id}}(j_0, 1) \\ \tau_2 \prec_\tau \tau_0 \prec \tau}} \sigma_{\tau_0}(\mathsf{b\text{-}auth}^{\textsc{id}}_{\textsc{u}}) = \mathsf{n}^j$$

Since $\{\tau_0 \mid \tau_0 = \_, \textsc{pu}_{\textsc{id}}(j_0, 1) \wedge \tau_2 \prec_\tau \tau_0 \prec \tau\}$ is a subset of $\{\tau_0 \mid \tau_0 \preceq \tau\}$, we deduce that:

$$\sigma_\tau(\mathsf{e\text{-}auth}^{j}_{\textsc{n}}) = \textsc{id} \;\rightarrow\; \rightarrow \bigvee_{\tau_0 \preceq \tau} \sigma^{\mathsf{in}}_{\tau_0}(\mathsf{b\text{-}auth}^{\textsc{id}}_{\textsc{u}}) = \mathsf{n}^j$$

- **Case ai** $=$ $\textsc{tn}(j, 1)$**:** This case is similar to the previous one. First, we check that $\neq$-Const implies that $\sigma_\tau(\mathsf{e\text{-}auth}^{j}_{\textsc{n}}) = \textsc{id} \rightarrow \mathsf{accept}^{\textsc{id}}_\tau$. Moreover, using **(Acc4)**, we know that:

$$\mathsf{accept}^{\textsc{id}}_\tau \;\rightarrow \bigvee_{\tau_0 = \_, \textsc{tu}_{\textsc{id}}(\_, 1) \prec \tau} \mathsf{accept}_{\tau_0} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \mathsf{n}^j$$

Moreover, for every $\tau_0 = \_, \textsc{tu}_{\textsc{id}}(\_, 1) \prec \tau$, we have:

$$\mathsf{accept}^{\textsc{id}}_{\tau_0} \;\wedge\; \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \mathsf{n}^j \;\rightarrow\; \sigma_{\tau_0}(\mathsf{b\text{-}auth}^{\textsc{id}}_{\textsc{u}}) = \mathsf{n}^j$$

Hence:

$$\begin{aligned}
\mathsf{accept}^{\textsc{id}}_\tau \;&\rightarrow \bigvee_{\tau_0 = \_, \textsc{tu}_{\textsc{id}}(\_, 1) \prec \tau} \mathsf{accept}_{\tau_0} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \mathsf{n}^j \\
&\rightarrow \bigvee_{\tau_0 = \_, \textsc{tu}_{\textsc{id}}(\_, 1) \prec \tau} \sigma_{\tau_0}(\mathsf{b\text{-}auth}^{\textsc{id}}_{\textsc{u}}) = \mathsf{n}^j \\
&\rightarrow \bigvee_{\tau_0 \preceq \tau} \sigma^{\mathsf{in}}_{\tau_0}(\mathsf{b\text{-}auth}^{\textsc{id}}_{\textsc{u}}) = \mathsf{n}^j
\end{aligned}$$

■

D.3 Authentication of the Network by the User

We prove that the AKA$^+$ protocols provides authentication of the network by the user. We actually prove the stronger result that for any valid action trace τ, if the authentication of $UE_{\textsc{id}}$ succeeded at instant τ (i.e. $\sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\textsc{id}}_{\textsc{u}}) \neq \mathsf{fail}$), then there exists some $j \in \mathbb{N}$ such that $UE_{\textsc{id}}$ authenticated $HN(j)$.

Lemma 8. *For all valid action trace τ on $\mathcal{S}_{id}$, the AKA$^+$ protocol provides authentication of the network by the user. Formally, for every* $\textsc{id} \in \mathcal{S}_{id}$ *and* $j \in \mathbb{N}$*, we let:*

$$\textit{suc-auth}_\tau(\textsc{id}) \equiv \sigma_\tau(\textit{e-auth}^{ID}_{U}) \neq \textit{fail} \qquad \textit{auth}_\tau(\textsc{id}, j) \equiv \sigma_\tau(\textit{b-auth}^{j}_{N}) = \textsc{id} \wedge n^j = \sigma_\tau(\textit{e-auth}^{ID}_{U})$$

Then:

$$\forall \textsc{id} \in \mathcal{S}_{id}, \;\; \textit{suc-auth}_\tau(\textsc{id}) \;\rightarrow\; \bigvee\nolimits_{\textit{s-started}_j(\tau)} \textit{auth}_\tau(\textsc{id}, j)$$

Proof. We prove this by induction on τ. First, for $\tau = \epsilon$ we have that for every $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$, $\sigma_\tau(\mathsf{e\text{-}auth}^{\textsc{id}}_{\textsc{u}}) \equiv \mathsf{fail}$. Therefore the property holds. Let $\tau = \tau_0, \mathsf{ai}$, and assume by induction that:

$$\forall\, \textsc{id} \in \mathcal{S}_{\mathsf{id}}, \;\; \mathsf{suc\text{-}auth}_{\tau_0}(\textsc{id}) \;\rightarrow\; \bigvee\nolimits_{\mathsf{s\text{-}started}_j(\tau_0)} \mathsf{auth}_{\tau_0}(\textsc{id}, j)$$

If for every j_0 and $\textsc{id}$ we have:

$$\sigma^{\mathsf{up}}_\tau(\mathsf{b\text{-}auth}^{j_0}_{\textsc{n}}) = \bot \qquad\qquad \sigma^{\mathsf{up}}_\tau(\mathsf{e\text{-}auth}^{\textsc{id}}_{\textsc{u}}) = \bot$$

then, by induction hypothesis, we have authentication of the network by the user at τ. Therefore it only remains to show that authentication holds for τ in the cases where ai is equal to $\textsc{pn}(j, 1)$, $\textsc{pu}_{\textsc{id}}(j, 1)$, $\textsc{pu}_{\textsc{id}}(j, 2)$, $\textsc{tu}_{\textsc{id}}(j, 0)$, $\textsc{tn}(j, 0)$ or $\textsc{tu}_{\textsc{id}}(j, 1)$.

Before starting the case disjunction, remark that if we can prove that for every $\textsc{id}_0 \in \mathcal{S}_{\mathsf{id}}$ and $j_0 \in \mathbb{N}$:

$$(\mathsf{suc\text{-}auth}_\tau(\textsc{id}_0) \ \wedge\ \mathsf{auth}_\tau(\textsc{id}_0, j_0)) \ \leftrightarrow\ (\mathsf{suc\text{-}auth}_{\tau_0}(\textsc{id}_0) \ \wedge\ \mathsf{auth}_{\tau_0}(\textsc{id}_0, j_0)) \tag{17}$$

Then we can directly conclude by applying the induction hypothesis. We now do a case disjunction on ai.

- **Cases ai** $=$ $\textbf{PU}_{\textbf{ID}}(j, 1)$ **and ai** $=$ $\textbf{TU}_{\textbf{ID}}(j, 0)$**.** In both cases, we have $\sigma_\tau(\mathsf{e\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \mathsf{fail}$, and therefore the property trivially holds for $\textsc{id}$. Besides, for every $\textsc{id}_0 \neq \textsc{id}$ and $j_0 \in \mathbb{N}$, (17) holds.
- **Case ai** $=$ $\textbf{TU}_{\textbf{ID}}(j, 1)$**.** For all $\textsc{id}_0 \neq \textsc{id}$ and for all $j_0 \in \mathbb{N}$, we easily check that (17) holds. It only remains to show that:

$$\mathsf{suc\text{-}auth}_\tau(\textsc{id}) \ \rightarrow\ \bigvee\nolimits_{\mathsf{s\text{-}started}_i(\tau)} \mathsf{auth}_\tau(\textsc{id}, i)$$

Let $\mathsf{k} \equiv \mathsf{k}^{\mathrm{ID}}$. We observe that:

$$\begin{aligned}
\mathsf{suc\text{-}auth}_\tau(\textsc{id}) \ &\rightarrow\ \sigma_\tau(\mathsf{e\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) \neq \mathsf{fail}\\
&\rightarrow\ \mathsf{accept}_\tau^{\mathrm{ID}}\\
&\rightarrow \bigvee_{\tau_0 = \_, \textsc{tn}(j_0, 0) \prec \tau} \begin{pmatrix} \mathsf{accept}_{\tau_0}^{\mathrm{ID}} \ \wedge\ \pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0} \ \wedge \\ \pi_2(g(\phi_\tau^{\mathsf{in}})) = \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \oplus \mathsf{f}_{\mathsf{k}}(\mathsf{n}^{j_0}) \end{pmatrix} && \text{(by } \textbf{(Acc3)}\text{)}
\end{aligned}$$

Let $\tau_0 = \textsc{tn}(j_0, 0)$ such that $\tau_0 \prec_\tau \tau$. Then:

$$\pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0} \wedge \mathsf{accept}_\tau^{\mathrm{ID}} \ \rightarrow\ \sigma_\tau(\mathsf{e\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{n}^{j_0}$$

Moreover using **(A7)** we know that $\mathsf{accept}_{\tau_0}^{\mathrm{ID}} \rightarrow \sigma_{\tau_0}(\mathsf{b\text{-}auth}_{\mathrm{N}}^{j_0}) = \textsc{id}$. Using the validity of τ, we can easily show that for all $\tau_0 \prec \tau' \preceq \tau$ we have $\sigma_{\tau'}^{\mathsf{up}}(\mathsf{b\text{-}auth}_{\mathrm{N}}^{j_0}) \equiv \bot$. We deduce that $\mathsf{accept}_{\tau_0}^{\mathrm{ID}} \rightarrow \sigma_\tau(\mathsf{b\text{-}auth}_{\mathrm{N}}^{j_0}) = \textsc{id}$. Hence:

$$\mathsf{suc\text{-}auth}_\tau(\textsc{id}) \ \rightarrow \bigvee_{\tau_0 = \_, \textsc{tn}(j_0, 0) \prec \tau} \mathsf{auth}_\tau(\textsc{id}, j_0) \ \rightarrow \bigvee_{\mathsf{s\text{-}started}_{j_0}(\tau)} \mathsf{auth}_\tau(\textsc{id}, j_0)$$

- **Case ai** $=$ $\textbf{PU}_{\textbf{ID}}(j, 2)$**.** For all $\textsc{id}_0 \neq \textsc{id}$ and for all $j_0 \in \mathbb{N}$, we check that (17) holds. It remains to prove that:

$$\mathsf{suc\text{-}auth}_\tau(\textsc{id}) \ \rightarrow\ \bigvee\nolimits_{\mathsf{s\text{-}started}_j(\tau)} \mathsf{auth}_\tau(\textsc{id}, j)$$

First, we observe that:

$$\begin{aligned}
\mathsf{suc\text{-}auth}_\tau(\textsc{id}) \ &\rightarrow\ \mathsf{accept}_\tau^{\mathrm{ID}}\\
&\rightarrow \bigvee_{\substack{\tau_0 = \_, \textsc{pn}(j_0, 1)\\ \tau_1 = \_, \textsc{pu}_{\mathrm{ID}}(j, 1)\\ \tau_1 \prec_\tau \tau_0}} \begin{pmatrix} \mathsf{accept}_{\tau_0}^{\mathrm{ID}} \ \wedge\ g(\phi_{\tau_1}^{\mathsf{in}}) = \mathsf{n}^{j_0} \ \wedge \\ \pi_1(g(\phi_{\tau_0}^{\mathsf{in}})) = \{\langle \textsc{id}\ ,\ \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}} \end{pmatrix} && \text{(by } \textbf{(Acc2)}\text{)}
\end{aligned}$$

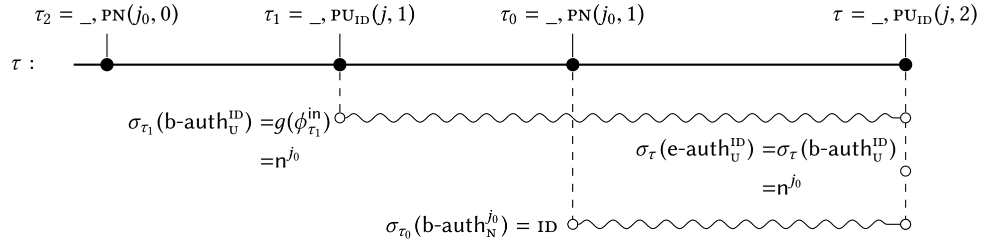
Let $\tau_0 = \_, \textsc{pn}(j_0, 1)$, $\tau_1 = \_, \textsc{pu}_{\mathrm{ID}}(j, 1)$ such that $\tau_1 \prec_\tau \tau_0$. Let $\tau_2 = \_, \textsc{pn}(j_0, 0)$, by validity of τ we know that $\tau_2 \prec_\tau \tau_0$. Moreover, if $\tau_1 \prec_\tau \tau_2$ then by **(A1)** we have $\mathsf{n}^{j_0} \not\in \mathsf{st}(\phi_{\tau_1}^{\mathsf{in}})$, and therefore using $=$-ind we obtain that $g(\phi_{\tau_1}^{\mathsf{in}}) \neq \mathsf{n}^{j_0}$. Hence:

$$\mathsf{suc\text{-}auth}_\tau(\textsc{id}) \ \rightarrow \bigvee_{\substack{\tau_0 = \_, \textsc{pn}(j_0, 1)\\ \tau_1 = \_, \textsc{pu}_{\mathrm{ID}}(j, 1)\\ \tau_2 = \_, \textsc{pn}(j_0, 0)\\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_0}} \overbrace{\mathsf{accept}_\tau^{\mathrm{ID}} \wedge \mathsf{accept}_{\tau_0}^{\mathrm{ID}} \wedge g(\phi_{\tau_1}^{\mathsf{in}}) = \mathsf{n}^{j_0} \wedge \pi_1(g(\phi_{\tau_0}^{\mathsf{in}})) = \{\langle \textsc{id}\ ,\ \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}}}^{\psi_{\tau_2, \tau_0}^{\tau_1}}$$

We know that $g(\phi^{\mathsf{in}}_{\tau_1}) = \mathsf{n}^{j_0} \rightarrow \sigma_{\tau_1}(\text{b-auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j_0}$, and that:

$$\text{accept}^{\text{ID}}_{\tau_0} \;\rightarrow\; \sigma_{\tau_0}(\text{b-auth}^{j_0}_{\text{N}}) = \text{ID} \qquad\qquad \text{accept}^{\text{ID}}_{\tau} \;\rightarrow\; \sigma_{\tau}(\text{e-auth}^{\text{ID}}_{\text{U}}) = \sigma_{\tau}(\text{b-auth}^{\text{ID}}_{\text{U}})$$

We represent graphically all the information we have below:


$\tau_2 = \_, \text{PN}(j_0, 0)$
$\tau_1 = \_, \text{PU}_{\text{ID}}(j, 1)$
$\tau_0 = \_, \text{PN}(j_0, 1)$
$\tau = \_, \text{PU}_{\text{ID}}(j, 2)$
τ :
$\sigma_{\tau_1}(\text{b-auth}^{\text{ID}}_{\text{U}}) = g(\phi^{\mathsf{in}}_{\tau_1})$
$= \mathsf{n}^{j_0}$
$\sigma_\tau(\text{e-auth}^{\text{ID}}_{\text{U}}) = \sigma_\tau(\text{b-auth}^{\text{ID}}_{\text{U}})$
$= \mathsf{n}^{j_0}$
$\sigma_{\tau_0}(\text{b-auth}^{j_0}_{\text{N}}) = \text{ID}$

It follows that $\psi^{\tau_1}_{\tau_2,\tau_0} \rightarrow \text{auth}_\tau(\text{ID}, j_0)$. Hence:

$$\text{suc-auth}_\tau(\text{ID}) \;\rightarrow\; \bigvee_{\substack{\tau_0 = \_, \text{PN}(j_0,1)\\ \tau_1 = \_, \text{PU}_{\text{ID}}(j,1)\\ \tau_2 = \_, \text{PN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_0}} \text{auth}_\tau(\text{ID}, j_0) \;\rightarrow\; \bigvee_{\text{s-started}_{j_0}(\tau)} \text{auth}_\tau(\text{ID}, j_0)$$

- **Case ai** $=$ **PN**$(j, 1)$**.** For all $\text{ID} \in \mathcal{S}_{\text{id}}$ and for all $j_0 \in \mathbb{N}$ such that $j_0 \neq j$ we have:

$$\text{suc-auth}_\tau(\text{ID}) \equiv \text{suc-auth}_{\tau_0}(\text{ID}) \qquad\qquad \text{auth}_\tau(\text{ID}, j_0) \equiv \text{auth}_{\tau_0}(\text{ID}, j_0)$$

Hence (17) holds. It only remains the case where $\text{ID} \in \mathcal{S}_{\text{id}}$ and $j_0 = j$. By validity of τ we know that $\sigma^{\mathsf{in}}_\tau(\text{b-auth}^{j}_{\text{N}}) \equiv \mathsf{fail}$. From $\neq$-Const it follows that $\sigma^{\mathsf{in}}_\tau(\text{b-auth}^{j}_{\text{N}}) \neq \text{ID}$, and therefore $\text{auth}_{\tau_0}(\text{ID}, j) \leftrightarrow \mathsf{false}$.
To conclude this case, we only need to show that $(\text{suc-auth}_\tau(\text{ID}) \wedge \text{auth}_\tau(\text{ID}, j)) \leftrightarrow \mathsf{false}$. We recall that $\text{suc-auth}_\tau(\text{ID}) \equiv \sigma_\tau(\text{e-auth}^{\text{ID}}_{\text{U}}) \neq \mathsf{fail}$. The only instants that can set $\text{e-auth}^{\text{ID}}_{\text{U}}$ to something other than fail are $\text{PU}_{\text{ID}}(\_, 2)$ and $\text{TU}_{\text{ID}}(\_, 1)$. Formally, we show by induction on τ that:

$$\sigma_\tau(\text{e-auth}^{\text{ID}}_{\text{U}}) \neq \mathsf{fail} \;\rightarrow \bigvee_{\substack{\tau_0 \preceq \tau\\ \tau_0 = \_, \text{PU}_{\text{ID}}(\_,2)\\ \vee\ \tau_0 = \text{TU}_{\text{ID}}(\_,1)}} \text{accept}^{\text{ID}}_{\tau_0} \wedge \sigma_\tau(\text{e-auth}^{\text{ID}}_{\text{U}}) = \sigma_{\tau_0}(\text{e-auth}^{\text{ID}}_{\text{U}}) \tag{18}$$

Therefore we only have to prove that for any τ_0 in the disjunction above, we have:

$$\Big(\text{suc-auth}_\tau(\text{ID}) \wedge \text{auth}_\tau(\text{ID}, j) \wedge \text{accept}^{\text{ID}}_{\tau_0} \wedge \sigma_\tau(\text{e-auth}^{\text{ID}}_{\text{U}}) = \sigma_{\tau_0}(\text{e-auth}^{\text{ID}}_{\text{U}})\Big) \leftrightarrow \mathsf{false}$$

We have two cases:

– Let $\tau_0 = \_, \text{PU}_{\text{ID}}(j_0, 2) \preceq \tau$. By validity of τ, we know that there exists $\tau_2 \prec_\tau \tau_0$ such that $\tau_2 = \_, \text{PU}_{\text{ID}}(j_0, 1)$. By **(Acc2)**:

$$\text{accept}^{\text{ID}}_{\tau_0} \;\rightarrow \bigvee_{\substack{\tau_1 = \_, \text{PN}(j_1,1)\\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_0}} g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1}$$

Moreover, $\text{accept}^{\text{ID}}_{\tau_0} \wedge g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1} \rightarrow \sigma_{\tau_0}(\text{e-auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j_1}$. Therefore:

$$\text{accept}^{\text{ID}}_{\tau_0} \wedge \sigma_\tau(\text{e-auth}^{\text{ID}}_{\text{U}}) = \sigma_{\tau_0}(\text{e-auth}^{\text{ID}}_{\text{U}}) \;\rightarrow \bigvee_{\substack{\tau_1 = \_, \text{PN}(j_1,1)\\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_0}} \sigma_\tau(\text{e-auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j_1}$$

Since $\tau_0 \prec \tau$ we know that for every $\tau_1 = \_, \textsc{pn}(j_1, 1) \in \{\tau_1 \mid \tau_2 \prec \tau_1 \prec_\tau \tau_0\}$, $j_1 \neq j$. Using =-ind we deduce that $\mathsf{n}^{j_1} \neq \mathsf{n}^j$. Since $\mathsf{auth}_\tau(\textsc{id}, j) \rightarrow \mathsf{n}^j = \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}})$, we obtain that:

$$\begin{aligned} \mathsf{accept}_{\tau_0}^{\textsc{id}} \wedge \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_0}(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) \wedge \mathsf{auth}_\tau(\textsc{id}, j) \;&\rightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{pn}(j_1,1) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_0}} \mathsf{n}^j = \mathsf{n}^{j_1} \\ &\rightarrow \;\mathsf{false} \end{aligned}$$

- Let $\tau_0 = \_, \textsc{tu}_{\textsc{id}}(j_0, 1) \preceq \tau$. We do a similar reasoning. By **(Acc3)**:

$$\mathsf{accept}_{\tau_0}^{\textsc{id}} \;\rightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{tn}(j_1,0) \\ \tau_1 \prec_\tau \tau_0}} \pi_1(g(\phi_{\tau_0}^{\mathsf{in}})) = \mathsf{n}^{j_1}$$

Remark that $\mathsf{accept}_{\tau_0}^{\textsc{id}} \wedge \pi_1(g(\phi_{\tau_0}^{\mathsf{in}})) = \mathsf{n}^{j_1} \rightarrow \sigma_{\tau_0}(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) = \mathsf{n}^{j_1}$. Hence:

$$\mathsf{accept}_{\tau_0}^{\textsc{id}} \wedge \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_0}(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) \;\rightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{tn}(j_1,0) \\ \tau_1 \prec_\tau \tau_0}} \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) = \mathsf{n}^{j_1}$$

By validity of τ, we know that for every $\tau_1 = \_, \textsc{tn}(j_1, 0)$ such that $\tau_1 \prec_\tau \tau_0$, we have $j_1 \neq j$, and by consequence $\mathsf{n}^{j_1} \neq \mathsf{n}^j$. Since $\mathsf{auth}_\tau(\textsc{id}, j) \rightarrow \mathsf{n}^j = \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}})$, we obtain that:

$$\begin{aligned} \mathsf{accept}_{\tau_0}^{\textsc{id}} \wedge \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_0}(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) \wedge \mathsf{auth}_\tau(\textsc{id}, j) \;&\rightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{tn}(j_1,0) \\ \tau_1 \prec_\tau \tau_0}} \mathsf{n}^j = \mathsf{n}^{j_1} \\ &\rightarrow \;\mathsf{false} \end{aligned}$$

- **Case ai** $= \textsc{tn}(j, 0)$. Again, for all $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$ and for all $j_0 \in \mathbb{N}$ such that $j_0 \neq j$:

$$\text{suc-auth}_\tau(\textsc{id}) \equiv \text{suc-auth}_{\tau_0}(\textsc{id}) \qquad\qquad \mathsf{auth}_\tau(\textsc{id}, j_0) \equiv \mathsf{auth}_{\tau_0}(\textsc{id}, j_0)$$

Hence (17) holds. It only remains the case $j_0 = j$. We know that $\sigma_\tau^{\mathsf{in}}(\text{b-auth}_{\textsc{n}}^{j}) \equiv \mathsf{fail}$, therefore $\text{suc-auth}_{\tau_0}(\textsc{id}, j) = \mathsf{false}$, which in turn implies that:

$$(\text{suc-auth}_{\tau_0}(\textsc{id}) \;\wedge\; \mathsf{auth}_{\tau_0}(\textsc{id}, j)) \leftrightarrow \mathsf{false}$$

Moreover:

$$\mathsf{auth}_\tau(\textsc{id}, j) \;\rightarrow\; \mathsf{n}^j = \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}})$$

Remark that $\sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) \equiv \sigma_\tau^{\mathsf{in}}(\text{e-auth}_{\textsc{u}}^{\textsc{id}})$. Using **(A1)** we easily show that n^j does not appear in $\mathsf{st}(\sigma_\tau^{\mathsf{in}}(\text{e-auth}_{\textsc{u}}^{\textsc{id}}))$. Therefore $\neg\mathsf{auth}_\tau(\textsc{id}, j)$ by =-ind. ■

Using Lemma 8, we can prove Lemma 3, which we recall below:

Lemma (3). *For every valid action trace τ on $\mathcal{S}_{id}$, $\textsc{id} \in \mathcal{S}_{id}$ and $j \in \mathbb{N}$, we have:*

$$\sigma_\tau(\textit{e-auth}_{U}^{ID}) = n^j \;\rightarrow\; \bigvee\nolimits_{\tau' \preceq \tau} \;\sigma_{\tau'}(\textit{b-auth}_{N}^{j}) = \textsc{id}$$

Proof. Let τ be a valid action trace. First, observe that $\sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) = \mathsf{n}^j$ implies that $\sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) \neq \mathsf{fail}$. Therefore, using Lemma 8 we get that:

$$\begin{aligned} \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) = \mathsf{n}^j \;&\rightarrow\; \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) \neq \mathsf{fail} \\ &\rightarrow\; \text{suc-auth}_\tau(\textsc{id}) \\ &\rightarrow\; \bigvee\nolimits_{\text{s-started}_{j'}(\tau)} \mathsf{auth}_\tau(\textsc{id}, j') \qquad \text{(By Lemma 8)} \end{aligned}$$

Since $(\mathsf{n}^j = \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) \wedge \mathsf{n}^{j'} = \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}})) \leftrightarrow \mathsf{false}$ if $j \neq j'$:

$$\begin{aligned} &\rightarrow\; \sigma_\tau(\text{b-auth}_{\textsc{n}}^{j}) = \textsc{id} \\ &\rightarrow\; \bigvee\nolimits_{\tau' \preceq \tau} \;\sigma_{\tau'}(\text{b-auth}_{\textsc{n}}^{j}) = \textsc{id} \end{aligned}$$

■

D.4 Injective Authentication of the Network by the User

We actually can show that the authentication of the network by the user is *injective.*

Lemma 9. *For every valid action trace τ on $\mathcal{S}_{id}$, the AKA$^+$ protocol provides* injective *authentication of the network by the user. Formally, for every* $\textsc{id} \in \mathcal{S}_{id}$ *and* $j \in \mathbb{N}$, *we define the formula:*

$$\textit{inj-auth}_\tau(\textsc{id}, j) \quad \equiv \quad \textit{auth}_\tau(\textsc{id}, j) \;\wedge\; \bigwedge_{\substack{i \neq j \\ \textit{s-started}_i(\tau)}} \neg \textit{auth}_\tau(\textsc{id}, i)$$

Then:

$$\forall \textsc{id} \in \mathcal{S}_{id}, \quad \textit{suc-auth}_\tau(\textsc{id}) \;\rightarrow\; \bigvee\nolimits_{\textit{s-started}_j(\tau)} \textit{inj-auth}_\tau(\textsc{id}, j)$$

Proof. First, we show that for $\textsc{id} \in \mathcal{S}_{\mathrm{id}}$ and $i_0, i_1 \in \mathbb{N}$ with $i_0 \neq i_1$:

$$\text{suc-auth}_\tau(\textsc{id}) \rightarrow (\neg\text{auth}_\tau(\textsc{id}, i_0) \vee \neg\text{auth}_\tau(\textsc{id}, i_1)) \tag{19}$$

Indeed:

$$\text{suc-auth}_\tau(\textsc{id}) \wedge \text{auth}_\tau(\textsc{id}, i_0) \wedge \text{auth}_\tau(\textsc{id}, i_1) \;\rightarrow\; \mathsf{n}^{i_0} = \sigma_\tau(\text{e-auth}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{n}^{i_1} = \sigma_\tau(\text{e-auth}_{\mathrm{U}}^{\mathrm{ID}})$$

Using =-ind, we know that $\mathsf{n}^{i_1} \neq \mathsf{n}^{i_0}$. Therefore:

$$\mathsf{n}^{i_0} = \sigma_\tau(\text{e-auth}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{n}^{i_1} = \sigma_\tau(\text{e-auth}_{\mathrm{U}}^{\mathrm{ID}}) \rightarrow \text{false}$$

This concludes the proof of (19). From Lemma 8 we know that:

$$\forall \textsc{id} \in \mathcal{S}_{\mathrm{id}}, \quad \text{suc-auth}_\tau(\textsc{id}) \;\rightarrow\; \bigvee\nolimits_{\text{s-started}_j(\tau)} \text{auth}_\tau(\textsc{id}, j)$$

Moreover, using (19) we have that for every $\textsc{id} \in \mathcal{S}_{\mathrm{id}}, j \in \mathbb{N}$:

$$\text{suc-auth}_\tau(\textsc{id}) \wedge \text{auth}_\tau(\textsc{id}, j) \;\rightarrow\; \bigwedge_{\substack{i \neq j \\ \text{s-started}_j(\tau)}} \neg\text{auth}_\tau(\textsc{id}, i)$$

We deduce that:

$$\forall \textsc{id} \in \mathcal{S}_{\mathrm{id}}, \quad \text{suc-auth}_\tau(\textsc{id}) \;\rightarrow\; \bigvee\nolimits_{\text{s-started}_j(\tau)} \text{inj-auth}_\tau(\textsc{id}, j) \qquad \blacksquare$$

Finally, we prove that $\textsc{id}$ authenticated j_0 at τ if and only if $\mathsf{n}^{j_0} = \sigma_\tau(\text{e-auth}_{\mathrm{U}}^{\mathrm{ID}})$.

Proposition 24. *For every valid action trace τ, for every $j_0 \in \mathbb{N}$:*

$$\textit{inj-auth}_\tau(\textsc{id}, j_0) \;\leftrightarrow\; n^{j_0} = \sigma_\tau(\textit{e-auth}_{U}^{ID})$$

Proof. To do this we show both directions. The first direction is trivial:

$$\text{inj-auth}_\tau(\textsc{id}, j_0) \;\rightarrow\; \text{auth}_\tau(\textsc{id}, j_0) \;\rightarrow\; \mathsf{n}^{j_0} = \sigma_\tau^{\mathsf{in}}(\text{e-auth}_{\mathrm{U}}^{\mathrm{ID}})$$

We now prove the converse direction:

$$\begin{aligned} \mathsf{n}^{j_0} = \sigma_\tau^{\mathsf{in}}(\text{e-auth}_{\mathrm{U}}^{\mathrm{ID}}) &\rightarrow \text{suc-auth}_\tau(\textsc{id}) && \text{(Using =-ind)} \\ &\rightarrow \bigvee\nolimits_{\text{s-started}_{j_1}(\tau)} \text{inj-auth}_\tau(\textsc{id}, j_1) && \text{(Lemma 9)} \end{aligned}$$

We conclude by observing that for every $j_1 \neq j_0$:

$$\begin{aligned} \mathsf{n}^{j_0} = \sigma_\tau(\text{e-auth}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \text{inj-auth}_\tau(\textsc{id}, j_1) &\rightarrow \mathsf{n}^{j_0} = \sigma_\tau(\text{e-auth}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{n}^{j_1} = \sigma_\tau(\text{e-auth}_{\mathrm{U}}^{\mathrm{ID}}) \\ &\rightarrow \text{false} \qquad\qquad \text{(Using =-ind)} \qquad \blacksquare \end{aligned}$$

D.5 Proof of Lemma 6

Proof of **(Acc1)**. Let $\mathsf{ai} = \textsc{pn}(j, 1)$ and $\mathsf{k_m} \equiv \mathsf{k}_\mathsf{m}^{\textsc{id}}$. Recall that:

$$\mathsf{accept}_\tau^{\textsc{id}} \;\equiv\; \mathsf{eq}(\pi_1(\mathsf{dec}(\pi_1(g(\phi_\tau^{\mathsf{in}})), \mathsf{sk}_\textsc{n})), \textsc{id}) \wedge \mathsf{eq}(\pi_2(g(\phi_\tau^{\mathsf{in}})), \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \pi_1(g(\phi_\tau^{\mathsf{in}}))\,,\, \mathsf{n}^j\rangle))$$

We apply the p-euf-mac^1 axiom (invariant (inv-key) guarantees that the syntactic side-conditions hold):

$$\begin{aligned}\mathsf{accept}_\tau^{\textsc{id}} \;&\rightarrow\; \pi_2(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \pi_1(g(\phi_\tau^{\mathsf{in}}))\,,\, \mathsf{n}^j\rangle)\\ &\rightarrow \bigvee_{\tau_0 = \_, \textsc{pu}_\textsc{id}(j_0,1) \prec \tau} \pi_2(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \{\langle \textsc{id}\,,\, \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_\textsc{u}^\textsc{id})\rangle\}_{\mathsf{pk}_\textsc{n}}^{\mathsf{n}_\mathsf{e}^{j_0}}\,,\, g(\phi_{\tau_0}^{\mathsf{in}})\rangle)\end{aligned}$$

Finally, we use cr^1, $\mathsf{EQInj}(\langle \_\,,\, \cdot\rangle)$ and $\mathsf{EQInj}(\langle \cdot\,,\, \_\rangle)$ to show that for every $\tau_0 = \_, \textsc{pu}_\textsc{id}(j_0, 1) \prec \tau$:

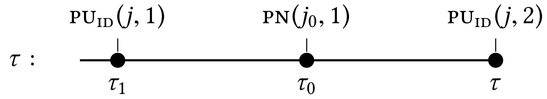
$$\mathsf{Mac}^1_{\mathsf{k_m}}(\langle \underline{\pi_1(g(\phi_\tau^{\mathsf{in}}))}\,,\, \underline{\mathsf{n}^j}\rangle) = \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \underline{\{\langle \textsc{id}\,,\, \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_\textsc{u}^\textsc{id})\rangle\}_{\mathsf{pk}_\textsc{n}}^{\mathsf{n}_\mathsf{e}^{j_0}}}\,,\, \underline{g(\phi_{\tau_0}^{\mathsf{in}})}\rangle) \;\rightarrow$$

$$\underline{\pi_1(g(\phi_\tau^{\mathsf{in}})) = \{\langle \textsc{id}\,,\, \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_\textsc{u}^\textsc{id})\rangle\}_{\mathsf{pk}_\textsc{n}}^{\mathsf{n}_\mathsf{e}^{j_0}}} \;\wedge\; \underline{\mathsf{n}^j = g(\phi_{\tau_0}^{\mathsf{in}})} \qquad \blacksquare$$

Proof of **(Acc2)**. If $\mathsf{ai} = \textsc{pu}_\textsc{id}(j, 2)$. Let $\mathsf{k_m} \equiv \mathsf{k}_\mathsf{m}^{\textsc{id}}$. Recall that:

$$\mathsf{accept}_\tau^{\textsc{id}} \;\equiv\; g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \sigma_\tau^{\mathsf{in}}(\mathsf{b\text{-}auth}_\textsc{u}^\textsc{id})\,,\, \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_\textsc{u}^\textsc{id})\rangle)$$

Graphically, we are in the situation:


$\textsc{pu}_\textsc{id}(j, 1)$
$\textsc{pn}(j_0, 1)$
$\textsc{pu}_\textsc{id}(j, 2)$
τ :
τ_1
τ_0
τ

Part 1 We are going to apply the p-euf-mac^2 axiom. We let:

$$S = \{\tau_0 \mid \tau_0 = \_, \textsc{pn}(j_0, 1) \prec \tau\}$$

and for all $S_0 \subseteq S$ we let:

$$b_{S_0} = \Big(\bigwedge_{\tau_0 \in S_0} \mathsf{accept}_{\tau_0}^{\textsc{id}}\Big) \wedge \Big(\bigwedge_{\tau_0 \in \overline{S_0}} \neg\mathsf{accept}_{\tau_0}^{\textsc{id}}\Big)$$

Then $(b_{S_0})_{S_0 \subseteq S}$ is a valid CS partition. It is straightforward to check that for every $S_0 \subseteq S$, for every $\tau_0 = \_, \textsc{pn}(j_0, 1) \prec \tau$, if $\tau_0 \in S_0$ then we can rewrite $[b_{S_0}]t_{\tau_0}$ into a term $[b_{S_0}]t_{\tau_0}^{S_0}$ by removing the branch corresponding to $\mathsf{accept}_{\tau_0}^{\textsc{id}}$. Therefore:

$$\mathsf{Mac}^2_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}\,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})), \mathsf{sk}_\textsc{n})))\rangle) \in \mathsf{set\text{-}mac}^2_{\mathsf{k_m}}(t_{\tau_0}^{S_0}) \text{ if and only if } \tau_0 \in S_0$$

Hence by applying the p-euf-mac^2 axiom we get that:

$$\mathsf{accept}_\tau^{\textsc{id}} \rightarrow \bigvee_{S_0 \subseteq S} b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}\,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})), \mathsf{sk}_\textsc{n})))\rangle)$$

For $S_0 = \emptyset$, we have:

$$\neg\Big(\bigvee_{\tau_0 \in S_0} g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \mathsf{n}^{j}\,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})), \mathsf{sk}_\textsc{n})))\rangle)\Big)$$

Hence:

$$\begin{aligned}
\mathsf{accept}_{\tau}^{\textsc{id}} \;\rightarrow\;& \bigvee_{\substack{S_0 \subseteq S\\ S_0 \neq \emptyset}} b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} g(\phi_{\tau}^{\mathsf{in}}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \mathsf{n}^j \,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})), \mathsf{sk_N})))\rangle)\\
\rightarrow\;& \bigvee_{\substack{S_0 \subseteq S\\ S_0 \neq \emptyset}} \bigvee_{\tau_0 \in S_0} \mathsf{accept}_{\tau_0}^{\textsc{id}} \;\wedge\; g(\phi_{\tau}^{\mathsf{in}}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \mathsf{n}^j \,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})), \mathsf{sk_N})))\rangle)\\
\rightarrow\;& \bigvee_{\substack{\tau_0 = \_, \textsc{pn}(j_0, 1)\\ \tau_0 \prec \tau}} \mathsf{accept}_{\tau_0}^{\textsc{id}} \;\wedge\; g(\phi_{\tau}^{\mathsf{in}}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \mathsf{n}^j \,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})), \mathsf{sk_N})))\rangle)\\
\rightarrow\;& \bigvee_{\substack{\tau_0 = \_, \textsc{pn}(j_0, 1)\\ \tau_0 \prec \tau}} \mathsf{accept}_{\tau_0}^{\textsc{id}} \wedge \begin{array}{l} \left\langle \sigma_{\tau}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\textsc{u}}^{\textsc{id}}) \,,\, \sigma_{\tau}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) \right\rangle \;=\\ \left\langle \mathsf{n}^j \,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})), \mathsf{sk_N}))) \right\rangle \end{array} && (\textsc{cr}^2)\\
\rightarrow\;& \bigvee_{\substack{\tau_0 = \_, \textsc{pn}(j_0, 1)\\ \tau_0 \prec \tau}} \begin{array}{l} \mathsf{accept}_{\tau_0}^{\textsc{id}} \wedge \sigma_{\tau}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\textsc{u}}^{\textsc{id}}) = \mathsf{n}^j\\ \wedge\;\; \sigma_{\tau}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) = \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})), \mathsf{sk_N}))) \end{array} && \left(\begin{array}{r} \mathsf{EQInj}(\langle \_ \,,\, \cdot \rangle)\\ \text{and } \mathsf{EQInj}(\langle \cdot \,,\, \_ \rangle) \end{array}\right)
\end{aligned}$$

Part 2 It only remains to show that we can restrict ourselves to the τ_0 such that $\tau_1 \prec_\tau \tau_0$. Using **(Acc1)** we know that:

$$\mathsf{accept}_{\tau_0}^{\textsc{id}} \;\rightarrow\; \bigvee_{\substack{\tau' = \_, \textsc{pu}_{\textsc{id}}(j', 1)\\ \tau' \prec_\tau \tau_0}} \pi_1(g(\phi_{\tau_0}^{\mathsf{in}})) = \{\left\langle \textsc{id} \,,\, \sigma_{\tau'}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) \right\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e}^{j'}} \wedge g(\phi_{\tau'}^{\mathsf{in}}) = \mathsf{n}^{j_0}$$

Let $\tau' = \_, \textsc{pu}_{\textsc{id}}(j', 1)$ such that $\tau' \prec_\tau \tau_0$. We now show that if $j' \neq j$ then the tests fail, which proves the impossibility of replaying an old message here. Assume $j' \neq j$, then:

$$\begin{aligned}
&\sigma_{\tau}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) = \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})), \mathsf{sk_N}))) \wedge \pi_1(g(\phi_{\tau_0}^{\mathsf{in}})) = \{\left\langle \textsc{id} \,,\, \sigma_{\tau'}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) \right\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e}^{j'}}\\
\rightarrow\;& \sigma_{\tau}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) = \mathsf{suc}(\sigma_{\tau'}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}))\\
\rightarrow\;& \mathsf{false} && \text{(By } \textbf{(A3)}\text{)}
\end{aligned}$$

We deduce that:

$$\mathsf{accept}_{\tau}^{\textsc{id}} \;\rightarrow\; \bigvee_{\substack{\tau_0 = \_, \textsc{pn}(j_0, 1)\\ \tau_1 \prec_\tau \tau_0}} \mathsf{accept}_{\tau_0}^{\textsc{id}} \;\wedge\; g(\phi_{\tau_1}^{\mathsf{in}}) = \mathsf{n}^{j_0} \;\wedge\; \pi_1(g(\phi_{\tau_0}^{\mathsf{in}})) = \{\langle \textsc{id} \,,\, \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) \rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e}^{j}} \qquad \blacksquare$$

Proof of **(Acc3)**. Let $\mathsf{ai} = \textsc{tu}_{\textsc{id}}(j, 1)$ and $\mathsf{k} \equiv \mathsf{k}^{\textsc{id}}$. We know that:

$$\mathsf{accept}_{\tau}^{\textsc{id}} \;\rightarrow\; \pi_3(g(\phi_{\tau}^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \pi_1(g(\phi_{\tau}^{\mathsf{in}})) \,,\, \pi_2(g(\phi_{\tau}^{\mathsf{in}})) \oplus \mathsf{f_k}(\pi_1(g(\phi_{\tau}^{\mathsf{in}}))) \,,\, \sigma_{\tau}^{\mathsf{in}}(\textsc{guti}_{\textsc{u}}^{\textsc{id}}) \rangle)$$

We are going to apply the $\textsc{p-euf-mac}^3$ axiom. We let S be the set of terms:

$$S = \{\tau_0 \mid \tau_0 = \_, \textsc{tn}(j_0, 1) \prec \tau\}$$

and for all $S_0 \subseteq S$ we let:

$$b_{S_0} = \Big(\bigwedge_{\tau_0 \in S_0} \mathsf{accept}_{\tau_0}^{\textsc{id}} \Big) \wedge \Big(\bigwedge_{\tau_0 \in \overline{S_0}} \neg \mathsf{accept}_{\tau_0}^{\textsc{id}} \Big)$$

Then $(b_{S_0})_{S_0 \subseteq S}$ is a valid CS partition. It is straightforward to check that for every $S_0 \subseteq S$, for every $\tau_0 = \_, \textsc{tn}(j_0, 1) \prec \tau$, if $\tau_0 \in S$ then we can rewrite $[b_{S_0}]t_{\tau_0}$ into a term $[b_{S_0}]t_{\tau_0}^{S_0}$ by removing the branch corresponding to $\mathsf{accept}_{\tau_0}^{\textsc{id}}$. Therefore:

$$\mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0} \,, \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) \,,\, \sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}}) \rangle) \in \mathsf{set\text{-}mac}^3_{\mathsf{k_m}}(t_{\tau_0}^{S_0}) \text{ if and only if } \tau_0 \in S_0$$

Hence by applying the $\textsc{p-euf-mac}^3$ axiom we get that:

$$\mathsf{accept}_\tau^{\textsc{id}} \rightarrow \bigvee_{S_0 \subseteq S} b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}, \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}), \sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}})\rangle)$$

By $\textsc{cr}^3$, $\mathsf{EQInj}(\langle\_\,,\,\cdot\rangle)$ and $\mathsf{EQInj}(\langle\cdot\,,\,\_\rangle)$ we know that for every $\tau_0 = \_, \textsc{tn}(j_0, 1) \in S$:

$$\mathsf{Mac}^3_{\mathsf{k_m}}(\langle \underline{\pi_1(g(\phi_\tau^{\mathsf{in}}))}, \underline{\pi_2(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f_k}(\pi_1(g(\phi_\tau^{\mathsf{in}})))}, \underline{\sigma_\tau^{\mathsf{in}}(\textsc{guti}_{\textsc{u}}^{\textsc{id}})}\rangle) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \underline{\mathsf{n}^{j_0}}, \underline{\sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}})}, \underline{\sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}})}\rangle)$$

$$\rightarrow \quad \underline{\pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0}} \wedge \underline{\pi_2(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f_k}(\pi_1(g(\phi_\tau^{\mathsf{in}}))) = \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}})} \wedge \underline{\sigma_\tau^{\mathsf{in}}(\textsc{guti}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}})}$$

Using the idempotence of the $\oplus$ we know that:

$$\left(\pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0} \;\wedge\; \pi_2(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f_k}(\pi_1(g(\phi_\tau^{\mathsf{in}}))) = \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}})\right) \quad\rightarrow\quad \pi_2(g(\phi_\tau^{\mathsf{in}})) = \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0})$$

Moreover, remark that if $S_0 \cap S_{\textsc{n}} = \emptyset$, we have:

$$\neg \bigvee_{S_0 \subseteq S} b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}, \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}), \sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}})\rangle)$$

Putting everything together, we get that:

$$\begin{aligned}
\mathsf{accept}_\tau^{\textsc{id}} \quad &\rightarrow \quad \bigvee_{\substack{S_0 \subseteq S \\ S_0 \neq \emptyset}} b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}, \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}), \sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}})\rangle)\\
&\rightarrow \quad \bigvee_{\substack{S_0 \subseteq S \\ S_0 \neq \emptyset}} \bigvee_{\tau_0 \in S_0} \mathsf{accept}_{\tau_0}^{\textsc{id}} \wedge \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}, \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}), \sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}})\rangle)\\
&\rightarrow \quad \bigvee_{\tau_0 = \_, \textsc{tn}(j_0, 0) \prec \tau} \mathsf{accept}_{\tau_0}^{\textsc{id}} \wedge \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}, \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}), \sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}})\rangle)\\
&\rightarrow \quad \bigvee_{\tau_0 = \_, \textsc{tn}(j_0, 0) \prec \tau} \mathsf{accept}_{\tau_0}^{\textsc{id}} \wedge \pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0} \begin{array}{r} \wedge\, \pi_2(g(\phi_\tau^{\mathsf{in}})) = \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0}) \\ \wedge\, \sigma_\tau^{\mathsf{in}}(\textsc{guti}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}}) \end{array} \qquad \blacksquare
\end{aligned}$$

Proof of **(Acc4)**. We are going to apply the $\textsc{p-euf-mac}^4$ axiom. We let $S = \{\tau_0 \mid \tau_0 = \_, \textsc{tu}_{\textsc{id}}(j_0, 1) \prec \tau\}$, and for all $S_0 \subseteq S$ we let :

$$b_{S_0} = \bigwedge_{\tau_0 \in S_0} \mathsf{accept}_{\tau_0}^{\textsc{id}} \wedge \bigwedge_{\tau_0 \in \overline{S_0}} \neg\mathsf{accept}_{\tau_0}^{\textsc{id}}$$

Then $(b_{S_0})_{S_0 \subseteq S}$ is a valid CS partition. It is straightforward to check that for every $S_0 \subseteq S$, for every $\tau_0 = \_, \textsc{tu}_{\textsc{id}}(j_0, 1) \prec \tau$:

$$[b_{S_0}]t_{\tau_0} = \begin{cases} [b_{S_0}]\mathsf{Mac}^4_{\mathsf{k_m}}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}}))) & \text{if } \tau_0 \in S_0 \\ [b_{S_0}]\mathsf{error} & \text{if } \tau_0 \in \overline{S_0} \end{cases}$$

Hence by applying the $\textsc{p-euf-mac}^4$ axiom we get that:

$$g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^j) \rightarrow \bigvee_{S_0 \subseteq S} b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^4_{\mathsf{k_m}}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})))$$

Remark that for $S_0 = \emptyset$, we have:

$$\neg\Big(b_{S_0} \wedge \bigvee\nolimits_{\tau_0 \in S_0} g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^4_{\mathsf{k_m}}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})))\Big)$$

Hence:

$$g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^j) \rightarrow \bigvee_{\substack{S_0 \subseteq S \\ S_0 \neq \emptyset}} b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^4_{\mathsf{k_m}}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})))$$

Let $S_0 \subseteq S$ with $S_0 \neq \emptyset$, and let $\tau_0 \in S_0$. Using the $\textsc{cr}^4$ axiom we know that:

$$g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^4_{\mathsf{k_m}}(\underline{\mathsf{n}^j}) \;\wedge\; g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^4_{\mathsf{k_m}}(\underline{\pi_1(g(\phi_{\tau_0}^{\mathsf{in}}))}) \;\rightarrow\; \underline{\pi_1(g(\phi_{\tau_0}^{\mathsf{in}})) = \mathsf{n}^j}$$

Therefore:

$$\begin{aligned} g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^j) &\rightarrow \bigvee_{\substack{S_0 \subseteq S \\ S_0 \neq \emptyset}} b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^4_{\mathsf{k_m}}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}}))) \\ &\rightarrow \bigvee_{\substack{S_0 \subseteq S \\ S_0 \neq \emptyset}} b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} \pi_1(g(\phi_{\tau_0}^{\mathsf{in}})) = \mathsf{n}^j \end{aligned}$$

And using the fact that $b_{S_0} \rightarrow \mathsf{accept}_{\tau_0}^{\mathrm{ID}}$:

$$g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^j) \rightarrow \bigvee_{\tau_0 = \_, \textsc{tu}_{\textsc{id}}(\_,1) \prec \tau} \mathsf{accept}_{\tau_0} \wedge \pi_1(g(\phi_{\tau_0}^{\mathsf{in}})) = \mathsf{n}^j \qquad \blacksquare$$

E ACCEPTANCE CONDITION CHARACTERIZATIONS

In this section, we prove acceptance characterizations, i.e. *necessary and sufficient* conditions for a message to be accepted by the user or the network. This section is organized as follows: we start by showing some properties of the AKA$^+$ protocol, which we use to obtain a first set of acceptance characterizations in Section E.1 and Section E.3; then, using these conditions, we prove in Section E.5 that the temporary identity $\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}}$ is concealed until the subscriber starts a session of the GUTI sub-protocol; finally, using the GUTI concealment property, we prove stronger acceptance characterizations in Section E.6.

E.1 A First Acceptance Condition Characterization

Before proving our first acceptance characterizations, we show two properties of the AKA$^+$ protocol.

The property **(B1)** states that the user and network sequence numbers are increasing, i.e. for every valid action trace τ, and for every prefixes τ_1, τ_0 of τ such that $\tau_0 \preceq \tau_1$, we have:

$$\sigma_{\tau_0}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) \leq \sigma_{\tau_1}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) \qquad\qquad \sigma_{\tau_0}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \leq \sigma_{\tau_1}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$$

The property **(B2)** is more complex. Let j_0 be a network session that authenticated a user at instant τ (i.e. $\sigma_\tau(\mathsf{e\text{-}auth}_{\mathrm{N}}^{j_0}) \neq \mathsf{UnknownId}$), and let ID be a user. We assume that ID has been reseted since the session j_0, and that ID already ran a full session of the AKA$^+$ protocol: formally, $\tau = \textsc{fu}_{\textsc{id}}(\_)$ and $\textsc{fn}(j_0) \prec_\tau \textsc{ns}_{\textsc{id}}(\_)$. Then either the *HN* session j_0 did not authenticate ID, or the current value value of $\mathsf{e\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}$ is not n^{j_0}. In both case we have $\neg\mathsf{inj\text{-}auth}_\tau(\textsc{id}, j_0)$.

We show **(B2)** by contradiction, by proving that if it does not hold, then there is a sequence number *inconsistency*. In that case, we prove that there exists an instant τ_1 such that $\sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}})$. We describe in an informal fashion how this is done. First, we prove that when a message is accepted, the user and network sequence numbers must be equal between some instants of the protocol executions (we prove two such equalities). Moreover, the sequence number are not decreasing **(B1)**, and the user increments his sequence number at the instant $\textsc{tu}_{\textsc{id}}(\_, 1)$ if it accepts. This allows us to obtain the situation depicted in Figure 19. We will use this proof technique multiple times in this paper.

Proposition 25. *For every valid action trace $\tau = \_, ai$ on $\mathcal{S}_{id}$ and identity $\textsc{id} \in \mathcal{S}_{id}$:*

- ***(B1)*** *For every $\tau_0 \preceq \tau_1 \preceq \tau$, for every $\textsc{x} \in \{\textsc{u}, \textsc{n}\}$, we have $\sigma_{\tau_0}(\textsc{sqn}_X^{ID}) \leq \sigma_{\tau_1}(\textsc{sqn}_X^{ID})$.*
- ***(B2)*** *If $ai = \textsc{fu}_{\textsc{id}}(j)$ then for every and $j_0 \in \mathbb{N}$, if $\textsc{fn}(j_0) \prec_\tau \textsc{ns}_{\textsc{id}}(\_)$ then:*

$$\sigma_\tau(\textit{e-auth}_N^{j_0}) \neq \textit{UnknownId} \rightarrow \neg\textit{inj-auth}_\tau(\textsc{id}, j_0)$$

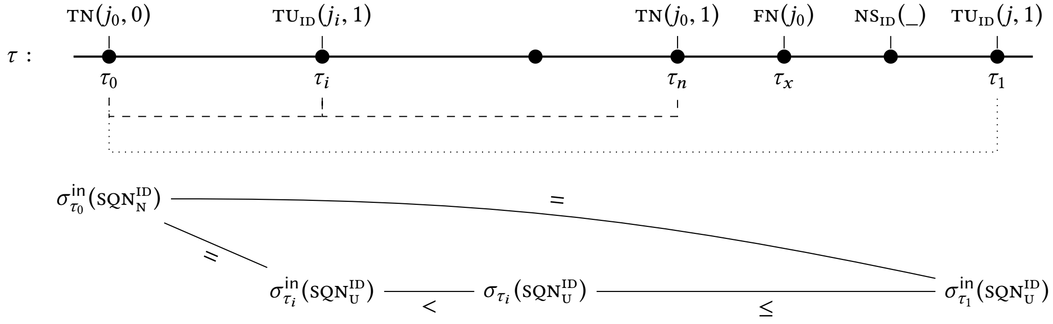

τ :
$\mathrm{TN}(j_0, 0)$
$\mathrm{TU}_{\mathrm{ID}}(j_i, 1)$
$\mathrm{TN}(j_0, 1)$
$\mathrm{FN}(j_0)$
$\mathrm{NS}_{\mathrm{ID}}(\_)$
$\mathrm{TU}_{\mathrm{ID}}(j, 1)$
τ_0
τ_i
τ_n
τ_x
τ_1
$\sigma^{\mathsf{in}}_{\tau_0}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$
=
=
$\sigma^{\mathsf{in}}_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$
<
$\sigma_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$
≤
$\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$

Fig. 19. Graphical Representation of the Proof of Proposition 25

Proof. Let $\tau = \_, \mathsf{ai}$ be a valid action trace and $\mathrm{ID} \in \mathcal{S}_{\mathsf{id}}$. The property **(B1)** is straightforward by induction over τ_1. Therefore, we focus on **(B2)**.

Let $\tau_x = \_, \mathrm{FN}(j_0) \prec \tau$. We do a case disjunction on the sub-protocol used by the user:

- If there exists τ_1 s.t. $\tau_1 = \_, \mathrm{TU}_{\mathrm{ID}}(j, 1) \prec \tau$. By validity of τ, there exists $\tau_n \prec \tau_x$ with $\tau_n = \_, \mathrm{PN}(j_0, 1)$ or $\_, \mathrm{TN}(j_0, 1)$. We can check that $\tau_n \prec \tau_x \prec \tau_1 \prec \tau$.

  Assume that $\tau_n = \_, \mathrm{PN}(j_0, 1)$. The sub-protocols used by the user and the network are different. In that case, it is very easy to show that we cannot have authentication. To prove this formally, observe first that $\mathsf{inj\text{-}auth}_\tau(\mathrm{ID}, j_0) \rightarrow \mathsf{accept}^{\mathrm{ID}}_{\tau_1}$. Therefore, using **(Acc3)**:

  $$\mathsf{inj\text{-}auth}_\tau(\mathrm{ID}, j_0) \;\rightarrow \bigvee_{\substack{\tau_2 = \_, \mathrm{TN}(j_2, 0) \\ \tau_2 \prec \tau_1}} \sigma_{\tau_1}(\mathsf{e\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^{j_2}$$

  For every $\tau_2 = \_, \mathrm{TN}(j_2, 0) \prec \tau_1$, we know that $j_2 \neq j_0$ (since $\tau_n = \_, \mathrm{PN}(j_0, 1)$). Hence:

  $$\mathsf{inj\text{-}auth}_\tau(\mathrm{ID}, j_0) \;\rightarrow\; \sigma_{\tau_1}(\mathsf{e\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}}) \neq \mathsf{n}^{j_0} \;\rightarrow\; \mathsf{false}$$

  Which is what we wanted.

  Now, assume that $\tau_n = \_, \mathrm{TN}(j_0, 1)$. We give a graphical representation of this case in Figure 19. The idea is that $\mathsf{inj\text{-}auth}_\tau(\mathrm{ID}, j_0)$ implies that $UE_{\mathrm{ID}}(j)$ must have accepted $HN(j_0)$ at instant τ_1. But since $HN(j_0)$ ran the GUTI sub-protocol at instant τ_n which is *before* τ_1, is must have accepted messages from a prior $UE_{\mathrm{ID}}(j_i)$ session (with $j_i \neq j$). It follows that $HN(j_0)$ must have accepted two different UE_{ID} sessions, j_i and j. This will yield a contradiction on sequence numbers.

  We now prove this formally. First, observe that $\sigma_{\tau_n}(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) \neq \mathsf{fail}$ and $\sigma_\tau(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) = \sigma_{\tau_n}(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}})$. Moreover, it is straightforward to check that for every valid action trace τ':

$$\mathsf{inj\text{-}auth}_{\tau'}(\mathrm{ID}, j_0) \wedge \sigma_{\tau'}(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) \neq \mathsf{UnknownId} \wedge \sigma_{\tau'}(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) \neq \mathsf{fail}$$
$$\rightarrow \sigma_{\tau'}(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) = \sigma_{\tau'}(\mathsf{b\text{-}auth}^{j_0}_{\mathrm{N}})$$

  Hence we deduce that:

  $$\mathsf{inj\text{-}auth}_\tau(\mathrm{ID}, j_0) \wedge \sigma_\tau(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) \neq \mathsf{UnknownId} \rightarrow \sigma_\tau(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) = \sigma_\tau(\mathsf{b\text{-}auth}^{j_0}_{\mathrm{N}})$$

  Since $\mathsf{inj\text{-}auth}_\tau(\mathrm{ID}, j_0) \rightarrow \sigma_\tau(\mathsf{b\text{-}auth}^{j_0}_{\mathrm{N}}) = \mathrm{ID}$, we get that:

  $$\mathsf{inj\text{-}auth}_\tau(\mathrm{ID}, j_0) \wedge \sigma_\tau(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) \neq \mathsf{UnknownId} \rightarrow \sigma_\tau(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) = \mathrm{ID}$$

Moreover, $\sigma_\tau(\text{e-auth}_{\textsc{n}}^{j_0}) = \textsc{id} \rightarrow \text{accept}_{\tau_n}^{\textsc{id}}$. Using **(Acc4)** on τ_n:

$$\text{accept}_{\tau_n}^{\textsc{id}} \rightarrow \bigvee_{\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1) \prec \tau_n} \text{accept}_{\tau_i}^{\textsc{id}} \wedge \pi_1(g(\phi_{\tau_i}^{\text{in}})) = \mathsf{n}^{j_0}$$

Let $\tau_0 = \textsc{tn}(j_0, 0)$ and $\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1) \prec \tau_n$. Observe that $\tau_i \neq \tau_1$. Using **(Acc3)**, we get that:

$$\text{accept}_{\tau_i}^{\textsc{id}} \wedge \pi_1(g(\phi_{\tau_i}^{\text{in}})) = \mathsf{n}^{j_0} \rightarrow \text{range}(\sigma_{\tau_i}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}), \sigma_{\tau_0}^{\text{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}})) \rightarrow \sigma_{\tau_i}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_0}^{\text{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}})$$

Recall that $\text{inj-auth}_\tau(\textsc{id}, j_0) \rightarrow \text{accept}_{\tau_1}^{\textsc{id}}$. Moreover, $\text{inj-auth}_\tau(\textsc{id}, j_0) \rightarrow \pi_1(g(\phi_{\tau_1}^{\text{in}})) = \mathsf{n}^{j_0}$. Hence using **(Acc3)** again we get:

$$\text{accept}_{\tau_1}^{\textsc{id}} \wedge \pi_1(g(\phi_{\tau_1}^{\text{in}})) = \mathsf{n}^{j_0} \rightarrow \text{range}(\sigma_{\tau_1}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}), \sigma_{\tau_0}^{\text{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}})) \rightarrow \sigma_{\tau_1}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_0}^{\text{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}})$$

Putting everything together:

$$\begin{aligned} \text{inj-auth}_\tau(\textsc{id}, j_0) \wedge \sigma_\tau(\text{e-auth}_{\textsc{n}}^{j_0}) \neq \mathsf{UnknownId} &\rightarrow \begin{pmatrix} \sigma_{\tau_i}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_0}^{\text{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) \\ \wedge\ \sigma_{\tau_1}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_0}^{\text{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) \end{pmatrix} \\ &\rightarrow \sigma_{\tau_1}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_i}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) \end{aligned}$$

Finally, $\text{accept}_{\tau_i}^{\textsc{id}} \rightarrow \sigma_{\tau_i}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) < \sigma_{\tau_i}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})$, and using **(B1)** we know that $\sigma_{\tau_i}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) \leq \sigma_{\tau_1}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})$. We deduce that:

$$\begin{aligned} \text{inj-auth}_\tau(\textsc{id}, j_0) \wedge \sigma_\tau(\text{e-auth}_{\textsc{n}}^{j_0}) \neq \mathsf{UnknownId} &\rightarrow \sigma_{\tau_1}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_i}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) < \sigma_{\tau_1}^{\text{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) \\ &\rightarrow \text{false} \end{aligned}$$

This concludes this case.

- If there exists $\tau_1 = \_, \textsc{pu}_{\textsc{id}}(j, 2) \prec \tau$. Let $\tau_3 = \_, \textsc{pu}_{\textsc{id}}(j, 1) \prec \tau_1$, we know that $\tau_x \prec \tau_3$. Remark that $\text{inj-auth}_\tau(\textsc{id}, j_0) \rightarrow \text{accept}_{\tau_1}^{\textsc{id}}$, and using **(Acc2)** we easily get that:

$$\text{accept}_{\tau_1}^{\textsc{id}} \rightarrow \bigvee_{\substack{\tau_2 = \_, \textsc{pn}(j_2, 1) \\ \tau_3 \prec \tau_2 \prec \tau_1}} \sigma_{\tau_1}(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) = \mathsf{n}^{j_2}$$

Since no $\textsc{id}$ action occurred between τ_1 and τ, we have $\sigma_{\tau_1}(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) = \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}})$. Moreover, $\text{inj-auth}_\tau(\textsc{id}, j_0) \rightarrow \sigma_\tau(\text{e-auth}_{\textsc{u}}^{\textsc{id}}) = \mathsf{n}^{j_0}$. Finally, for every $\tau_2 = \_, \textsc{pn}(j_2, 1)$ such that $\tau_3 \prec \tau_2 \prec \tau_1$, since $\tau_x \prec \tau_3$ we know that $j_2 \neq j_0$. It follows that:

$$\text{inj-auth}_\tau(\textsc{id}, j_0) \rightarrow \bigvee_{\substack{\tau_2 = \_, \textsc{pn}(j_2, 1) \\ \tau_3 \prec \tau_2 \prec \tau_1}} \mathsf{n}^{j_0} = \mathsf{n}^{j_2} \rightarrow \text{false} \qquad \blacksquare$$

We now prove a first acceptance characterization:

Lemma 10. *For every valid action trace $\tau = \_, ai$ on $\mathcal{S}_{id}$ and identity $\textsc{id} \in \mathcal{S}_{id}$:*

- ***(Equ1)*** *If $ai = \textsc{fu}_{\textsc{id}}(j)$. For every $\tau_0 = \_, \textsc{fn}(j_0) \prec \tau$, we let:*

$$\text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_0} \equiv \begin{pmatrix} \text{inj-auth}_\tau(\textsc{id}, j_0) \wedge \sigma_\tau^{\text{in}}(\text{e-auth}_{\textsc{n}}^{j_0}) \neq \mathsf{UnknownId} \\ \wedge\ \pi_1(g(\phi_\tau^{\text{in}})) = \textsc{guti}^{j_0} \oplus \mathsf{f}_{\mathsf{k}}^{\mathsf{r}}(\mathsf{n}^{j_0}) \wedge \pi_2(g(\phi_\tau^{\text{in}})) = \mathsf{Mac}_{\mathsf{k_m}}^5(\langle \textsc{guti}^{j_0}, \mathsf{n}^{j_0} \rangle) \end{pmatrix}$$

Then:

$$\text{accept}_\tau^{ID} \leftrightarrow \bigvee_{\substack{\tau_0 = \_, \textsc{fn}(j_0) \prec \tau \\ \tau_0 \not\prec_\tau \textsc{ns}_{ID}(\_)}} \text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_0}$$

Proof. Using Lemma 9 we know that:

$$\text{suc-auth}_\tau(\textsc{id}) \rightarrow \bigvee_{\text{s-started}_{j_0}(\tau)} \text{inj-auth}_\tau(\textsc{id}, j_0)$$

Let $\mathsf{k} \equiv \mathsf{k}_{\textsc{id}}$ and $\mathsf{k}_\mathsf{m} \equiv \mathsf{k}_\mathsf{m}^{\textsc{id}}$. Since:

$$\mathsf{accept}_\tau^{\textsc{id}} \;\equiv\; \mathsf{suc\text{-}auth}_\tau(\textsc{id}) \wedge \underbrace{\pi_2(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^5_{\mathsf{k_m}}(\langle \pi_1(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\mathrm{U}}^{\textsc{id}}))\,,\, \sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\mathrm{U}}^{\textsc{id}})\rangle)}_{\mathsf{EQMac}}$$

And since $\mathsf{inj\text{-}auth}_\tau(\textsc{id}, j_0) \;\rightarrow\; \mathsf{suc\text{-}auth}_\tau(\textsc{id})$ we have:

$$\begin{aligned}
\mathsf{accept}_\tau^{\textsc{id}} \;&\leftrightarrow\; \bigvee_{\mathsf{s\text{-}started}_{j_0}(\tau)} \mathsf{inj\text{-}auth}_\tau(\textsc{id}, j_0) \wedge \mathsf{EQMac}\\
&\leftrightarrow\; \bigvee_{\mathsf{s\text{-}started}_{j_0}(\tau)} \mathsf{inj\text{-}auth}_\tau(\textsc{id}, j_0) \wedge \pi_2(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^5_{\mathsf{k_m}}(\langle \pi_1(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0})\,,\, \mathsf{n}^{j_0}\rangle)
\end{aligned}$$

Using the $\textsc{p-euf-mac}^5$ and $\textsc{cr}^5$ axioms, it is easy to show that for every $j_0 \in \mathbb{N}$:

$$\pi_2(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^5_{\mathsf{k_m}}(\langle \pi_1(g(\phi_\tau^{\mathsf{in}}))\oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0})\,,\, \mathsf{n}^{j_0}\rangle) \rightarrow \begin{cases} \begin{pmatrix} \pi_1(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0}) = \textsc{guti}^{j_0} \\ \wedge\;\; \sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\mathrm{N}}^{j_0}) \neq \mathsf{UnknownId} \end{pmatrix} & \text{if } \textsc{fn}(j_0) \in \tau \\ \mathsf{false} & \text{otherwise} \end{cases}$$

Hence:

$$\begin{aligned}
\mathsf{accept}_\tau^{\textsc{id}} \;&\leftrightarrow\; \bigvee\nolimits_{\tau_0 = \_, \textsc{fn}(j_0) \prec \tau} \begin{pmatrix} \mathsf{inj\text{-}auth}_\tau(\textsc{id}, j_0) \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\mathrm{N}}^{j_0}) \neq \mathsf{UnknownId} \\ \wedge\; \pi_1(g(\phi_\tau^{\mathsf{in}})) = \textsc{guti}^{j_0} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0}) \wedge \pi_2(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^5_{\mathsf{k_m}}(\langle \textsc{guti}^{j_0}\,,\, \mathsf{n}^{j_0}\rangle) \end{pmatrix}\\
&\leftrightarrow\; \bigvee\nolimits_{\tau_0 = \_, \textsc{fn}(j_0) \prec \tau}\; \mathsf{fu\text{-}tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_0}
\end{aligned}$$

We conclude using **(B2)**:

$$\mathsf{accept}_\tau^{\textsc{id}} \;\;\leftrightarrow\;\; \bigvee_{\substack{\tau_0 = \_, \textsc{fn}(j_0) \prec \tau \\ \tau_0 \not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)}} \mathsf{fu\text{-}tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_0} \qquad \blacksquare$$

Using this acceptance characterization, we prove additional properties of the protocol:

- **(B3)**: if the user has a valid temporary identity (i.e. $\sigma_\tau(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\textsc{id}})$), then the variable $\textsc{guti}_{\mathrm{U}}^{\textsc{id}}$ is not unset.
- **(B4)**: if the network sequence number for $\textsc{id}$ increased between two instants τ_2 and τ_1, then this increase has been recorded by the variable $\mathsf{session}_{\mathrm{N}}^{\textsc{id}}$: there must exists an instant τ_x between τ_2 and τ_1 such that $\sigma_{\tau_1}^{\mathsf{in}}(\mathsf{session}_{\mathrm{N}}^{\textsc{id}}) = \mathsf{n}^{j_x}$, where τ_x ends by $\textsc{tn}(j_x, 0)$, $\textsc{tn}(j_x, 1)$ or $\textsc{pn}(j_x, 1)$.
- **(B5)**: the network sequence number is always smaller than the user sequence number: for every $\textsc{id}$, we have $\sigma_\tau(\textsc{sqn}_{\mathrm{N}}^{\textsc{id}}) \leq \sigma_\tau(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})$.
- **(B6)**: if τ_0 is the last reset of user $\textsc{id}$ (i.e. $\tau_0 = \_, \textsc{ns}_{\textsc{id}}(\_) \prec \tau$ and $\tau_0 \not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)$), and if $\textsc{id}$ is synced at an instant τ_1 between τ_0 and τ, then the *network* sequence number at instant τ_1 is greater than the *user* sequence number at the time of the reset (i.e. at τ_0).
- **(B7)**: if no $\textsc{assign-guti}$ session took place since the last reset of user $\textsc{id}$, then $\textsc{id}$ has no valid temporary identity.

Proposition 26. *For every valid action trace $\tau = \_, ai$ on $\mathcal{S}_{id}$ and identity $\textsc{id} \in \mathcal{S}_{id}$:*

- ***(B3)*** $\sigma_\tau(\mathsf{valid\text{-}guti}_{U}^{ID}) \;\rightarrow\; \sigma_\tau(\textsc{guti}_U^{ID}) \neq \mathit{UnSet}.$
- ***(B4)*** *For every $\tau_2 \prec_\tau \tau_1$:*

$$\sigma_{\tau_2}(\textsc{sqn}_N^{ID}) < \sigma_{\tau_1}^{in}(\textsc{sqn}_N^{ID}) \;\rightarrow\; \bigvee_{\substack{\tau_2 \prec_\tau \tau_x \prec_\tau \tau_1 \\ \tau_x = \_, \textsc{tn}(j_x, 0), \_, \textsc{tn}(j_x, 1) \text{ or } \_, \textsc{pn}(j_x, 1)}} \sigma_{\tau_1}^{in}(\mathsf{session}_N^{ID}) = n^{j_x}$$

- ***(B5)*** $\sigma_\tau(\textsc{sqn}_N^{ID}) \leq \sigma_\tau(\textsc{sqn}_U^{ID}).$

- ***(B6)*** *For every $\tau_0 \prec_\tau \tau_1$ such that $\tau_0 = \_, \textsc{ns}_{ID}(\_)$ or ϵ, and such that $\tau_0 \not\prec_\tau \textsc{ns}_{ID}(\_)$, we have:*
$$\sigma_{\tau_1}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \;\rightarrow\; \sigma_{\tau_1}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) > \sigma_{\tau_0}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}})$$
- ***(B7)*** *If for all $\tau' \leq \tau$ such that $\tau' \not\prec_\tau \textsc{ns}_{ID}(\_)$ we have $\tau' \neq \_, \textsc{fu}_{ID}(\_)$, then:*
$$\sigma_\tau(\mathsf{valid\text{-}guti}_{U}^{ID}) \;\rightarrow\; \mathit{false}$$

E.2 Proof of Proposition 26

Proof of **(B3)**. We show this by induction over τ. If $\tau = \epsilon$, we know from Definition 3 that $\sigma_\epsilon(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \mathsf{false}$ and $\sigma_\epsilon(\textsc{guti}_{\mathrm{X}}^{\mathrm{ID}}) \equiv \mathsf{UnSet}$. Therefore the property holds. Let $\tau = \tau_0, \mathsf{ai}$, assume by induction that the property holds for τ_0. If ai is different from $\textsc{tu}_{\mathrm{ID}}(j, 0), \textsc{pu}_{\mathrm{ID}}(j, 1)$ and $\textsc{fu}(j)$ then $\sigma_\tau^{\mathsf{up}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \sigma_\tau^{\mathsf{up}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \bot$, in which case we conclude immediately by induction hypothesis. We have three cases remaining:

- If $\mathsf{ai} = \textsc{tu}_{\mathrm{ID}}(j, 0)$ or $\mathsf{ai} = \textsc{pu}_{\mathrm{ID}}(j, 1)$ then $\sigma_\tau^{\mathsf{up}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \mathsf{false}$. Therefore the property holds.
- If $\mathsf{ai} = \textsc{fu}(j)$, using **(Equ1)** we can check that:
$$\mathsf{accept}_\tau^{\mathrm{ID}} \;\rightarrow\; \bigvee_{\substack{\tau_1 = \_, \textsc{fn}(j_0) \prec \tau \\ \tau_1 \not\prec_\tau \textsc{ns}_{\mathrm{ID}}(\_)}} \sigma_\tau(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}}) = \textsc{guti}^{j_0} \;\rightarrow\; \sigma_\tau(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}}) \neq \mathsf{UnSet}$$

We conclude by observing that $\sigma_\epsilon(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \mathsf{accept}_\tau^{\mathrm{ID}}$. ■

Proof of **(B4)**. We prove this directly. Intuitively, this holds because if $\sigma_{\tau_2}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$ then we know that $\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}$ was updated between τ_2 and τ_1. Moreover, if such an update occurs at $\tau_x = \_, \textsc{pn}(j_x, 1)$ or $\textsc{tn}(j_x, 1)$ then $\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}$ has to be equal to n^{j_x} after the update. Finally, the fact that $\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}$ is equal to n^{j_x} for some τ_x between τ_2 and τ_1 with $\tau_x = \_, \textsc{tn}(j_x, 0), \_, \textsc{tn}(j_x, 1)$ or $\_, \textsc{pn}(j_x, 1)$ is an invariant of the protocol. Now we give the formal proof.

First, we remark that $\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}$ is updated only at $\textsc{pn}(\_, 1)$ and $\textsc{tn}(\_, 1)$. Moreover, each update either left $\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}$ unchanged or increments it by at least one. Finally, it is updated at $\tau_x \prec \tau$ if and only if $\mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}}$ holds. If follows that:
$$\sigma_{\tau_2}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \;\rightarrow\; \bigvee_{\substack{\tau_2 \prec_\tau \tau_x \prec_\tau \tau_1 \\ \tau_x =, \_, \textsc{tn}(j_x, 1) \text{ or } \_, \textsc{pn}(j_x, 1)}} \mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}}$$

We know that for every $\tau_2 \prec_\tau \tau_x \prec_\tau \tau_1$, if:

- $\tau_x =, \_, \textsc{pn}(j_x, 1)$ then $\mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}} \rightarrow \sigma_{\tau_x}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j_x}$.
- $\tau_x = \_, \textsc{tn}(j_x, 1)$ then since $\mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}} \equiv \mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}} \wedge \sigma_{\tau_x}^{\mathsf{in}}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j_x}$, we know that $\mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}} \rightarrow \sigma_{\tau_x}^{\mathsf{in}}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j_x}$. Besides, since $\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}$ is not updated at $\textsc{tn}(j_x, 1)$ we deduce that $\mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}} \rightarrow \sigma_{\tau_x}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j_x}$.

Hence:
$$\sigma_{\tau_2}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \;\rightarrow\; \bigvee_{\substack{\tau_2 \prec_\tau \tau_x \prec \tau_1 \\ \tau_x =, \_, \textsc{tn}(j_x, 1) \text{ or } \_, \textsc{pn}(j_x, 1)}} \sigma_{\tau_x}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j_x} \tag{20}$$

Let $\tau_2 \prec_\tau \tau_x \prec_\tau \tau_1$ such that $\tau_x =, \_, \textsc{tn}(j_x, 1)$ or $\_, \textsc{pn}(j_x, 1)$. Now, we prove by induction over τ' such that $\tau_x \leq \tau' \prec \tau_1$ that:
$$\sigma_{\tau_x}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j_x} \;\rightarrow\; \bigvee_{\substack{\tau_x \leq \tau_n \leq \tau' \\ \tau_n = \_, \textsc{tn}(j_n, 0), \_, \textsc{tn}(j_n, 1) \text{ or } \_, \textsc{pn}(j_n, 1)}} \sigma_{\tau'}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j_n}$$

If $\tau' = \tau_x$ this is obvious. For the inductive case, we do a disjunction over the final action of τ'. If $\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}$ is not updated then we conclude by induction, otherwise we are in one of the following cases:

- If $\tau' = \_, \textsc{tn}(j', 0)$ then we do a case disjunction on $\mathsf{accept}^{\mathrm{ID}}_{\tau'}$:

$$\neg\mathsf{accept}^{\mathrm{ID}}_{\tau'} \rightarrow \sigma_{\tau'}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma^{\mathsf{in}}_{\tau'}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) \tag{21}$$

  Hence:

$$\begin{aligned}
&\neg\mathsf{accept}^{\mathrm{ID}}_{\tau'} \wedge \sigma_{\tau_x}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{n}^{j_x} \\
&\qquad \rightarrow \bigvee_{\substack{\tau_x \leq \tau_n < \tau' \\ \tau_n = \_, \textsc{tn}(j_n,0), \_, \textsc{tn}(j_n,1) \text{ or } \_, \textsc{pn}(j_n,1)}} \sigma_{\tau'}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{n}^{j_n} && \text{(By induction hypothesis and (21))} \\
&\qquad \rightarrow \bigvee_{\substack{\tau_x \leq \tau_n \leq \tau' \\ \tau_n = \_, \textsc{tn}(j_n,0), \_, \textsc{tn}(j_n,1) \text{ or } \_, \textsc{pn}(j_n,1)}} \sigma_{\tau'}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{n}^{j_n} && \text{(Relaxing the condition } \tau_n \prec \tau')
\end{aligned}$$

  Moreover,

$$\mathsf{accept}^{\mathrm{ID}}_{\tau'} \rightarrow \sigma_{\tau'}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{n}^{j'} \;\rightarrow \bigvee_{\substack{\tau_x \leq \tau_n \leq \tau' \\ \tau_n = \_, \textsc{tn}(j_n,0), \_, \textsc{tn}(j_n,1) \text{ or } \_, \textsc{pn}(j_n,1)}} \sigma_{\tau'}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{n}^{j_n}$$

  This concludes this case.
- If $\tau_n = \_, \textsc{pn}(j_n, 1)$ then the proof is the same than in the previous case, but doing a case disjunction over $\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau'}$.

Let $\tau_0{}'$ be such that $\tau_1 = \tau_0{}', \mathsf{ai}_1$. By applying the induction hypothesis to $\tau_0{}'$, we get:

$$\sigma_{\tau_x}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{n}^{j_x} \;\rightarrow \bigvee_{\substack{\tau_x \leq \tau_n \leq \tau_0{}' \\ \tau_n = \_, \textsc{tn}(j_n,0), \_, \textsc{tn}(j_n,1) \text{ or } \_, \textsc{pn}(j_n,1)}} \sigma_{\tau_0{}'}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{n}^{j_n} \;\rightarrow \bigvee_{\substack{\tau_x \leq \tau_n < \tau_1 \\ \tau_n = \_, \textsc{tn}(j_n,0), \_, \textsc{tn}(j_n,1) \text{ or } \_, \textsc{pn}(j_n,1)}} \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{n}^{j_n}$$

We conclude using (20) and the property above. ■

Proof of **(B5)**. We prove this by induction over τ. For $\tau = \epsilon$, from Definition 3 we know that $\sigma_\epsilon(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}) \equiv \mathsf{sqn\text{-}init}^{\mathrm{ID}}_{\mathrm{U}}$ and $\sigma_\epsilon(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}}) \equiv \mathsf{sqn\text{-}init}^{\mathrm{ID}}_{\mathrm{N}}$. Using $\textsc{sqn}$-ini, we know that $\mathsf{sqn\text{-}init}^{\mathrm{ID}}_{\mathrm{N}} \leq \mathsf{sqn\text{-}init}^{\mathrm{ID}}_{\mathrm{U}}$.

For the inductive case, let $\tau = \tau_0, \mathsf{ai}$ and assume that the property holds for τ_0. We have three cases:

- If ai is such that $\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}}$ is not updated. Using **(B1)** we know that $\sigma_\tau(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}) \geq \sigma_{\tau_0}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}})$, and we conclude by applying the induction hypothesis.
- If $\mathsf{ai} = \textsc{pn}(j, 1)$, then we do a case disjunction on $\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau}$. If it is true then:

$$\begin{aligned}
\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau} &\rightarrow \bigvee_{\tau_0 = \_, \textsc{pu}_{\mathrm{ID}}(j_0,1) \prec \tau} \sigma_\tau(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma^{\mathsf{in}}_{\tau_0}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}) && \text{(By } \textbf{(Acc1)}\text{)} \\
&\rightarrow \bigvee_{\tau_0 = \_, \textsc{pu}_{\mathrm{ID}}(j_0,1) \prec \tau} \sigma_\tau(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma^{\mathsf{in}}_{\tau_0}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \sigma^{\mathsf{in}}_{\tau_0}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}) \leq \sigma_\tau(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}) && \text{(By } \textbf{(B1)}\text{)} \\
&\rightarrow \sigma_\tau(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}}) \leq \sigma_\tau(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}})
\end{aligned}$$

  If $\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau}$ is false then $\neg\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau} \rightarrow \sigma_\tau(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}})$, and we conclude by applying the induction hypothesis.
- If $\mathsf{ai} = \textsc{tn}(j, 1)$, then we do a case disjunction on $\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau}$. First we handle the case where it is true. We summarize graphically this case in Figure 20. Let $\tau_2 = \_, \textsc{tn}(j, 0) \prec \tau$. We know that $\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau} \rightarrow \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{n}^{j}$. Moreover:

$$\sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{n}^{j} \;\rightarrow \bigwedge_{\substack{\tau_2 < \tau_1 < \tau \\ \tau_1 = \_, \textsc{tn}(j_x,0), \_, \textsc{tn}(j_x,1) \text{ or } \_, \textsc{pn}(j_x,1)}} \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{n}^{j_x}$$

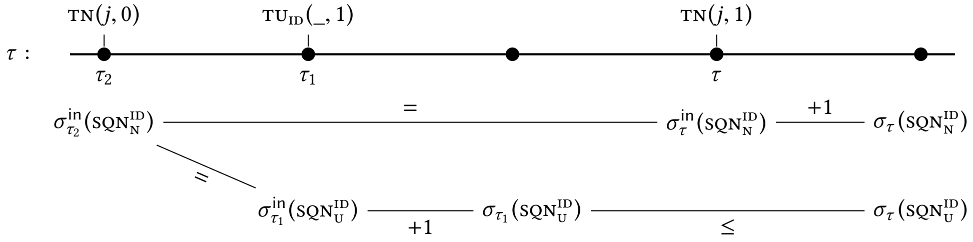

$\textsc{tn}(j,0)$
$\textsc{tu}_{\textsc{id}}(\_,1)$
$\textsc{tn}(j,1)$
τ :
τ_2
τ_1
τ
$\sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$
=
$\sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$
+1
$\sigma_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$
=
$\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
+1
$\sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
≤
$\sigma_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$

Fig. 20. Graphical Representation Used in the Proof of **(B5)**.

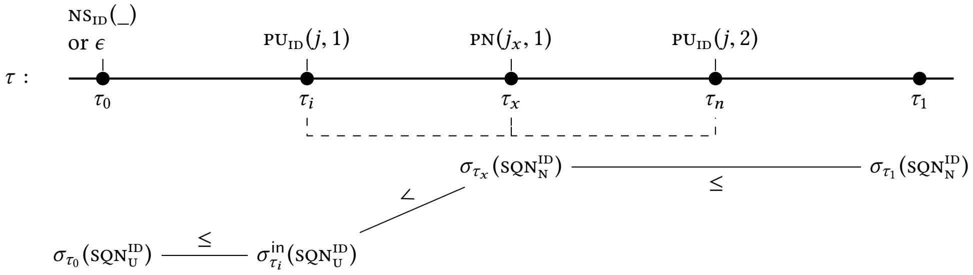

$\textsc{ns}_{\textsc{id}}(\_)$
or ϵ
$\textsc{pu}_{\textsc{id}}(j,1)$
$\textsc{pn}(j_x,1)$
$\textsc{pu}_{\textsc{id}}(j,2)$
τ :
τ_0
τ_i
τ_x
τ_n
τ_1
$\sigma_{\tau_x}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$
≤
$\sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$
∠
$\sigma_{\tau_0}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
≤
$\sigma^{\mathsf{in}}_{\tau_i}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$

Fig. 21. Graphical Representation Used in the Proof of **(B6)**.

$$\rightarrow\ \sigma_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \qquad \text{(Using the contrapositive of } \textbf{(B4)}\text{)}$$

$$\rightarrow\ \sigma_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \qquad \text{(Using } \textbf{(B1)}\text{)}$$

We know that $\mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau} \rightarrow \mathsf{accept}^{\textsc{id}}_{\tau}$. Moreover, using **(Acc3)** and **(Acc4)**, we check that:

$$\mathsf{accept}^{\textsc{id}}_{\tau} \ \rightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{tu}_{\textsc{id}}(\_,1) \\ \tau_2 \prec \tau_1 \prec \tau}} \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) = \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$$

Besides, $\mathsf{accept}^{\textsc{id}}_{\tau} \rightarrow \sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) = \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) + 1$, and using **(B1)** we know that $\sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) \leq \sigma_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$. Finally, $\mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau} \rightarrow \sigma_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) + 1$. Putting everything together:

$$\mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau} \rightarrow \sigma_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$$

Which is what we wanted.

If $\mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau}$ is false then $\neg\mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau} \rightarrow \sigma_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$, and we conclude by applying the induction hypothesis. ■

Proof of **(B6)**. First, observe that:

$$\sigma_{\tau_1}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \rightarrow \bigvee_{\substack{\tau_n = \_, \textsc{pu}_{\textsc{id}}(j,2) \\ \tau_0 \prec \tau_n \prec \tau_1}} \mathsf{accept}^{\textsc{id}}_{\tau_n} \tag{22}$$

Let $\tau_n = \_, \textsc{pu}_{\textsc{id}}(j,2)$ such that $\tau_0 \prec \tau_n \prec \tau_1$. Let $\tau_i = \_, \textsc{pu}_{\textsc{id}}(j,1)$ such that $\tau_i \prec \tau_n$. We know that $\tau_i \prec \tau_0$. We give a graphical summary of this proof in Figure 21. First, we apply **(Acc2)**:

$$\mathsf{accept}^{\textsc{id}}_{\tau_n} \ \rightarrow \bigvee_{\substack{\tau_x = \_, \textsc{pn}(j_x,1) \\ \tau_i \prec \tau_x \prec \tau_n}} \mathsf{accept}^{\textsc{id}}_{\tau_x} \ \wedge\ g(\phi^{\mathsf{in}}_{\tau_i}) = \mathsf{n}^{j_x} \ \wedge\ \pi_1(g(\phi^{\mathsf{in}}_{\tau_x})) = \{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_i}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\rangle\}^{\mathsf{n}^{j}_{\mathsf{e}}}_{\mathsf{pk}_{\textsc{n}}} \tag{23}$$

Let $\tau_x = \_, \textsc{pn}(j_x, 1)$ such that $\tau_i \prec \tau_x \prec \tau_n$. Using **(B1)**, we get that $\sigma_{\tau_0}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) \leq \sigma_{\tau_i}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}})$ and that $\sigma_{\tau_x}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \leq \sigma_{\tau_1}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$. There are two cases, depending on whether we have $\mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}}$.

- We know that $\mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}} \rightarrow \sigma_{\tau_x}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) = \sigma_{\tau_i}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) + 1 > \sigma_{\tau_i}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}})$. Putting everything together, we get that:

$$\mathsf{accept}_{\tau_n}^{\mathrm{ID}} \wedge \mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}} \rightarrow \sigma_{\tau_0}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau_1}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$$

- We know that:

$$\mathsf{accept}_{\tau_x}^{\mathrm{ID}} \wedge \neg\mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}} \wedge \pi_1(g(\phi_{\tau_x}^{\mathsf{in}})) = \{\langle \textsc{id}\,,\ \sigma_{\tau_i}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}} \rightarrow \sigma_{\tau_i}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau_x}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$$

  Moreover, $\neg\mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}} \rightarrow \sigma_{\tau_x}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) = \sigma_{\tau_x}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$. We recall that $\sigma_{\tau_0}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) \leq \sigma_{\tau_i}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}})$ and that $\sigma_{\tau_x}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \leq \sigma_{\tau_1}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$. Therefore:

$$\mathsf{accept}_{\tau_x}^{\mathrm{ID}} \wedge \neg\mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}} \wedge \pi_1(g(\phi_{\tau_x}^{\mathsf{in}})) = \{\langle \textsc{id}\,,\ \sigma_{\tau_i}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}} \rightarrow \sigma_{\tau_0}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau_1}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$$

Using (23) and the two cases above, we get that $\mathsf{accept}_{\tau_n}^{\mathrm{ID}} \rightarrow \sigma_{\tau_0}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau_1}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$.

Since this is true for all $\tau_n = \_, \textsc{pu}_{\textsc{id}}(j, 2)$ such that $\tau_0 \prec \tau_n \prec \tau_1$, we deduce from (22) that

$$\sigma_{\tau_1}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \rightarrow \sigma_{\tau_0}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau_1}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \qquad \blacksquare$$

Proof of **(B7)**. Let $\tau_{\textsc{ns}} = \epsilon$ or $\textsc{ns}_{\textsc{id}}(\_)$ be such that $\tau_{\textsc{ns}} \leq \tau$ and $\tau_{\textsc{ns}} \not\prec_{\tau} \textsc{ns}_{\textsc{id}}(\_)$. We show by induction over τ' with $\tau_{\textsc{ns}} \leq \tau' \leq \tau$ that $\sigma_{\tau'}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \mathsf{false}$.

For $\tau' = \tau_{\textsc{ns}}$, this is true using from Definition 3 if if $\tau_{\textsc{ns}} = \epsilon$, and from the protocol term definitions if $\tau_{\textsc{ns}} = \textsc{ns}_{\textsc{id}}(\_)$. The inductive case is straightforward. $\blacksquare$

E.3 A Full Set of Acceptance Condition Characterizations

We now design acceptance condition characterizations for all relevant action labels.

Lemma 11. *For every valid action trace $\tau = \_, ai$ on $\mathcal{S}_{id}$ and identity $\textsc{id} \in \mathcal{S}_{id}$:*

- ***(Equ2)*** *If $ai = \textsc{pu}_{\textsc{id}}(j, 2)$. Let $\tau_2 = \_, \textsc{pu}_{\textsc{id}}(j, 1)$ such that $\tau_2 \prec \tau$. For every $\tau_1 = \_, \textsc{pn}(j_1, 1)$, let:*

$$\mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\,\tau}^{\mathsf{n}:\tau_1} \equiv \begin{pmatrix} g(\phi_{\tau}^{\mathsf{in}}) = \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}^{2}(\langle \mathsf{n}^{j_1}\,,\ \mathsf{suc}(\sigma_{\tau_2}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}))\rangle) \\ \wedge\ g(\phi_{\tau_2}^{\mathsf{in}}) = \mathsf{n}^{j_1}\ \wedge\ \pi_1(g(\phi_{\tau_1}^{\mathsf{in}})) = \{\langle \textsc{id}\,,\ \sigma_{\tau_2}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}} \end{pmatrix}$$

  Then:

$$\mathsf{accept}_{\tau}^{ID} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{pn}(j_1, 1) \\ \tau_2 \prec_{\tau} \tau_1}} \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\,\tau}^{\mathsf{n}:\tau_1}$$

- ***(Equ3)*** *If $ai = \textsc{pn}(j, 1)$. Then:*

$$\begin{aligned} \mathsf{accept}_{\tau}^{ID} &\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{pu}_{ID}(j_1, 1) \\ \tau_1 \prec \tau}} \begin{pmatrix} g(\phi_{\tau_1}^{in}) = n^{j} \wedge \pi_1(g(\phi_{\tau}^{in})) = \{\langle \textsc{id},\ \sigma_{\tau_1}^{in}(\textsc{sqn}_{U}^{ID})\rangle\}_{pk_N}^{n_e^{j_1}} \\ \wedge\ \pi_2(g(\phi_{\tau}^{in})) = Mac_{k_m^{ID}}^{1}(\langle \{\langle \textsc{id},\ \sigma_{\tau_1}^{in}(\textsc{sqn}_{U}^{ID})\rangle\}_{pk_N}^{n_e^{j_1}}\,,\ g(\phi_{\tau_1}^{in})\rangle) \end{pmatrix} \\ &\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{pu}_{ID}(j_1, 1) \\ \tau_1 \prec \tau}} g(\phi_{\tau_1}^{in}) = n^{j} \wedge g(\phi_{\tau}^{in}) = t_{\tau_1} \end{aligned}$$

- ***(Equ4)*** *If $ai = \textsc{tu}_{ID}(j, 1)$. For every $\tau_1 = \_, \textsc{tn}(j_0, 0)$ such that $\tau_1 \prec \tau$, we let:*

$$\mathsf{c\text{-}tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \equiv \begin{pmatrix} \pi_3(g(\phi_{\tau}^{in})) = Mac_{k_m}^{3}(\langle n^{j_0}\,, \sigma_{\tau_1}^{in}(\textsc{sqn}_{N}^{ID})\,,\ \sigma_{\tau}^{in}(\textsc{guti}_{U}^{ID})\rangle) \wedge \sigma_{\tau}^{in}(\mathsf{s\text{-}valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \\ \wedge\ range(\sigma_{\tau}^{in}(\textsc{sqn}_{U}^{ID}), \sigma_{\tau_1}^{in}(\textsc{sqn}_{N}^{ID})) \wedge g(\phi_{\tau_1}^{in}) = \sigma_{\tau_1}^{in}(\textsc{guti}_{N}^{ID}) \wedge \pi_1(g(\phi_{\tau}^{in})) = n^{j_0} \\ \wedge\ \pi_2(g(\phi_{\tau}^{in})) = \sigma_{\tau_1}^{in}(\textsc{sqn}_{N}^{ID}) \oplus f_k(n^{j_0}) \wedge \sigma_{\tau}^{in}(\textsc{guti}_{U}^{ID}) = \sigma_{\tau_1}^{in}(\textsc{guti}_{N}^{ID}) \end{pmatrix}$$

Then:

$$\left(\mathsf{c\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \rightarrow \mathsf{accept}^{\mathrm{ID}}_{\tau_1}\right)_{\substack{\tau_1 = \_,\textsc{tn}(j_0,0)\\ \tau_1 \prec \tau}} \qquad\qquad \mathsf{accept}^{ID}_{\tau} \;\leftrightarrow\; \bigvee_{\substack{\tau_1 = \_,\textsc{tn}(j_0,0)\\ \tau_1 \prec \tau}} \mathsf{c\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$$

- ***(Equ5)*** *If $ai = \textsc{tn}(j,1)$. Let $\tau_1 = \_, \textsc{tn}(j,0)$ such that $\tau_1 \prec \tau$, and let $\textsc{id} \in \mathcal{S}_{id}$. Then:*

$$\mathsf{accept}^{ID}_{\tau} \;\leftrightarrow\; \bigvee_{\substack{\tau_i = \_,\textsc{tu}_{ID}(j_i,1)\\ \tau_1 \prec_\tau \tau_i}} \mathsf{c\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_i} \wedge g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^{4}_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\mathsf{n}^{j})$$

E.4 Proof of Lemma 11

Proof of **(Equ2)**. Using **(Acc2)** we know that:

$$\begin{aligned}
\mathsf{accept}^{\mathrm{ID}}_{\tau} \;&\leftrightarrow\; \bigvee_{\substack{\tau_1 = \_,\textsc{pn}(j_1,1)\\ \tau_2 \prec_\tau \tau_1}} \mathsf{accept}^{\mathrm{ID}}_{\tau} \;\wedge\; g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1} \;\wedge\; \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}}\\
&\leftrightarrow\; \bigvee_{\substack{\tau_1 = \_,\textsc{pn}(j_1,1)\\ \tau_2 \prec_\tau \tau_1}} \left(\begin{array}{l} \quad g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^{2}_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}\,,\, \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}})\rangle) \;\wedge\; g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1}\\ \wedge\; \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}} \end{array}\right)
\end{aligned}$$

Since $\sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}) \;\equiv\; \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}))$:

$$\begin{aligned}
&\leftrightarrow\; \bigvee_{\substack{\tau_1 = \_,\textsc{pn}(j_1,1)\\ \tau_2 \prec_\tau \tau_1}} \left(\begin{array}{l} \quad g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^{2}_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}\,,\, \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}))\rangle) \;\wedge\; g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1}\\ \wedge\; \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}} \end{array}\right)\\
&\leftrightarrow\; \bigvee_{\substack{\tau_1 = \_,\textsc{pn}(j_1,1)\\ \tau_2 \prec_\tau \tau_1}} \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}
\end{aligned}$$

■

Proof of **(Equ3)**. Using **(Acc1)** it is easy to check that:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau} \;\leftrightarrow\; \bigvee_{\tau_1 = \_,\textsc{pu}_{\mathrm{ID}}(j_1,1) \prec \tau} \left(\begin{array}{l} \quad \underset{\cdots\cdots\cdots}{g(\phi^{\mathsf{in}}_{\tau_1}) = \mathsf{n}^{j}} \wedge \underset{\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim}{\pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}}}\\ \wedge\; \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^{1}_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \underset{\sim\sim\sim\sim\sim}{\pi_1(g(\phi^{\mathsf{in}}_{\tau}))}\,,\; \underset{\cdots}{\mathsf{n}^{j}}\rangle) \end{array}\right)$$

Which can be rewritten as follows (we identify above, using waves and dots, which equalities are used, and which terms are rewritten):

$$\leftrightarrow\; \bigvee_{\tau_1 = \_,\textsc{pu}_{\mathrm{ID}}(j_1,1) \prec \tau} \left(\begin{array}{l} \quad g(\phi^{\mathsf{in}}_{\tau_1}) = \mathsf{n}^{j} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}}\\ \wedge\; \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^{1}_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}}\,,\, g(\phi^{\mathsf{in}}_{\tau_1})\rangle) \end{array}\right)$$

First, observe that:

$$\{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}} = \pi_1(t_{\tau_1}) \qquad\qquad \mathsf{Mac}^{1}_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}}\,,\, g(\phi^{\mathsf{in}}_{\tau_1})\rangle) = \pi_2(t_{\tau_1})$$

We conclude using the injectivity of the pair. ■

Proof of **(Equ4)**. Using **(Acc3)** we know that:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau} \leftrightarrow \bigvee_{\substack{\tau_1 = \_,\textsc{tn}(j_0,0)\\ \tau_1 \prec \tau}} \left(\begin{array}{l} \mathsf{accept}^{\mathrm{ID}}_{\tau} \wedge \mathsf{accept}^{\mathrm{ID}}_{\tau_1} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0}\\ \wedge\; \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f}_{\mathsf{k}}(\mathsf{n}^{j_0}) \wedge \sigma^{\mathsf{in}}_{\tau}(\textsc{guti}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\textsc{guti}^{\mathrm{ID}}_{\mathrm{N}}) \end{array}\right)$$

Inlining the definition of $\mathrm{accept}^{\mathrm{ID}}_{\tau_1}$:

$$\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \mathrm{TN}(j_0,0)\\ \tau_1 \prec \tau}} \left(\begin{array}{l} \mathrm{accept}^{\mathrm{ID}}_{\tau} \wedge g(\phi^{\mathsf{in}}_{\tau_1}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{UnSet} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0} \\ \wedge\, \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0}) \wedge \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \end{array} \right)$$

Inlining the definition of $\mathrm{accept}^{\mathrm{ID}}_{\tau}$:

$$\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \mathrm{TN}(j_0,0)\\ \tau_1 \prec \tau}} \left(\begin{array}{l} \pi_3(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \underline{\pi_1(g(\phi^{\mathsf{in}}_{\tau}))}\, , \pi_2(g(\phi^{\mathsf{in}}_{\tau})) \oplus \mathsf{f_k}(\underline{\pi_1(g(\phi^{\mathsf{in}}_{\tau}))})\, ,\, \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})\rangle) \\ \wedge\, \sigma^{\mathsf{in}}_{\tau}(\text{s-valid-guti}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{range}(\sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}), \pi_2(g(\phi^{\mathsf{in}}_{\tau})) \oplus \mathsf{f_k}(\underline{\pi_1(g(\phi^{\mathsf{in}}_{\tau}))})) \\ g(\phi^{\mathsf{in}}_{\tau_1}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{UnSet} \wedge \underline{\pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0}} \\ \wedge\, \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0}) \wedge \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \end{array} \right)$$

We rewrite $\pi_1(g(\phi^{\mathsf{in}}_{\tau}))$ into n^{j_0}:

$$\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \mathrm{TN}(j_0,0)\\ \tau_1 \prec \tau}} \left(\begin{array}{l} \pi_3(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \underline{\mathsf{n}^{j_0}}\, , \underline{\pi_2(g(\phi^{\mathsf{in}}_{\tau})) \oplus \mathsf{f_k}(\underline{\mathsf{n}^{j_0}})}\, ,\, \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})\rangle) \\ \wedge\, \sigma^{\mathsf{in}}_{\tau}(\text{s-valid-guti}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{range}(\sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}), \underline{\pi_2(g(\phi^{\mathsf{in}}_{\tau})) \oplus \mathsf{f_k}(\underline{\mathsf{n}^{j_0}})}) \\ g(\phi^{\mathsf{in}}_{\tau_1}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{UnSet} \wedge \underline{\pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0}} \\ \wedge\, \underline{\pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0})} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \end{array} \right)$$

We rewrite $\pi_2(g(\phi^{\mathsf{in}}_{\tau})) \oplus \mathsf{f_k}(\mathsf{n}^{j_0})$ into $\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$:

$$\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \mathrm{TN}(j_0,0)\\ \tau_1 \prec \tau}} \left(\begin{array}{l} \pi_3(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}\, , \underline{\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})}\, ,\, \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})\rangle) \\ \wedge\, \sigma^{\mathsf{in}}_{\tau}(\text{s-valid-guti}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{range}(\sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}), \underline{\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})}) \\ \wedge\, g(\phi^{\mathsf{in}}_{\tau_1}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{UnSet} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0} \\ \wedge\, \underline{\pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0})} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \end{array} \right) \tag{24}$$

Let $\tau_2 = \_, \mathrm{TU}_{\mathrm{ID}}(j_0, 0) \prec \tau$. By validity of τ, there are no user ID actions between τ_2 and τ, and therefore it is easy to check that $\sigma^{\mathsf{in}}_{\tau}(\text{s-valid-guti}^{\mathrm{ID}}_{\mathrm{U}}) \rightarrow \sigma^{\mathsf{in}}_{\tau_2}(\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}})$, and that $\sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})$. Moreover, using **(B3)** we know that $\sigma^{\mathsf{in}}_{\tau_2}(\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}}) \rightarrow \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) \neq \mathsf{UnSet}$. Therefore $\sigma^{\mathsf{in}}_{\tau}(\text{s-valid-guti}^{\mathrm{ID}}_{\mathrm{U}}) \rightarrow \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) \neq \mathsf{UnSet}$. It follows that:

$$\left(\sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \sigma^{\mathsf{in}}_{\tau}(\text{s-valid-guti}^{\mathrm{ID}}_{\mathrm{U}})\right) \;\rightarrow\; \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{UnSet}$$

Hence we can simplify (24) by removing $\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{UnSet}$. This yields:

$$\begin{aligned} \mathrm{accept}^{\mathrm{ID}}_{\tau} &\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \mathrm{TN}(j_0,0)\\ \tau_1 \prec \tau}} \left(\begin{array}{l} \pi_3(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}\, , \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})\, ,\, \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})\rangle) \wedge \sigma^{\mathsf{in}}_{\tau}(\text{s-valid-guti}^{\mathrm{ID}}_{\mathrm{U}}) \\ \wedge\, \mathsf{range}(\sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})) \wedge g(\phi^{\mathsf{in}}_{\tau_1}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0} \\ \wedge\, \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0}) \wedge \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \end{array} \right) \\ &\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \mathrm{TN}(j_0,0)\\ \tau_1 \prec \tau}} \text{c-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \end{aligned}$$

Finally, we check that for every $\tau_1 = \_, \mathrm{TN}(j_0, 0)$ such that $\tau_1 \prec \tau$, we have $\text{c-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \rightarrow \mathrm{accept}^{\mathrm{ID}}_{\tau_1}$. ■

Proof of **(Equ5)**. Using **(Acc4)** we know that:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau} \;\leftrightarrow\; \bigvee_{\tau_i = \_, \textsc{tu}_{\mathrm{ID}}(j_i,1) \prec \tau} \mathsf{accept}^{\mathrm{ID}}_{\tau} \wedge \mathsf{accept}_{\tau_i} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^j$$

Moreover, using **(Equ4)** we know that:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau} \leftrightarrow \bigvee_{\substack{\tau_i = \_, \textsc{tu}_{\mathrm{ID}}(j_i,1) \prec \tau \\ \tau_2 = \_, \textsc{tn}(j_2,0) \prec \tau_i}} \mathsf{accept}^{\mathrm{ID}}_{\tau} \wedge \text{c-tr}^{\mathsf{n}:\tau_2}_{\mathsf{u}:\tau_i} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^j$$

Let $\tau_2 = \_, \textsc{tn}(j_2, 0) \prec \tau_i$. Then we know that $\text{c-tr}^{\mathsf{n}:\tau_2}_{\mathsf{u}:\tau_i} \rightarrow \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^{j_2}$. Therefore using =-ind we know that if $j_2 \neq j$:

$$\left(\text{c-tr}^{\mathsf{n}:\tau_2}_{\mathsf{u}:\tau_i} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^j\right) \rightarrow \left(\pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^{j_2} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^j\right) \rightarrow \mathsf{false}$$

Hence:

$$\begin{aligned} \mathsf{accept}^{\mathrm{ID}}_{\tau} &\leftrightarrow \bigvee_{\substack{\tau_i = \_, \textsc{tu}_{\mathrm{ID}}(j_i,1) \\ \tau_1 \prec_\tau \tau_i}} \mathsf{accept}^{\mathrm{ID}}_{\tau} \wedge \text{c-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_i} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^j \\ &\leftrightarrow \bigvee_{\substack{\tau_i = \_, \textsc{tu}_{\mathrm{ID}}(j_i,1) \\ \tau_1 \prec_\tau \tau_i}} \mathsf{accept}^{\mathrm{ID}}_{\tau} \wedge \text{c-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_i} \qquad (\text{Since } \text{c-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_i} \rightarrow \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^j) \end{aligned}$$

We inline the definition of $\mathsf{accept}^{\mathrm{ID}}_{\tau}$:

$$\leftrightarrow \bigvee_{\substack{\tau_i = \_, \textsc{tu}_{\mathrm{ID}}(j_i,1) \\ \tau_1 \prec_\tau \tau_i}} g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^4_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\mathsf{n}^j) \wedge \sigma^{\mathsf{in}}_{\tau}(\text{b-auth}^j_{\mathrm{N}}) = \textsc{id} \wedge \text{c-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_i}$$

Using **(Equ4)**, we know that for every $\tau_1 = \_, \textsc{tn}(j_0, 0)$ such that $\tau_1 \prec \tau$, $\text{c-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \rightarrow \mathsf{accept}^{\mathrm{ID}}_{\tau_1}$. Moreover, using **(A6)** we know that $\mathsf{accept}^{\mathrm{ID}}_{\tau_1} \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\text{b-auth}^j_{\mathrm{N}}) = \textsc{id}$. Besides, $\sigma^{\mathsf{in}}_{\tau_1}(\text{b-auth}^j_{\mathrm{N}}) = \textsc{id} \rightarrow \sigma^{\mathsf{in}}_{\tau}(\text{b-auth}^j_{\mathrm{N}}) = \textsc{id}$. Hence $\text{c-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \rightarrow \sigma^{\mathsf{in}}_{\tau}(\text{b-auth}^j_{\mathrm{N}}) = \textsc{id}$. By consequence:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau} \;\leftrightarrow\; \bigvee_{\substack{\tau_i = \_, \textsc{tu}_{\mathrm{ID}}(j_i,1) \\ \tau_1 \prec_\tau \tau_i}} g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^4_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\mathsf{n}^j) \wedge \text{c-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_i} \qquad \blacksquare$$

E.5 $\textsc{guti}^{\mathrm{ID}}_{\mathrm{U}}$ Concealment

Lemma 12. *Let τ be a valid action trace on $\mathcal{S}_{id}$ and $\textsc{id}_x \in \mathcal{S}_{id}$. For every $\tau_a = \_, \textit{TN}(j_a, 1)$ or $\tau_a = \_, \textit{PN}(j_a, 1)$ such that $\tau_a \preceq \tau$, and for every $\tau_b = \textit{PU}_{\textit{ID}_x}(j_i, 1)$ or $\tau_b = \textit{TU}_{\textit{ID}_x}(j_i, 1)$ such that $\tau_b \prec \tau_a$, if:*

$$\{\tau_1 \mid \tau_b \prec_\tau \tau_1\} \cap \{\textit{PU}_{\textit{ID}_x}(j, \_), \textit{TU}_{\textit{ID}_x}(j, \_), \textit{FU}_{\textit{ID}_x}(j) \mid j \in \mathbb{N}\} \subseteq \{\textit{PU}_{\textit{ID}_x}(j_i, 2), \textit{FU}_{\textit{ID}_x}(j_i)\}$$

Then there exists a derivation of:

$$\text{inc-accept}^{\textit{ID}_x}_{\tau_a} \wedge \sigma_{\tau_b}(\textit{b-auth}^{\textit{ID}_x}_{U}) = n^{j_a} \wedge \mathsf{accept}^{\textit{ID}_x}_{\tau_b} \rightarrow g(\phi^{in}_{\tau}) \neq \textit{GUTI}^{j_a}$$

Proof. Let β_τ be the term:

$$\beta_\tau \equiv \text{inc-accept}^{\mathrm{ID_x}}_{\tau_a} \wedge \sigma_{\tau_b}(\text{b-auth}^{\mathrm{ID_x}}_{\mathrm{U}}) = \mathsf{n}^{j_a} \wedge \mathsf{accept}^{\mathrm{ID_x}}_{\tau_b}$$

For every $\tau_a \preceq \tau_x \preceq \tau$, we let $\mathsf{leak}^{\mathsf{in}}_{\tau_x}$ be the vector containing the terms (in an arbitrary but fixed order):

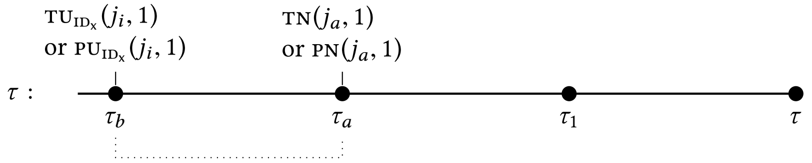
- $\mathsf{leak}^{\mathsf{in}}_{\tau_0}$ if $\tau_x = \tau_0, \mathsf{ai}_0$ and $\tau_a \prec \tau_x$.
- The term β_τ.
- All the keys except $\mathsf{k}^{\mathrm{ID_x}}$, $\mathsf{k}^{\mathrm{ID_x}}_{\mathsf{m}}$ and the asymmetric secret key sk_{N}.
- All elements of $\sigma^{\mathsf{in}}_{\tau_x}$, except:

  - All the user $\textsc{id}_{\textsc{x}}$ values, i.e. for every $\textsc{x}$, $\sigma^{\mathsf{in}}_{\tau_x}(\textsc{x}^{\textsc{id}_\textsc{x}}_{\textsc{u}}) \notin \mathsf{leak}^{\mathsf{in}}_{\tau_x}$.
  - The network's $\textsc{guti}$ value of user $\textsc{id}_{\textsc{x}}$, i.e. $\sigma^{\mathsf{in}}_{\tau_x}(\textsc{guti}^{\textsc{id}_\textsc{x}}_{\textsc{n}}) \notin \mathsf{leak}^{\mathsf{in}}_{\tau_x}$.
- For every $\tau_a \preceq \tau_n \preceq \tau$ such that $\tau_n = \_, \textsc{fn}(j)$, the term $\mathsf{Mac}^4_{\mathsf{k}^{\textsc{id}_\textsc{x}}_{\mathsf{m}}}(\mathsf{n}^j)$.
- For every $\tau_a \preceq \tau_n \preceq \tau$ such that $\tau_n = \_, \textsc{pn}(j, 1)$ then $\mathsf{Mac}^4_{\mathsf{k}^{\textsc{id}_\textsc{x}}_{\mathsf{m}}}(\mathsf{n}^j)$, for every $\tau_2 = \_, \textsc{pu}_{\textsc{id}_\textsc{x}}(j_2, 1) \preceq \tau_b$, the term $\mathsf{Mac}^2_{\mathsf{k}^{\textsc{id}_\textsc{x}}_{\mathsf{m}}}(\langle \mathsf{n}^j\ , \ \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))\rangle)$.

Let $\textsc{guti}$ be a fresh name. We show by induction on τ_1 in $\tau_a \preceq \tau_1 \prec \tau$ that there are derivations of:

$$[\beta_\tau]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \textsc{guti}^{j_a}\right) \sim [\beta_\tau]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \textsc{guti}\right) \qquad \text{and} \qquad \beta_\tau \rightarrow \sigma_{\tau_1}(\textsc{guti}^{\textsc{id}_\textsc{x}}_{\textsc{n}}) = \textsc{guti}^{j_a}$$

We depict the situation below:



$\textsc{tu}_{\textsc{id}_\textsc{x}}(j_i, 1)$
or $\textsc{pu}_{\textsc{id}_\textsc{x}}(j_i, 1)$
$\textsc{tn}(j_a, 1)$
or $\textsc{pn}(j_a, 1)$
τ :
τ_b
τ_a
τ_1
τ

Case $\tau_1 = \tau_a$ First, $\beta_\tau \rightarrow \mathsf{inc\text{-}accept}^{\textsc{id}_\textsc{x}}_{\tau_a}$, and $\mathsf{inc\text{-}accept}^{\textsc{id}_\textsc{x}}_{\tau_a} \rightarrow \sigma_{\tau_a}(\textsc{guti}^{\textsc{id}_\textsc{x}}_{\textsc{n}}) = \textsc{guti}^{j_a}$. Therefore:

$$\beta_\tau \rightarrow \sigma_{\tau_a}(\textsc{guti}^{\textsc{id}_\textsc{x}}_{\textsc{n}}) = \textsc{guti}^{j_a}$$

Then, we observe from the definition of leak_{τ_a} that $\textsc{guti}^{j_a} \notin \mathsf{st}(\mathsf{leak}_{\tau_a})$ (since $\sigma_{\tau_a}(\textsc{guti}^{\textsc{id}_\textsc{x}}_{\textsc{n}})$ is *not* in leak_{τ_a}). Moreover $\textsc{guti}^{j_a}$ does not appear in $\phi^{\mathsf{in}}_{\tau_a}$ and t_{τ_a}. Besides, $\textsc{guti}$ is a fresh name. By consequence we can apply the Fresh axiom, and then conclude using Refl:

$$\dfrac{\dfrac{}{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}\right) \sim \left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}\right)}\ \mathsf{Refl}}{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \textsc{guti}^{j_a}\right) \sim \left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \textsc{guti}\right)}\ \mathsf{Fresh}$$

Case $\tau_a \prec \tau_1$ Let ai be such that $\tau_1 = \_, \mathsf{ai}$. Assume by induction that we have derivations of:

$$\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \textsc{guti}^{j_a}\right) \sim \left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \textsc{guti}\right) \tag{25}$$

$$\beta_\tau \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\textsc{guti}^{\textsc{id}_\textsc{x}}_{\textsc{n}}) = \textsc{guti}^{j_a} \tag{26}$$

Part 1 First, we show that:

$$\beta_\tau \rightarrow \sigma_{\tau_1}(\textsc{guti}^{\textsc{id}_\textsc{x}}_{\textsc{n}}) = \textsc{guti}^{j_a}$$

Since we know that (26) holds, we just need to look at the ai that update $\textsc{guti}^{\textsc{id}_\textsc{x}}_{\textsc{n}}$ to conclude:

- If $\mathsf{ai} = \textsc{tn}(j, 0)$. Using (25), we know that $\left[\beta_\tau\right]g(\phi^{\mathsf{in}}_{\tau_1}) \neq \textsc{guti}^{j_a}$. Hence using (26):

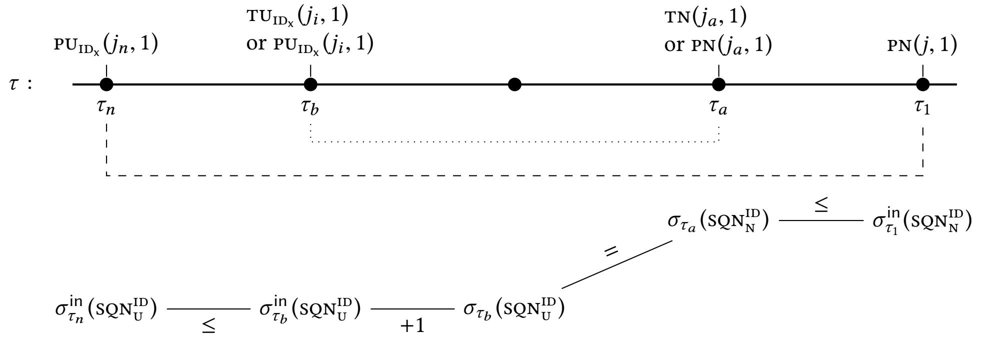
  $$\beta_\tau \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\textsc{guti}^{\textsc{id}_\textsc{x}}_{\textsc{n}}) \neq g(\phi^{\mathsf{in}}_{\tau_1})$$

  Which shows that $\beta_\tau \rightarrow \neg\mathsf{accept}^{\textsc{id}_\textsc{x}}_{\tau_1}$. This concludes this case.
- If $\mathsf{ai} = \textsc{pn}(j, 1)$. Since $\tau_a = \textsc{tn}(j_a, 1)$ or $\textsc{pn}(j_a, 1)$, we know by validity of τ that $j_a \neq j$. We give a graphical summary of this proof in Figure 22. Using **(Equ3)** we know that:

  $$\mathsf{accept}^{\textsc{id}_\textsc{x}}_{\tau_1} \rightarrow \bigvee_{\substack{\tau_n = \_, \textsc{pu}_{\textsc{id}}(j_n, 1)\\ \tau_n \prec \tau_1}} g(\phi^{\mathsf{in}}_{\tau_n}) = \mathsf{n}^j \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \{\langle \textsc{id}_\textsc{x}\ , \ \sigma^{\mathsf{in}}_{\tau_n}(\textsc{sqn}^{\textsc{id}_\textsc{x}}_{\textsc{u}})\rangle\}^{\mathsf{n}^{j_n}_{\mathsf{e}}}_{\mathsf{pk}_\textsc{n}} \tag{27}$$

  Since $j_a \neq j$ we know that $\mathsf{n}^j \neq \mathsf{n}^{j_a}$. Moreover:

  $$\sigma_{\tau_b}(\mathsf{b\text{-}auth}^{\textsc{id}_\textsc{x}}_{\textsc{u}}) = \mathsf{n}^{j_a} \wedge \mathsf{accept}^{\textsc{id}_\textsc{x}}_{\tau_b} \rightarrow g(\phi^{\mathsf{in}}_{\tau_b}) = \mathsf{n}^{j_a}$$



$\mathrm{PU}_{\mathrm{ID_x}}(j_n,1)$
$\mathrm{TU}_{\mathrm{ID_x}}(j_i,1)$
or $\mathrm{PU}_{\mathrm{ID_x}}(j_i,1)$
$\mathrm{TN}(j_a,1)$
or $\mathrm{PN}(j_a,1)$
$\mathrm{PN}(j,1)$
τ :
τ_n
τ_b
τ_a
τ_1
$\sigma_{\tau_a}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$
$\leq$
$\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$
$=$
$\sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$
$\leq$
$\sigma^{\mathsf{in}}_{\tau_b}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$
$+1$
$\sigma_{\tau_b}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$

Fig. 22. Graphical Representation Used in the Proof of Lemma 12

Hence $\beta_\tau \rightarrow g(\phi^{\mathsf{in}}_{\tau_b}) \neq \mathsf{n}^j$. Moreover, for every τ' between τ_b and τ_1, we know that $\tau' \neq \mathrm{PU}_{\mathrm{ID_x}}(\_,1)$. Therefore we know that:

$$\beta_\tau \wedge \mathsf{accept}^{\mathrm{ID_x}}_{\tau_1} \rightarrow \bigvee_{\substack{\tau_n = \_, \mathrm{PU}_{\mathrm{ID}}(j_n,1)\\ \tau_n \prec \tau_b}} g(\phi^{\mathsf{in}}_{\tau_n}) = \mathsf{n}^j \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \{\langle \mathrm{ID_x}\, ,\, \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{U}})\rangle\}^{\mathsf{n}_{\mathsf{e}}^{j_n}}_{\mathsf{pk}_{\mathrm{N}}}$$

Let $\tau_n = \_, \mathrm{PU}_{\mathrm{ID}}(j_n,1)$ such that $\tau_n \prec \tau_b$. We know that:

$$\beta_\tau \rightarrow \sigma_{\tau_a}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{N}}) = \sigma_{\tau_b}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{U}}) = \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_b}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{U}}))$$

Since $\sigma_{\tau_a}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{N}}) \leq \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{N}})$ and $\sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{U}}) \leq \sigma^{\mathsf{in}}_{\tau_b}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{U}})$, we deduce that:

$$\beta_\tau \wedge \mathsf{accept}^{\mathrm{ID_x}}_{\tau_1} \wedge g(\phi^{\mathsf{in}}_{\tau_n}) = \mathsf{n}^j \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{N}}) > \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{U}})$$

Moreover:

$$\begin{aligned}\beta_\tau \wedge \mathsf{inc\text{-}accept}^{\mathrm{ID_x}}_{\tau_1} \wedge g(\phi^{\mathsf{in}}_{\tau_n}) = \mathsf{n}^j \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \{\langle \mathrm{ID_x}\, ,\, \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{U}})\rangle\}^{\mathsf{n}_{\mathsf{e}}^{j_n}}_{\mathsf{pk}_{\mathrm{N}}}&\\ \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{N}}) \leq \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{U}})&\end{aligned}$$

Hence:

$$\beta_\tau \wedge \mathsf{accept}^{\mathrm{ID_x}}_{\tau_1} \wedge g(\phi^{\mathsf{in}}_{\tau_n}) = \mathsf{n}^j \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \{\langle \mathrm{ID_x}\, ,\, \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID_x}}_{\mathrm{U}})\rangle\}^{\mathsf{n}_{\mathsf{e}}^{j_n}}_{\mathsf{pk}_{\mathrm{N}}} \rightarrow \neg\mathsf{inc\text{-}accept}^{\mathrm{ID_x}}_{\tau_1}$$

Using (27), this shows that:

$$\beta_\tau \wedge \mathsf{accept}^{\mathrm{ID_x}}_{\tau_1} \rightarrow \neg\mathsf{inc\text{-}accept}^{\mathrm{ID_x}}_{\tau_1} \tag{28}$$

This concludes this case.

- If ai $= \mathrm{TN}(j,1)$. Since $\tau_a = \mathrm{TN}(j_a,1)$ or $\mathrm{PN}(j_a,1)$, we know by validity of τ that $j_a \neq j$. From the induction hypothesis we know that $\beta_\tau \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID_x}}_{\mathrm{N}}) = \mathrm{GUTI}^{j_a}$. It is easy to check that:

$$\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID_x}}_{\mathrm{N}}) = \mathrm{GUTI}^{j_a} \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{session}^{\mathrm{ID_x}}_{\mathrm{N}}) = \mathsf{n}^{j_a}$$

Hence, since $j \neq j_a$:

$$\begin{aligned}\beta_\tau \quad\rightarrow\quad \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{session}^{\mathrm{ID_x}}_{\mathrm{N}}) = \mathsf{n}^{j_a} \quad\rightarrow\quad \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{session}^{\mathrm{ID_x}}_{\mathrm{N}}) \neq \mathsf{n}^j&\\ \rightarrow\quad \neg\mathsf{inc\text{-}accept}^{\mathrm{ID_x}}_{\tau_1} \quad\rightarrow\quad \sigma_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID_x}}_{\mathrm{N}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID_x}}_{\mathrm{N}}) = \mathrm{GUTI}^{j_a}&\end{aligned}$$

Which concludes this case.

Part 2 We now show that:

$$\left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \textsc{guti}^{j_a}\right) \sim \left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \textsc{guti}\right)$$

We do a case disjunction on ai. We only details the case where ai is a symbolic action of user $\textsc{id}$, with $\textsc{id} \neq \textsc{id}_{\mathsf{x}}$, and the case where ai $= \textsc{fn}(j_a)$. All the other cases are similar to these two cases, and their proof will only be sketched.

- If ai is a symbolic action of user $\textsc{id}$, with $\textsc{id} \neq \textsc{id}_{\mathsf{x}}$, then for every $u \in \mathsf{leak}_{\tau_1} \backslash \mathsf{leak}^{\mathsf{in}}_{\tau_1}$ (resp. $u \equiv t_{\tau_1}$) we show that there exists a many-hole context C_u such that $u \equiv C_u[\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}]$ and C_u does not contain any nonce in $\mathcal{N}$.

  We only detail the case ai $= \textsc{fu}_{\textsc{id}}(j)$. First, observe that:

$$\mathsf{accept}^{\textsc{id}}_{\tau_1} \equiv \left(\begin{array}{ll} & \mathsf{eq}(\pi_2(g(\underline{\phi^{\mathsf{in}}_{\tau_1}})), \mathsf{Mac}^5_{\underline{\mathsf{k_m}}}(\langle \pi_1(g(\underline{\phi^{\mathsf{in}}_{\tau_1}})) \oplus \mathsf{f}^{\mathsf{r}}_{\underline{\mathsf{k}}}(\underline{\sigma^{\mathsf{in}}_{\tau_1}(\text{e-auth}^{\textsc{id}}_{\textsc{u}})}) \,,\, \underline{\sigma^{\mathsf{in}}_{\tau_1}(\text{e-auth}^{\textsc{id}}_{\textsc{u}})}\rangle)) \\ \wedge & \neg\mathsf{eq}(\underline{\sigma^{\mathsf{in}}_{\tau_1}(\text{e-auth}^{\textsc{id}}_{\textsc{u}})}, \mathsf{fail}) \end{array} \right)$$

  All the underlined subterms are in $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}$, therefore there exists C_{accept} such that $\mathsf{accept}^{\textsc{id}}_{\tau_1} \equiv C_{\mathsf{accept}}[\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}]$. Remark that $\mathsf{leak}_{\tau_1} \backslash \mathsf{leak}^{\mathsf{in}}_{\tau_1} = \{\sigma^{\mathsf{in}}_{\tau_1}(\text{valid-guti}^{\textsc{id}}_{\textsc{u}}), \sigma^{\mathsf{in}}_{\tau_1}(\textsc{guti}^{\textsc{id}}_{\textsc{u}})\}$. Moreover:

$$t_{\tau_1} \equiv \text{if } \mathsf{accept}^{\textsc{id}}_{\tau_1} \text{ then ok else error} \qquad \sigma^{\mathsf{in}}_{\tau_1}(\text{valid-guti}^{\textsc{id}}_{\textsc{u}}) \equiv \mathsf{accept}^{\textsc{id}}_{\tau_1}$$

$$\sigma^{\mathsf{in}}_{\tau_1}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) \equiv \text{if } \mathsf{accept}^{\textsc{id}}_{\tau_1} \text{ then } \pi_1(g(\underline{\phi^{\mathsf{in}}_{\tau_1}})) \oplus \mathsf{f}^{\mathsf{r}}_{\underline{\mathsf{k}}}(\underline{\sigma^{\mathsf{in}}_{\tau_1}(\text{e-auth}^{\textsc{id}}_{\textsc{u}})}) \text{ else UnSet}$$

  Using the fact that all the underlined subterms are in $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}$, and using C_{accept} it is easy to build the wanted contexts.

  We then conclude using the FA rule under context, the Dup rule and the induction hypothesis:

$$\dfrac{\dfrac{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \textsc{guti}^{j_a}\right) \sim \left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \textsc{guti}\right)}{\begin{array}{c}\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \textsc{guti}^{j_a}, (C_u[\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}])_{u \in \{t_{\tau_1}, \mathsf{leak}_{\tau_1} \backslash \mathsf{leak}^{\mathsf{in}}_{\tau_1}\}}\right) \\ \sim \left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \textsc{guti}, (C_u[\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}])_{u \in \{t_{\tau_1}, \mathsf{leak}_{\tau_1} \backslash \mathsf{leak}^{\mathsf{in}}_{\tau_1}\}}\right)\end{array}} (\mathsf{FA_c} + \mathsf{Dup})^*}{\left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \textsc{guti}^{j_a}\right) \sim \left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \textsc{guti}\right)} R$$

- If ai $= \textsc{fn}(j_a)$. It is easy to check that:

$$\sigma^{\mathsf{in}}_{\tau_a}(\text{e-auth}^{j_a}_{\textsc{n}}) \neq \textsc{id}_{\mathsf{x}} \rightarrow \sigma^{\mathsf{in}}_{\tau_a}(\textsc{guti}^{\textsc{id}_{\mathsf{x}}}_{\textsc{n}}) \neq \textsc{guti}^{j_a} \rightarrow \sigma^{\mathsf{in}}_{\tau}(\textsc{guti}^{\textsc{id}_{\mathsf{x}}}_{\textsc{n}}) \neq \textsc{guti}^{j_a}$$

  Therefore using the induction property (26) we deduce that $\beta_\tau \rightarrow \sigma^{\mathsf{in}}_{\tau_a}(\text{e-auth}^{j_a}_{\textsc{n}}) = \textsc{id}_{\mathsf{x}}$. Moreover by validity of τ, there are no session j_a network actions between τ_a and τ_1. It follows that $\sigma^{\mathsf{in}}_{\tau_a}(\text{e-auth}^{j_a}_{\textsc{n}}) = \textsc{id}_{\mathsf{x}} \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\text{e-auth}^{j_a}_{\textsc{n}}) = \textsc{id}_{\mathsf{x}}$. Hence:

$$[\beta_\tau] t_{\tau_1} = [\beta_\tau] \langle \textsc{guti}^{j_a} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\textsc{id}_{\mathsf{x}}}}(\mathsf{n}^{j_a}) \,,\, \mathsf{Mac}^5_{\mathsf{k}^{\textsc{id}_{\mathsf{x}}}_{\mathsf{m}}}(\langle \textsc{guti}^{j_a} \,,\, \mathsf{n}^{j_a} \rangle) \rangle$$

  Observe that:

$$\left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \textsc{guti}^{j_a}\right) = \left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \langle \textsc{guti}^{j_a} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\textsc{id}_{\mathsf{x}}}}(\mathsf{n}^{j_a}) \,,\, \mathsf{Mac}^5_{\mathsf{k}^{\textsc{id}_{\mathsf{x}}}_{\mathsf{m}}}(\langle \textsc{guti}^{j_a} \,,\, \mathsf{n}^{j_a} \rangle) \rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \textsc{guti}^{j_a}\right)$$

  We are now going to apply the $\textsc{prf}$-f axiom on the left to replace $\textsc{guti}^{j_a} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\textsc{id}_{\mathsf{x}}}}(\mathsf{n}^{j_a})$ with $\textsc{guti}^{j_a} \oplus \mathsf{n_f}$ where $\mathsf{n_f}$ is a fresh nonce. For every $\tau_2 = \_, \textsc{fu}_{\textsc{id}}(\_) \prec \tau_1$, we use **(Equ1)** to replace every occurrences of accept_{τ_2} in $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \beta_\tau$ with:

$$\gamma_{\tau_2} \equiv \bigvee_{\substack{\tau_3 = \_, \textsc{fn}(\_) \prec \tau_2 \\ \tau_3 \not\prec_{\tau_2} \textsc{ns}_{\textsc{id}}(\_)}} \text{fu-tr}^{\mathsf{n}:\tau_3}_{\mathsf{u}:\tau_2}$$

which yields the terms $\phi'^{\mathsf{in}}_{\tau_1}, \mathsf{leak}'^{\mathsf{in}}_{\tau_1}, \beta'_\tau$. We can check that:

$$\text{set-prf}^{\,\mathsf{f}^{\mathsf{r}}}_{\mathsf{k}^{\mathrm{ID_x}}}(\gamma_{\tau_2}) \subseteq \{\mathsf{n}^p \mid \exists \tau' = \_, \textsc{fn}(p) \prec \tau_1\}$$

And that:

$$\text{set-prf}^{\,\mathsf{f}^{\mathsf{r}}}_{\mathsf{k}^{\mathrm{ID_x}}}(\phi'^{\mathsf{in}}_{\tau_1}, \mathsf{leak}'^{\mathsf{in}}_{\tau_1}) = \{\mathsf{n}^p \mid \exists \tau' = \_, \textsc{fn}(p) \prec \tau_1\}$$

Therefore we can apply the PRF-f axiom as wanted: first we replace $\phi^{\mathsf{in}}_{\tau_1}$, $\mathsf{leak}^{\mathsf{in}}_{\tau_1}$, β_τ by $\phi'^{\mathsf{in}}_{\tau_1}$, $\mathsf{leak}'^{\mathsf{in}}_{\tau_1}$, β'_τ using rule R; then we apply the PRF-f axiom; and finally we rewrite all γ_{τ_2} back into $\mathsf{accept}^{\mathrm{ID_x}}_{\tau_2}$. Finally, we use the $\oplus$-indep axiom to replace $\mathrm{GUTI}^{j_a} \oplus \mathsf{n_f}$ with a fresh nonce n'_{f}. This yields:

$$\cfrac{\cfrac{\cfrac{\cfrac{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \langle \mathsf{n}'_{\mathsf{f}}\,,\ \mathrm{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_{\mathsf{m}}}(\langle \mathrm{GUTI}^{j_a}\ ,\ \mathsf{n}^{j_a}\rangle)\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \ \sim\ \left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \langle \mathrm{GUTI}^{j_a} \oplus \mathsf{n_f}\,,\ \mathrm{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_{\mathsf{m}}}(\langle \mathrm{GUTI}^{j_a}\ ,\ \mathsf{n}^{j_a}\rangle)\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \ \sim\ \left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ \oplus\text{-indep}}{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \langle \mathrm{GUTI}^{j_a} \oplus \mathsf{n_f}\,,\ \mathrm{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_{\mathsf{m}}}(\langle \mathrm{GUTI}^{j_a}\ ,\ \mathsf{n}^{j_a}\rangle)\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \ \sim\ \left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ R}{\left[\beta'_\tau\right]\left(\phi'^{\mathsf{in}}_{\tau_1}, \langle \mathrm{GUTI}^{j_a} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\mathrm{ID_x}}}(\mathsf{n}^{j_a})\,,\ \mathrm{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_{\mathsf{m}}}(\langle \mathrm{GUTI}^{j_a}\ ,\ \mathsf{n}^{j_a}\rangle)\rangle, \mathsf{leak}'^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \ \sim\ \left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ \textsc{prf}\text{-f}}{\left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \ \sim\ \left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ R$$

We do a similar reasoning to replace $\mathrm{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_{\mathsf{m}}}(\langle \mathrm{GUTI}^{j_a}\ ,\ \mathsf{n}^{j_a}\rangle)$ with a fresh nonce $\mathsf{n}''_{\mathsf{f}}$ using the PRF-MAC^5 axiom (we omit the details):

$$\frac{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \langle \mathsf{n}'_{\mathsf{f}}\,,\ \mathsf{n}''_{\mathsf{f}}\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim \left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \left\langle \mathsf{n}'_{\mathsf{f}}\,,\ \mathrm{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_{\mathsf{m}}}(\langle \mathrm{GUTI}^{j_a}\ ,\ \mathsf{n}^{j_a}\rangle)\right\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim \left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ (R + \textsc{prf-mac}^5)^*$$

We then do the same thing on the right side, and use the FA axiom under context

$$\cfrac{\cfrac{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{n}'_{\mathsf{f}}, \mathsf{n}''_{\mathsf{f}}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \ \sim\ \left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{n}'_{\mathsf{f}}, \mathsf{n}''_{\mathsf{f}}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right)}{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \left\langle \mathsf{n}'_{\mathsf{f}}\,,\ \mathsf{n}''_{\mathsf{f}}\right\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \ \sim\ \left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \left\langle \mathsf{n}'_{\mathsf{f}}\,,\ \mathsf{n}''_{\mathsf{f}}\right\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right)}\ \mathsf{FA_c}}{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \left\langle \mathsf{n}'_{\mathsf{f}}\,,\ \mathsf{n}''_{\mathsf{f}}\right\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \ \sim\ \left[\beta_\tau\right]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ \mathsf{Ax}^*$$

Using the fact that $\beta_\tau \in \mathsf{leak}^{\mathsf{in}}_{\tau_1}$, we have:

$$\frac{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right), \mathsf{n}'_{\mathsf{f}}, \mathsf{n}''_{\mathsf{f}}, \ \sim\ \left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right), \mathsf{n}'_{\mathsf{f}}, \mathsf{n}''_{\mathsf{f}},}{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{n}'_{\mathsf{f}}, \mathsf{n}''_{\mathsf{f}}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \ \sim\ \left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{n}'_{\mathsf{f}}, \mathsf{n}''_{\mathsf{f}}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right)}\ \mathsf{Simp}$$

We then conclude using Fresh twice:

$$\frac{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \ \sim\ \left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right)}{\left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right), \mathsf{n}'_{\mathsf{f}}, \mathsf{n}''_{\mathsf{f}} \ \sim\ \left[\beta_\tau\right]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right), \mathsf{n}'_{\mathsf{f}}, \mathsf{n}''_{\mathsf{f}}}\ \mathsf{Fresh}^2$$

- We now sketch the proof of the induction property for the remaining cases:
  - If $\mathsf{ai} = \textsc{fn}(j)$ with $j \neq j_a$. First, we decompose t_{τ_1} into terms of $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}$, except for the term:

    $$\left\langle \mathrm{GUTI}^{j} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\mathrm{ID_x}}}(\mathsf{n}^{j})\,,\ \mathrm{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_{\mathsf{m}}}(\langle \mathrm{GUTI}^{j}\ ,\ \mathsf{n}^{j}\rangle)\right\rangle$$

    The rest of the proof goes as in case $\mathsf{ai} = \textsc{fn}(j_a)$. On both side, we do the following:
    * We apply the PRF-f axiom to replace $\mathrm{GUTI}^{j} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\mathrm{ID_x}}}(\mathsf{n}^{j})$ with $\mathrm{GUTI}^{j} \oplus \mathsf{n_f}$ where $\mathsf{n_f}$ is a fresh nonce.
    * We use the $\oplus$-ind axiom to replace $\mathrm{GUTI}^{j} \oplus \mathsf{n_f}$ with a fresh nonce n'_{f}

  ∗ We apply the PRF-MAC^5 axiom to replace $\mathsf{Mac}^5_{\mathsf{k}_\mathsf{m}^{\mathrm{ID_x}}}(\langle \mathrm{GUTI}^j, \mathsf{n}^j\rangle)$ with a fresh nonce n_f''. Finally we use Fresh to get rid of the introduced nonces n_f' and n_f''.

- If ai $=$ TN$(j,0)$. Using the induction hypothesis we know that $\beta_\tau \rightarrow \neg\mathsf{accept}_{\tau_1}^{\mathrm{ID_x}}$. We can therefore rewrite all occurrences of $\mathsf{accept}_{\tau_1}^{\mathrm{ID_x}}$ into false under the condition β_τ. This removes all occurrences of $\sigma_{\tau_1}^{\mathsf{in}}(\mathrm{GUTI}_\mathrm{N}^{\mathrm{ID_x}})$ in $\mathsf{leak}_{\tau_1}\backslash\mathsf{leak}_{\tau_1}^{\mathsf{in}}$ and t_{τ_1}. We can then decompose the resulting terms into terms of $\phi_{\tau_1}^{\mathsf{in}}, \mathsf{leak}_{\tau_1}^{\mathsf{in}}$.
- If ai $=$ TN$(j,1)$. We can decompose $\mathsf{leak}_{\tau_1}\backslash\mathsf{leak}_{\tau_1}^{\mathsf{in}}$ and t_{τ_1} into terms of $\phi_{\tau_1}^{\mathsf{in}}, \mathsf{leak}_{\tau_1}^{\mathsf{in}}$ (we use the fact that $\mathsf{leak}_{\tau_1}^{\mathsf{in}}$ contains $\mathsf{Mac}^4_{\mathsf{k}_\mathsf{m}^{\mathrm{ID_x}}}(\mathsf{n}^j)$).
- If ai $=$ PN$(j,0)$. This is trivial using Fresh.
- If ai $=$ PN$(j,1)$. We use **(Equ3)** to rewrite all occurrences of $\mathsf{accept}_{\tau_1}^{\mathrm{ID_x}}$ in $\mathsf{leak}_{\tau_1}\backslash\mathsf{leak}_{\tau_1}^{\mathsf{in}}$ and t_{τ_1}:

$$\mathsf{accept}_{\tau_1}^{\mathrm{ID_x}} \leftrightarrow \bigvee_{\substack{\tau_2 = \_,\mathrm{PU}_{\mathrm{ID_x}}(j_2,1)\\ \tau_2 < \tau_1}} g(\phi_{\tau_2}^{\mathsf{in}}) = \mathsf{n}^j \wedge g(\phi_{\tau_1}^{\mathsf{in}}) = t_{\tau_2}$$

  We can then decompose the resulting terms into terms of $\phi_{\tau_1}^{\mathsf{in}}, \mathsf{leak}_{\tau_1}^{\mathsf{in}}$. This uses the fact that the terms:

$$\left(\mathsf{Mac}^2_{\mathsf{k}_\mathsf{m}^{\mathrm{ID_x}}}(\langle \mathsf{n}^j, \mathsf{suc}(\sigma_{\tau_2}^{\mathsf{in}}(\mathrm{SQN}_\mathrm{U}^{\mathrm{ID}}))\rangle)\right)_{\substack{\tau_2 = \_,\mathrm{PU}_{\mathrm{ID_x}}(j_2,1)\\ \tau_2 < \tau_1}}$$

  are included in $\mathsf{leak}_{\tau_1}^{\mathsf{in}}$, since $\{\tau_2 = \_, \mathrm{PU}_{\mathrm{ID_x}}(j_2,1) \mid \tau_2 \prec \tau_1\} = \{\tau_2 = \_, \mathrm{PU}_{\mathrm{ID_x}}(j_2,1) \mid \tau_2 \prec \tau_b\}$.
- If ai is a symbolic action of user ID, with ID $=$ ID$_\mathrm{x}$, then either ai $=$ PU$_{\mathrm{ID_x}}(j_i, 2)$ or ai $=$ FU$_{\mathrm{ID_x}}(j_i)$.

  ∗ If ai $=$ PU$_{\mathrm{ID_x}}(j_i,2)$, then we show using **(Equ2)** that:

$$\beta_\tau \rightarrow \left(\mathsf{accept}_{\tau_1}^{\mathrm{ID_x}} \leftrightarrow g(\phi_{\tau_1}^{\mathsf{in}}) = t_{\tau_a}\right)$$

  Therefore we can rewrite $\mathsf{accept}_{\tau_1}^{\mathrm{ID_x}}$ into $g(\phi_{\tau_1}^{\mathsf{in}}) = t_{\tau_a}$ under β_τ in t_{τ_1}. The resulting term can be easily decomposed into terms of $\phi_{\tau_1}^{\mathsf{in}}, \mathsf{leak}_{\tau_1}^{\mathsf{in}}$.

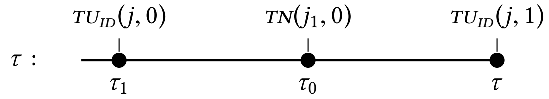
  ∗ ai $=$ FU$_{\mathrm{ID_x}}(j_i)$. We do a similar reasoning, but using **(Equ1)** instead of **(Equ2)**. We omit the details. ■

E.6 Stronger Characterizations

Using the GUTI concealment lemma, we can show the following stronger version of **(Acc3)**:

LEMMA 13. *For every valid action trace $\tau = \_, ai$ on $\mathcal{S}_{id}$ and identity ID $\in \mathcal{S}_{id}$:*

- ***(StrAcc1)*** *If ai $=$ TU$_{ID}(j,1)$. Let $\tau_1 = _, $ TU$_{ID}(j,0)$ such that $\tau_1 \prec \tau$, and let $k \equiv k^{ID}$. Then:*



$$\mathsf{accept}_\tau^{ID} \rightarrow \bigvee_{\substack{\tau_0 = \_,TN(j_0,0)\\ \tau_1 <_\tau \tau_0}} \left(\begin{array}{l} \mathsf{accept}_{\tau_0}^{ID} \ \wedge\ g(\phi_{\tau_0}^{in}) = \sigma_{\tau_1}^{in}(GUTI_U^{ID}) \ \wedge\ \pi_1(g(\phi_\tau^{in})) = n^{j_0} \\ \wedge\ \pi_2(g(\phi_\tau^{in})) = \sigma_{\tau_0}^{in}(SQN_N^{ID}) \oplus f_k(n^{j_0}) \wedge \sigma_\tau^{in}(GUTI_U^{ID}) = \sigma_{\tau_0}^{in}(GUTI_N^{ID}) \end{array}\right)$$

PROOF. First, by applying **(Acc3)** we get that:

$$\mathsf{accept}_\tau^{\mathrm{ID}} \rightarrow \bigvee_{\substack{\tau_0 = \_,\mathrm{TN}(j_0,0)\\ \tau_0 < \tau}} \left(\begin{array}{l} \mathsf{accept}_{\tau_0}^{\mathrm{ID}} \wedge \pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0} \wedge \pi_2(g(\phi_\tau^{\mathsf{in}})) = \sigma_{\tau_0}^{\mathsf{in}}(\mathrm{SQN}_\mathrm{N}^{\mathrm{ID}}) \oplus \mathsf{f}_\mathsf{k}(\mathsf{n}^{j_0}) \\ \wedge\ \sigma_\tau^{\mathsf{in}}(\mathrm{GUTI}_\mathrm{U}^{\mathrm{ID}}) = \sigma_{\tau_0}^{\mathsf{in}}(\mathrm{GUTI}_\mathrm{N}^{\mathrm{ID}}) \end{array}\right) \qquad (29)$$

We have $\text{accept}_\tau^{\textsc{id}} \rightarrow \sigma_\tau^{\mathsf{in}}(\text{s-valid-guti}_{\textsc{u}}^{\textsc{id}})$, and $\sigma_\tau^{\mathsf{in}}(\text{s-valid-guti}_{\textsc{u}}^{\textsc{id}}) \rightarrow \sigma_{\tau_1}^{\mathsf{in}}(\text{valid-guti}_{\textsc{u}}^{\textsc{id}})$. Let $\tau_0 = \_, \textsc{tn}(j_0, 0)$, we know that $\text{accept}_{\tau_0}^{\textsc{id}} \rightarrow \sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}}) \neq \text{UnSet}$. Therefore:

$$\text{accept}_\tau^{\textsc{id}} \rightarrow \bigvee_{\substack{\tau_0 = \_, \textsc{tn}(j_0,0) \\ \tau_0 \prec \tau}} \begin{pmatrix} \text{accept}_{\tau_0}^{\textsc{id}} \wedge \pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0} \wedge \pi_2(g(\phi_\tau^{\mathsf{in}})) = \sigma_{\tau_0}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) \oplus \mathsf{f}_{\mathsf{k}}(\mathsf{n}^{j_0}) \\ \wedge\ \sigma_\tau^{\mathsf{in}}(\textsc{guti}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}}) \wedge \sigma_\tau^{\mathsf{in}}(\textsc{guti}_{\textsc{u}}^{\textsc{id}}) \neq \text{UnSet} \wedge \sigma_{\tau_1}^{\mathsf{in}}(\text{valid-guti}_{\textsc{u}}^{\textsc{id}}) \end{pmatrix}$$

We want to get a contradiction if $\tau_0 \prec \tau_1$. Let $\tau_0 = \_, \textsc{tn}(j_0, 0) \prec \tau$, and assume that $\tau_0 \prec \tau_1$. If there does not exists any τ_2 such that $\tau_2 = \_, \textsc{fu}_{\textsc{id}}(j_i) \prec \tau_1$, then it is easy to show that $\sigma_\tau^{\mathsf{in}}(\textsc{guti}_{\textsc{u}}^{\textsc{id}}) = \text{UnSet}$. In that case, from the equation above we get that $\neg\text{accept}_\tau^{\textsc{id}}$, which concludes this case.

Therefore, let τ_2 be maximal w.r.t. $\prec$ such that $\tau_2 = \_, \textsc{fu}_{\textsc{id}}(j_i) \prec \tau_1$. We have $\tau_2 \not\prec_\tau \textsc{fu}_{\textsc{id}}(\_)$. Assume that there exists a user $\textsc{id}$ action between τ_2 and τ_1. It is easy to show by induction over τ' in $\tau_2 \prec \tau' \leq \tau_1$ that, since there are no $\textsc{fu}_{\textsc{id}}(\_)$ action between τ_2 and τ_1, we have $\neg\sigma_{\tau_1}^{\mathsf{in}}(\text{valid-guti}_{\textsc{u}}^{\textsc{id}})$. This implies $\neg\text{accept}_\tau^{\textsc{id}}$, which concludes this case.

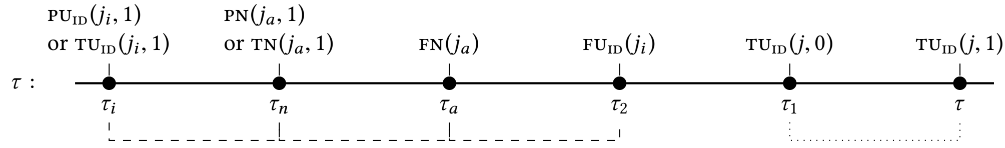
Therefore we can safely assume that there are no user $\textsc{id}$ actions between τ_2 and τ_1. We deduce that $\sigma_{\tau_1}^{\mathsf{in}}(\text{valid-guti}_{\textsc{u}}^{\textsc{id}}) \rightarrow \text{accept}_{\tau_2}^{\textsc{id}}$. Hence $\text{accept}_\tau^{\textsc{id}} \rightarrow \text{accept}_{\tau_2}^{\textsc{id}}$. By applying **(Equ1)** to τ_2, we know that:

$$\text{accept}_\tau^{\textsc{id}} \rightarrow \bigvee_{\substack{\tau_a = \_, \textsc{fn}(j_a) \prec \tau_2 \\ \tau_a \not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)}} \text{fu-tr}_{\mathsf{u}:\tau_2}^{\mathsf{n}:\tau_a} \tag{30}$$

We recall that:

$$\text{fu-tr}_{\mathsf{u}:\tau_2}^{\mathsf{n}:\tau_a} \equiv \begin{pmatrix} \text{inj-auth}_{\tau_2}(\textsc{id}, j_a) \wedge \sigma_{\tau_2}^{\mathsf{in}}(\text{e-auth}_{\textsc{n}}^{j_a}) \neq \text{UnknownId} \\ \wedge\ \pi_1(g(\phi_{\tau_2}^{\mathsf{in}})) = \textsc{guti}^{j_a} \oplus \mathsf{f}_{\mathsf{k}}^{\mathsf{r}}(\mathsf{n}^{j_a}) \wedge\ \pi_2(g(\phi_{\tau_2}^{\mathsf{in}})) = \mathsf{Mac}_{\mathsf{k_m}}^5(\langle \textsc{guti}^{j_a}\ ,\ \mathsf{n}^{j_a} \rangle) \end{pmatrix}$$

Let $\tau_a = \_, \textsc{fn}(j_a) \prec \tau_2$ such that $\tau_a \not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)$. We know that there exists $\tau_n = \_, \textsc{pn}(j_a, 1)$ or $\tau_n = \_, \textsc{tn}(j_a, 1)$ such that $\tau_n \prec \tau_a$, and that $\text{fu-tr}_{\mathsf{u}:\tau_2}^{\mathsf{n}:\tau_a} \rightarrow \text{accept}_{\tau_n}^{\textsc{id}}$. Let $\tau_i = \_, \textsc{pu}_{\textsc{id}}(j_i, 1)$ or $\_, \textsc{tu}_{\textsc{id}}(j_i, 1)$ such that $\tau_i \prec \tau_2$. If $\tau_n \prec \tau_i$, we show using **(Acc1)** if $\tau_n = \_, \textsc{pn}(j_a, 1)$ or **(Acc4)** if $\tau_n = \_, \textsc{pn}(j_a, 1)$ that we have $\neg\text{fu-tr}_{\mathsf{u}:\tau_2}^{\mathsf{n}:\tau_a}$. Therefore, we assume that $\tau_i \prec \tau_n$. We depict the situation below:


$\textsc{pu}_{\textsc{id}}(j_i, 1)$
or $\textsc{tu}_{\textsc{id}}(j_i, 1)$
$\textsc{pn}(j_a, 1)$
or $\textsc{tn}(j_a, 1)$
$\textsc{fn}(j_a)$
$\textsc{fu}_{\textsc{id}}(j_i)$
$\textsc{tu}_{\textsc{id}}(j, 0)$
$\textsc{tu}_{\textsc{id}}(j, 1)$
τ :
τ_i
τ_n
τ_a
τ_2
τ_1
τ

We check that $\text{fu-tr}_{\mathsf{u}:\tau_2}^{\mathsf{n}:\tau_a} \rightarrow \sigma_{\tau_2}(\textsc{guti}_{\textsc{u}}^{\textsc{id}}) = \textsc{guti}^{j_a}$. Moreover, since there are no user $\textsc{id}$ actions between τ_2 and τ_1 or between τ_1 and τ, $\sigma_{\tau_2}(\textsc{guti}_{\textsc{u}}^{\textsc{id}}) = \sigma_\tau^{\mathsf{in}}(\textsc{guti}_{\textsc{u}}^{\textsc{id}})$. From (29), we know that $\text{accept}_\tau^{\textsc{id}} \rightarrow \sigma_\tau^{\mathsf{in}}(\textsc{guti}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}})$. It follows that:

$$\text{accept}_\tau^{\textsc{id}} \wedge \text{fu-tr}_{\mathsf{u}:\tau_2}^{\mathsf{n}:\tau_a} \rightarrow \sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}}) = \textsc{guti}^{j_a} \tag{31}$$

If $\tau_0 \prec \tau_n$, then it is easy to check that $\sigma_{\tau_0}^{\mathsf{in}}(\textsc{guti}_{\textsc{n}}^{\textsc{id}}) \neq \textsc{guti}^{j_a}$. Therefore we have $\neg(\text{accept}_\tau^{\textsc{id}} \wedge \text{fu-tr}_{\mathsf{u}:\tau_2}^{\mathsf{n}:\tau_a})$.

Now, we assume that $\tau_n \prec \tau_0$. Recall that we assumed $\tau_0 \prec \tau_1$. Our goal is to apply the $\textsc{guti}$ concealment lemma (Lemma 12) to τ_0 get a contradiction. We can check that the following hypothesis of Lemma 12 is true:

$$\{\tau' \mid \tau_i \prec_{\tau_0} \tau_b\} \cap \{\textsc{pu}_{\textsc{id}}(j, \_), \textsc{tu}_{\textsc{id}}(j, \_), \textsc{fu}_{\textsc{id}}(j) \mid j \in \mathbb{N}\} \subseteq \{\textsc{pu}_{\textsc{id}}(j_i, 2), \textsc{fu}_{\textsc{id}}(j_i)\}$$

We deduce that:

$$\text{inc-accept}_{\tau_n}^{\textsc{id}} \wedge \sigma_{\tau_i}(\text{b-auth}_{\textsc{u}}^{\textsc{id}}) = \mathsf{n}^{j_a} \wedge \text{accept}_{\tau_i}^{\textsc{id}_{\mathsf{x}}} \rightarrow g(\phi_{\tau_0}^{\mathsf{in}}) \neq \textsc{guti}^{j_a} \tag{32}$$

We know that:

$$\text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_2} \rightarrow \text{accept}^{\textsc{id}}_{\tau_i} \wedge \sigma_{\tau_i}(\text{b-auth}^{\textsc{id}}_{\textsc{u}}) = \text{n}^{j_a} \tag{33}$$

Moreover, $\neg\text{inc-accept}^{\textsc{id}}_{\tau_n} \rightarrow \sigma_{\tau_n}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) \neq \textsc{guti}^{j_a}$. It is straightforward to check that $\neg\text{inc-accept}^{\textsc{id}}_{\tau_n} \rightarrow \sigma_{\tau_0}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) \neq \textsc{guti}^{j_a}$. Therefore, using (31) we get that:

$$\text{accept}^{\textsc{id}}_{\tau} \wedge \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_2} \wedge \neg\text{inc-accept}^{\textsc{id}}_{\tau_n} \rightarrow \left(\sigma^{\text{in}}_{\tau_0}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) = \textsc{guti}^{j_a} \wedge \sigma^{\text{in}}_{\tau_0}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) \neq \textsc{guti}^{j_a}\right) \rightarrow \text{false}$$

Hence $\text{accept}^{\textsc{id}}_{\tau} \wedge \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_2} \rightarrow \text{inc-accept}^{\textsc{id}}_{\tau_n}$. Therefore using (32) and (33), we get:

$$\text{accept}^{\textsc{id}}_{\tau} \wedge \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_2} \rightarrow g(\phi^{\text{in}}_{\tau_0}) \neq \textsc{guti}^{j_a} \tag{34}$$

We have $\text{accept}^{\textsc{id}}_{\tau_0} \rightarrow g(\phi^{\text{in}}_{\tau_0}) = \sigma^{\text{in}}_{\tau_0}(\textsc{guti}^{\textsc{id}}_{\textsc{n}})$. We get from this, (31) and (34) that:

$$\text{accept}^{\textsc{id}}_{\tau} \wedge \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_2} \wedge \text{accept}^{\textsc{id}}_{\tau_0} \rightarrow \text{false}$$

This holds for every $\tau_a = \_, \textsc{fn}(j_a) \prec \tau_2$. We deduce from (30) that:

$$\text{accept}^{\textsc{id}}_{\tau} \wedge \text{accept}^{\textsc{id}}_{\tau_0} \rightarrow \text{false}$$

Since we have this for every $\tau_0 \prec \tau_1$, we can rewrite (29) to get:

$$\text{accept}^{\textsc{id}}_{\tau} \rightarrow \bigvee_{\substack{\tau_0 = \_, \textsc{tn}(j_0, 0) \\ \tau_1 \prec \tau_0 \prec \tau}} \begin{pmatrix} \text{accept}^{\textsc{id}}_{\tau_0} \wedge \pi_1(g(\phi^{\text{in}}_{\tau})) = \text{n}^{j_0} \wedge \pi_2(g(\phi^{\text{in}}_{\tau})) = \sigma^{\text{in}}_{\tau_0}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \oplus \mathsf{f}_{\mathsf{k}}(\text{n}^{j_0}) \\ \wedge\ \sigma^{\text{in}}_{\tau}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) = \sigma^{\text{in}}_{\tau_0}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) \end{pmatrix} \tag{35}$$

To conclude, we observe that $\text{accept}^{\textsc{id}}_{\tau} \wedge \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_2} \rightarrow \sigma^{\text{in}}_{\tau_1}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) = \textsc{guti}^{j_a}$. We recall that $\text{accept}^{\textsc{id}}_{\tau_0} \rightarrow g(\phi^{\text{in}}_{\tau_0}) = \sigma^{\text{in}}_{\tau_0}(\textsc{guti}^{\textsc{id}}_{\textsc{n}})$. We conclude using (31) that:

$$\text{accept}^{\textsc{id}}_{\tau} \wedge \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_2} \rightarrow \sigma^{\text{in}}_{\tau_1}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) = g(\phi^{\text{in}}_{\tau_0})$$

Since this holds for every $\tau_a = \_, \textsc{fn}(j_a) \prec \tau_2$, we deduce from (30) that:

$$\text{accept}^{\textsc{id}}_{\tau} \wedge \text{accept}^{\textsc{id}}_{\tau_0} \rightarrow \sigma^{\text{in}}_{\tau_1}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) = g(\phi^{\text{in}}_{\tau_0})$$

Hence using (35) we get:

$$\text{accept}^{\textsc{id}}_{\tau} \rightarrow \bigvee_{\substack{\tau_0 = \_, \textsc{tn}(j_0, 0) \\ \tau_1 \prec \tau_0 \prec \tau}} \begin{pmatrix} \text{accept}^{\textsc{id}}_{\tau_0} \wedge \pi_1(g(\phi^{\text{in}}_{\tau})) = \text{n}^{j_0} \wedge \pi_2(g(\phi^{\text{in}}_{\tau})) = \sigma^{\text{in}}_{\tau_0}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \oplus \mathsf{f}_{\mathsf{k}}(\text{n}^{j_0}) \\ \wedge\ \sigma^{\text{in}}_{\tau}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) = \sigma^{\text{in}}_{\tau_0}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) \wedge \sigma^{\text{in}}_{\tau_1}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) = g(\phi^{\text{in}}_{\tau_0}) \end{pmatrix} \quad \blacksquare$$

We now prove the following strong acceptance characterization properties:

Lemma 14. *For every valid action trace $\tau = \_, ai$ on $\mathcal{S}_{id}$ and identity $\textsc{id} \in \mathcal{S}_{id}$:*

- ***(StrEqu1)*** *If $ai = \textsc{fu}_{\textsc{id}}(j)$. Let $\tau_2 = \_, \textsc{tu}_{\textsc{id}}(j, 0)$ or $\_, \textsc{pu}_{\textsc{id}}(j, 1)$ such that $\tau_2 \prec \tau$, then:*

$$\text{accept}^{ID}_{\tau} \leftrightarrow \bigvee_{\tau_2 \prec_\tau \tau_1 = \_, FN(j_0)} \text{fu-tr}^{\text{n}:\tau_1}_{\text{u}:\tau}$$

- ***(StrEqu2)*** *If $ai = \textsc{tu}_{\textsc{id}}(j, 1)$. Let $\tau_2 = \_, \textsc{tu}_{\textsc{id}}(j, 0)$ such that $\tau_2 \prec \tau$. Then for every τ_1 such that $\tau_1 = \_, \textsc{tn}(j_1, 0)$ and $\tau_2 \prec_\tau \tau_1$, we let:*

$$\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \equiv \begin{pmatrix} \quad \pi_1(g(\phi^{in}_{\tau})) = n^{j_1} \ \wedge\ \pi_2(g(\phi^{in}_{\tau})) = \sigma^{in}_{\tau_1}(SQN^{ID}_{N}) \oplus f_{k^{ID}}(n^{j_1}) \\ \wedge\ \pi_3(g(\phi^{in}_{\tau})) = Mac^{3}_{k^{ID}_m}(\langle n^{j_1}, \sigma^{in}_{\tau_1}(SQN^{ID}_{N}), \sigma^{in}_{\tau_2}(GUTI^{ID}_{U})\rangle) \\ \wedge\ g(\phi^{in}_{\tau_1}) = \sigma^{in}_{\tau_2}(GUTI^{ID}_{U}) \ \wedge\ \sigma^{in}_{\tau_2}(GUTI^{ID}_{U}) = \sigma^{in}_{\tau_1}(GUTI^{ID}_{N}) \ \wedge\ \sigma^{in}_{\tau_2}(\text{valid-guti}^{ID}_{U}) \\ \wedge\ range(\sigma^{in}_{\tau}(SQN^{ID}_{U}), \sigma^{in}_{\tau_1}(SQN^{ID}_{N})) \end{pmatrix}$$

Then:

$$\Big(\text{part-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \;\rightarrow\; \text{accept}^{\textsc{id}}_{\tau} \wedge \text{accept}^{\textsc{id}}_{\tau_1}\Big)_{\substack{\tau_1=\_,\textsc{tn}(j_1,0)\\ \tau_2\prec_\tau \tau_1}} \qquad \text{accept}^{\mathit{ID}}_{\tau} \leftrightarrow \bigvee_{\substack{\tau_1=\_,\textsc{tn}(j_1,0)\\ \tau_2\prec_\tau \tau_1}} \text{part-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}$$

- ***(StrEqu3)*** *If $ai = \textsc{tn}(j,1)$. Let $\tau_1 = \_, \textsc{tn}(j,0)$ such that $\tau_1 \prec \tau$. Let $\textsc{id} \in \mathcal{S}_{id}$ and τ_i, τ_2 be such that $\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i,1)$, $\tau_2 = \_, \textsc{tu}_{\textsc{id}}(j_i,0)$ and $\tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i$. Let:*

  $$\text{full-tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i} \;\equiv\; \text{part-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau_i} \wedge g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^4_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\mathsf{n}^j)$$

  Then:

  $$\Big(\text{full-tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i} \;\rightarrow\; \text{accept}^{\textsc{id}}_{\tau} \wedge \text{accept}^{\textsc{id}}_{\tau_i} \wedge \text{accept}^{\textsc{id}}_{\tau_1}\Big)_{\substack{\tau_2=\_,\textsc{tu}_{\mathit{ID}}(j_i,0)\\ \tau_i=\_,\textsc{tu}_{\mathit{ID}}(j_i,1)\\ \tau_2\prec_\tau \tau_1\prec_\tau \tau_i}}$$

  $$\text{accept}^{\mathit{ID}}_{\tau} \leftrightarrow \bigvee_{\substack{\tau_2=\_,\textsc{tu}_{\mathit{ID}}(j_i,0)\\ \tau_i=\_,\textsc{tu}_{\mathit{ID}}(j_i,1)\\ \tau_2\prec_\tau \tau_1\prec_\tau \tau_i}} \text{full-tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i}$$

- ***(StrEqu4)*** *If $ai = \textsc{pu}_{\textsc{id}}(j,2)$ then for every $\tau_1 = \_, \textsc{pn}(j_1,1)$ such that $\tau_2 \prec_\tau \tau_1$, we have:*

  $$\neg\sigma^{in}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \text{supi-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \;\rightarrow\; \text{inc-accept}^{\textsc{id}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) - \sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = 0$$

  Moreover:

  $$\neg\sigma^{in}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \text{accept}^{\textsc{id}}_{\tau} \;\rightarrow\; \sigma_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) - \sigma_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = 0$$

E.7 Proof of Lemma 14

Proof of **(StrEqu1)**. First, we apply **(Equ1)**:

$$\text{accept}^{\textsc{id}}_{\tau} \;\leftrightarrow\; \bigvee_{\substack{\tau_1=\_,\textsc{fn}(j_0)\prec\tau\\ \tau_1\not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)}} \text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$$

Let $\tau_1 = \_, \textsc{fn}(j_0) \prec \tau$. Remark that if $\tau_2 \prec \tau_1$ then $\tau_1 \not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)$. Hence to conclude we just need to show that if $\tau_1 \prec \tau_2$ then $\neg\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$.

Let $\tau_i = \_, \textsc{pu}_{\textsc{id}}(j,2)$ or $\_, \textsc{tu}_{\textsc{id}}(j,1)$ such that $\tau_i \prec \tau$. We do a case disjunction on τ_i:

- If $\tau_i = \_, \textsc{pu}_{\textsc{id}}(j,2)$. We know that $\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \rightarrow \text{accept}^{\textsc{id}}_{\tau_i}$, hence by applying **(Acc2)** to τ_i:

  $$\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \;\rightarrow\; \bigvee_{\substack{\tau_x=\_,\textsc{pn}(j_x,1)\\ \tau_2\prec\tau_x\prec\tau_i}} \text{accept}^{\textsc{id}}_{\tau_x} \;\wedge\; g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_x} \;\wedge\; \pi_1(g(\phi^{\mathsf{in}}_{\tau_x})) = \{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\textsc{n}}}$$

  We know that $\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \rightarrow g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_0}$. We deduce that the main term of the disjunction above is false whenever $j_x \neq j_0$. Hence we have $\neg\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$ if there does not exist any τ_0 such that $\tau_2 \prec \tau_0 \prec \tau_i$ and $\tau_0 = \_, \textsc{pn}(j_0,1)$.

  If $\tau_1 \prec \tau_2$ then we know that for every τ_0, if $\tau_0 = \_, \textsc{pn}(j_0,1) \prec \tau$ then $\tau_0 \prec \tau_1$, and by transitivity $\tau_0 \prec \tau_2$. Hence there does not exist any τ_0 such that $\tau_2 \prec \tau_0 \prec \tau_i$ and $\tau_0 = \_, \textsc{pn}(j_0,1)$. We deduce that if $\tau_1 \prec \tau_2$ then $\neg\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$ holds, which is what we wanted.
- If $\tau_i = \_, \textsc{tu}_{\textsc{id}}(j,1)$. We know that $\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \rightarrow \text{accept}^{\textsc{id}}_{\tau_i}$, hence by applying **(StrAcc1)** to τ_i:

  $$\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \;\rightarrow\; \bigvee_{\substack{\tau_x=\_,\textsc{tn}(j_x,0)\\ \tau_2\prec\tau_x\prec\tau_i}} \begin{pmatrix} \text{accept}^{\textsc{id}}_{\tau_x} \;\wedge\; g(\phi^{\mathsf{in}}_{\tau_x}) = \sigma^{\mathsf{in}}_{\tau_2}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) \;\wedge\; \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^{j_x} \\ \wedge\; \pi_2(g(\phi^{\mathsf{in}}_{\tau_i})) = \sigma^{\mathsf{in}}_{\tau_x}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_x}) \wedge \sigma^{\mathsf{in}}_{\tau_i}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) = \sigma^{\mathsf{in}}_{\tau_x}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) \end{pmatrix}$$

  Similarly to what we did for $\tau_i = \_, \textsc{pu}_{\textsc{id}}(j_i,2)$, the main term above if false if $j_x \neq j_0$. Hence we have $\neg\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$ if there does not exist any τ_0 such that $\tau_2 \prec \tau_0 \prec \tau_i$ and $\tau_0 = \_, \textsc{tn}(j_0,0)$. Since this is the case whenever $\tau_1 \prec \tau_2$, we deduce that if $\tau_1 \prec \tau_2$ then $\neg\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$ holds. ■

Proof of **(StrEqu2)**. We repeating the proof of **(Equ4)**, but using **(StrAcc1)** instead of **(Acc3)**. All the reasonings we did apply, only the set of τ_1 the disjunction quantifies upon changes. We quantify over τ_1 in $\{\tau_1 \mid \tau_1 = \_, \textsc{tn}(j_0, 0) \wedge \tau_2 \prec_\tau \tau_1\}$ instead of $\{\tau_1 \mid \tau_1 = \_, \textsc{tn}(j_0, 0) \wedge \tau_1 \prec \tau\}$. We get that:

$$\mathsf{accept}_\tau^{\mathrm{ID}} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \left(\begin{array}{l} \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}, \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}), \sigma_\tau^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}})\rangle) \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{s\text{-}valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \\ \wedge\ \mathsf{range}(\sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}), \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})) \wedge g(\phi_{\tau_1}^{\mathsf{in}}) = \sigma_{\tau_1}^{\mathsf{in}}(\textsc{guti}_{\mathrm{N}}^{\mathrm{ID}}) \wedge \pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0} \\ \wedge\ \pi_2(g(\phi_\tau^{\mathsf{in}})) = \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0}) \wedge \sigma_\tau^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}}) = \sigma_{\tau_1}^{\mathsf{in}}(\textsc{guti}_{\mathrm{N}}^{\mathrm{ID}}) \end{array}\right)$$

Since no user ID action occurs between τ_2 and τ, we know that:

$$\sigma_\tau^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}}) = \sigma_{\tau_2}^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}}) \qquad \sigma_\tau^{\mathsf{in}}(\mathsf{s\text{-}valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \leftrightarrow \sigma_{\tau_2}^{\mathsf{in}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}})$$

Using this, we can rewrite the characterization of $\mathsf{accept}_\tau^{\mathrm{ID}}$ as follows (we underline the subterms where rewriting occurred):

$$\mathsf{accept}_\tau^{\mathrm{ID}} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \left(\begin{array}{l} \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}, \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}), \underline{\sigma_{\tau_2}^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}})}\rangle) \wedge \underline{\sigma_{\tau_2}^{\mathsf{in}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}})} \\ \wedge\ \mathsf{range}(\sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}), \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})) \wedge g(\phi_{\tau_1}^{\mathsf{in}}) = \sigma_{\tau_1}^{\mathsf{in}}(\textsc{guti}_{\mathrm{N}}^{\mathrm{ID}}) \wedge \pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0} \\ \wedge\ \pi_2(g(\phi_\tau^{\mathsf{in}})) = \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0}) \wedge \underline{\sigma_{\tau_2}^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}})} = \sigma_{\tau_1}^{\mathsf{in}}(\textsc{guti}_{\mathrm{N}}^{\mathrm{ID}}) \end{array}\right)$$

We rewrite $\sigma_{\tau_1}^{\mathsf{in}}(\textsc{guti}_{\mathrm{N}}^{\mathrm{ID}})$ into $\sigma_{\tau_2}^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}})$:

$$\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \left(\begin{array}{l} \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}, \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}), \sigma_{\tau_2}^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}})\rangle) \wedge \sigma_{\tau_2}^{\mathsf{in}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \\ \wedge\ \mathsf{range}(\sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}), \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})) \wedge g(\phi_{\tau_1}^{\mathsf{in}}) = \underline{\sigma_{\tau_2}^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}})} \wedge \pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0} \\ \wedge\ \pi_2(g(\phi_\tau^{\mathsf{in}})) = \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0}) \wedge \sigma_{\tau_2}^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}}) = \sigma_{\tau_1}^{\mathsf{in}}(\textsc{guti}_{\mathrm{N}}^{\mathrm{ID}}) \end{array}\right)$$

Finally we re-order the conjuncts:

$$\begin{aligned} &\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \left(\begin{array}{ll} & \pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_1} \ \wedge\ \pi_2(g(\phi_\tau^{\mathsf{in}})) = \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \oplus \mathsf{f}_{\mathsf{k}^{\mathrm{ID}}}(\mathsf{n}^{j_1}) \\ \wedge & \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k}_{\mathsf{m}}^{\mathrm{ID}}}(\langle \mathsf{n}^{j_1}, \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}), \sigma_{\tau_2}^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}})\rangle) \\ \wedge & g(\phi_{\tau_1}^{\mathsf{in}}) = \sigma_{\tau_2}^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}}) \ \wedge\ \sigma_{\tau_2}^{\mathsf{in}}(\textsc{guti}_{\mathrm{U}}^{\mathrm{ID}}) = \sigma_{\tau_1}^{\mathsf{in}}(\textsc{guti}_{\mathrm{N}}^{\mathrm{ID}}) \ \wedge\ \sigma_{\tau_2}^{\mathsf{in}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \\ \wedge & \mathsf{range}(\sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}), \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})) \end{array}\right) \\ &\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \mathsf{part\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \end{aligned}$$

Finally, for every $\tau_1 = \_, \textsc{tn}(j_1, 0)\tau_2 \prec_\tau \tau_1$ we can check that:

$$\mathsf{part\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \rightarrow \mathsf{accept}_\tau^{\mathrm{ID}} \wedge \mathsf{accept}_{\tau_1}^{\mathrm{ID}} \qquad \blacksquare$$

Proof of **(StrEqu3)**. The proof that:

$$\mathsf{accept}_\tau^{\mathrm{ID}} \leftrightarrow \bigvee_{\substack{\tau_2 = \_, \textsc{tu}_{\mathrm{ID}}(j_i,0)\\ \tau_i = \_, \textsc{tu}_{\mathrm{ID}}(j_i,1)\\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i}} \mathsf{full\text{-}tr}_{\mathsf{u}:\tau_2,\tau_i}^{\mathsf{n}:\tau_1,\tau}$$

is exactly the same than the proof of **(Equ5)**, but using **(StrEqu2)** instead of **(Equ4)**.

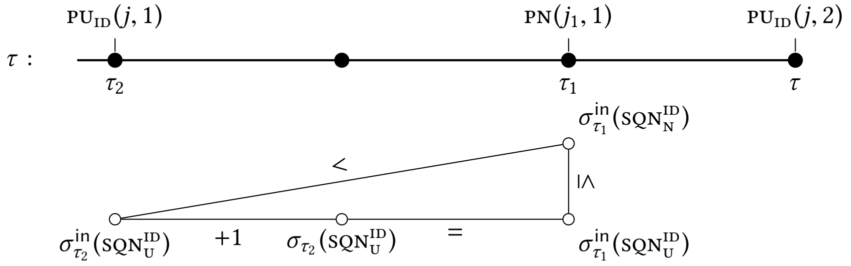

$\textsc{pu}_{\textsc{id}}(j,1)$
$\textsc{pn}(j_1,1)$
$\textsc{pu}_{\textsc{id}}(j,2)$
τ :
τ_2
τ_1
τ
$\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$
$<$
$\leq$
$\sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$+1$
$\sigma_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$=$
$\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$

Fig. 23. First Graphical Representation Used in the Proof of Lemma 14

Finally, it is straightforward to check that for every $\tau_2 = \_, \textsc{tu}_{\textsc{id}}(j_i, 0)$, $\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1)$ such that $\tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i$ we have:

$$\mathsf{full\text{-}tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i} \rightarrow \mathsf{accept}^{\textsc{id}}_{\tau} \wedge \mathsf{accept}^{\textsc{id}}_{\tau_i} \wedge \mathsf{accept}^{\textsc{id}}_{\tau_1} \qquad \blacksquare$$

Proof of **(StrEqu4)**. Let $\tau_2 = \_\textsc{pu}_{\textsc{id}}(j, 1)$ such that $\tau_2 \prec \tau$. Using **(Equ2)**, we know that:

$$\mathsf{accept}^{\textsc{id}}_{\tau} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{pn}(j_1,1) \\ \tau_2 \prec_\tau \tau_1}} \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}$$

Therefore to prove **(StrEqu4)** it is sufficient to show that for every τ_1 such that $\tau_1 = \_, \textsc{pn}(j_1, 1)$ and $\tau_2 \prec_\tau \tau_1$ we have:

$$\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow \mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) - \sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = 0 \wedge \sigma_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) - \sigma_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = 0$$

Hence let τ_1 with $\tau_1 = \_, \textsc{pn}(j_1, 1)$ and $\tau_2 \prec_\tau \tau_1$.

Part 1 First, we are going to show that:

$$\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow \sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = \sigma_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) \tag{36}$$

We know that $\mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau_1} \rightarrow \sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = \sigma_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$, which is what we wanted. Hence it only remains to show (36) when $\neg\mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau_1}$. Using **(B5)** we know that $\sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$. By validity of τ there are no user action between τ_2 and τ, hence $\sigma_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) = \sigma_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$. Observe that:

$$\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \neg\mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau_1} \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) > \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) \qquad \sigma_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) = \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) + 1$$

We summarize this graphically in Figure 23. We deduce that:

$$\begin{aligned} \neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \neg\mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau_1} &\rightarrow \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) < \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) + 1 \\ &\rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) + 1 \\ &\rightarrow \sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = \sigma_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) \end{aligned} \tag{37}$$

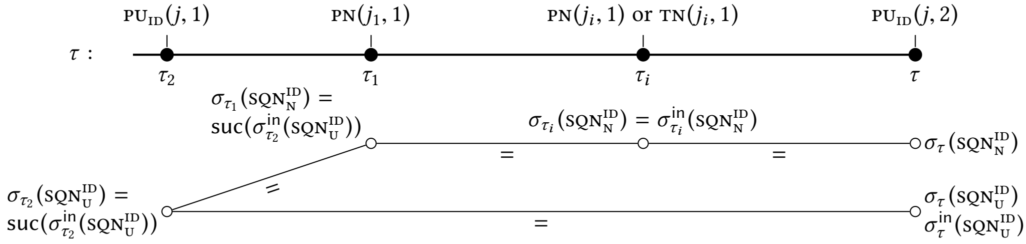
Which is what we wanted to show.

Part 2 We now show that:

$$\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow \sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) > \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \tag{38}$$

First, notice that:

$$\begin{aligned} \mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau_1} &\rightarrow \sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) + 1 \\ &\rightarrow \sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) > \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \end{aligned}$$



$\textsc{pu}_{\textsc{id}}(j,1)$
$\textsc{pn}(j_1,1)$
$\textsc{pn}(j_i,1)$ or $\textsc{tn}(j_i,1)$
$\textsc{pu}_{\textsc{id}}(j,2)$
τ :
τ_2
τ_1
τ_i
τ
$\sigma_{\tau_1}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) =$
$\mathsf{suc}(\sigma_{\tau_2}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}))$
$\sigma_{\tau_i}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) = \sigma_{\tau_i}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}})$
$\sigma_{\tau}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}})$
$=$
$=$
$=$
$\sigma_{\tau_2}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) =$
$\mathsf{suc}(\sigma_{\tau_2}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}))$
$=$
$\sigma_{\tau}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) =$
$\sigma_{\tau}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})$

Fig. 24. Second Graphical Representation Used in the Proof of Lemma 14

$$\rightarrow \sigma_{\tau_1}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) > \sigma_{\tau_2}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) \qquad \text{(By } \mathbf{(B1)}\text{)}$$

Therefore we only need to prove:

$$\neg\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \wedge \neg\mathsf{inc\text{-}accept}_{\tau_1}^{\textsc{id}} \;\rightarrow\; \sigma_{\tau_1}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) > \sigma_{\tau_2}^{\mathsf{in}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}})$$

Which is straightforward:

$$\begin{aligned}\neg\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \wedge \neg\mathsf{inc\text{-}accept}_{\tau_1}^{\textsc{id}} &\rightarrow \sigma_{\tau_1}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) = \sigma_{\tau_2}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) + 1 && \text{(By (37))}\\ &\rightarrow \sigma_{\tau_1}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) > \sigma_{\tau_2}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})\\ &\rightarrow \sigma_{\tau_1}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) > \sigma_{\tau_2}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) && \text{(By } \mathbf{(B5)}\text{)}\end{aligned}$$

Which concludes the proof of (38).

Part 3 We give the proof of:

$$\neg\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \;\rightarrow\; \sigma_{\tau}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) = \sigma_{\tau_1}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) \wedge \sigma_{\tau}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) \qquad (39)$$

By validity of τ we know that $\sigma_{\tau}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau_2}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})$, therefore using (36) we know that:

$$\neg\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \;\rightarrow\; \sigma_{\tau_1}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) = \sigma_{\tau}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})$$

To conclude, we need to show that $\textsc{sqn}_{\textsc{n}}^{\textsc{id}}$ was kept unchanged since τ_1, i.e. that $\neg\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1}$ implies that $\sigma_{\tau_1}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) = \sigma_{\tau}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}})$. This requires that no SUPI or GUTI network session incremented $\textsc{sqn}_{\textsc{n}}^{\textsc{id}}$. Therefore we need to show the two following properties:

- **SUPI:** For every $\tau_1 \prec_{\tau} \tau_i$ such that $\tau_i = \_, \textsc{pn}(j_i, 1)$:
$$\neg\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \;\rightarrow\; \neg\mathsf{inc\text{-}accept}_{\tau_i}^{\textsc{id}} \qquad (40)$$
- **GUTI:** For every $\tau_1 \prec_{\tau} \tau_i$ such that $\tau_i = \_, \textsc{tn}(j_i, 1)$:
$$\neg\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \;\rightarrow\; \neg\mathsf{inc\text{-}accept}_{\tau_i}^{\textsc{id}} \qquad (41)$$

Assuming the two properties above, showing that (39) holds is easy. First, using (40) and (41) we know that:

$$\neg\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \;\rightarrow\; \sigma_{\tau}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) = \sigma_{\tau_1}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}})$$

We know that $\sigma_{\tau}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) = \sigma_{\tau}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})$. We deduce that $\sigma_{\tau}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) = \sigma_{\tau}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})$, which concludes this case. We summarize this graphically in Figure 24.

Part 4 (Proof of (40)**)** Let $\tau_1 \prec_{\tau} \tau_i$ such that $\tau_i = \_, \textsc{pn}(j_i, 1)$. Using **(Acc1)** we know that:

$$\mathsf{accept}_{\tau_i}^{\textsc{id}} \;\rightarrow \bigvee_{\tau' = \_, \textsc{pu}_{\textsc{id}}(j',1) \prec_{\tau} \tau_i} \pi_1(g(\phi_{\tau_i}^{\mathsf{in}})) = \{\langle \textsc{id}\,,\, \sigma_{\tau'}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})\rangle\}_{\mathsf{pk_N}}^{\mathsf{n}_{\mathsf{e}}^{j'}} \wedge g(\phi_{\tau'}^{\mathsf{in}}) = \mathsf{n}^{j_i}$$

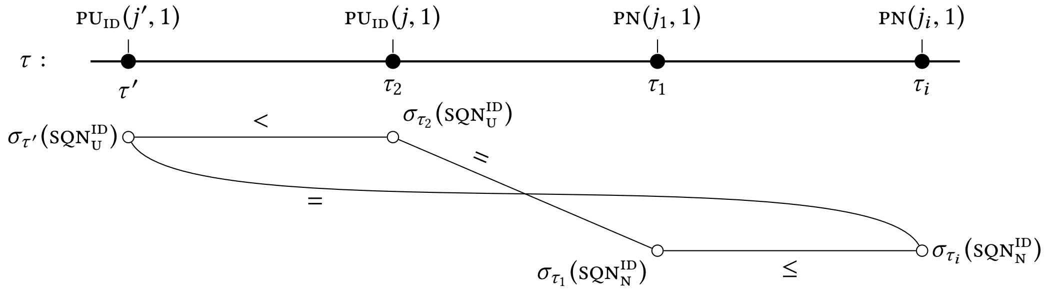

$\mathrm{PU}_{\mathrm{ID}}(j',1)$
$\mathrm{PU}_{\mathrm{ID}}(j,1)$
$\mathrm{PN}(j_1,1)$
$\mathrm{PN}(j_i,1)$
τ :
τ'
τ_2
τ_1
τ_i
$\sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$
$<$
$\sigma_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$
$=$
$=$
$\sigma_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$
$\leq$
$\sigma_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$

Fig. 25. Third Graphical Representation Used in the Proof of Lemma 14

We know that $\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1} \neq \mathsf{n}^{j_i}$. Moreover from the validity of τ we know that for every τ'' such that:

$$\tau_2 = \_, \mathrm{PU}_{\mathrm{ID}}(j,1) \prec_\tau \tau'' = \_, \mathsf{ai}'' \prec_\tau \tau = \_, \mathrm{PU}_{\mathrm{ID}}(j,2)$$

We have $\mathsf{ai}'' \neq \mathrm{PU}_{\mathrm{ID}}(\_,\_)$. Hence:

$$\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \mathsf{accept}^{\mathrm{ID}}_{\tau_i} \rightarrow \bigvee_{\tau'=\_,\mathrm{PU}_{\mathrm{ID}}(j',1)\prec_\tau \tau_2} \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \{\langle \mathrm{ID}\,,\, \sigma^{\mathsf{in}}_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}_{\mathsf{e}}^{j'}}_{\mathsf{pk}_{\mathrm{N}}} \wedge g(\phi^{\mathsf{in}}_{\tau'}) = \mathsf{n}^{j_i}$$

Which implies that:

$$\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_i} \rightarrow \bigvee_{\tau'=\_,\mathrm{PU}_{\mathrm{ID}}(j',1)\prec_\tau \tau_2} \sigma_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}))$$

We recall (36):

$$\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow \sigma_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$$

Let $\tau' = \_, \mathrm{PU}_{\mathrm{ID}}(j',1) \prec_\tau \tau_2$. We know using **(B1)** that:

$$\sigma_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \leq \sigma_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \qquad\qquad \sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \leq \sigma_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$$

Moreover using **(A2)** we know that $\sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \neq \sigma_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$, hence $\sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) < \sigma_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$. We summarize what we know graphically in Figure 25. Therefore:

$$\begin{aligned}
&\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_i}\\
\rightarrow\ & \bigvee_{\tau'=\_,\mathrm{PU}_{\mathrm{ID}}(j',1)\prec_\tau \tau_2} \begin{pmatrix} \sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) < \sigma_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \sigma_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})\\ \wedge \sigma_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \leq \sigma_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \sigma_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \end{pmatrix}\\
\rightarrow\ & \bigvee_{\tau'=\_,\mathrm{PU}_{\mathrm{ID}}(j',1)\prec_\tau \tau_2} \sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) < \sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\\
\rightarrow\ & \mathsf{false}
\end{aligned}$$

Which concludes this proof.

Part 5 (Proof of (41)**)** Let $\tau_1 \prec_\tau \tau_i$ such that $\tau_i = \_, \mathrm{TN}(j_i,1)$. Using Lemma 7, we know that:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau_i} \rightarrow \sigma^{\mathsf{in}}_{\tau_i}(\mathsf{e\text{-}auth}^{j}_{\mathrm{N}}) = \mathrm{ID} \rightarrow \bigvee_{\substack{\tau'=\_,\mathrm{TU}_{\mathrm{ID}}(\_,1)\\ \tau'\prec_\tau \tau_i}} \sigma_{\tau'}(\mathsf{b\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^{j_i}$$

Since $\text{supi-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow g(\phi^{\text{in}}_{\tau_2}) = \text{n}^{j_1}$, we know that $\text{supi-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \sigma_{\tau_2}(\text{b-auth}^{\text{ID}}_{\text{U}}) = \text{n}^{j_1}$. As we know that $\text{n}^{j_1} \neq \text{n}^{j_i}$, we deduce that $\text{supi-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \sigma_{\tau_2}(\text{b-auth}^{\text{ID}}_{\text{U}}) \neq \text{n}^{j_i}$. Moreover using the validity of τ we know that $\sigma_{\tau_i}(\text{b-auth}^{\text{ID}}_{\text{U}}) = \sigma_{\tau_2}(\text{b-auth}^{\text{ID}}_{\text{U}})$. Therefore:

$$\text{supi-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \wedge \text{accept}^{\text{ID}}_{\tau_i} \rightarrow \bigvee_{\substack{\tau'=\_,\text{TU}_{\text{ID}}(\_,1)\\ \tau' \prec_\tau \tau_2}} \sigma_{\tau'}(\text{b-auth}^{\text{ID}}_{\text{U}}) = \text{n}^{j_i}$$

Let $\tau' = \_, \text{TU}_{\text{ID}}(\_, 1)$ with $\tau' \prec_\tau \tau_2$. We know that $\sigma_{\tau'}(\text{b-auth}^{\text{ID}}_{\text{U}}) = \text{n}^{j_i}$ implies that $\sigma_{\tau'}(\text{b-auth}^{\text{ID}}_{\text{U}}) \neq \text{fail}$, and therefore $\text{accept}^{\text{ID}}_{\tau'}$ holds:

$$\sigma_{\tau'}(\text{b-auth}^{\text{ID}}_{\text{U}}) = \text{n}^{j_i} \rightarrow \sigma_{\tau'}(\text{b-auth}^{\text{ID}}_{\text{U}}) \neq \text{fail} \rightarrow \text{accept}^{\text{ID}}_{\tau'}$$

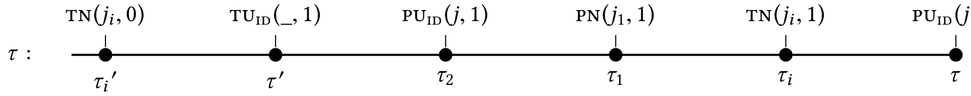
By applying **(Acc3)** we know that:

$$\text{accept}^{\text{ID}}_{\tau'} \rightarrow \bigvee_{\tau_i{}'=\_,\text{TN}(j_i',0)\prec_\tau \tau'} \pi_1(g(\phi^{\text{in}}_{\tau'})) = \text{n}^{j_i'}$$

Since $[\text{accept}^{\text{ID}}_{\tau'}]\sigma_{\tau'}(\text{b-auth}^{\text{ID}}_{\text{U}}) = [\text{accept}^{\text{ID}}_{\tau'}]\pi_1(g(\phi^{\text{in}}_{\tau'}))$ we deduce:

$$\sigma_{\tau'}(\text{b-auth}^{\text{ID}}_{\text{U}}) = \text{n}^{j_i} \rightarrow \text{false} \qquad \text{if } \tau' \prec_\tau \text{TN}(j_i, 0)$$

Hence if $\tau' \prec_\tau \text{TN}(j_i, 0)$ we know that $\neg\left(\text{supi-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \wedge \text{accept}^{\text{ID}}_{\tau_i}\right)$, which is what we wanted to show. Therefore let $\tau_i{}' = \_, \text{TN}(j_i, 0)$, and assume $\tau_i{}' \prec_\tau \tau'$. We summarize graphically this below:



We recall (38):

$$\neg\sigma^{\text{in}}_\tau(\text{sync}^{\text{ID}}_{\text{U}}) \wedge \text{supi-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \sigma^{\text{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{N}}) < \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}})$$

Hence, using **(B4)** we know that:

$$\neg\sigma^{\text{in}}_\tau(\text{sync}^{\text{ID}}_{\text{U}}) \wedge \text{supi-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \bigvee_{\substack{\tau_2 \preceq \tau_x \preceq \tau_1\\ \tau_x=\_,\text{TN}(j_x,0) \text{ or } \_,\text{TN}(j_x,1) \text{ or } \_,\text{PN}(j_x,1)}} \sigma_{\tau_1}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_x}$$

Since $\text{TN}(j_i, 0) \prec_\tau \tau_2$ and $\tau_1 \prec_\tau \text{TN}(j_i, 1)$:

$$\neg\sigma^{\text{in}}_\tau(\text{sync}^{\text{ID}}_{\text{U}}) \wedge \text{supi-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \sigma_{\tau_1}(\text{session}^{\text{ID}}_{\text{N}}) \neq \text{n}^{j_i}$$

For every $\tau_1 \preceq \tau''$ we have:

$$\sigma_{\tau''}(\text{session}^{\text{ID}}_{\text{N}}) = \begin{cases} \text{if inc-accept}^{\text{ID}}_{\tau''} \text{ then n}^{j''} \text{ else } \sigma^{\text{in}}_{\tau''}(\text{session}^{\text{ID}}_{\text{N}}) & \text{if } \tau'' = \_, \text{PN}(j'', 1) \\ \text{if accept}^{\text{ID}}_{\tau''} \text{ then n}^{j''} \text{ else } \sigma^{\text{in}}_{\tau''}(\text{session}^{\text{ID}}_{\text{N}}) & \text{if } \tau'' = \_, \text{TN}(j'', 0) \\ \sigma^{\text{in}}_{\tau''}(\text{session}^{\text{ID}}_{\text{N}}) & \text{otherwise} \end{cases}$$

Since $\tau' \not\prec_\tau \text{TN}(j_i, 0)$, we know that after having set $\sigma_{\tau''}(\text{session}^{\text{ID}}_{\text{N}})$ to n^{j_1} at τ_1, it can never be set to n^{j_i}. Formally, we show by induction that:

$$\sigma_{\tau_1}(\text{session}^{\text{ID}}_{\text{N}}) \neq \text{n}^{j_i} \rightarrow \sigma_{\tau''}(\text{session}^{\text{ID}}_{\text{N}}) \neq \text{n}^{j_i}$$

We conclude by observing that $\sigma^{\text{in}}_{\tau_i}(\text{session}^{\text{ID}}_{\text{N}}) \neq \text{n}^{j_i} \rightarrow \neg\text{inc-accept}^{\text{ID}}_{\tau_i}$.

Part 6 To conclude the proof of **(StrEqu4)**, it only remains to show that:

$$\neg\sigma^{\text{in}}_\tau(\text{sync}^{\text{ID}}_{\text{U}}) \wedge \text{supi-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \text{inc-accept}^{\text{ID}}_{\tau_1} \qquad (42)$$

Since $\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \longrightarrow \mathsf{accept}^{\textsc{id}}_{\tau_1}$, and since:

$$\mathsf{accept}^{\textsc{id}}_{\tau_1} \wedge \neg\mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau_1} \;\leftrightarrow\; \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) > \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$$

To show that (42) holds, it is sufficient to show that:

$$\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \;\rightarrow\; \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$$

We generalize this, and show by induction that for every τ_n such that $\tau_2 \preceq \tau_n \prec_\tau \tau_1$, we have:

$$\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \;\rightarrow\; \sigma_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$$

If $\tau_n = \tau_2$, this is immediate using **(B5)** and the fact that $\sigma_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = \sigma^{\mathsf{in}}_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$. Therefore let $\tau_n >_\tau \tau_2$, and assume by induction that:

$$\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \;\rightarrow\; \sigma^{\mathsf{in}}_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$$

We then have three cases:

- If $\tau_n \neq \_, \textsc{pn}(\_, 1)$ and $\tau_n \neq \_, \textsc{tn}(\_, 1)$, we know that $\sigma_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = \sigma^{\mathsf{in}}_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$, and we conclude directly using the induction hypothesis.
- If $\tau_n = \_, \textsc{pn}(j_n, 1)$. Using **(Equ3)** we know that:

$$\begin{aligned}\sigma_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \neq \sigma^{\mathsf{in}}_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \;&\rightarrow\; \mathsf{accept}^{\textsc{id}}_{\tau_n}\\ &\rightarrow \bigvee_{\substack{\tau_x = \_, \textsc{pu}_{\textsc{id}}(j_x, 1)\\ \tau_x \prec_\tau \tau_n}} \underbrace{\begin{pmatrix} g(\phi^{\mathsf{in}}_{\tau_x}) = \mathsf{n}^{j_n} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_n})) = \{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_x}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\rangle\}^{\mathsf{n}^{j_n}_{\mathsf{e}}}_{\mathsf{pk}_{\textsc{n}}}\\ \wedge\; \pi_2(g(\phi^{\mathsf{in}}_{\tau_n})) = \mathsf{Mac}^1_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle\{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_x}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\rangle\}^{\mathsf{n}^{j_n}_{\mathsf{e}}}_{\mathsf{pk}_{\textsc{n}}}\,,\, g(\phi^{\mathsf{in}}_{\tau_x})\rangle)\end{pmatrix}}_{\theta_{\tau_x}}\end{aligned}$$

Since $\tau_n \prec_\tau \tau_1$, we know that $j_n \neq j_1$. Moreover, $\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \longrightarrow g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1}$. By consequence:

$$\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \longrightarrow g(\phi^{\mathsf{in}}_{\tau_2}) \neq \mathsf{n}^{j_n}$$

Which shows that $\neg(\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \theta_{\tau_2})$. Hence:

$$\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \sigma_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \neq \sigma^{\mathsf{in}}_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \rightarrow \bigvee_{\substack{\tau_x = \_, \textsc{pu}_{\textsc{id}}(j_x, 1)\\ \tau_x \prec_\tau \tau_2}} \theta_{\tau_x}$$

Observe that for every $\tau_x = \_, \textsc{pu}_{\textsc{id}}(j_x, 1)$ such that $\tau_x \prec_\tau \tau_2$:

$$\theta_{\tau_x} \rightarrow\; \sigma_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \;=\; \mathsf{if}\ \sigma^{\mathsf{in}}_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma^{\mathsf{in}}_{\tau_x}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\ \mathsf{then}\ \sigma^{\mathsf{in}}_{\tau_x}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\ \mathsf{else}\ \sigma^{\mathsf{in}}_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$$

Using **(B1)**, we know that $\sigma^{\mathsf{in}}_{\tau_x}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$. Therefore we have the inequality:

$$\theta_{\tau_x} \rightarrow\; \sigma_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \;\leq\; \mathsf{if}\ \sigma^{\mathsf{in}}_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma^{\mathsf{in}}_{\tau_x}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\ \mathsf{then}\ \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\ \mathsf{else}\ \sigma^{\mathsf{in}}_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$$

And using the induction hypothesis, we get that:

$$\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \theta_{\tau_x} \;\rightarrow\; \sigma_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$$

Hence:

$$\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \sigma_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \neq \sigma^{\mathsf{in}}_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \;\rightarrow\; \sigma_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$$

From which we deduce, using the induction hypothesis, that:

$$\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \;\rightarrow\; \sigma_{\tau_n}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$$

- If $\tau_n = \_, \textsc{tn}(j_n, 1)$. Using **(StrEqu2)**, we know that:

$$\sigma_{\tau_n}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \neq \sigma_{\tau_n}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \;\rightarrow\; \mathsf{accept}_{\tau_n}^{\mathrm{ID}} \;\rightarrow\; \bigvee_{\substack{\tau_x{}'=\_,\textsc{tu}_{\mathrm{ID}}(j_x,0)\\ \tau_n{}'=\_,\textsc{tn}(j_n,0)\\ \tau_x=\_,\textsc{tu}_{\mathrm{ID}}(j_x,1)\\ \tau_x{}'\prec_\tau\tau_n{}'\prec_\tau\tau_x\prec_\tau\tau_n}} \mathsf{full\text{-}tr}_{\mathsf{u}:\tau_x{}',\tau_x}^{\mathsf{n}:\tau_n{}',\tau_n}$$

Let $\tau_x = \_, \textsc{tu}_{\mathrm{ID}}(j_x, 1), \tau_n{}' = \_, \textsc{tn}(j_n, 0), \tau_x{}' = \_, \textsc{tu}_{\mathrm{ID}}(j_x, 0)$ s.t. $\tau_x{}' \prec_\tau \tau_n{}' \prec_\tau \tau_x \prec_\tau \tau_n$. Then:

$$\mathsf{full\text{-}tr}_{\mathsf{u}:\tau_x{}',\tau_x}^{\mathsf{n}:\tau_n{}',\tau_n} \wedge \mathsf{inc\text{-}accept}_{\tau_n}^{\mathrm{ID}} \;\rightarrow\; \bigwedge_{\tau_n{}'\prec_\tau\tau_i\prec_\tau\tau_n} \neg\mathsf{inc\text{-}accept}_{\tau_i}^{\mathrm{ID}} \;\rightarrow\; \sigma_{\tau_n{}'}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) = \sigma_{\tau_n}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})$$

Moreover, since:

$$\mathsf{full\text{-}tr}_{\mathsf{u}:\tau_x{}',\tau_x}^{\mathsf{n}:\tau_n{}',\tau_n} \wedge \mathsf{inc\text{-}accept}_{\tau_n}^{\mathrm{ID}} \;\rightarrow\; \sigma_{\tau_x}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \;=\; \sigma_{\tau_n{}'}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})$$

We deduce that:

$$\mathsf{full\text{-}tr}_{\mathsf{u}:\tau_x{}',\tau_x}^{\mathsf{n}:\tau_n{}',\tau_n} \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{if}\ \mathsf{inc\text{-}accept}_{\tau_n}^{\mathrm{ID}}\ \mathsf{then}\ \mathsf{suc}(\sigma_{\tau_x}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}))\ \mathsf{else}\ \sigma_{\tau_n}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})$$

By validity of τ, we know that $j_x \neq j$ and that $\tau_x \prec_\tau \tau_2$. Therefore using **(B1)** we know that $\sigma_{\tau_x}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \leq \sigma_{\tau_2}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})$. Moreover $\sigma_{\tau_x}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{suc}(\sigma_{\tau_x}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}))$. Hence:

$$\mathsf{full\text{-}tr}_{\mathsf{u}:\tau_x{}',\tau_x}^{\mathsf{n}:\tau_n{}',\tau_n} \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \leq \mathsf{if}\ \mathsf{inc\text{-}accept}_{\tau_n}^{\mathrm{ID}}\ \mathsf{then}\ \sigma_{\tau_2}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\ \mathsf{else}\ \sigma_{\tau_n}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})$$

And using the induction hypothesis, we get that:

$$\neg\sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \wedge \mathsf{full\text{-}tr}_{\mathsf{u}:\tau_x{}',\tau_x}^{\mathsf{n}:\tau_n{}',\tau_n} \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \leq \sigma_{\tau_2}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})$$

Hence:

$$\neg\sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \wedge \sigma_{\tau_n}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \neq \sigma_{\tau_n}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \leq \sigma_{\tau_2}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})$$

From which we deduce, using the induction hypothesis, that:

$$\neg\sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \leq \sigma_{\tau_2}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \qquad \blacksquare$$

F UNLINKABILITY

In this section, we prove the σ_{ul}-unlinkability of the AKA$^+$ protocol. To do this, we need, for every valid basic action trace τ, to show that there exists a derivation of $\phi_\tau \sim \phi_{\underline{\tau}}$. We show this by induction on τ.

F.1 Resistance Against De-Synchronization Attacks

To show that the GUTI protocol is σ_{ul}-unlinkable, we need the protocol the be secure against de-synchronization attacks: for every agent ID, the adversary should not be able to keep ID synchronized in the left protocol, while de-synchronizing $\nu_\tau(\mathrm{ID})$ in the right protocol.

Therefore, we need the range check on the sequence number to hold on the left if and only if the range check holds on the right. More precisely, for every left identity ID and matching right identity $\nu_\tau(\mathrm{ID})$, the result of the range checks should be indistinguishable:

$$\mathsf{range}(\sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}), \sigma_\tau(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})) \;\sim\; \mathsf{range}(\sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}), \sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{N}}^{\nu_\tau(\mathrm{ID})})) \tag{43}$$

Unfortunately, this property is not a invariant of the AKA$^+$ protocol, for two reasons:

- First, knowing that the range checks are indistinguishable after a symbolic execution τ is not enough to show that they are indistinguishable after $\tau_1 = \tau, \mathsf{ai}$ (for some ai). For example, take a model where $\mathsf{range}(u, v)$ is implemented as a check that the difference between u and v lies in some interval:

$$[\![\mathsf{range}(u, v)]\!] \text{ if and only if } [\![u]\!] - [\![v]\!] \in \{0, \ldots, D\}$$

for some constant $D > 0$, and where suc is an increment by one. Then, a priori, we may have:

$$[\![\sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})]\!] - [\![\sigma_\tau(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})]\!] = 0 \in \{0, \dots, D\}$$

$$[\![\sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})]\!] - [\![\sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{N}}^{\nu_\tau(\mathrm{ID})})]\!] = D \in \{0, \dots, D\}$$

While (43) holds for τ, it does not hold for $\tau_1 = \tau, \mathrm{PU}_{\mathrm{ID}}(j, 1)$. Indeed, after executing $\mathrm{PU}_{\mathrm{ID}}(j, 1)$:

$$[\![\sigma_{\tau_1}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})]\!] - [\![\sigma_{\tau_1}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})]\!] = 1 \in \{0, \dots, D\}$$

$$[\![\sigma_{\underline{\tau_1}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_{\tau_1}(\mathrm{ID})})]\!] - [\![\sigma_{\underline{\tau_1}}(\mathrm{SQN}_{\mathrm{N}}^{\nu_{\tau_1}(\mathrm{ID})})]\!] = D + 1 \notin \{0, \dots, D\}$$

To avoid this, we require that range(_, _) and suc(_) are implemented as, respectively, an equality check and an integer by-one increment. Moreover, we strengthen the induction property to show that the difference between the sequence numbers are indistinguishable, i.e.:

$$\sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_\tau(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \quad \sim \quad \sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) - \sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{N}}^{\nu_\tau(\mathrm{ID})}) \tag{44}$$

- Second, the property in (44) does not always hold: after a $\mathrm{NS}_{\mathrm{ID}}(\_)$ action, the agent ID and the network may be synchronized on the left (if, e.g., the SUPI protocol has just been successfully executed), but $\nu_\tau(\mathrm{ID})$ is not synchronized with the network.

  Even though the property does not hold, there is no σ_{ul}-unlinkability attack. Indeed a desynchronization attack would need the GUTI protocol to succeed on the left and fail on the right. But the GUTI protocol requires that a fresh GUTI has been established between ID (resp. $\nu_\tau(\mathrm{ID})$) and the network. This can only be achieved through a honest execution of the SUPI protocol. As such a execution will re-synchronize the agent and the network sequence numbers *on both side*, there is no attack.

  To model this, we extended, in Section C.4, the state with a new boolean variable, $\mathrm{sync}_{\mathrm{U}}^{\mathrm{ID}}$, that records whether there was a successful execution of the SUPI protocol with agent ID since the last reset $\mathrm{NS}_{\mathrm{ID}}(\_)$. This variable is only here for proof purposes, and is never used in the actual protocol. We can then state the synchronization invariant:

$$\underbrace{\begin{array}{c}\text{if } \sigma_\tau(\mathrm{sync}_{\mathrm{U}}^{\mathrm{ID}}) \text{ then } \sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_\tau(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \\ \text{else error}\end{array}}_{\text{sync-diff}_\tau^{\mathrm{ID}}} \sim \underbrace{\begin{array}{c}\text{if } \sigma_{\underline{\tau}}(\mathrm{sync}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \text{ then } \sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) - \sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{N}}^{\nu_\tau(\mathrm{ID})}) \\ \text{else error}\end{array}}_{\text{sync-diff}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}}$$

F.2 The Case Term Construction

We give some definitions that are useful to handle sequences of if_then_else_ in terms.

Definition 43. Let $L = (i_1, \dots, i_l)$ be a list of indices, and $(b_i)_{i \in L}$, $(t_i)_{i \in L}$ two list of terms. Then:

$$\underset{i \in L}{\mathrm{case}}((b_i)_{i \in L} : (m_i)_{i \in L}) \equiv \begin{cases} \text{if } b_{i_1} \text{ then } m_{i_1} \text{ else } \underset{i \in L_0}{\mathrm{case}}((b_i)_{i \in L_0} : (m_i)_{i \in L_0}) & \text{when } L \neq \emptyset \\ & \text{and } L_0 = (i_2, \dots, i_l) \\ \text{defaut} & \text{otherwise} \end{cases}$$

We often abuse notation, and write $\underset{i \in L}{\mathrm{case}}(b_i : m_i)$ instead of $\underset{i \in L}{\mathrm{case}}((b_i)_{i \in L} : (m_i)_{i \in L})$.

Proposition 27. *Let $L = (i_1, \dots, i_l)$ be a list of indices, and $(b_i)_{i \in L}$, $(t_i)_{i \in L}$ two list of terms. If $(b_i)_{i \in L}$ is a CS partition, then for any permutation π of $\{1, \dots, l\}$, if we let $L_\pi = (i_{\pi(1)}, \dots, i_{\pi l})$ then:*

$$\underset{i \in L}{case}(b_i : m_i) \;=\; \underset{i \in L_\pi}{case}(b_i : m_i)$$

In that case, we write $\underset{i \in \{i_1, \dots, i_l\}}{case}(b_i : m_i)$ (i.e. we use a set notation instead of list notation).

Proof. The proof is straightforward by induction over $|L|$. ■

If $(b_i)_{i \in L}$ is such that $(\bigvee_{i \in L} b_i) = \text{true}$ then the case where all tests fail and we return defaut never happens. This motivates the introduction of a second definition.

Definition 44. Let $L = (i_1, \dots, i_l)$ be a list of indices with $l \geq 1$, and $(b_i)_{i \in L}$, $(t_i)_{i \in L}$ two list of terms. Then:

$$\underset{i \in L}{\text{s-case}}((b_i)_{i \in L} : (m_i)_{i \in L}) \;\equiv\; \begin{cases} \text{if } b_{i_1} \text{ then } m_{i_1} \text{ else } \underset{i \in L_0}{\text{case}}((b_i)_{i \in L_0} : (m_i)_{i \in L_0}) & \text{if } L_0 = (i_2, \dots, i_l) \\ & \text{and } l > 1 \\ m_1 & \text{if } l = 1 \end{cases}$$

Proposition 28. *For every list of terms $(b_i)_{i \in L}$ and $(t_i)_{i \in L}$, if $(\bigvee_{i \in L} b_i) = \mathit{true}$ then:*

$$\underset{i \in L}{\mathit{case}}(b_i : m_i) = \underset{i \in L}{\mathit{s\text{-}case}}(b_i : m_i)$$

Proof. We omit the proof. ■

F.3 Strengthened Induction Hypothesis

We want to prove that for every valid action trace τ, we have a derivation of:

$$\phi_\tau^{\mathrm{AKA}^+_N} \sim \phi_{\underline{\tau}}^{\mathrm{AKA}^+_{\underline{N}}}$$

for some $\underline{N} = C.N$ large enough (more precisely, C must be larger than $|\tau|$). Instead of proving the formula above, we prove that we have a derivation of the stronger formula:

$$\phi_\tau^{\mathrm{AKA}^+_N}, \text{l-reveal}_\tau^C \sim \phi_{\underline{\tau}}^{\mathrm{AKA}^+_{\underline{N}}}, \text{r-reveal}_\tau^C$$

where l-reveal_τ^C and r-reveal_τ^C are terms used in the proof by induction on τ. Basically, we anticipate and include in l-reveal_τ^C and r-reveal_τ^C elements that we will need later in the proof. Morally, they contain terms representing information that can be safely leaked to the adversary, either because he already knows it, or because he can learn this information later in the protocol execution.

Definition 45. Let $\tau = \tau_0, \text{ai}$ be a valid basic action trace on $\mathcal{S}_{\text{id}}$ and C an integer. Then reveal_τ^C is a list of elements of the form $u \sim v$ containing exactly the elements:

(1) All the elements from $\text{reveal}_{\tau_0}^C$.
(2) For every identity $\textsc{id}$, let:

$$\text{m-suci}_\tau^{\textsc{id}} \;\equiv\; [\sigma_\tau(\text{valid-guti}_{\mathrm{U}}^{\textsc{id}})]\sigma_\tau(\textsc{guti}_{\mathrm{U}}^{\textsc{id}})$$

Then, for every $\textsc{id} \in \mathcal{S}_{\text{id}}$, reveal_τ^C contains the following elements:

$$\sigma_\tau(\text{valid-guti}_{\mathrm{U}}^{\textsc{id}}) \;\sim\; \sigma_{\underline{\tau}}(\text{valid-guti}_{\mathrm{U}}^{\nu_\tau(\textsc{id})}) \qquad\qquad \text{m-suci}_\tau^{\textsc{id}} \;\sim\; \text{m-suci}_{\underline{\tau}}^{\nu_\tau(\textsc{id})}$$

$$\sigma_\tau(\text{sync}_{\mathrm{U}}^{\textsc{id}}) \;\sim\; \sigma_{\underline{\tau}}(\text{sync}_{\mathrm{U}}^{\nu_\tau(\textsc{id})}) \qquad\qquad \text{sync-diff}_\tau^{\textsc{id}} \;\sim\; \text{sync-diff}_{\underline{\tau}}^{\nu_\tau(\textsc{id})}$$

(3) If $\text{ai} \neq \textsc{ns}\_(\_)$ then for every identity $\textsc{id} \in \mathcal{S}_{\text{id}}$:

$$\sigma_\tau(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}}) - \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}}) \;\sim\; \sigma_{\underline{\tau}}(\textsc{sqn}_{\mathrm{U}}^{\nu_\tau(\textsc{id})}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\nu_\tau(\textsc{id})})$$

(4) If $\text{ai} = \textsc{tu}_{\textsc{id}}(j, 0)$, then:

$$\sigma_\tau(\text{s-valid-guti}_{\mathrm{U}}^{\textsc{id}}) \;\sim\; \sigma_{\underline{\tau}}(\text{s-valid-guti}_{\mathrm{U}}^{\nu_\tau(\textsc{id})})$$

(5) If $\mathsf{ai} = \textsc{pu}_{\textsc{id}}(j, 1)$, then:

$$\{\langle \textsc{id}\,,\ \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\textsc{n}}} \sim \{\langle \nu_\tau(\textsc{id})\,,\ \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\nu_\tau(\textsc{id})}_{\textsc{u}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\textsc{n}}}$$

$$\mathsf{Mac}^1_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle\{\langle \textsc{id}\,,\ \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\textsc{n}}}\,,\ g(\phi^{\mathsf{in}}_{\tau})\rangle) \sim \mathsf{Mac}^1_{\mathsf{k}^{\nu_\tau(\textsc{id})}_{\mathsf{m}}}(\langle\{\langle \nu_\tau(\textsc{id})\,,\ \sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\nu_\tau(\textsc{id})}_{\textsc{u}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\textsc{n}}}\,,\ g(\phi^{\mathsf{in}}_{\underline{\tau}})\rangle)$$

(6) If $\mathsf{ai} = \textsc{pu}_{\textsc{id}}(\_, 2)$, $\textsc{tu}_{\textsc{id}}(\_, 1)$ or $\textsc{fu}_{\textsc{id}}(\_)$:

$$\sigma_\tau(\mathsf{e\text{-}auth}^{\textsc{id}}_{\textsc{u}}) \sim \sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^{\nu_\tau(\textsc{id})}_{\textsc{u}})$$

(7) If $\textsc{tu}_{\textsc{id}}(j, 1)$ then for every $\tau_1 = \_, \textsc{tn}(j_0, 0)$ such that $\textsc{tu}_{\textsc{id}}(j, 0) \prec_\tau \tau_1$:

$$\mathsf{Mac}^4_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\mathsf{n}^{j_0}) \sim \mathsf{Mac}^4_{\mathsf{k}^{\nu_\tau(\textsc{id})}_{\mathsf{m}}}(\mathsf{n}^{j_0})$$

(8) If $\mathsf{ai} = \textsc{pn}(j, 1)$ then for every $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$, for every $\tau_1 = \_, \textsc{pu}_{\textsc{id}}(j_1, 1) \prec \tau$ such that $\tau_1 \not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)$:

$$\mathsf{Mac}^2_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \mathsf{n}^j\,,\ \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))\rangle) \sim \mathsf{Mac}^2_{\mathsf{k}^{\nu_\tau(\textsc{id})}_{\mathsf{m}}}(\langle \mathsf{n}^j\,,\ \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}^{\nu_\tau(\textsc{id})}_{\textsc{u}}))\rangle)$$

(9) If $\mathsf{ai} = \textsc{pn}(j, 1)$ or $\mathsf{ai} = \textsc{tn}(j, 1)$, for every identity $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$, we let:

$$\begin{aligned} \mathsf{net\text{-}e\text{-}auth}_\tau(\textsc{id}, j) &\equiv \mathsf{eq}(\sigma_\tau(\mathsf{e\text{-}auth}^j_{\textsc{n}}), \textsc{id}) \\ \underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\textsc{id}, j) &\equiv \bigvee_{\underline{\textsc{id}} \in \mathsf{copies\text{-}id}_C(\textsc{id})} \mathsf{eq}(\sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^j_{\textsc{n}}), \underline{\textsc{id}}) \end{aligned}$$

Then we ask that:

$$\mathsf{net\text{-}e\text{-}auth}_\tau(\textsc{id}, j) \sim \underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\textsc{id}, j)$$

(10) If $\mathsf{ai} = \textsc{fn}(j)$ for every identity $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$ we let $\{\underline{\textsc{id}}_1, \ldots, \underline{\textsc{id}}_{l_{\textsc{id}}}\} = \mathsf{copies\text{-}id}_C(\textsc{id})$. We define:

$$\begin{aligned} \mathsf{t\text{-}suci\text{-}}\oplus_\tau(\textsc{id}, j) &\equiv \textsc{guti}^j \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\textsc{id}}}(\mathsf{n}^j) \\ \underline{\mathsf{t\text{-}suci\text{-}}\oplus_{\underline{\tau}}}(\textsc{id}, j) &\equiv \underset{1 \leq i \leq l_{\textsc{id}}}{\mathsf{s\text{-}case}}(\mathsf{eq}(\sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^j_{\textsc{n}}), \underline{\textsc{id}}_i) : \textsc{guti}^j \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\textsc{id}}_i}}(\mathsf{n}^j)) \\ \mathsf{t\text{-}mac}_\tau(\textsc{id}, j) &\equiv \mathsf{Mac}^5_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \textsc{guti}^j\,,\ \mathsf{n}^j\rangle) \\ \underline{\mathsf{t\text{-}mac}_{\underline{\tau}}}(\textsc{id}, j) &\equiv \underset{1 \leq i \leq l_{\textsc{id}}}{\mathsf{s\text{-}case}}(\mathsf{eq}(\sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^j_{\textsc{n}}), \underline{\textsc{id}}_i) : \mathsf{Mac}^5_{\mathsf{k}^{\underline{\textsc{id}}_i}_{\mathsf{m}}}(\langle \textsc{guti}^j\,,\ \mathsf{n}^j\rangle)) \end{aligned}$$

Then we ask that:

$$\begin{aligned} \textsc{guti}^j &\sim \textsc{guti}^j \\ [\mathsf{net\text{-}e\text{-}auth}_\tau(\textsc{id}, j)]\,(\mathsf{t\text{-}suci\text{-}}\oplus_\tau(\textsc{id}, j)) &\sim [\underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\textsc{id}, j)]\left(\underline{\mathsf{t\text{-}suci\text{-}}\oplus_{\underline{\tau}}}(\textsc{id}, j)\right) \\ [\mathsf{net\text{-}e\text{-}auth}_\tau(\textsc{id}, j)]\,(\mathsf{t\text{-}mac}_\tau(\textsc{id}, j)) &\sim [\underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\textsc{id}, j)]\left(\underline{\mathsf{t\text{-}mac}_{\underline{\tau}}}(\textsc{id}, j)\right) \end{aligned}$$

Let $(u_i \sim v_i)_{i \in I}$ be such that $\mathsf{reveal}^C_\tau = (u_i \sim v_i)_{i \in I}$. Then we let $\mathsf{l\text{-}reveal}^C_\tau = (u_i)_{i \in I}$ be the list of left elements of reveal^C_τ, and $\mathsf{r\text{-}reveal}^C_\tau = (v_i)_{i \in I}$ list of left elements of reveal^C_τ (in the same order).

Lemma 15. *Let N be a number of identities, τ a valid basic action trace on N identities, C a number of copies larger than $|\tau|$ and $\underline{N} = C.N$. Then there exists a derivation of:*

$$\phi^{AKA^+_N}_\tau, \mathsf{l\text{-}reveal}^C_\tau \sim \phi^{AKA^+_{\underline{N}}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}^C_\tau$$

Proof. The proof is given in Section G. ■

Using this lemma, we can prove our main theorem, which we recall below:

Theorem. *The AKA$^+$ protocol is σ_{ul}-unlinkable for an arbitrary number of agents and sessions when the asymmetric encryption $\{\_\}^{\_}_{\_}$ is IND-CCA$_1$ secure and f and f^{r} (resp. $Mac^1 - Mac^5$) satisfy jointly the PRF assumption.*

Proof. Using Proposition 3, we only need to show that for every $\tau \in \text{support}(\mathcal{R}_{\mathsf{ul}})$, there is a derivation of:

$$\phi_\tau^{\mathrm{AKA}^+_N} \sim \phi_{\underline{\tau}}^{\mathrm{AKA}^+_{\underline{N}}} \tag{45}$$

Moreover, using Proposition 1, we know that for every $\tau \in \text{support}(\mathcal{R}_{\mathsf{ul}})$, τ is a valid action trace. Moreover, τ uses only the identities $\{\text{ID}_1, \dots, \text{ID}_N\}$, and is by consequence a basic action trace. Therefore, it is sufficient to prove that there exists a derivation of the formula in (45) for every valid basic action trace τ. We conclude using the Restr rule and Lemma 15:

$$\frac{\phi_\tau^{\mathrm{AKA}^+_N}, \text{l-reveal}_\tau^C \sim \phi_{\underline{\tau}}^{\mathrm{AKA}^+_{\underline{N}}}, \text{r-reveal}_\tau^C}{\phi_\tau^{\mathrm{AKA}^+_N} \sim \phi_{\underline{\tau}}^{\mathrm{AKA}^+_{\underline{N}}}}\ \text{Restr}$$

■

G PROOF OF LEMMA 15

The proof is by induction over τ. For $\tau = \epsilon$, we just need to check that the elements of item 2 of Definition 45 are indistinguishable, which is obvious from the definition of σ_ϵ in Definition 3.

We now show the inductive case: let $\tau = \tau_0, \text{ai}$ be a valid basic action trace on $\mathcal{S}_{\text{id}}$, and let $C \geq |\tau|$. From now on, the number of copies C is implicit, and we omit it (except when necessary). We want to build of derivation of:

$$\phi_\tau, \text{l-reveal}_\tau \sim \phi_{\underline{\tau}}, \text{r-reveal}_\tau$$

By induction, we assume that there exists a derivation of:

$$\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}$$

The proof is a case disjunction on the value of ai. Before starting, we assume that the following proposition is true (we postpone its proof to the end of this paper, in Section H).

Proposition 29. *For every basic valid action trace $\tau = \_, ai$ on $\mathcal{S}_{id}$*

- ***(Der1)*** *For every identity $\text{ID} \in \mathcal{S}_{id}$, for every τ_1 such that $\tau_1 \prec \tau$ and $\tau_1 \not\prec_\tau \text{NS}_{\text{ID}}(\_)$, there exist derivations using only Simp of:*

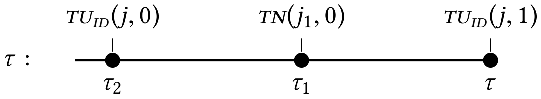
$$\frac{\phi_\tau^{in}, \text{l-reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{in}, \text{r-reveal}_{\tau_0}}{\begin{array}{c}\text{l-reveal}_{\tau_0}, \sigma_\tau^{in}(\text{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \sigma_\tau^{\text{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau_1}^{\text{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \\ \sim\ \text{r-reveal}_{\tau_0}, \sigma_{\underline{\tau}}^{in}(\text{sync}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \wedge \sigma_{\underline{\tau}}^{\text{in}}(\mathrm{SQN}_{\mathrm{N}}^{\nu_\tau(\mathrm{ID})}) < \sigma_{\underline{\tau_1}}^{\text{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})\end{array}}\ \textit{Simp}$$

$$\frac{\phi_\tau^{in}, \text{l-reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{in}, \text{r-reveal}_{\tau_0}}{\begin{array}{c}\text{l-reveal}_{\tau_0}, \sigma_{\tau_1}^{in}(\text{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \sigma_{\tau_1}^{\text{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau}^{\text{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \\ \sim\ \text{r-reveal}_{\tau_0}, \sigma_{\underline{\tau_1}}^{in}(\text{sync}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \wedge \sigma_{\underline{\tau_1}}^{\text{in}}(\mathrm{SQN}_{\mathrm{N}}^{\nu_\tau(\mathrm{ID})}) < \sigma_{\underline{\tau}}^{\text{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})\end{array}}\ \textit{Simp}$$

- ***(Der2)*** *If $ai = \text{FU}_{\text{ID}}(j)$. For every $\text{ID} \in \mathcal{S}_{id}$, for every $\tau_1 = \_, \text{FN}(j_0) \prec \tau$ such that $\tau_1 \not\prec_\tau \text{NS}_{\text{ID}}(\_)$:*
  - *We have $\underline{\tau_1} = \_, \text{FN}(j_0)$, $\underline{\tau} = \_, \text{FU}_{\nu_\tau(\text{ID})}(j)$, $\underline{\tau_1} \prec_{\underline{\tau}} \underline{\tau}$ and $\underline{\tau_1} \not\prec_{\underline{\tau}} \text{NS}_{\nu_\tau(\text{ID})}(\_)$. Therefore,* $\text{fu-tr}_{\mathsf{u}:\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}}$ *is well-defined.*
  - *There is a derivation of:*

$$\frac{\phi_\tau^{in}, \text{l-reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{in}, \text{r-reveal}_{\tau_0}}{\phi_\tau^{in}, \text{l-reveal}_{\tau_0}, \text{fu-tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \ \sim\ \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \text{fu-tr}_{\mathsf{u}:\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}}}\ \textit{Simp}$$

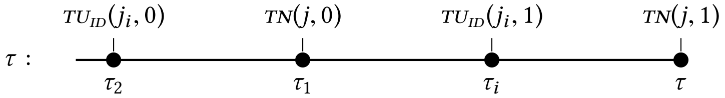
- ***(Der3)*** *If* $ai = \textsc{tu}_{\textsc{id}}(j, 1)$. *For every* $\tau_1 = \_, \textsc{tn}(j_1, 0)$, $\tau_2 = \_, \textsc{tu}_{\textsc{id}}(j, 0)$ *such that* $\tau_2 \prec_\tau \tau_1$*:*


$\textsc{tu}_{\textsc{id}}(j, 0)$
$\textsc{tn}(j_1, 0)$
$\textsc{tu}_{\textsc{id}}(j, 1)$
τ :
τ_2
τ_1
τ

  - *We have* $\underline{\tau_2} = \_, \textsc{tu}_{\nu_\tau(\textsc{id})}(j, 0)$, $\underline{\tau_1} = \_, \textsc{tu}_{\nu_\tau(\textsc{id})}(j, 1)$ *and* $\underline{\tau_2} \prec_{\underline{\tau}} \underline{\tau_1} \prec_{\underline{\tau}} \underline{\tau}$. *Therefore,* $\text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}}$ *is well-defined.*
  - *There is a derivation of:*

$$\frac{\phi^{in}_{\tau}, \text{l-reveal}_{\tau_0} \sim \phi^{in}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{in}_{\tau}, \text{l-reveal}_{\tau_0}, \text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}}}\ \textit{Simp}$$

- ***(Der4)*** *If* $ai = \textsc{tn}(j, 1)$. *For every* $\textsc{id} \in \mathcal{S}_{id}$, $\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1)$, $\tau_1 = \_, \textsc{tn}(j, 0)$, $\tau_2 = \_, \textsc{tu}_{\textsc{id}}(j_i, 0)$ *such that* $\tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i$*:*



  - *We have* $\underline{\tau_2} = \_, \textsc{tu}_{\nu_{\tau_1}(\textsc{id})}(j_i, 0)$, $\underline{\tau_i} = \_, \textsc{tu}_{\nu_{\tau_1}(\textsc{id})}(j_i, 1)$ *and* $\underline{\tau_2} \prec_{\underline{\tau}} \underline{\tau_1} \prec_{\underline{\tau}} \underline{\tau_i} \prec_{\underline{\tau}} \underline{\tau}$. *Therefore,* $\text{full-tr}^{\text{n}:\underline{\tau_1},\underline{\tau}}_{\text{u}:\underline{\tau_2},\underline{\tau_i}}$ *is well-defined.*
  - *There is a derivation of:*

$$\frac{\phi^{in}_{\tau}, \text{l-reveal}_{\tau_0} \sim \phi^{in}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{in}_{\tau}, \text{l-reveal}_{\tau_0}, \text{full-tr}^{\text{n}:\tau_1,\tau}_{\text{u}:\tau_2,\tau_i} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{full-tr}^{\text{n}:\underline{\tau_1},\underline{\tau}}_{\text{u}:\underline{\tau_2},\underline{\tau_i}}}\ \textit{Simp}$$

Proof. The proof is given in Section H ■

We now proceed with the proof of Lemma 15. Let $\underline{\text{ai}}$ be such that $\underline{\tau} = \_, \underline{\text{ai}}$.

G.1 Case ai = $\textsc{ns}_{\textsc{id}}(j)$

We know that $\underline{\text{ai}} = \textsc{ns}_{\nu_{\underline{\tau}}(\textsc{id})}(j)$ and $\nu_\tau(\textsc{id}) = \text{fresh-id}(\nu_{\tau_0}(\textsc{id}))$. Moreover, $\phi_\tau \equiv \phi^{\text{in}}_\tau$ and $\phi_{\underline{\tau}} \equiv \phi^{\text{in}}_{\underline{\tau}}$. Hence l-reveal$_\tau$ and l-reveal$_{\tau_0}$ coincide everywhere except on:

$$\sigma_\tau(\text{valid-guti}^{\text{ID}}_{\text{U}}) \sim \sigma_{\underline{\tau}}(\text{valid-guti}^{\nu_\tau(\text{ID})}_{\text{U}}) \qquad \text{sync-diff}^{\text{ID}}_{\tau} \sim \text{sync-diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}} \qquad \text{m-suci}^{\ \text{ID}}_{\tau} \sim \text{m-suci}^{\ \nu_\tau(\text{ID})}_{\underline{\tau}}$$

We conclude with the following derivation:

$$\cfrac{\cfrac{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{false}, \text{defaut}, \text{false} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{false}, \text{defaut}, \text{false}}\ \text{Simp}}{\begin{array}{c}\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \sigma_\tau(\text{valid-guti}^{\text{ID}}_{\text{U}}), \text{m-suci}^{\ \text{ID}}_{\tau}, \text{sync-diff}^{\text{ID}}_{\tau} \\ \sim\ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \sigma_{\underline{\tau}}(\text{valid-guti}^{\nu_\tau(\text{ID})}_{\text{U}}), \text{m-suci}^{\ \nu_\tau(\text{ID})}_{\underline{\tau}}, \text{sync-diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}}\end{array}}\ R$$

G.2 Case ai = $\textsc{pn}(j, 0)$

We know that $\underline{\text{ai}} = \textsc{pn}(j, 0)$. Here l-reveal$_\tau$ and l-reveal$_{\tau_0}$ coincides completely. Using invariant **(A1)** we know that $\text{n}^j \notin \text{st}(\phi^{\text{in}}_\tau)$, and $\text{n}^j \notin \text{st}(\phi_{\underline{\tau_0}})$. Therefore we conclude this case using the axiom Fresh:

$$\frac{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{n}^j \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{n}^j}\ \text{Fresh}$$

G.3 Case ai = $\mathrm{PU}_{\mathrm{ID}}(j, 1)$

We know that $\underline{\mathrm{ai}} = \mathrm{PU}_{\nu_\tau(\mathrm{ID})}(j, 1)$. Here $\mathsf{l\text{-}reveal}_\tau$ and $\mathsf{l\text{-}reveal}_{\tau_0}$ coincides everywhere except on the pairs:

$$\sigma_\tau(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \sim \sigma_{\underline{\tau}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \qquad \mathsf{m\text{-}suci}_{\tau}^{\mathrm{ID}} \sim \mathsf{m\text{-}suci}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}$$

$$\mathsf{sync\text{-}diff}_{\tau}^{\mathrm{ID}} \sim \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})} \qquad \sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \sim \sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})$$

$$\{\langle \mathrm{ID}\,,\ \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e^{\mathit{j}}}} \sim \{\langle \nu_\tau(\mathrm{ID})\,,\ \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e^{\mathit{j}}}}$$

$$\mathsf{Mac}^1_{\mathsf{k}_\mathsf{m}^{\mathrm{ID}}}(\langle\{\langle \mathrm{ID}\,,\ \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e^{\mathit{j}}}}\,,\ g(\phi_\tau^{\mathsf{in}})\rangle) \sim \mathsf{Mac}^1_{\mathsf{k}_\mathsf{m}^{\nu_\tau(\mathrm{ID})}}(\langle\{\langle \nu_\tau(\mathrm{ID})\,,\ \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e^{\mathit{j}}}}\,,\ g(\phi_{\underline{\tau}}^{\mathsf{in}})\rangle)$$

Part 1 We know that $\sigma_\tau(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \sigma_{\underline{\tau}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \equiv \mathsf{false}$. We deduce that $\mathsf{m\text{-}suci}_{\tau}^{\mathrm{ID}} = \mathsf{m\text{-}suci}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})} = \mathsf{defaut}$. It follows that:

$$\dfrac{\dfrac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{false}, \mathsf{defaut} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{false}, \mathsf{defaut}}\ \mathsf{FA}^*}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma_\tau(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}), \mathsf{m\text{-}suci}_{\tau}^{\mathrm{ID}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma_{\underline{\tau}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}), \mathsf{m\text{-}suci}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}}\ R \tag{46}$$

Part 2 We have:

$$\begin{array}{rcl} \sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) & = & \mathsf{suc}(\sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})) - \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \quad = \quad \mathbf{1} \\ \sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) & = & \mathsf{suc}(\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \quad = \quad \mathbf{1} \end{array}$$

And:

$$\mathsf{sync\text{-}diff}_{\tau}^{\mathrm{ID}} \;=\; [\sigma_\tau(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})]\ (\sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_\tau(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})) \;=\; \left[\sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})\right]\left(\mathsf{suc}(\mathsf{sync\text{-}diff}_{\tau_0}^{\mathrm{ID}})\right)$$

Similarly, $\mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})} = \left[\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})\right]\left(\mathsf{suc}(\mathsf{sync\text{-}diff}_{\underline{\tau_0}}^{\nu_\tau(\mathrm{ID})})\right)$. Hence:

$$\dfrac{\dfrac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}), \mathsf{sync\text{-}diff}_{\tau_0}^{\mathrm{ID}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}), \mathsf{sync\text{-}diff}_{\underline{\tau_0}}^{\nu_\tau(\mathrm{ID})}}\ \mathsf{Dup}^*}{\begin{array}{l} \phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0},\ \mathsf{sync\text{-}diff}_{\tau}^{\mathrm{ID}},\quad \sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \\ \sim\ \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})},\ \sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \end{array}}\ \mathsf{Simp} \tag{47}$$

Part 3 Let $s_l \equiv \mathsf{len}(\langle \mathrm{ID}\,,\ \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\rangle)$. Using the CCA_1 axiom we directly have that:

$$\dfrac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, s_l \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, s_l \qquad \dfrac{\dfrac{}{\mathsf{len}(\mathrm{ID}) = \mathsf{len}(\nu_\tau(\mathrm{ID}))} \qquad \mathsf{len}(\sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})) = \mathsf{len}(\sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}))}{\mathsf{len}(\langle \mathrm{ID}\,,\ \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\rangle) = \mathsf{len}(\langle \nu_\tau(\mathrm{ID})\,,\ \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})\rangle)}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \{\langle \mathrm{ID}\,,\ \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e^{\mathit{j}}}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \{\langle \nu_\tau(\mathrm{ID})\,,\ \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e^{\mathit{j}}}}}\ \mathrm{CCA}_1 \tag{48}$$

Moreover, using Proposition 20, we know that:

$$\mathsf{len}(\sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})) = \mathsf{len}(\sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})) = \mathsf{len}(\mathsf{sqn\text{-}init}_{\mathrm{U}}^{\mathrm{ID}})$$

We deduce that $s_l = \mathsf{len}(\langle \textsc{id}\,,\ \mathsf{sqn\text{-}init}_{\mathrm{U}}^{\textsc{id}}\rangle)$, therefore:

$$\frac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, s_l \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, s_l} \qquad \text{and} \qquad \frac{}{\mathsf{len}(\sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})) = \mathsf{len}(\sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\nu_\tau(\textsc{id})}))}$$

This completes the derivation in (48).

Part 4 To conclude, it only remains to deal with the Mac^1 terms. We start by computing $\mathsf{set\text{-}mac}^1_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}$:

$$\begin{aligned}
\mathsf{set\text{-}mac}^1_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}) \quad = \quad & \left\{ \langle \{\langle \textsc{id}\,,\ \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_1}}\,,\ g(\phi_{\tau_1}^{\mathsf{in}})\rangle \mid \tau_1 = \_, \textsc{pu}_{\textsc{id}}(j_1, 1) \prec \tau \right\} \\
\cup \quad & \left\{ \langle \pi_1(g(\phi_{\tau_1}^{\mathsf{in}}))\,,\ \mathsf{n}^{j_1}\rangle \mid \tau_1 = \_, \textsc{pn}(j_1, 1) \prec \tau \right\}
\end{aligned}$$

We want to get rid of the second set above: using **(Equ3)**, we know that for every $\tau_1 = \_, \textsc{pn}(j_1, 1) \prec \tau$:

$$\mathsf{accept}_\tau^{\textsc{id}} \quad \leftrightarrow \quad \bigvee_{\substack{\tau_2 = \_, \textsc{pu}_{\textsc{id}}(j_2, 1) \\ \tau_2 \prec_\tau \tau_1}} \left(\begin{array}{c} g(\phi_{\tau_2}^{\mathsf{in}}) = \mathsf{n}^j \wedge \pi_1(g(\phi_{\tau_1}^{\mathsf{in}})) = \{\langle \textsc{id}\,,\ \sigma_{\tau_2}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_2}} \\ \wedge\ \pi_2(g(\phi_{\tau_1}^{\mathsf{in}})) = \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle \{\langle \textsc{id}\,,\ \sigma_{\tau_2}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_2}}\,,\ g(\phi_{\tau_2}^{\mathsf{in}})\rangle) \end{array} \right) \tag{49}$$

We let Ψ' be the vector of terms $\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}$ where we replaced every occurrence of $\mathsf{accept}_{\tau_1}^{\textsc{id}}$ (where $\tau_1 = \_, \textsc{pn}(j_1, 1) \prec \tau$) by the equivalent term from (49). We can check that we have:

$$\mathsf{set\text{-}mac}^1_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\Psi') \quad = \quad \left\{ \langle \{\langle \textsc{id}\,,\ \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_1}}\,,\ g(\phi_{\tau_1}^{\mathsf{in}})\rangle \mid \tau_1 = \_, \textsc{pu}_{\textsc{id}}(j_1, 1) \prec \tau \right\}$$

For every $\tau_1 = \_, \textsc{pu}_{\textsc{id}}(j_1, 1) \prec \tau$, using Proposition 20 we know that:

$$\mathsf{len}(\langle \textsc{id}\,,\ \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle) = \mathsf{len}(\langle \textsc{id}\,,\ \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle)$$

Moreover, using the axioms in $\mathsf{Ax}_{\mathsf{len}}$ we know that $\mathsf{len}(\langle \textsc{id}\,,\ \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle) \neq 0$. Therefore, using Proposition 19 we get that we have:

$$\{\langle \textsc{id}\,,\ \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}} \neq \{\langle \textsc{id}\,,\ \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_1}}$$

Hence by left injectivity of $\langle \cdot\,,\ \_\rangle$:

$$\langle \{\langle \textsc{id}\,,\ \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}}\,,\ g(\phi_\tau^{\mathsf{in}})\rangle \neq \langle \{\langle \textsc{id}\,,\ \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_1}}\,,\ g(\phi_{\tau_1}^{\mathsf{in}})\rangle$$

It follows that we can apply the $\textsc{prf-mac}^1$ axiom to replace the following term by a fresh nonce n:

$$\mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle \{\langle \textsc{id}\,,\ \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}}\,,\ g(\phi_\tau^{\mathsf{in}})\rangle)$$

We then rewrite every occurrence of the right-hand side of (49) into $\mathsf{accept}_{\tau_1}^{\textsc{id}}$:

$$\frac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n} \ \sim\ \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0} \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\nu_\tau(\textsc{id})}}(\langle \{\langle \nu_\tau(\textsc{id})\,,\ \sigma_{\underline{\tau}}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\nu_\tau(\textsc{id})})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}}\,,\ g(\phi_{\underline{\tau}}^{\mathsf{in}})\rangle)}{\begin{array}{c} \phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0},\ \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle \{\langle \textsc{id}\,,\ \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}}\,,\ g(\phi_\tau^{\mathsf{in}})\rangle) \\ \sim\ \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\nu_\tau(\textsc{id})}}(\langle \{\langle \nu_\tau(\textsc{id})\,,\ \sigma_{\underline{\tau}}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\nu_\tau(\textsc{id})})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}}\,,\ g(\phi_{\underline{\tau}}^{\mathsf{in}})\rangle) \end{array}} \ \textsc{prf-mac}^1$$

We then do the same on the right side (we omit the details), and conclude using Fresh:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{n}}\;\mathsf{Fresh}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0} \mathsf{Mac}^1_{\mathsf{k}_\mathsf{m}^{\nu_\tau(\textsc{id})}}(\langle\{\langle \nu_\tau(\textsc{id})\,,\, \sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}_\mathrm{U}^{\nu_\tau(\textsc{id})})\rangle\}^{\mathsf{n}_\mathsf{e}^{j}}_{\mathsf{pk}_\mathrm{N}}\,,\, g(\phi^{\mathsf{in}}_{\underline{\tau}})\rangle)}\;\textsc{prf-mac}^1$$

We conclude the proof by combining the derivation above with the derivations in (46), (47) and (48), and by using the induction hypothesis.

G.4 Case ai = $\textsc{pn}(j, 1)$

We know that $\underline{\mathrm{ai}} = \textsc{pn}(j, 1)$. For every $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$, let $M_{\textsc{id}}$ be the set:

$$M_{\textsc{id}} \;=\; \{\tau_2 \mid \tau_2 = \_, \textsc{pu}_{\textsc{id}}(j_1, 1) \prec \tau \wedge \tau_2 \not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)\}$$

Here $\mathsf{l\text{-}reveal}_\tau$ and $\mathsf{l\text{-}reveal}_{\tau_0}$ coincides everywhere except on the following pairs:

$$\Big(\mathsf{sync\text{-}diff}^{\textsc{id}}_{\tau} \;\sim\; \mathsf{sync\text{-}diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau}}\Big)_{\textsc{id}\in\mathcal{S}_{\mathsf{id}}} \qquad \Big(\mathsf{net\text{-}e\text{-}auth}_\tau(\textsc{id}, j) \;\sim\; \underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\textsc{id}, j)\Big)_{\textsc{id}\in\mathcal{S}_{\mathsf{id}}}$$

$$\Big(\mathsf{Mac}^2_{\mathsf{k}_\mathsf{m}^{\textsc{id}}}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}_\mathrm{U}^{\textsc{id}}))\rangle) \;\sim\; \mathsf{Mac}^2_{\mathsf{k}_\mathsf{m}^{\nu_\tau(\textsc{id})}}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_2}}(\textsc{sqn}_\mathrm{U}^{\nu_\tau(\textsc{id})}))\rangle)\Big)_{\tau_2\in M_{\textsc{id}},\, \textsc{id}\in\mathcal{S}_{\mathsf{id}}}$$

Part 1 Let $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$, we consider all the new sessions started with identity $\textsc{id}$ in τ:

$$\{\textsc{ns}_{\textsc{id}}(0), \dots, \textsc{ns}_{\textsc{id}}(l_{\textsc{id}})\} = \{\textsc{ns}_{\textsc{id}}(i) \mid \textsc{ns}_{\textsc{id}}(i) \in \tau\}$$

This induce a partition of symbolic actions in τ for identity $\textsc{id}$. Indeed, let k be such that $\textsc{id} = \mathsf{A}_{k,0}$, and for every $-1 \le i \le l_{\textsc{id}}$, let $\underline{\textsc{id}}_i = \mathsf{A}_{k,i+1}$. Then we define, for every $-1 \le i \le l_{\textsc{id}}$:

$$T^i_{\textsc{id}} \;=\; \left\{\tau_1 \mid \tau_1 = \_, \textsc{pu}_{\textsc{id}}(j_1, 1) \wedge \begin{cases} \textsc{ns}_{\textsc{id}}(i) \prec_\tau \tau_1 \prec_\tau \textsc{ns}_{\textsc{id}}(i+1) & \text{if } 0 \le i < l_{\textsc{id}} \\ \tau_1 \prec_\tau \textsc{ns}_{\textsc{id}}(0) & \text{if } i = -1 \\ \textsc{ns}_{\textsc{id}}(l_{\textsc{id}}) \prec_\tau \tau_1 \prec \tau & \text{if } i = l_{\textsc{id}} \end{cases}\right\}$$

And $T_{\textsc{id}} = \{\tau_1 \mid \tau_1 = \_, \textsc{pu}_{\textsc{id}}(j_1, 1) \wedge \tau_1 \prec \tau\}$. We have $T_{\textsc{id}} = \biguplus_{-1\le i\le l_{\textsc{id}}} T^i_{\textsc{id}}$, and for every $-1 \le i \le l_{\textsc{id}}$:

$$\forall \tau_1 \in T^i_{\textsc{id}},\ \nu_{\tau_1}(\textsc{id}) = \underline{\textsc{id}}_i \quad \text{ and } \quad T^i_{\textsc{id}} \;=\; \Big\{\tau_1 \mid \underline{\tau_1} = \_, \textsc{pu}_{\underline{\textsc{id}}_i}(j_1, 1) \wedge \underline{\tau_1} \prec \underline{\tau_1}\Big\}$$

Part 2 Using **(Equ3)** we know that:

$$\mathsf{accept}^{\textsc{id}}_\tau \;\leftrightarrow\; \bigvee_{\tau_1 = \_, \textsc{pu}_{\textsc{id}}(j_1,1)\in T_{\textsc{id}}} \underbrace{\begin{pmatrix} g(\phi^{\mathsf{in}}_{\tau_1}) = \mathsf{n}^j \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}_\mathrm{U}^{\textsc{id}})\rangle\}^{\mathsf{n}_\mathsf{e}^{j_1}}_{\mathsf{pk}_\mathrm{N}} \\ \wedge\ \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^1_{\mathsf{k}_\mathsf{m}^{\textsc{id}}}(\langle\{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}_\mathrm{U}^{\textsc{id}})\rangle\}^{\mathsf{n}_\mathsf{e}^{j_1}}_{\mathsf{pk}_\mathrm{N}}\,,\, g(\phi^{\mathsf{in}}_{\tau_1})\rangle) \end{pmatrix}}_{b^{\textsc{id}}_{\tau_1}} \tag{50}$$

For all $\tau_1 \in T_{\textsc{id}}$, we let $b^{\textsc{id}}_{\tau_1}$ be the main term of the disjunction above.

Similarly, using **(Equ3)** on $\underline{\tau}$, we have that for every $-1 \le i \le l_{\textsc{id}}$:

$$\mathsf{accept}^{\underline{\textsc{id}}_i}_{\underline{\tau}} \;\leftrightarrow\; \bigvee_{\tau_1 = \_, \textsc{pu}_{\textsc{id}}(j_1,1)\in T^i_{\textsc{id}}} \underbrace{\begin{pmatrix} g(\phi^{\mathsf{in}}_{\underline{\tau_1}}) = \mathsf{n}^j \wedge \pi_1(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \{\langle \underline{\textsc{id}}_i\,,\, \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}_\mathrm{U}^{\underline{\textsc{id}}_i})\rangle\}^{\mathsf{n}_\mathsf{e}^{j_1}}_{\mathsf{pk}_\mathrm{N}} \\ \wedge\ \pi_2(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \mathsf{Mac}^1_{\mathsf{k}_\mathsf{m}^{\underline{\textsc{id}}_i}}(\langle\{\langle \underline{\textsc{id}}_i\,,\, \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}_\mathrm{U}^{\underline{\textsc{id}}_i})\rangle\}^{\mathsf{n}_\mathsf{e}^{j_1}}_{\mathsf{pk}_\mathrm{N}}\,,\, g(\phi^{\mathsf{in}}_{\underline{\tau_1}})\rangle) \end{pmatrix}}_{\underline{b^{\underline{\textsc{id}}_i}_{\tau_1}}} \tag{51}$$

Moreover, if we let $\{\underline{\textsc{id}}_{l_{\textsc{id}}+1}, \dots, \underline{\textsc{id}}_m\}$ be such that:

$$\mathsf{copies\text{-}id}_C(\textsc{id}) = \{\underline{\textsc{id}}_0, \dots, \underline{\textsc{id}}_{l_{\textsc{id}}}\} \uplus \{\underline{\textsc{id}}_{l_{\textsc{id}}+1}, \dots, \underline{\textsc{id}}_m\}$$

Then, for all $i > l_{\textsc{id}}$, we have $\mathsf{accept}_{\underline{\tau}}^{\underline{\textsc{id}}_i} \leftrightarrow \mathsf{false}$. Therefore, using **(A5)**, we can show that:

$$\underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}^{\textsc{id}} \;\leftrightarrow\; \bigvee_{-1 \leq i \leq l} \mathsf{accept}_{\underline{\tau}}^{\underline{\textsc{id}}_i} \tag{52}$$

Part 3 For every $\tau_1, \tau_2 \in T_{\textsc{id}}$ such that $\tau_1 \neq \tau_2$, $\tau_1 = \_, \textsc{pu}_{\textsc{id}}(j_1, 1)$ and $\tau_2 = \_, \textsc{pu}_{\textsc{id}}(j_2, 1)$, using Proposition 19 and 20 we can show that:

$$b_{\tau_1}^{\textsc{id}} \wedge b_{\tau_2}^{\textsc{id}} \quad \rightarrow \quad \{\langle \textsc{id}\,,\, \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\textsc{n}}}^{\mathsf{n}_{\mathsf{e}}^{j_1}} = \{\langle \textsc{id}\,,\, \sigma_{\tau_2}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\textsc{n}}}^{\mathsf{n}_{\mathsf{e}}^{j_2}} \quad \rightarrow \quad \mathsf{false}$$

Similarly, for every $\tau_1, \tau_2 \in T_{\textsc{id}}^{\underline{\textsc{id}}_i}$ such that $\tau_1 \neq \tau_2$:

$$\underline{b}_{\underline{\tau_1}}^{\underline{\textsc{id}}_i} \wedge \underline{b}_{\underline{\tau_2}}^{\underline{\textsc{id}}_i} \quad \rightarrow \quad \mathsf{false}$$

Moreover, since for all identities $\textsc{id}_1 \neq \textsc{id}_2$, we have $\mathsf{eq}(\textsc{id}_1, \textsc{id}_2) = \mathsf{false}$ we know that:

$$\neg\Big(\mathsf{accept}_{\tau}^{\textsc{id}_1} \wedge \mathsf{accept}_{\tau}^{\textsc{id}_2}\Big) \qquad\qquad \neg\Big(\mathsf{accept}_{\underline{\tau}}^{\textsc{id}_1} \wedge \mathsf{accept}_{\underline{\tau}}^{\textsc{id}_2}\Big)$$

We deduce that:

$$\bigg(\Big((b_{\tau_1}^{\textsc{id}})_{\tau_1 \in T_{\textsc{id}}}\Big)_{\textsc{id} \in \mathcal{S}_{\mathsf{id}}}, \underbrace{\textstyle\bigwedge_{\textsc{id} \in \mathcal{S}_{\mathsf{id}}} \neg \mathsf{accept}_{\tau}^{\textsc{id}}}_{b_{\mathsf{unk}}}\bigg)$$

$$\text{and} \quad \bigg(\Big((\underline{b}_{\underline{\tau_1}}^{\underline{\textsc{id}}_i})_{\tau_1 \in T_{\textsc{id}}^i \wedge -1 \leq i \leq l_{\textsc{id}}}\Big)_{\textsc{id} \in \mathcal{S}_{\mathsf{id}}}, \underbrace{\textstyle\bigwedge_{\textsc{id} \in \mathsf{copies\text{-}id}_C(\mathcal{S}_{\mathsf{id}})} \neg \mathsf{accept}_{\tau}^{\textsc{id}}}_{\underline{b_{\mathsf{unk}}}}\bigg)$$

are CS partitions. Besides, for all $\tau_1 \in T_{\textsc{id}}$ we have:

$$\Big[b_{\tau_1}^{\textsc{id}}\Big]\Big(t_\tau \;=\; \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}^{2}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}))\rangle)\Big) \qquad \text{and} \qquad [b_{\mathsf{unk}}]\,(t_\tau = \mathsf{UnknownId})$$

From Proposition 27 we deduce:

$$\begin{aligned} t_\tau \;=\; & \mathsf{if}\ \neg b_{\mathsf{unk}}\ \mathsf{then}\ \underset{\substack{\tau_1 \in T_{\textsc{id}} \\ \textsc{id} \in \mathcal{S}_{\mathsf{id}}}}{\mathsf{case}}\,(b_{\tau_1}^{\textsc{id}} : \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}^{2}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}))\rangle)) \\ & \mathsf{else}\ \mathsf{UnknownId} \end{aligned} \tag{53}$$

Similarly, for every $-1 \leq i \leq l_{\textsc{id}}$, for every $\tau_1 \in T_i^{\textsc{id}}$:

$$\Big[\underline{b}_{\underline{\tau_1}}^{\underline{\textsc{id}}_i}\Big]\Big(t_{\underline{\tau}} \;=\; \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\underline{\textsc{id}}_i}}^{2}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\sigma_{\underline{\tau_1}}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\underline{\textsc{id}}_i}))\rangle)\Big) \qquad \text{and} \qquad \Big[\underline{b_{\mathsf{unk}}}\Big]\,\Big(t_{\underline{\tau}} = \mathsf{UnknownId}\Big)$$

Again, from Proposition 27 we deduce:

$$\begin{aligned} t_{\underline{\tau}} \;=\; & \mathsf{if}\ \neg \underline{b_{\mathsf{unk}}}\ \mathsf{then}\ \underset{\substack{\tau_1 \in T_{\textsc{id}}^i \\ -1 \leq i \leq l_{\textsc{id}} \\ \textsc{id} \in \mathcal{S}_{\mathsf{id}}}}{\mathsf{case}}\,(\underline{b}_{\underline{\tau_1}}^{\underline{\textsc{id}}_i} : \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\underline{\textsc{id}}_i}}^{2}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\sigma_{\underline{\tau_1}}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\underline{\textsc{id}}_i}))\rangle)) \\ & \mathsf{else}\ \mathsf{UnknownId} \end{aligned}$$

Since $T_{\textsc{id}} \;=\; \biguplus_{-1 \leq i \leq l_{\textsc{id}}} T_{\textsc{id}}^i$, and since $\forall \tau_1 \in T_{\textsc{id}}^i$, $\underline{\textsc{id}}_i = \nu_{\tau_1}(\textsc{id})$, we know that:

$$\begin{aligned} t_{\underline{\tau}} \;=\; & \mathsf{if}\ \neg \underline{b_{\mathsf{unk}}}\ \mathsf{then}\ \underset{\substack{\tau_1 \in T_{\textsc{id}} \\ \textsc{id} \in \mathcal{S}_{\mathsf{id}}}}{\mathsf{case}}\,(\underline{b}_{\underline{\tau_1}}^{\nu_{\tau_1}(\textsc{id})} : \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\nu_{\tau_1}(\textsc{id})}}^{2}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\sigma_{\underline{\tau_1}}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\nu_{\tau_1}(\textsc{id})}))\rangle)) \\ & \mathsf{else}\ \mathsf{UnknownId} \end{aligned} \tag{54}$$

Part 4 We are going to show that for every $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$, $-1 \leq i \leq l_{\textsc{id}}$, and $\tau_1 = \textsc{pu}_{\textsc{id}}(j_1, 1) \in T_{\textsc{id}}^i$:

$$\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, b_{\tau_1}^{\textsc{id}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b}_{\underline{\tau_1}}^{\underline{\textsc{id}}_i} \tag{55}$$

For this, we rewrite $b_{\tau_1}^{\textsc{id}}$ and $\underline{b}_{\underline{\tau_1}}^{\textsc{id}_i}$ using, respectively, (50) and (51). First, remark that the following pairs of terms are in reveal_{τ_0}:

$$(\mathsf{n}^j, \mathsf{n}^j) \qquad \left(\{\langle \textsc{id}\,,\ \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\textsc{n}}}^{\mathsf{n}_{\mathsf{e}}^{j_1}}, \{\langle \nu_{\tau_1}(\textsc{id})\,,\ \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\nu_{\tau_1}(\textsc{id})})\rangle\}_{\mathsf{pk}_{\textsc{n}}}^{\mathsf{n}_{\mathsf{e}}^{j_1}}\right)$$

$$\left(\mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle\{\langle \textsc{id}\,,\ \sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}})\rangle\}_{\mathsf{pk}_{\textsc{n}}}^{\mathsf{n}_{\mathsf{e}}^{j_1}}\,,\ g(\phi_{\tau_1}^{\mathsf{in}})\rangle), \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\nu_{\tau_1}(\textsc{id})}}(\langle\{\langle \nu_{\tau_1}(\textsc{id})\,,\ \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\nu_{\tau_1}(\textsc{id})})\rangle\}_{\mathsf{pk}_{\textsc{n}}}^{\mathsf{n}_{\mathsf{e}}^{j_1}}\,,\ g(\phi_{\underline{\tau_1}}^{\mathsf{in}})\rangle)\right)$$

Therefore:

$$\frac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, b_{\tau_1}^{\textsc{id}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b}_{\underline{\tau_1}}^{\textsc{id}_i}}\ \mathsf{Simp} \tag{56}$$

This concludes the proof of (55). Combining this with (50), (51) and (52), we have:

$$\frac{\dfrac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(b_{\tau_1}^{\textsc{id}}\right)_{\tau_1 \in T_{\textsc{id}}^i, -1 \le i \le l_{\textsc{id}}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\underline{b}_{\underline{\tau_1}}^{\textsc{id}_i}\right)_{\tau_1 \in T_{\textsc{id}}^i, -1 \le i \le l_{\textsc{id}}}}\ \mathsf{Simp}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{net\text{-}e\text{-}auth}_\tau^{\textsc{id}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}^{\textsc{id}}}}\ \mathsf{Simp} \tag{57}$$

And:

$$\frac{\dfrac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(b_{\tau_1}^{\textsc{id}}\right)_{\tau_1 \in T_{\textsc{id}}^i, -1 \le i \le l_{\textsc{id}}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\underline{b}_{\underline{\tau_1}}^{\textsc{id}_i}\right)_{\tau_1 \in T_{\textsc{id}}^i, -1 \le i \le l_{\textsc{id}}}}\ \mathsf{Simp}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, b_{\mathsf{unk}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b_{\mathsf{unk}}}}\ \mathsf{Simp} \tag{58}$$

We can now prove that $t_\tau \sim t_{\underline{\tau}}$. First we rewrite t_τ and $t_{\underline{\tau}}$ using, respectively, (53) and (54). Then we split the proof with FA, and combine it with (56) and (58). This yields:

$$\frac{\dfrac{\begin{array}{c}\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle \mathsf{n}^j\,,\ \mathsf{suc}(\sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}))\rangle)\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}} \\ \sim\ \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\nu_{\tau_1}(\textsc{id})}}(\langle \mathsf{n}^j\,,\ \mathsf{suc}(\sigma_{\underline{\tau_1}}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\nu_{\tau_1}(\textsc{id})}))\rangle)\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}}\end{array}}{\begin{array}{c}\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, b_{\mathsf{unk}}, \left(b_{\tau_1}^{\textsc{id}}, \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle \mathsf{n}^j\,,\ \mathsf{suc}(\sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}))\rangle)\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}} \\ \sim\ \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b_{\mathsf{unk}}}, \left(\underline{b}_{\underline{\tau_1}}^{\nu_{\tau_1}(\textsc{id})}, \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\nu_{\tau_1}(\textsc{id})}}(\langle \mathsf{n}^j\,,\ \mathsf{suc}(\sigma_{\underline{\tau_1}}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\nu_{\tau_1}(\textsc{id})}))\rangle)\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}}\end{array}}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, t_\tau \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}}}\ \mathsf{Simp} \tag{59}$$

Notice that for every $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$, $M_{\textsc{id}} = T_{\textsc{id}}^{l_{\textsc{id}}}$. Therefore the Mac part in $\mathsf{reveal}_\tau \backslash \mathsf{reveal}_{\tau_0}$ appears in the derivation above, i.e.:

$$\begin{array}{rl} & \left(\mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle \mathsf{n}^j\,,\ \mathsf{suc}(\sigma_{\tau_2}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}))\rangle), \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\nu_\tau(\textsc{id})}}(\langle \mathsf{n}^j\,,\ \mathsf{suc}(\sigma_{\underline{\tau_2}}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\nu_\tau(\textsc{id})}))\rangle)\right)_{\tau_2 \in M_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}} \\ \subseteq & \left(\mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle \mathsf{n}^j\,,\ \mathsf{suc}(\sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}))\rangle), \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\nu_{\tau_1}(\textsc{id})}}(\langle \mathsf{n}^j\,,\ \mathsf{suc}(\sigma_{\underline{\tau_1}}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\nu_{\tau_1}(\textsc{id})}))\rangle)\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}} \end{array} \tag{60}$$

Part 5 Let $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$. Our goal is to apply the $\textsc{prf-mac}^2$ hypothesis to $\mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle \mathsf{n}^j\,,\ \mathsf{suc}(\sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}))\rangle)$ simultaneously for every $\tau_1 \in T_{\textsc{id}}$ in:

$$\Psi\ \equiv\ \phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\langle \mathsf{n}^j\,,\ \mathsf{suc}(\sigma_{\tau_1}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}))\rangle)\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}}$$

Using **(Equ2)** we know that for every $\textsc{ns}_{\textsc{id}}(l_{\textsc{id}}) \prec_\tau \tau_i = \_, \textsc{pu}_{\textsc{id}}(j_i, 2)$:

$$\mathsf{accept}^{\textsc{id}}_{\tau_i} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{pn}(j_1, 1) \\ \tau_2 = \_, \textsc{pu}_{\textsc{id}}(j_i, 1) \\ \tau_2 \prec_\tau \tau_1 \prec \tau}} g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^2_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))\rangle) \ \wedge\ g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1} \tag{61}$$

Let Ψ' be the formula obtained from Ψ by rewriting every $\mathsf{accept}^{\textsc{id}}_{\tau_i}$ s.t. $\textsc{ns}_{\textsc{id}}(l_{\textsc{id}}) \prec_\tau \tau_i = \_, \textsc{pu}_{\textsc{id}}(j_i, 2)$ using the equation above. Then we can check that for every $\tau_1 \in T_{\textsc{id}}$, there is only one occurrence of $\mathsf{Mac}^2_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \mathsf{n}^{j} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))\rangle)$ in Ψ'. Moreover:

$$\begin{aligned} \mathsf{set\text{-}mac}^2_{\textsc{id}}(\Psi') \backslash \{\langle \mathsf{n}^{j} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))\rangle\} \ = & \\ \Big\{\langle \mathsf{n}^{j} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))\rangle \mid \tau_2 \in T_{\textsc{id}} \wedge \tau_1 \neq \tau_2\Big\} & \\ \cup\ \Big\{\langle \mathsf{n}^{j_0} , \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_i})), \mathsf{sk}_{\textsc{n}})))\rangle \mid \tau_i = \_, \textsc{pn}(j_0, 1) \prec \tau\Big\} & \end{aligned}$$

To apply the $\textsc{prf-mac}^2$ axioms, it is sufficient to show that for every element u in the set above, we have $(\langle \mathsf{n}^{j} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))\rangle \neq u$:

- Using **(A2)** we know that for every $\tau_1, \tau_2 \in T_{\textsc{id}}$, if $\tau_1 \neq \tau_2$ then $\sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})) \neq \sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))$. Hence:
$$\langle \mathsf{n}^{j} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))\rangle \ \neq\ \langle \mathsf{n}^{j} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))\rangle$$
- for every $\tau_i = \_, \textsc{pn}(j_0, 1) \prec \tau$, we have $j_0 < j$, hence $\mathsf{n}^{j_0} \neq \mathsf{n}^{j}$ and by consequence:
$$\langle \mathsf{n}^{j} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))\rangle \ \neq\ \langle \mathsf{n}^{j_0} , \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_i})), \mathsf{sk}_{\textsc{n}})))\rangle$$

We can conclude: we rewrite Ψ into Ψ'; we apply $\textsc{prf-mac}^2$ for every $\tau_1 \in T_{\textsc{id}}$, replacing the term $\mathsf{Mac}^2_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \mathsf{n}^{j} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))\rangle)$ by a fresh nonce n^{j,τ_1}; and we rewrite any term of (61) back into $\mathsf{accept}^{\textsc{id}}_{\tau_i}$. Doing this for every identity $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$, this yields:

$$\frac{\begin{array}{l} \phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{n}^{j,\tau_1}\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}} \\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\nu_{\tau_1}(\textsc{id})}}(\langle \mathsf{n}^{j} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}_{\textsc{u}}^{\nu_{\tau_1}(\textsc{id})}))\rangle)\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}} \end{array}}{\begin{array}{l} \phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^2_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \mathsf{n}^{j} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}))\rangle)\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}} \\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\nu_{\tau_1}(\textsc{id})}}(\langle \mathsf{n}^{j} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}_{\textsc{u}}^{\nu_{\tau_1}(\textsc{id})}))\rangle)\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}} \end{array}} \ (\mathsf{Simp} + \textsc{prf-mac}^2)^*$$

We do the same thing on the Big-side, which yields (we omit the details):

$$\frac{\dfrac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{n}^{j,\tau_1}\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}} \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{n}^{j,\tau_1}\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}}}\ \mathsf{Fresh}^*}{\begin{array}{l} \phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{n}^{j,\tau_1}\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}} \\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\nu_{\tau_1}(\textsc{id})}}(\langle \mathsf{n}^{j} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}_{\textsc{u}}^{\nu_{\tau_1}(\textsc{id})}))\rangle)\right)_{\tau_1 \in T_{\textsc{id}}, \textsc{id} \in \mathcal{S}_{\mathsf{id}}} \end{array}} \ (\mathsf{Simp} + \textsc{prf-mac}^2)^*$$

Combining this with (59), we get:

$$\frac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, t_\tau \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}}} \tag{62}$$

Part 6 We now deal with the $\text{sync-diff}^{\textsc{id}}_{\tau} \sim \text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau}}$ part. We first handle the case where $\sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}})$ is false. Observe that $\sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}}) = \sigma^{\text{in}}_{\tau_0}(\text{sync}^{\textsc{id}}_{\textsc{u}})$, $\sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}}) = \sigma^{\text{in}}_{\underline{\tau_0}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}})$ and that the pair of terms $(\sigma^{\text{in}}_{\tau_0}(\text{sync}^{\textsc{id}}_{\textsc{u}}), \sigma^{\text{in}}_{\underline{\tau_0}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}}))$ appears in reveal_{τ_0}. Moreover:

$$[\neg\sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}})]\text{sync-diff}^{\textsc{id}}_{\tau} \;=\; \text{error} \qquad\qquad [\neg\sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}})]\text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau}} \;=\; \text{error}$$

Hence:

$$\dfrac{\dfrac{\text{l-reveal}_{\tau_0}, [\sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}})]\text{sync-diff}^{\textsc{id}}_{\tau} \;\sim\; \text{r-reveal}_{\tau_0}, [\sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}})]\text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau}}}{\begin{array}{c}\text{l-reveal}_{\tau_0}, \sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}}), \quad [\sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}})]\text{sync-diff}^{\textsc{id}}_{\tau}, \quad [\neg\sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}})]\text{sync-diff}^{\textsc{id}}_{\tau} \\ \sim\; \text{r-reveal}_{\tau_0}, \sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}}), [\sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}})]\text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau}}, [\neg\sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}})]\text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau}}\end{array}}\,\text{Simp}}{\text{l-reveal}_{\tau_0}, \text{sync-diff}^{\textsc{id}}_{\tau} \;\sim\; \text{r-reveal}_{\tau_0}, \text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau}}}\,\text{FA}^* \tag{63}$$

Therefore we can focus on the case where $\sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}})$ is true. For all $\textsc{id} \in \mathcal{S}_{\text{id}}$, we let:

$$\text{inc-}\textsc{sqn}^{\textsc{id}}_{\tau} \;\equiv\; \pi_2(\text{dec}(\pi_1(g(\phi^{\text{in}}_{\tau})), \text{sk}^{\textsc{id}}_{\textsc{n}})) \geq \sigma^{\text{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$$

Then:

$$[\sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}})]\text{sync-diff}^{\textsc{id}}_{\tau} \;=\; \underset{\tau_1 \in T_{\textsc{id}}}{\text{case}} \left(b^{\textsc{id}}_{\tau_1} : \begin{array}{r} \text{if} \begin{pmatrix} \sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}}) \\ \wedge\, \text{inc-}\textsc{sqn}^{\textsc{id}}_{\tau} \end{pmatrix} \text{then } \sigma^{\text{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) - \text{suc}(\sigma^{\text{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})) \\ \text{else } [\sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}})]\text{sync-diff}^{\textsc{id}}_{\tau_0} \end{array} \right) \tag{64}$$

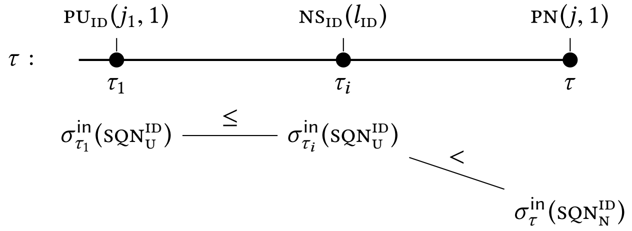
And:

$$[\sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}})]\text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau}} \;=\;$$

$$\underset{\tau_1 \in T_{\textsc{id}}^{\underline{\textsc{id}}_{l_{\textsc{id}}}}}{\text{case}} \left(\underline{b}^{\nu_\tau(\textsc{id})}_{\underline{\tau_1}} : \begin{array}{r} \text{if} \begin{pmatrix} \sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}}) \\ \wedge\, \text{inc-}\textsc{sqn}^{\nu_\tau(\textsc{id})}_{\underline{\tau}} \end{pmatrix} \text{then } \sigma^{\text{in}}_{\underline{\tau}}(\textsc{sqn}^{\nu_\tau(\textsc{id})}_{\textsc{u}}) - \text{suc}(\sigma^{\text{in}}_{\underline{\tau}}(\textsc{sqn}^{\nu_\tau(\textsc{id})}_{\textsc{n}})) \\ \text{else } [\sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}})]\text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau_0}} \end{array} \right) \tag{65}$$

Take $\tau_1 \in T_{\textsc{id}}$, and let τ_i be such that $\tau_i = \_, \textsc{ns}_{\textsc{id}}(l_{\textsc{id}})$ and $\tau_i \prec \tau$. We have two cases:

- If $\tau_1 \prec_\tau \textsc{ns}_{\textsc{id}}(l_{\textsc{id}})$, then using **(B1)** and **(B6)**, we know that $\sigma^{\text{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) \leq \sigma^{\text{in}}_{\tau_i}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$ and that $\sigma^{\text{in}}_{\tau_1}(\text{sync}^{\textsc{id}}_{\textsc{u}}) \rightarrow \sigma^{\text{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) > \sigma^{\text{in}}_{\tau_i}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$. We summarize this below:



$\textsc{pu}_{\textsc{id}}(j_1, 1)$
$\textsc{ns}_{\textsc{id}}(l_{\textsc{id}})$
$\textsc{pn}(j, 1)$
τ :
τ_1
τ_i
τ
$\sigma^{\text{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$\leq$
$\sigma^{\text{in}}_{\tau_i}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$<$
$\sigma^{\text{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$

Hence $\neg(b^{\textsc{id}}_{\tau_1} \wedge \sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \text{inc-}\textsc{sqn}^{\textsc{id}}_{\tau})$.
Now we look at the right protocol: since $\tau_1 \prec_\tau \textsc{ns}_{\textsc{id}}(l_{\textsc{id}})$, we know that $\nu_{\tau_1}(\textsc{id}) = \underline{\textsc{id}}_{l_{\textsc{id}}-p}$ for some $p > 0$. Hence $\nu_{\tau_1}(\textsc{id}) \neq \underline{\textsc{id}}_{l_{\textsc{id}}} = \nu_\tau(\textsc{id})$, which implies that:

$$\underline{b}^{\nu_{\tau_1}(\textsc{id})}_{\underline{\tau_1}} \;\rightarrow\; \text{accept}^{\nu_{\tau_1}(\textsc{id})}_{\underline{\tau}} \;\rightarrow\; \neg\text{accept}^{\nu_\tau(\textsc{id})}_{\underline{\tau}} \;\rightarrow\; \bigwedge_{\tau_2 \in T^{l_{\textsc{id}}}_{\textsc{id}}} \neg\underline{b}^{\nu_\tau(\textsc{id})}_{\underline{\tau_2}}$$

We deduce that:

$$\begin{aligned}
[b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau} &= [b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau_0}\\
[\underline{b}^{\nu_{\tau_1}(\mathrm{ID})}_{\underline{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}} &= [\underline{b}^{\nu_{\tau_1}(\mathrm{ID})}_{\underline{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau_0}}
\end{aligned}$$

Since $(\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau_0}, \mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau_0}}) \in \mathsf{reveal}_{\tau_0}$, we have:

$$\dfrac{\dfrac{\mathsf{l\text{-}reveal}_{\tau_0}, b^{\mathrm{ID}}_{\tau_1} \sim \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b}^{\nu_{\tau_1}(\mathrm{ID})}_{\underline{\tau_1}}}{\mathsf{l\text{-}reveal}_{\tau_0}, b^{\mathrm{ID}}_{\tau_1}, \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}), \mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau_0} \sim \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b}^{\nu_{\tau_1}(\mathrm{ID})}_{\underline{\tau_1}}, \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}), \mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau_0}}}\ \mathsf{Dup}^*}{\mathsf{l\text{-}reveal}_{\tau_0}, [b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau} \sim \mathsf{r\text{-}reveal}_{\tau_0}, [\underline{b}^{\nu_{\tau_1}(\mathrm{ID})}_{\underline{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}}\ \mathsf{FA}^*$$

Combining this with (56), we can get rid of $b^{\mathrm{ID}}_{\tau_1} \sim \underline{b}^{\nu_{\tau_1}(\mathrm{ID})}_{\underline{\tau_1}}$:

$$\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\begin{array}{l}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, [b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau}\\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, [\underline{b}^{\nu_{\tau_1}(\mathrm{ID})}_{\underline{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}\end{array}} \tag{66}$$

- If $\tau_1 \not\prec_\tau \textsc{ns}_{\mathrm{ID}}(l_{\mathrm{ID}})$, then $\nu_{\tau_1}(\mathrm{ID}) = \nu_\tau(\mathrm{ID})$. Let $\underline{\mathrm{ID}} = \nu_\tau(\mathrm{ID})$, and using (64) and (65) we get that:

$$\begin{aligned}
[b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau} = \ & \left[b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})\right]\left(\sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}) - \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}}))\right)\\
&+ \mathsf{if}\ b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{inc\text{-}}\textsc{sqn}^{\mathrm{ID}}_{\tau}\ \mathsf{then}\ \mathbf{-1}\ \mathsf{else}\ 0\\
[\underline{b}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\underline{\mathrm{ID}}}_{\underline{\tau}} = \ & \left[\underline{b}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}})\right]\left(\sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) - \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\mathrm{ID}}}_{\mathrm{N}}))\right)\\
&+ \mathsf{if}\ \underline{b}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \mathsf{inc\text{-}}\textsc{sqn}^{\underline{\mathrm{ID}}}_{\underline{\tau}}\ \mathsf{then}\ \mathbf{-1}\ \mathsf{else}\ 0
\end{aligned}$$

Hence using (56) we get:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{inc\text{-}}\textsc{sqn}^{\mathrm{ID}}_{\tau} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \mathsf{inc\text{-}}\textsc{sqn}^{\underline{\mathrm{ID}}}_{\underline{\tau}}}{\begin{array}{l}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, b^{\mathrm{ID}}_{\tau_1}, \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}) - \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}}), b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{inc\text{-}}\textsc{sqn}^{\mathrm{ID}}_{\tau}\\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}}, \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) - \sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\mathrm{ID}}}_{\mathrm{N}}), \underline{b}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \mathsf{inc\text{-}}\textsc{sqn}^{\underline{\mathrm{ID}}}_{\underline{\tau}}\end{array}}\ \mathsf{Dup}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, [b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, [\underline{b}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\underline{\mathrm{ID}}}_{\underline{\tau}}}\ \mathsf{FA}^*$$

We split the proof in two, depending on whether $\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$ is true or not.

– If it is true, this is simple:

$$\begin{aligned}
\left(\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{inc\text{-}}\textsc{sqn}^{\mathrm{ID}}_{\tau}\right) &\leftrightarrow \left(b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}) < \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}})\right)\\
\left(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{b}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \mathsf{inc\text{-}}\textsc{sqn}^{\underline{\mathrm{ID}}}_{\underline{\tau}}\right) &\leftrightarrow \left(\underline{b}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) < \sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\mathrm{ID}}}_{\mathrm{N}})\right)
\end{aligned}$$

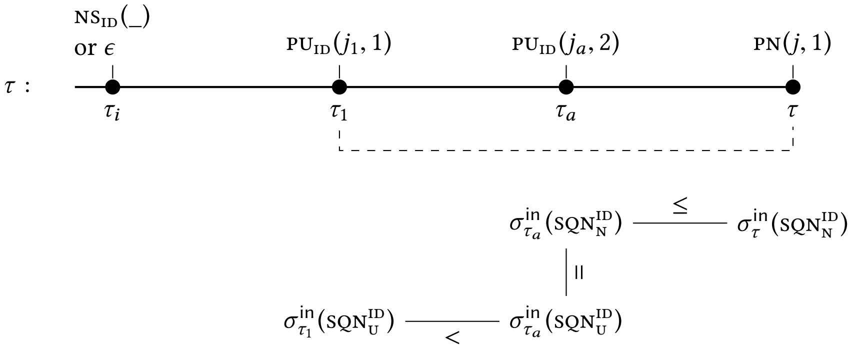

$\textsc{ns}_{\textsc{id}}(\_)$ or ϵ
$\textsc{pu}_{\textsc{id}}(j_1, 1)$
$\textsc{pu}_{\textsc{id}}(j_a, 2)$
$\textsc{pn}(j, 1)$
τ :
τ_i
τ_1
τ_a
τ
$\sigma^{\mathsf{in}}_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$
$\leq$
$\sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$
$\parallel$
$\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$<$
$\sigma^{\mathsf{in}}_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$

Fig. 26. Graphical Representation Used in the Proof of the Case $\textsc{pn}(j, 1)$ of Lemma 15.

Hence using (56) we get:

$$\dfrac{\dfrac{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) < \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})\\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}}) \wedge \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}}) < \sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{n}})\end{array}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, b^{\textsc{id}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) < \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})\\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b^{\textsc{id}}_{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}}) \wedge \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}}) < \sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{n}})\end{array}}\ \mathsf{Simp}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge b^{\textsc{id}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{inc\text{-}}\textsc{sqn}^{\textsc{id}}_{\tau}\\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}}) \wedge \underline{b^{\textsc{id}}_{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}}) \wedge \mathsf{inc\text{-}}\textsc{sqn}^{\underline{\textsc{id}}}_{\underline{\tau}}\end{array}}\ R$$

We conclude the case $\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}})$ using **(Der1)**:

$$\dfrac{\mathsf{l\text{-}reveal}_{\tau_0}\ \sim\ \mathsf{r\text{-}reveal}_{\tau_0}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) < \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})\\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}}) \wedge \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}}) < \sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{n}})\end{array}}\ \mathsf{Simp}$$

– If $\mathsf{sync}^{\textsc{id}}_{\textsc{u}}$ is false at τ_1 and true at τ, then we know that there is an instant $\tau_1 \preceq \tau_a$ such that $\neg\sigma^{\mathsf{in}}_{\tau_a}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \sigma^{\mathsf{in}}_{\tau_a}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}})$. Since $\mathsf{sync}^{\textsc{id}}_{\textsc{u}}$ is only updated at instant $\textsc{pu}_{\textsc{id}}(\_,\_)$ and $\textsc{ns}_{\textsc{id}}(\_)$, and since $\tau_1 \not\prec_{\tau} \textsc{ns}_{\textsc{id}}(\_)$, the only possibilities are τ_a of the form $\_, \textsc{pu}_{\textsc{id}}(j_a, 2)$. In that case, we must have $\mathsf{accept}^{\textsc{id}}_{\tau_a}$. Formally, it is straightforward to show by induction that:

$$b^{\textsc{id}}_{\tau_1} \wedge \neg\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \ \rightarrow \bigvee_{\substack{\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 2)\\ \tau_1 \prec_{\tau} \tau_a}} \neg\sigma^{\mathsf{in}}_{\tau_a}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{accept}^{\textsc{id}}_{\tau_a} \qquad (67)$$

Using **(StrEqu4)**, we know that:

$$\mathsf{accept}^{\textsc{id}}_{\tau_a} \wedge \neg\sigma^{\mathsf{in}}_{\tau_a}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \ \rightarrow\ \sigma_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) = \sigma_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$$

We know that $\sigma_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) = \sigma^{\mathsf{in}}_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$ and $\sigma_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) = \sigma^{\mathsf{in}}_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$. Moreover using **(B1)**:

$$\sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) \leq \sigma_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) \qquad\qquad \sigma_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$$

Finally, we know that $\sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) = \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) + 1$, and therefore $\sigma_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) > \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$. We summarize this graphically in Figure 26. Therefore:

$$\neg\sigma^{\mathsf{in}}_{\tau_a}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \mathsf{accept}^{\textsc{id}}_{\tau_a} \ \rightarrow\ \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) < \sigma^{\mathsf{in}}_{\tau_a}(\mathsf{sync}^{\textsc{id}}_{\textsc{n}})$$

Hence we deduce from (67) that:

$$b_{\tau_1}^{\textsc{id}} \wedge \neg\sigma_{\tau_1}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge \sigma_{\tau}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\textsc{id}}) \;\rightarrow\; \textsf{inc-}\textsc{sqn}_{\tau}^{\textsc{id}}$$

Similarly, we show that:

$$\underline{b}_{\underline{\tau_1}}^{\underline{\textsc{id}}} \wedge \neg\sigma_{\underline{\tau_1}}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\underline{\textsc{id}}}) \wedge \sigma_{\underline{\tau}}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\underline{\textsc{id}}}) \;\rightarrow\; \textsf{inc-}\textsc{sqn}_{\underline{\tau}}^{\underline{\textsc{id}}}$$

Hence using (56) we get:

$$\dfrac{\dfrac{\dfrac{\phi_{\tau}^{\textsf{in}}, \textsf{l-reveal}_{\tau_0} \;\sim\; \phi_{\underline{\tau}}^{\textsf{in}}, \textsf{r-reveal}_{\tau_0}}{\phi_{\tau}^{\textsf{in}}, \textsf{l-reveal}_{\tau_0}, \sigma_{\tau_1}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\textsc{id}}), b_{\tau_1}^{\textsc{id}}, \sigma_{\tau}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\textsc{id}}) \sim \phi_{\underline{\tau}}^{\textsf{in}}, \textsf{r-reveal}_{\tau_0}, \sigma_{\underline{\tau_1}}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\underline{\textsc{id}}}), \underline{b}_{\underline{\tau_1}}^{\underline{\textsc{id}}}, \sigma_{\underline{\tau}}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\underline{\textsc{id}}})}\,\textsf{Dup}^*}{\begin{array}{c}\phi_{\tau}^{\textsf{in}}, \textsf{l-reveal}_{\tau_0}, \neg\sigma_{\tau_1}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge b_{\tau_1}^{\textsc{id}} \wedge \sigma_{\tau}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\textsc{id}}) \\ \sim\; \phi_{\underline{\tau}}^{\textsf{in}}, \textsf{r-reveal}_{\tau_0}, \neg\sigma_{\underline{\tau_1}}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\underline{\textsc{id}}}) \wedge \underline{b}_{\underline{\tau_1}}^{\underline{\textsc{id}}} \wedge \sigma_{\underline{\tau}}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\underline{\textsc{id}}})\end{array}}\,\textsf{Simp}}{\begin{array}{c}\phi_{\tau}^{\textsf{in}}, \textsf{l-reveal}_{\tau_0}, \neg\sigma_{\tau_1}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge b_{\tau_1}^{\textsc{id}} \wedge \sigma_{\tau}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge \textsf{inc-}\textsc{sqn}_{\tau}^{\textsc{id}} \\ \sim\; \phi_{\underline{\tau}}^{\textsf{in}}, \textsf{r-reveal}_{\tau_0}, \neg\sigma_{\underline{\tau_1}}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\underline{\textsc{id}}}) \wedge \underline{b}_{\underline{\tau_1}}^{\underline{\textsc{id}}} \wedge \sigma_{\underline{\tau}}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\underline{\textsc{id}}}) \wedge \textsf{inc-}\textsc{sqn}_{\underline{\tau}}^{\underline{\textsc{id}}}\end{array}}\,R$$

Combining the derivations we build above, we get a derivation of:

$$\dfrac{\phi_{\tau}^{\textsf{in}}, \textsf{l-reveal}_{\tau_0} \;\sim\; \phi_{\underline{\tau}}^{\textsf{in}}, \textsf{r-reveal}_{\tau_0}}{\phi_{\tau}^{\textsf{in}}, \textsf{l-reveal}_{\tau_0}, [b_{\tau_1}^{\textsc{id}} \wedge \sigma_{\tau}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\textsc{id}})]\textsf{sync-diff}_{\tau}^{\textsc{id}} \sim \phi_{\underline{\tau}}^{\textsf{in}}, \textsf{r-reveal}_{\tau_0}, [\underline{b}_{\underline{\tau_1}}^{\nu_{\tau_1}(\textsc{id})} \wedge \sigma_{\underline{\tau}}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\underline{\textsc{id}}})]\textsf{sync-diff}_{\underline{\tau}}^{\underline{\textsc{id}}}} \tag{68}$$

Part 7 It only remains to put everything together. First combining (56), (66) and (68), we get:

$$\dfrac{\dfrac{\dfrac{\phi_{\tau}^{\textsf{in}}, \textsf{l-reveal}_{\tau_0} \;\sim\; \phi_{\underline{\tau}}^{\textsf{in}}, \textsf{r-reveal}_{\tau_0}}{\vdots}}{\begin{array}{c}\phi_{\tau}^{\textsf{in}},\textsf{l-reveal}_{\tau_0}, \left(b_{\tau_1}^{\textsc{id}}, [\sigma_{\tau}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\textsc{id}}) \wedge b_{\tau_1}^{\textsc{id}}]\textsf{sync-diff}_{\tau}^{\textsc{id}}\right)_{\tau_1 \in T_{\textsc{id}}} \\ \sim\; \phi_{\underline{\tau}}^{\textsf{in}},\textsf{r-reveal}_{\tau_0}, \left(\underline{b}_{\underline{\tau_1}}^{\nu_{\tau_1}(\textsc{id})}, [\sigma_{\underline{\tau}}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\underline{\textsc{id}}}) \wedge \underline{b}_{\underline{\tau_1}}^{\nu_{\tau_1}(\textsc{id})}]\textsf{sync-diff}_{\underline{\tau}}^{\underline{\textsc{id}}}\right)_{\tau_1 \in T_{\textsc{id}}}\end{array}}}{\phi_{\tau}^{\textsf{in}}, \textsf{l-reveal}_{\tau_0}, [\sigma_{\tau}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\textsc{id}})]\textsf{sync-diff}_{\tau}^{\textsc{id}} \;\sim\; \phi_{\underline{\tau}}^{\textsf{in}}, \textsf{r-reveal}_{\tau_0}, [\sigma_{\underline{\tau}}^{\textsf{in}}(\textsf{sync}_{\textsc{u}}^{\underline{\textsc{id}}})]\textsf{sync-diff}_{\underline{\tau}}^{\underline{\textsc{id}}}}\,\textsf{FA}^*$$

Combine with (63), this yields:

$$\dfrac{\phi_{\tau}^{\textsf{in}}, \textsf{l-reveal}_{\tau_0} \;\sim\; \phi_{\underline{\tau}}^{\textsf{in}}, \textsf{r-reveal}_{\tau_0}}{\phi_{\tau}^{\textsf{in}}, \textsf{l-reveal}_{\tau_0}, \textsf{sync-diff}_{\tau}^{\textsc{id}} \;\sim\; \phi_{\underline{\tau}}^{\textsf{in}}, \textsf{r-reveal}_{\tau_0}, \textsf{sync-diff}_{\underline{\tau}}^{\underline{\textsc{id}}}}$$

We conclude the proof of this case by combining this derivation with (57) and (62) (recall that the Macs in $\textsf{reveal}_{\tau} \backslash \textsf{reveal}_{\tau_0}$ were handled in (60)).

G.5 Case ai = $\textsc{pu}_{\textsc{id}}(j, 2)$

We know that $\underline{\textsf{ai}} = \textsc{pu}_{\nu_\tau(\textsc{id})}(j, 2)$. Here $\textsf{l-reveal}_{\tau}$ and $\textsf{l-reveal}_{\tau_0}$ coincides everywhere except on the pairs:

$$\textsf{sync-diff}_{\tau}^{\textsc{id}} \;\sim\; \textsf{sync-diff}_{\underline{\tau}}^{\nu_\tau(\textsc{id})} \qquad\qquad \sigma_{\tau}(\textsf{e-auth}_{\textsc{u}}^{\textsc{id}}) \;\sim\; \sigma_{\underline{\tau}}(\textsf{e-auth}_{\textsc{u}}^{\nu_\tau(\textsc{id})})$$

$$\sigma_{\tau}(\textsf{sync}_{\textsc{u}}^{\textsc{id}}) \;\sim\; \sigma_{\underline{\tau}}(\textsf{sync}_{\textsc{u}}^{\nu_\tau(\textsc{id})})$$

Therefore we are looking for a derivation of:

$$\Phi \;\equiv\; \begin{array}{c} \phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}_{\tau}^{\mathrm{ID}}, \sigma_{\tau}(\mathsf{e\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}), \sigma_{\tau}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}), \mathsf{accept}_{\tau}^{\mathrm{ID}} \\ \sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}, \sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}), \sigma_{\underline{\tau}}(\mathsf{sync}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}), \mathsf{accept}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})} \end{array} \tag{69}$$

Let $\tau_2 = \_, \mathrm{PU}_{\mathrm{ID}}(j,1) \prec \tau$. We know that $\tau_2 \not\prec_\tau \mathrm{NS}_{\mathrm{ID}}(\_)$, and therefore $\underline{\tau_2} = \_, \mathrm{PU}_{\nu_\tau(\mathrm{ID})}(j,1)$. Also:

$$\sigma_{\tau}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \sigma_{\tau_2}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) \equiv g(\phi_{\tau_2}^{\mathsf{in}}) \qquad \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \equiv \sigma_{\underline{\tau_2}}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \equiv g(\phi_{\underline{\tau_2}}^{\mathsf{in}})$$

Hence we can start deconstructing the terms using FA and simplifying with Dup:

$$\dfrac{\dfrac{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}_{\tau}^{\mathrm{ID}}, \mathsf{accept}_{\tau}^{\mathrm{ID}} \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}, \mathsf{accept}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}}{\begin{array}{c}\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\mathrm{ID}}, \mathsf{accept}_{\tau}^{\mathrm{ID}}, g(\phi_{\tau_2}) \\ \sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}, \mathsf{accept}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}, g(\phi_{\underline{\tau_2}})\end{array}}\;\mathsf{Simp}}{\Phi}\;\mathsf{Simp}$$

Part 1 We now focus on $\mathsf{accept}_{\tau}^{\mathrm{ID}}$. Let:

$$T = \{\tau_1 \mid \tau_1 = \_, \mathrm{PN}(j_1, 1) \wedge \tau_2 \prec_\tau \tau_1 \prec \tau\}$$

Using **(Equ2)** we know that:

$$\mathsf{accept}_{\tau}^{\mathrm{ID}} \;\leftrightarrow\; \bigvee_{\tau_1 = \_, \mathrm{PN}(j_1,1) \in T} \begin{pmatrix} g(\phi_{\tau}^{\mathsf{in}}) = \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\mathrm{ID}}}(\langle \mathsf{n}^{j_1}, \mathsf{suc}(\sigma_{\tau_2}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}))\rangle) \;\wedge\; g(\phi_{\tau_2}^{\mathsf{in}}) = \mathsf{n}^{j_1} \\ \wedge\; \pi_1(g(\phi_{\tau_1}^{\mathsf{in}})) = \{\langle \mathrm{ID}, \sigma_{\tau_2}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}} \end{pmatrix}$$

Using again **(Equ2)** on $\underline{\tau}$ (which is a valid action trace) we also have:

$$\mathsf{accept}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})} \;\leftrightarrow\; \bigvee_{\tau_1 = \_, \mathrm{PN}(j_1,1) \in T} \begin{pmatrix} g(\phi_{\underline{\tau}}^{\mathsf{in}}) = \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\nu_\tau(\mathrm{ID})}}(\langle \mathsf{n}^{j_1}, \mathsf{suc}(\sigma_{\underline{\tau_2}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}))\rangle) \;\wedge\; g(\phi_{\underline{\tau_2}}^{\mathsf{in}}) = \mathsf{n}^{j_1} \\ \wedge\; \pi_1(g(\phi_{\underline{\tau_1}}^{\mathsf{in}})) = \{\langle \mathrm{ID}^{\nu_\tau(\mathrm{ID})}, \sigma_{\underline{\tau_2}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}} \end{pmatrix}$$

It is straightforward to check that the formulas above can be decomposed using FA into matching elements of $\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}$. Indeed, for every $\tau_1 = \_, \mathrm{PN}(j_1, 1) \in T$, since $\tau_2 \prec_\tau \tau_1$ and $\tau_2 \not\prec_\tau \mathrm{NS}_{\mathrm{ID}}(\_)$:

$$\left(\mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\mathrm{ID}}}(\langle \mathsf{n}^{j_1}, \mathsf{suc}(\sigma_{\tau_2}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}))\rangle), \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\nu_\tau(\mathrm{ID})}}(\langle \mathsf{n}^{j_1}, \mathsf{suc}(\sigma_{\underline{\tau_2}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}))\rangle)\right) \in \mathsf{reveal}_{\tau_0}$$

$$\left(\mathsf{n}^{j_1}, \mathsf{n}^{j_1}\right) \in \mathsf{reveal}_{\tau_0} \qquad \left(\{\langle \mathrm{ID}, \sigma_{\tau_2}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}}, \{\langle \mathrm{ID}^{\nu_\tau(\mathrm{ID})}, \sigma_{\underline{\tau_2}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}}\right) \in \mathsf{reveal}_{\tau_0}$$

Hence:

$$\dfrac{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{accept}_{\tau}^{\mathrm{ID}} \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{accept}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}} \tag{70}$$

Part 2 We focus on $\mathsf{sync\text{-}diff}_{\tau}^{\mathrm{ID}}$. First we get rid of the case where $\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})$ is true. Indeed, we have:

$$[\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})]\mathsf{sync\text{-}diff}_{\tau}^{\mathrm{ID}} \;=\; [\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})]\mathsf{suc}(\mathsf{sync\text{-}diff}_{\tau_0}^{\mathrm{ID}})$$

$$[\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})]\mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})} \;=\; [\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})]\mathsf{suc}(\mathsf{sync\text{-}diff}_{\underline{\tau_0}}^{\nu_\tau(\mathrm{ID})})$$

And:

$$\left(\mathsf{sync\text{-}diff}_{\tau_0}^{\mathrm{ID}}, \mathsf{sync\text{-}diff}_{\underline{\tau_0}}^{\nu_\tau(\mathrm{ID})}\right) \in \mathsf{reveal}_{\tau_0} \qquad \left(\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}), \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})\right) \in \mathsf{reveal}_{\tau_0}$$

Therefore:

$$\frac{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, [\neg\sigma^{\text{in}}_{\tau}(\text{sync}^{\mathrm{ID}}_{\mathrm{U}})]\text{sync-diff}^{\mathrm{ID}}_{\tau} \;\sim\; \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, [\neg\sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})]\text{sync-diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{sync-diff}^{\mathrm{ID}}_{\tau} \;\sim\; \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{sync-diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}}\ \text{Simp}$$

Similarly:

$$[\neg\sigma^{\text{in}}_{\tau}(\text{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \neg\text{accept}^{\mathrm{ID}}_{\tau}]\text{sync-diff}^{\mathrm{ID}}_{\tau} \;=\; \text{error}$$

$$[\neg\sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}) \wedge \neg\text{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}]\text{sync-diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}} \;=\; \text{error}$$

Hence we can go one step further:

$$\frac{\begin{array}{c}\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{accept}^{\mathrm{ID}}_{\tau}, \quad [\neg\sigma^{\text{in}}_{\tau}(\text{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \text{accept}^{\mathrm{ID}}_{\tau}]\text{sync-diff}^{\mathrm{ID}}_{\tau} \\ \sim\; \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}, [\neg\sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}) \wedge \text{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}]\text{sync-diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}\end{array}}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{accept}^{\mathrm{ID}}_{\tau}, \text{sync-diff}^{\mathrm{ID}}_{\tau} \;\sim\; \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}, \text{sync-diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}}\ \text{Simp} \tag{71}$$

Part 3 Using **(StrEqu4)** twice, we know that for every $\tau_1 \in T$:

$$\neg\sigma^{\text{in}}_{\tau}(\text{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \text{accept}^{\mathrm{ID}}_{\tau} \;\rightarrow\; \text{sync-diff}^{\mathrm{ID}}_{\tau} = 0$$

$$\neg\sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}) \wedge \text{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}} \;\rightarrow\; \text{sync-diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}} = 0$$

Therefore we can extend the derivation in (71):

$$\frac{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{accept}^{\mathrm{ID}}_{\tau} \;\sim\; \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{accept}^{\mathrm{ID}}_{\tau}, \text{sync-diff}^{\mathrm{ID}}_{\tau} \;\sim\; \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}},\; \text{sync-diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}}\ \text{Simp}$$

We conclude using the derivation in (70) and the induction hypothesis.

G.6 Case ai $= \mathrm{FN}(j)$

We know that ai $= \mathrm{FN}(j)$. Here l-reveal_{τ} and l-reveal_{τ_0} coincides everywhere except on the pairs:

$$\begin{array}{rcl} \mathrm{GUTI}^{j} & \sim & \mathrm{GUTI}^{j} \\ [\text{net-e-auth}_{\tau}(\mathrm{ID}, j)]\big(\text{t-suci-}\oplus_{\tau}(\mathrm{ID}, j)\big) & \sim & [\underline{\text{net-e-auth}}_{\underline{\tau}}(\mathrm{ID}, j)]\big(\underline{\text{t-suci-}\oplus}_{\underline{\tau}}(\mathrm{ID}, j)\big) \\ [\text{net-e-auth}_{\tau}(\mathrm{ID}, j)]\big(\text{t-mac}_{\tau}(\mathrm{ID}, j)\big) & \sim & [\underline{\text{net-e-auth}}_{\underline{\tau}}(\mathrm{ID}, j)]\big(\underline{\text{t-mac}}_{\underline{\tau}}(\mathrm{ID}, j)\big) \end{array}$$

for every identity $\mathrm{ID} \in \mathcal{S}_{\text{id}}$.

Part 1 Let $\mathrm{ID} \in \mathcal{S}_{\text{id}}$. Using Lemma 7, we know that:

$$\sigma_\tau(\text{e-auth}^{j}_{\mathrm{N}}) = \mathrm{ID} \;\rightarrow\; \bigvee_{\tau' \preceq \tau} \sigma_{\tau'}(\text{b-auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^{j}$$

We check that:

$$t_\tau \;=\; \begin{array}{l} \text{if net-e-auth}_{\tau}(\mathrm{A}_1, j) \text{ then} \\ \quad \langle \text{t-suci-}\oplus_{\tau}(\mathrm{A}_1, j)\,,\, \text{t-mac}_{\tau}(\mathrm{A}_1, j)\rangle \\ \text{else if net-e-auth}_{\tau}(\mathrm{A}_2, j) \text{ then} \\ \quad \langle \text{t-suci-}\oplus_{\tau}(\mathrm{A}_2, j)\,,\, \text{t-mac}_{\tau}(\mathrm{A}_2, j)\rangle \\ \qquad \ldots \\ \text{else UnknownId} \end{array} \qquad t_{\underline{\tau}} \;=\; \begin{array}{l} \text{if } \underline{\text{net-e-auth}}_{\underline{\tau}}(\mathrm{A}_1, j) \text{ then} \\ \quad \langle \underline{\text{t-suci-}\oplus}_{\underline{\tau}}(\mathrm{A}_1, j)\,,\, \underline{\text{t-mac}}_{\underline{\tau}}(\mathrm{A}_1, j)\rangle \\ \text{else if } \underline{\text{net-e-auth}}_{\underline{\tau}}(\mathrm{A}_2, j) \text{ then} \\ \quad \langle \underline{\text{t-suci-}\oplus}_{\underline{\tau}}(\mathrm{A}_2, j)\,,\, \underline{\text{t-mac}}_{\underline{\tau}}(\mathrm{A}_2, j)\rangle \\ \qquad \ldots \\ \text{else UnknownId} \end{array}$$

Using the FA axiom, we split t_τ and $t_{\underline{\tau}}$ as follows:

$$\frac{\begin{array}{c}\Big(\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j),\ [\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j)]\mathsf{t\text{-}suci\text{-}}{\oplus}_\tau(\mathsf{A}_i, j),\ [\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j)]\mathsf{t\text{-}mac}_\tau(\mathsf{A}_i, j)\Big)_{i \leq B} \\ \sim \Big(\underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\mathsf{A}_i, j),\ [\underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}}{\oplus}}_{\underline{\tau}}(\mathsf{A}_i, j),\ [\underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}}_{\underline{\tau}}(\mathsf{A}_i, j)\Big)_{i \leq B}\end{array}}{t_\tau \sim t_{\underline{\tau}}}\ \mathsf{FA}^*$$

Since:

$$\Big(\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j), \underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\mathsf{A}_i, j)\Big) \in \mathsf{reveal}_{\tau_0}$$

We just need to prove that there is a derivation of:

$$\begin{array}{l}\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0},\ \Big([\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j)]\mathsf{t\text{-}suci\text{-}}{\oplus}_\tau(\mathsf{A}_i, j),\ [\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j)]\mathsf{t\text{-}mac}_\tau(\mathsf{A}_i, j)\Big)_{i \leq B} \\ \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \Big([\underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}}{\oplus}}_{\underline{\tau}}(\mathsf{A}_i, j),\ [\underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}}_{\underline{\tau}}(\mathsf{A}_i, j)\Big)_{i \leq B}\end{array}$$

Assume that we have a proof of

$$\begin{array}{l}\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0},\ \Big([\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j)]\mathsf{t\text{-}suci\text{-}}{\oplus}_\tau(\mathsf{A}_i, j),\ [\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j)]\mathsf{t\text{-}mac}_\tau(\mathsf{A}_i, j)\Big)_{i \leq B} \\ \sim \phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0},\ \Big(\mathsf{n}_{i,j},\ \mathsf{n}'_{i,j}\Big)_{i \leq B}\end{array} \tag{72}$$

And:

$$\begin{array}{l}\phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \Big(\mathsf{n}_{i,j},\ \mathsf{n}'_{i,j}\Big)_{i \leq B} \\ \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \Big([\underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}}{\oplus}}_{\underline{\tau}}(\mathsf{A}_i, j),\ [\underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}}_{\underline{\tau}}(\mathsf{A}_i, j)\Big)_{i \leq B}\end{array} \tag{73}$$

Where for all $\{\mathsf{n}_{i,j}, \mathsf{n}'_{i,j} \mid 1 \leq i \leq B\}$ are fresh distinct nonces. Since:

$$\frac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0},\ \Big(\mathsf{n}_{i,j},\ \mathsf{n}'_{i,j}\Big)_{i \leq B} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \Big(\mathsf{n}_{i,j},\ \mathsf{n}'_{i,j}\Big)_{i \leq B}}\ \mathsf{Fresh}$$

We can conclude using the transitivity axiom Trans and the induction hypothesis.

Part 2 It only remains to give derivations of the formulas in (72) and (73). We only give the proof for Eq. (73) (the derivation of (72) is similar).

Instead of doing the proof simultaneously for all i in $\{1, \ldots, B\}$, we give the proof for a single i. We let the reader check that the syntactic side-conditions necessary for the derivations for i and i', with $i \neq i'$, are compatible. Therefore the derivations can be sequentially composed, which yield the full proof.

Let $1 \leq i \leq B$. By transitivity, we only have to show that:

$$\phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ \mathsf{n}'_{i,j} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ [\underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}}_{\underline{\tau}}(\mathsf{A}_i, j) \tag{74}$$

And:

$$\begin{array}{l}\phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ [\underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}}_{\underline{\tau}}(\mathsf{A}_i, j) \\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ [\underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}}{\oplus}}_{\underline{\tau}}(\mathsf{A}_i, j),\ [\underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}}_{\underline{\tau}}(\mathsf{A}_i, j)\end{array} \tag{75}$$

Derivation of (75) Let $\{\underline{\mathrm{ID}}_1, \dots, \underline{\mathrm{ID}}_l\} = \text{copies-id}_C(\mathrm{ID}_i)$. We define, for every $0 \leq y \leq l$, the partially randomized terms $\underline{\text{t-suci-}\oplus}^{y}_{\underline{\tau}}(\mathrm{ID}_i, j)$:

$$\begin{aligned}
\underline{\text{t-suci-}\oplus}^{y}_{\underline{\tau}}(\mathrm{ID}_i, j) \quad \equiv \quad & \text{if } \mathrm{eq}(\sigma_{\underline{\tau}}(\text{e-auth}^{j}_{\mathrm{N}}), \underline{\mathrm{ID}}_1) \text{ then } \mathsf{n}^{1}_{i,j} \\
& \qquad \cdots \\
& \text{else if } \mathrm{eq}(\sigma_{\underline{\tau}}(\text{e-auth}^{j}_{\mathrm{N}}), \underline{\mathrm{ID}}_{y-1}) \text{ then } \mathsf{n}^{y-1}_{i,j} \\
& \text{else if } \mathrm{eq}(\sigma_{\underline{\tau}}(\text{e-auth}^{j}_{\mathrm{N}}), \underline{\mathrm{ID}}_{y}) \text{ then } \mathrm{GUTI}^{j} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(\mathsf{n}^{j}) \\
& \qquad \cdots \\
& \text{else } \mathrm{GUTI}^{j} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\mathrm{ID}}_l}}(\mathsf{n}^{j})
\end{aligned}$$

Remark that:

$$[\underline{\text{net-e-auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\text{t-suci-}\oplus}^{0}_{\underline{\tau}}(\mathrm{ID}_i, j) \quad = \quad [\underline{\text{net-e-auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\text{t-suci-}\oplus}_{\underline{\tau}}(\mathsf{A}_i, j)$$

And that:

$$\frac{}{\begin{array}{l}\phi^{\mathsf{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0},\ \mathsf{n}_{i,j}, \qquad\qquad\qquad\qquad\qquad\qquad [\underline{\text{net-e-auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\text{t-mac}}_{\underline{\tau}}(\mathsf{A}_i, j) \\ \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0},\ [\underline{\text{net-e-auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\text{t-suci-}\oplus}^{l}_{\underline{\tau}}(\mathrm{ID}_i, j),\ [\underline{\text{net-e-auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\text{t-mac}}_{\underline{\tau}}(\mathsf{A}_i, j)\end{array}}\ \text{indep-branch}$$

Hence by transitivity, to prove that there exists a derivation of Formula (75) it is sufficient to prove that, for every $0 < y \leq l$, that we have a derivation of $\phi_{y-1} \sim \phi_y$, where:

$$\begin{aligned}
\phi_{y-1} \quad &\equiv \quad \phi^{\mathsf{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0},\ [\underline{\text{net-e-auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\text{t-suci-}\oplus}^{y-1}_{\underline{\tau}}(\mathrm{ID}_i, j),\ [\underline{\text{net-e-auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\text{t-mac}}_{\underline{\tau}}(\mathsf{A}_i, j) \\
\phi_{y} \quad &\equiv \quad \phi^{\mathsf{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0},\ [\underline{\text{net-e-auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\text{t-suci-}\oplus}^{y}_{\underline{\tau}}(\mathrm{ID}_i, j),\ [\underline{\text{net-e-auth}}_{\underline{\tau}}(\mathsf{A}_i, j)]\underline{\text{t-mac}}_{\underline{\tau}}(\mathsf{A}_i, j)
\end{aligned}$$

Let $1 \leq y \leq B$, we are going to give a derivation of $\phi_{y-1} \sim \phi_y$. This is done in two times:

- First, we are going to use the PRF-f^{r} axiom applied to f^{r}, with key $\mathsf{k}^{\underline{\mathrm{ID}}_y}$, to replace $\mathrm{GUTI}^{j} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(\mathsf{n}^{j})$ with $\mathrm{GUTI}^{j} \oplus \mathsf{n}''^{y}_{i,j}$ (where $\mathsf{n}''^{y}_{i,j}$ is a fresh nonce).
  Observe that there is only one occurrence of $\mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(\mathsf{n}^{j})$ in ϕ_{y-1} (and none in ϕ_y). Moreover:

  $$\begin{aligned}
  \text{set-prf}^{\mathsf{f}^{\mathsf{r}}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}\left(\phi_{y-1}, \phi_y\right) \backslash \{\mathsf{n}^{j}\} \quad = \quad & \left\{\sigma^{\mathsf{in}}_{\tau_1}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) \mid \tau_1 = \_, \mathrm{FU}_{\underline{\mathrm{ID}}_y}(p) \prec \tau\right\} \\
  & \cup \ \{\mathsf{n}^{p} \mid \tau_1 = \_, \mathrm{FN}(p) \prec \tau\}
  \end{aligned}$$

  Let $\tau_1 = \_, \mathrm{FN}(p) \prec \tau$. We know that $p \neq j$, and therefore that $\neg(\mathsf{n}^{p} = \mathsf{n}^{j})$.We still need guards for $\sigma^{\mathsf{in}}_{\tau_1}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^{j}$, for every $\tau_1 = \_, \mathrm{FU}_{\underline{\mathrm{ID}}_y}(p) \prec \tau$. The problem is that we do not have $(\sigma^{\mathsf{in}}_{\tau_1}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^{j}) = \text{false}$. We solve this problem by rewriting ϕ_{y-1} (resp. ϕ_y) into the vector of terms ϕ'_{y-1} (resp. ϕ'_y) obtained by replacing any occurrence of $\text{accept}^{\underline{\mathrm{ID}}_y}_{\tau_1}$ by:

  $$\bigvee_{\substack{\tau_0 = \_\mathrm{FN}(j_0) \prec \tau_1 \\ \tau_0 \not\prec \tau_1\, \mathrm{NS}_{\underline{\mathrm{ID}}_y}(\_)}} \begin{pmatrix} \text{inj-auth}_{\tau_1}(\underline{\mathrm{ID}}_y, j_0) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\text{e-auth}^{j_0}_{\mathrm{N}}) \neq \text{UnknownId} \\ \wedge\ \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \mathrm{GUTI}^{j_0} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(\mathsf{n}^{j_0}) \wedge\ \pi_2(g(\phi^{\mathsf{in}}_{\tau_1})) = \mathrm{Mac}^{5}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}_{\mathsf{m}}}(\langle \mathrm{GUTI}^{j_0}, \mathsf{n}^{j_0}\rangle) \end{pmatrix} \tag{76}$$

  Which is sound using **(Equ1)**. We then have:

  $$\text{set-prf}^{\mathsf{f}^{\mathsf{r}}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(\phi') \quad = \quad \{\mathsf{n}^{p} \mid \tau_1 = \_, \mathrm{FN}(p) \prec \tau\}$$

  Therefore we can apply the PRF-f^{r} axioms as wanted: first we replace ϕ_{y-1} and ϕ_y by ϕ'_{y-1} and ϕ'_y using rule R; then we apply the PRF-f^{r} axiom; and finally we rewrite any term of the form (76) back into $\text{accept}^{\underline{\mathrm{ID}}_y}_{\tau_1}$.

- Then, we use the $\oplus$-ind axiom to replace $\textsc{guti}^j \oplus \mathsf{n}''^{y}_{i,j}$ with $\mathsf{n}^y_{i,j}$.

Derivation of (74) We use the same proof technique. We define, for every $0 \leq y \leq l$, the partially randomized terms $\underline{\text{t-mac}^y_{\underline{\tau}}}(\textsc{id}_i, j)$:

$$\begin{aligned}
\underline{\text{t-mac}^y_{\underline{\tau}}}(\textsc{id}_i, j) \;\; \equiv \;\; & \text{if } \mathsf{eq}(\sigma_{\underline{\tau}}(\text{e-auth}^j_{\textsc{n}}), \underline{\textsc{id}}_1) \text{ then } \mathsf{n}'^{1}_{i,j} \\
& \quad \ldots \\
& \text{else if } \mathsf{eq}(\sigma_{\underline{\tau}}(\text{e-auth}^j_{\textsc{n}}), \underline{\textsc{id}}_{y-1}) \text{ then } \mathsf{n}'^{y-1}_{i,j} \\
& \text{else if } \mathsf{eq}(\sigma_{\underline{\tau}}(\text{e-auth}^j_{\textsc{n}}), \underline{\textsc{id}}_y) \text{ then } \mathsf{Mac}^5_{\mathsf{k}_{\mathsf{m}}^{\underline{\textsc{id}}_y}}(\langle \textsc{guti}^j \,,\, \mathsf{n}^j \rangle) \\
& \quad \ldots \\
& \text{else } \mathsf{Mac}^5_{\mathsf{k}_{\mathsf{m}}^{\underline{\textsc{id}}_l}}(\langle \textsc{guti}^j \,,\, \mathsf{n}^j \rangle)
\end{aligned}$$

Remark that:

$$[\underline{\text{net-e-auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\text{t-mac}^0_{\underline{\tau}}}(\textsc{id}_i, j) \;\; = \;\; [\underline{\text{net-e-auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\text{t-mac}_{\underline{\tau}}}(\mathsf{A}_i, j)$$

And that:

$$\frac{}{\phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0},\ \mathsf{n}_{i,j}, \mathsf{n}'_{i,j} \;\sim\; \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ [\underline{\text{net-e-auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\text{t-mac}^l_{\underline{\tau}}}(\mathsf{A}_i, j)}\ \text{indep-branch}$$

Hence by transitivity, to prove that there exists a derivation of Formula (74) it is sufficient to prove that, for every $0 < y \leq l$, that we have a derivation of $\psi_{y-1} \sim \psi_y$, where:

$$\begin{aligned}
\psi_{y-1} \;\; &\equiv \;\; \psi_{\underline{\tau_0}}, \text{r-reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ [\underline{\text{net-e-auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\text{t-mac}^{y-1}_{\underline{\tau}}}(\textsc{id}_i, j) \\
\psi_y \;\; &\equiv \;\; \psi_{\underline{\tau_0}}, \text{r-reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ [\underline{\text{net-e-auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\text{t-mac}^{y}_{\underline{\tau}}}(\textsc{id}_i, j)
\end{aligned}$$

Let $1 \leq y \leq B$, we are going to give a derivation of $\psi_{y-1} \sim \psi_y$. For this, we are going to use the $\textsc{prf-mac}^5$ axiom with key $\mathsf{k}_{\mathsf{m}}^{\underline{\textsc{id}}_y}$, to replace $\mathsf{Mac}^5_{\mathsf{k}_{\mathsf{m}}^{\underline{\textsc{id}}_y}}(\langle \textsc{guti}^j \,,\, \mathsf{n}^j \rangle)$ with a fresh nonce $\tilde{\mathsf{n}}^y_{i,j}$. Observe that there is only one occurrence of $\mathsf{Mac}^5_{\mathsf{k}_{\mathsf{m}}^{\underline{\textsc{id}}_y}}(\langle \textsc{guti}^j \,,\, \mathsf{n}^j \rangle)$ in ψ_{y-1} (and none in ψ_y). Moreover:

$$\begin{aligned}
\text{set-mac}^5_{\mathsf{k}^{\underline{\textsc{id}}_y}} \left(\psi_{y-1}, \psi_y\right) \setminus \left\{\langle \textsc{guti}^j \,,\, \mathsf{n}^j \rangle\right\} \;\; = & \\
& \{\langle \textsc{guti}^p \,,\, \mathsf{n}^p \rangle \mid \tau_1 = \_, \textsc{fn}(p) \prec \tau\} \\
& \cup \left\{\langle \pi_1(g(\phi^{\text{in}}_{\tau_1})) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\sigma^{\text{in}}_{\tau_1}(\text{e-auth}^{\mathsf{k}^{\underline{\textsc{id}}_y}}_{\textsc{u}})) \,,\, \sigma^{\text{in}}_{\tau_1}(\text{e-auth}^{\mathsf{k}^{\underline{\textsc{id}}_y}}_{\textsc{u}}) \rangle \mid \tau_1 = \_, \textsc{fn}(p) \prec \tau\right\}
\end{aligned}$$

Let $\tau_1 = \_, \textsc{fn}(p) \prec \tau$. Since $\textsc{guti}^j$ is a fresh nonce, using =-ind and the injectivity of the pair:

$$\neg\left(\langle \textsc{guti}^j \,,\, \mathsf{n}^j \rangle = \langle \textsc{guti}^p \,,\, \mathsf{n}^p \rangle\right)$$

$$\neg\left(\langle \textsc{guti}^j \,,\, \mathsf{n}^j \rangle = \langle \pi_1(g(\phi^{\text{in}}_{\tau_1})) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\sigma^{\text{in}}_{\tau_1}(\text{e-auth}^{\mathsf{k}^{\underline{\textsc{id}}_y}}_{\textsc{u}})) \,,\, \sigma^{\text{in}}_{\tau_1}(\text{e-auth}^{\mathsf{k}^{\underline{\textsc{id}}_y}}_{\textsc{u}}) \rangle\right)$$

Therefore we can directly apply the $\textsc{prf-mac}^5$ axiom, which concludes this case.

G.7 Case ai = $\textsc{fu}_{\textsc{id}}(j)$

We know that $\underline{\text{ai}} = \textsc{fu}_{\nu_\tau(\textsc{id})}(j)$. Here l-reveal$_\tau$ and l-reveal$_{\tau_0}$ coincides everywhere except on the pairs:

$$\sigma_\tau(\text{valid-guti}_{\text{U}}^{\textsc{id}}) \sim \sigma_{\underline{\tau}}(\text{valid-guti}_{\text{U}}^{\nu_\tau(\textsc{id})})$$

$$\underbrace{\begin{array}{r}\text{if } \sigma_\tau(\text{valid-guti}_{\text{U}}^{\textsc{id}}) \text{ then } \sigma_\tau(\textsc{guti}_{\text{U}}^{\textsc{id}})\\ \text{else defaut}\end{array}}_{\text{m-suci}_{\tau}^{\textsc{id}}} \sim \underbrace{\begin{array}{r}\text{if } \sigma_{\underline{\tau}}(\text{valid-guti}_{\text{U}}^{\nu_\tau(\textsc{id})}) \text{ then } \sigma_{\underline{\tau}}(\textsc{guti}_{\text{U}}^{\nu_\tau(\textsc{id})})\\ \text{else defaut}\end{array}}_{\text{m-suci}_{\underline{\tau}}^{\nu_\tau(\textsc{id})}}$$

Moreover, we need to show that $\text{accept}_\tau^{\textsc{id}} \sim \text{accept}_{\underline{\tau}}^{\nu_\tau(\textsc{id})}$.First, using FA and Dup, we check that it is sufficient to give a derivation of:

$$\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \text{accept}_\tau^{\textsc{id}}, \text{m-suci}_{\tau}^{\textsc{id}} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \text{accept}_{\underline{\tau}}^{\nu_\tau(\textsc{id})}, \text{m-suci}_{\underline{\tau}}^{\nu_\tau(\textsc{id})} \tag{77}$$

Using **(Equ1)** twice:

$$\text{accept}_\tau^{\textsc{id}} \leftrightarrow \bigvee_{\substack{\tau_1 = \_,\textsc{fn}(j_0) \prec \tau \\ \tau_1 \not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)}} \text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_1} \qquad \text{accept}_{\underline{\tau}}^{\nu_\tau(\textsc{id})} \leftrightarrow \bigvee_{\substack{\tau_1 = \_,\textsc{fn}(j_0) \prec \tau \\ \tau_1 \not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)}} \text{fu-tr}_{\text{u}:\underline{\tau}}^{\text{n}:\underline{\tau_1}}$$

Let:

$$\{j_0, \dots, j_l\} = \{i \mid \tau' = \_, \textsc{fn}(i) \prec \tau \land \tau' \not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)\}$$

We check that:

$$\{j_0, \dots, j_l\} = \{i \mid \tau' = \_, \textsc{fn}(i) \prec \underline{\tau} \land \tau' \not\prec_{\underline{\tau}} \textsc{ns}_{\nu_\tau(\textsc{id})}(\_)\}$$

For all $0 \leq i \leq l$, let τ_{j_i} be such that $\tau_{j_i} = \_, \textsc{fn}(j_i) \prec \tau$. One can check that:

$$\begin{aligned}\text{m-suci}_{\tau}^{\textsc{id}} = {} & \text{if fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_{j_0}} \text{ then } \textsc{guti}^{j_0}\\ & \text{else if fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_{j_1}} \text{ then } \textsc{guti}^{j_1}\\ & \dots\\ & \text{else } \textsc{guti}^{j_l}\end{aligned} \qquad \begin{aligned}\text{m-suci}_{\underline{\tau}}^{\nu_\tau(\textsc{id})} = {} & \text{if fu-tr}_{\text{u}:\underline{\tau}}^{\text{n}:\underline{\tau_{j_0}}} \text{ then } \textsc{guti}^{j_0}\\ & \text{else if fu-tr}_{\text{u}:\underline{\tau}}^{\text{n}:\underline{\tau_{j_1}}} \text{ then } \textsc{guti}^{j_1}\\ & \dots\\ & \text{else } \textsc{guti}^{j_l}\end{aligned}$$

We can now start giving a derivation of (77):

$$\dfrac{\dfrac{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \left(\text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_{j_i}}\right)_{i \leq l} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \left(\text{fu-tr}_{\text{u}:\underline{\tau}}^{\text{n}:\underline{\tau_{j_i}}}\right)_{i \leq l}}{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \left(\text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_{j_i}}\right)_{i \leq l}, \left(\textsc{guti}^{j_i}\right)_{i \leq l} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \left(\text{fu-tr}_{\text{u}:\underline{\tau}}^{\text{n}:\underline{\tau_{j_i}}}\right)_{i \leq l}, \left(\textsc{guti}^{j_i}\right)_{i \leq l}}\ \text{Dup}^*}{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \text{accept}_\tau^{\textsc{id}}, \text{m-suci}_{\tau}^{\textsc{id}} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \text{accept}_{\underline{\tau}}^{\nu_\tau(\textsc{id})}, \text{m-suci}_{\underline{\tau}}^{\nu_\tau(\textsc{id})}}\ \text{FA}^*$$

Since for all $1 \leq i \leq l$, $(\textsc{guti}^{j_i} \sim \textsc{guti}^{j_i}) \in \text{reveal}_{\tau_0}$. We conclude using **(Der2)** for every $0 \leq i \leq l$:

$$\dfrac{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}}{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \left(\text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_{j_i}}\right)_{i \leq l} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \left(\text{fu-tr}_{\text{u}:\underline{\tau}}^{\text{n}:\underline{\tau_{j_i}}}\right)_{i \leq l}}\ \text{FA}^*$$

G.8 Case ai = $\textsc{tu}_{\textsc{id}}(j, 0)$

Let $\underline{\textsc{id}} = \nu_\tau(\textsc{id})$, we know that $\underline{\text{ai}} = \textsc{tu}_{\underline{\textsc{id}}}(j, 0)$. l-reveal$_\tau$ and l-reveal$_{\tau_0}$ coincides everywhere except on:

$$\sigma_\tau(\text{valid-guti}_{\text{U}}^{\textsc{id}}) \sim \sigma_{\underline{\tau}}(\text{valid-guti}_{\text{U}}^{\underline{\textsc{id}}}) \qquad \sigma_\tau(\text{s-valid-guti}_{\text{U}}^{\textsc{id}}) \sim \sigma_{\underline{\tau}}(\text{s-valid-guti}_{\text{U}}^{\underline{\textsc{id}}})$$

$$\text{m-suci}_{\tau}^{\textsc{id}} \sim \text{m-suci}_{\underline{\tau}}^{\underline{\textsc{id}}}$$

Handling these is simple since:

$$\sigma_\tau(\text{valid-guti}_{\text{U}}^{\text{ID}}) \equiv \text{false} \qquad \sigma_{\underline{\tau}}(\text{valid-guti}_{\text{U}}^{\underline{\text{ID}}}) \equiv \text{false} \qquad \sigma_\tau(\text{s-valid-guti}_{\text{U}}^{\text{ID}}) \equiv \sigma_\tau^{\text{in}}(\text{valid-guti}_{\text{U}}^{\text{ID}})$$

$$\sigma_{\underline{\tau}}(\text{s-valid-guti}_{\text{U}}^{\underline{\text{ID}}}) \equiv \sigma_{\underline{\tau}}^{\text{in}}(\text{valid-guti}_{\text{U}}^{\underline{\text{ID}}}) \qquad \text{m-suci}_{\,\tau}^{\,\text{ID}} = \text{defaut} \qquad \text{m-suci}_{\,\underline{\tau}}^{\,\underline{\text{ID}}} = \text{defaut}$$

Observe that:

$$t_\tau = \text{if } \sigma_\tau^{\text{in}}(\text{valid-guti}_{\text{U}}^{\text{ID}}) \text{ then m-suci}_{\,\tau_0}^{\,\text{ID}} \text{ else NoGuti}$$

$$t_{\underline{\tau}} = \text{if } \sigma_{\underline{\tau}}^{\text{in}}(\text{valid-guti}_{\text{U}}^{\underline{\text{ID}}}) \text{ then m-suci}_{\,\underline{\tau_0}}^{\,\underline{\text{ID}}} \text{ else NoGuti}$$

Since $(\sigma_\tau^{\text{in}}(\text{valid-guti}_{\text{U}}^{\text{ID}}), \sigma_{\underline{\tau}}^{\text{in}}(\text{valid-guti}_{\text{U}}^{\underline{\text{ID}}})) \in \text{reveal}_{\tau_0}$ and $(\text{m-suci}_{\,\tau_0}^{\,\text{ID}} \sim \text{m-suci}_{\,\underline{\tau_0}}^{\,\underline{\text{ID}}}) \in \text{reveal}_{\tau_0}$, we conclude:

$$\dfrac{\dfrac{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0} \;\sim\; \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}}{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \sigma_\tau^{\text{in}}(\text{valid-guti}_{\text{U}}^{\text{ID}}), \text{m-suci}_{\,\tau}^{\,\text{ID}}, \text{NoGuti} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \sigma_{\underline{\tau}}^{\text{in}}(\text{valid-guti}_{\text{U}}^{\underline{\text{ID}}}), \text{m-suci}_{\,\underline{\tau}}^{\,\underline{\text{ID}}}, \text{NoGuti}}\,\text{Dup}^*}{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, t_\tau \;\sim\; \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, t_{\underline{\tau}}}\,\text{Simp}$$

G.9 Case ai = $\textsc{tn}(j, 0)$

We know that $\underline{\text{ai}} = \textsc{tn}(j, 0)$. Using **(A6)**, we know that for every $\textsc{id} \neq \textsc{id}'$, $\neg\text{accept}_\tau^{\text{ID}} \leftrightarrow \neg\text{accept}_\tau^{\text{ID}'}$. Therefore the answer from the network does not depend on the order in which we make the $\text{accept}_\tau^{\text{ID}}$ tests. Formally, the following list of conditionals is a CS partition:

$$\left((\text{accept}_\tau^{\text{ID}})_{\textsc{id}\in\mathcal{S}_{\text{id}}}, \bigwedge_{\textsc{id}\in\mathcal{S}_{\text{id}}} \neg\text{accept}_\tau^{\text{ID}} \right)$$

To get a uniform notation, we let $\text{accept}_\tau^{\text{ID}_{\text{dum}}} \equiv \bigwedge_{\textsc{id}\in\mathcal{S}_{\text{id}}} \neg\text{accept}_\tau^{\text{ID}}$, and $\mathcal{S}_{\text{ext-id}} = \mathcal{S}_{\text{id}} \cup \{\textsc{id}_{\text{dum}}\}$. Hence using Proposition 27 we get that:

$$t_\tau \;=\; \underset{\textsc{id}\in\mathcal{S}_{\text{ext-id}}}{\text{case}} (\text{accept}_\tau^{\text{ID}} : \text{msg}_\tau^{\text{ID}})$$

We are now going to show that for every $\textsc{id} \in \mathcal{S}_{\text{ext-id}}$, the term $\text{msg}_\tau^{\text{ID}}$ can be replaced by $\left\langle \text{n}^j, \text{n}_{\text{ID}}^{\oplus}, \text{n}_{\text{ID}}^{\text{Mac}} \right\rangle$ (where $(\text{n}_{\text{ID}}^{\oplus})_{\textsc{id}\in\mathcal{S}_{\text{ext-id}}}$ and $(\text{n}_{\text{ID}}^{\text{Mac}})_{\textsc{id}\in\mathcal{S}_{\text{ext-id}}}$ are fresh distinct nonces). We will then conclude easily using the Fresh axiom.

Let $\textsc{id}_1, \dots, \textsc{id}_l$ be an arbitrary enumeration of $\mathcal{S}_{\text{ext-id}}$. For every $1 \leq n \leq l$, and for every $\textsc{id}_i \in \{\textsc{id}_1, \dots, \textsc{id}_l\}$, we let:

$$\text{rnd-msg}_n^{\text{ID}_i} \equiv \begin{cases} \left\langle \text{n}^j, \text{n}_{\text{ID}_i}^{\oplus}, \text{n}_{\text{ID}_i}^{\text{Mac}} \right\rangle & \text{if } i \leq n \\ \text{rnd-msg}_\tau^{\text{ID}_i} & \text{if } i > n \end{cases}$$

And we let t_n be the term t_τ where the subterms $\text{msg}_\tau^{\text{ID}}$ have been replaced by $\left\langle \text{n}^j, \text{n}_{\text{ID}}^{\oplus}, \text{n}_{\text{ID}}^{\text{Mac}} \right\rangle$ for the first n identities:

$$t_n \equiv \underset{\textsc{id}\in\mathcal{S}_{\text{ext-id}}}{\text{case}} (\text{accept}_\tau^{\text{ID}} : \text{rnd-msg}_n^{\text{ID}})$$

We check that $t_0 \equiv t_\tau$.

Part 1 We now show that for every $1 \leq n \leq l$, we have a derivation of:

$$\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, t_{n-1} \;\sim\; \phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, t_n \tag{78}$$

Let n be in $\{1, \dots, l\}$. Let $\textsc{id} = \textsc{id}_n$, $\mathsf{k} = \mathsf{k}^{\textsc{id}}$ and $\mathsf{k_m} = \mathsf{k}^{\textsc{id}}_{\mathsf{m}}$. We are going to apply $\textsc{prf}$-f axiom with key k to replace $\mathsf{f_k}(\mathsf{n}^j)$ by $\mathsf{n}_{\textsc{id}}$, where $\mathsf{n}_{\textsc{id}}$ is a fresh nonce. Recall that:

$$\mathsf{msg}^{\textsc{id}}_\tau \;\equiv\; \langle \mathsf{n}^j \,, \underbrace{\sigma^{\mathsf{in}}_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})}_{u_{\textsc{sqn}}} \oplus \mathsf{f}_{\mathsf{k}^{\textsc{id}}}(\mathsf{n}^j) \,, \underbrace{\mathsf{Mac}^3_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle \mathsf{n}^j \,, \sigma^{\mathsf{in}}_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \,, \sigma^{\mathsf{in}}_\tau(\textsc{guti}^{\textsc{id}}_{\textsc{n}})\rangle)}_{u_{\mathsf{Mac}}}\rangle$$

We let ψ be the context with one hole (which has only one occurrence) such that:

$$\psi[\left\langle \mathsf{n}^j \,, u_{\textsc{sqn}} \oplus \mathsf{f}_{\mathsf{k}^{\textsc{id}}}(\mathsf{n}^j) \,, u_{\mathsf{Mac}} \right\rangle] \equiv \phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, t_{n-1} \qquad\qquad \psi[\left\langle \mathsf{n}^j \,, \mathsf{n}^{\oplus}_{\textsc{id}} \,, \mathsf{n}^{\mathsf{Mac}}_{\textsc{id}} \right\rangle] \equiv \phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, t_n$$

Let $\psi_0[] \equiv \psi[\left\langle \mathsf{n}^j \,, u_{\textsc{sqn}} \oplus [] \,, u_{\mathsf{Mac}} \right\rangle]$. Notice that:

$$\mathsf{set\text{-}prf}^{\,\mathsf{f}}_{\,\mathsf{k}}\,(\psi_0[]) \;\;=\;\; \left\{ \pi_1(\phi^{\mathsf{in}}_{\tau_1}) \mid \tau_1 = \_, \textsc{tu}_{\textsc{id}}(p, 1) \prec \tau \right\} \;\cup\; \left\{ \mathsf{n}^p \mid \tau_1 = \_, \textsc{tn}(p) \prec \tau \right\}$$

We want to get rid of the sub-terms of the form $\mathsf{f_k}(\pi_1(\phi^{\mathsf{in}}_{\tau_1}))$, for any τ_1 such that $\tau_1 = \_, \textsc{tu}_{\textsc{id}}(p, 1) \prec \tau$. To do this, for every $\tau_1 = \_, \textsc{tu}_{\textsc{id}}(p, 1) \prec \tau$, we let $\tau_3 = \_, \textsc{tu}_{\textsc{id}}(j_p, 0) \prec \tau$, and we apply **(StrEqu2)** to rewrite all occurrence of $\mathsf{accept}^{\textsc{id}}_{\tau_1}$ in ψ_0 using:

$$\mathsf{accept}^{\textsc{id}}_{\tau_1} \leftrightarrow \bigvee_{\substack{\tau_2 = \_, \textsc{tn}(j_1, 0) \\ \tau_3 \prec_{\tau_1} \tau_2 \prec_{\tau_1} \tau_1}} \mathsf{part\text{-}tr}^{\mathsf{n}:\tau_2}_{\mathsf{u}:\tau_3, \tau_1} \tag{79}$$

This yields a vector of terms $\psi_0'[]$ with one hole. It is easy to check that:

$$\mathsf{set\text{-}prf}^{\,\mathsf{f}}_{\,\mathsf{k}}\,(\psi_0'[]) \;\;=\;\; \{ \mathsf{n}^p \mid \tau_1 = \_, \textsc{tn}(p) \prec \tau \}$$

By validity of τ, we know that for every $\tau_1 = \_, \textsc{tn}(p) \prec \tau$, we have $p \neq j$. Therefore using Fresh we have $\neg(\mathsf{n}^j = \mathsf{n}^P)$. It follows that we can apply the $\textsc{prf}$-f axiom in $\psi_0'[\mathsf{f_k}(\mathsf{n}^j)]$, replacing $\mathsf{f_k}(\mathsf{n}^j)$ by $\mathsf{n}_{\textsc{id}}$, which yields $\psi_0'[\mathsf{n}_{\textsc{id}}]$. More precisely, we deconstruct the context ψ_0' using FA, without touching at the mac terms, until we get $\vec{w}, \mathsf{f_k}(\mathsf{n}^j) \sim \vec{w}, \mathsf{n}_{\textsc{id}}$, at which point we can apply the $\textsc{prf}$-f axiom. We then rewrite any term of the form in (79) back into $\mathsf{accept}^{\textsc{id}}_{\tau_1}$, obtaining $\psi_0[\mathsf{n}_{\textsc{id}}] \equiv \psi[\left\langle \mathsf{n}^j \,, u_{\textsc{sqn}} \oplus \mathsf{n}_{\textsc{id}} \,, u_{\mathsf{Mac}} \right\rangle]$. We then use $\oplus$-ind to replace $u_{\textsc{sqn}} \oplus \mathsf{n}_{\textsc{id}}$ by $\mathsf{n}^{\oplus}_{\textsc{id}}$. For this, we use the fact that $\mathsf{len}(u_{\textsc{sqn}}) = \mathsf{len}(\mathsf{n}_{\textsc{id}})$ by Proposition 20.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vec{w}, \mathsf{f_k}(\mathsf{n}^j) \sim \vec{w}, \mathsf{n}_{\textsc{id}}}\ \textsc{prf}\text{-f}}{\vdots}}{\psi_0'[\mathsf{f_k}(\mathsf{n}^j)] \sim \psi_0'[\mathsf{n}_{\textsc{id}}]}\ \mathsf{FA}^* \qquad \dfrac{\dfrac{\psi[\left\langle \mathsf{n}^j \,, \mathsf{n}^{\oplus}_{\textsc{id}} \,, u_{\mathsf{Mac}} \right\rangle] \sim \psi[\left\langle \mathsf{n}^j \,, \mathsf{n}^{\oplus}_{\textsc{id}} \,, \mathsf{n}^{\mathsf{Mac}}_{\textsc{id}} \right\rangle]}{\psi[\left\langle \mathsf{n}^j \,, u_{\textsc{sqn}} \oplus \mathsf{n}_{\textsc{id}} \,, u_{\mathsf{Mac}} \right\rangle] \sim \psi[\left\langle \mathsf{n}^j \,, \mathsf{n}^{\oplus}_{\textsc{id}} \,, \mathsf{n}^{\mathsf{Mac}}_{\textsc{id}} \right\rangle]}\ \oplus\text{-ind}}{\psi_0'[\mathsf{n}_{\textsc{id}}] \sim \psi[\left\langle \mathsf{n}^j \,, \mathsf{n}^{\oplus}_{\textsc{id}} \,, \mathsf{n}^{\mathsf{Mac}}_{\textsc{id}} \right\rangle]}\ R}{\dfrac{\dfrac{\psi_0'[\mathsf{f_k}(\mathsf{n}^j)] \sim \psi[\left\langle \mathsf{n}^j \,, \mathsf{n}^{\oplus}_{\textsc{id}} \,, \mathsf{n}^{\mathsf{Mac}}_{\textsc{id}} \right\rangle]}{\psi[\left\langle \mathsf{n}^j \,, u_{\textsc{sqn}} \oplus \mathsf{f}_{\mathsf{k}^{\textsc{id}}}(\mathsf{n}^j) \,, u_{\mathsf{Mac}} \right\rangle] \sim \psi[\left\langle \mathsf{n}^j \,, \mathsf{n}^{\oplus}_{\textsc{id}} \,, \mathsf{n}^{\mathsf{Mac}}_{\textsc{id}} \right\rangle]}\ R}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, t_{n-1} \;\sim\; \phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, t_n}\ R}\ \mathsf{Trans}$$

We now the same thing with u_{Mac}, applying $\textsc{prf-mac}^3$ axiom to replace u_{Mac} by $\mathsf{n}^{\mathsf{Mac}}_{\textsc{id}}$. The proof is similar to the one we just did for $\textsc{prf}$-f, and we omit the details. We conclude using Refl. This yields:

$$\dfrac{\dfrac{}{\psi[\left\langle \mathsf{n}^j \,, \mathsf{n}^{\oplus}_{\textsc{id}} \,, \mathsf{n}^{\mathsf{Mac}}_{\textsc{id}} \right\rangle] \sim \psi[\left\langle \mathsf{n}^j \,, \mathsf{n}^{\oplus}_{\textsc{id}} \,, \mathsf{n}^{\mathsf{Mac}}_{\textsc{id}} \right\rangle]}\ \mathsf{Refl}}{\dfrac{\vdots}{\psi[\left\langle \mathsf{n}^j \,, \mathsf{n}^{\oplus}_{\textsc{id}} \,, u_{\mathsf{Mac}} \right\rangle] \sim \psi[\left\langle \mathsf{n}^j \,, \mathsf{n}^{\oplus}_{\textsc{id}} \,, \mathsf{n}^{\mathsf{Mac}}_{\textsc{id}} \right\rangle]}}$$

Part 2 Using the fact that $t_0 \equiv t_\tau$ and (78), and using the transitivity axiom, we get:

$$\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, t_\tau \;\sim\; \phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, t_l$$

Moreover, using the indep-branch axiom we know that:

$$\frac{}{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, t_l \;\sim\; \phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n}}\;\text{indep-branch}$$

where n is a fresh nonce. Using transitivity again, we get a derivation of:

$$\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, t_{\tau} \;\sim\; \phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n} \tag{80}$$

Repeating everything we did in **Part 1**, we can show that we have a derivation of:

$$\phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{n}' \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}} \tag{81}$$

where n' is a fresh nonce. We then conclude using the transitivity and Fresh:

$$\frac{\dfrac{(80)}{\begin{array}{c}\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, t_{\tau}\\ \sim \phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n}\end{array}} \qquad \dfrac{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{n}'}\;\text{Fresh} \qquad \dfrac{(81)}{\begin{array}{c}\phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{n}'\\ \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}}\end{array}}}{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, t_{\tau} \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}}}\;\text{Trans}$$

G.10 Case ai = $\textbf{TU}_{\textbf{ID}}(j, 1)$

We know that $\underline{\mathrm{ai}} = \textsc{tu}_{\nu_\tau(\textsc{id})}(j, 1)$. Let $\underline{\textsc{id}} = \nu_\tau(\textsc{id})$. By validity of τ, we know that there exists $\tau_2 = \_, \textsc{tu}_{\textsc{id}}(j, 0)$ such that $\tau_2 \prec \tau$. Here $\mathsf{l\text{-}reveal}_{\tau}$ and $\mathsf{l\text{-}reveal}_{\tau_0}$ coincides everywhere except on:

$$\sigma_\tau(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) - \sigma_\tau^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\textsc{id}}) \;\sim\; \sigma_{\underline{\tau}}(\textsc{sqn}_{\textsc{u}}^{\underline{\textsc{id}}}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\textsc{sqn}_{\textsc{u}}^{\underline{\textsc{id}}}) \qquad\qquad \sigma_\tau(\mathsf{e\text{-}auth}_{\textsc{u}}^{\textsc{id}}) \;\sim\; \sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}_{\textsc{u}}^{\underline{\textsc{id}}})$$

$$\left(\mathsf{Mac}^4_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\mathsf{n}^{j_0}) \;\sim\; \mathsf{Mac}^4_{\mathsf{k}_{\mathsf{m}}^{\underline{\textsc{id}}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \textsc{tn}(j_0, 0)\\ \tau_2 \prec_\tau \tau_1}}$$

First, using **(StrEqu2)** twice we know that:

$$\mathsf{accept}_{\tau}^{\textsc{id}} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{tn}(j_1, 0)\\ \tau_2 \prec_\tau \tau_1}} \mathsf{part\text{-}tr}_{\mathsf{u}:\tau_2, \tau}^{\mathsf{n}:\tau_1} \qquad\qquad \mathsf{accept}_{\underline{\tau}}^{\underline{\textsc{id}}} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \textsc{tn}(j_1, 0)\\ \tau_2 \prec_\tau \tau_1}} \mathsf{part\text{-}tr}_{\mathsf{u}:\underline{\tau_2}, \underline{\tau}}^{\mathsf{n}:\underline{\tau_1}}$$

Using **(Der3)** we know that for every $\tau_1 = \_, \textsc{tn}(j_1, 0)$ such that $\tau_2 \prec_\tau \tau_1$ we have a derivation:

$$\frac{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{part\text{-}tr}_{\mathsf{u}:\tau_2, \tau}^{\mathsf{n}:\tau_1} \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{part\text{-}tr}_{\mathsf{u}:\underline{\tau_2}, \underline{\tau}}^{\mathsf{n}:\underline{\tau_1}}}\;\text{Simp} \tag{82}$$

Therefore we can build the following derivation:

$$\dfrac{\dfrac{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{part\text{-}tr}_{\mathsf{u}:\tau_2, \tau}^{\mathsf{n}:\tau_1}\right)_{\substack{\tau_1 = \_, \textsc{tn}(j_1, 0)\\ \tau_2 \prec_\tau \tau_1}} \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{part\text{-}tr}_{\mathsf{u}:\underline{\tau_2}, \underline{\tau}}^{\mathsf{n}:\underline{\tau_1}}\right)_{\substack{\tau_1 = \_, \textsc{tn}(j_1, 0)\\ \tau_2 \prec_\tau \tau_1}}}\;\text{Simp}}{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{accept}_{\tau}^{\textsc{id}} \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{accept}_{\underline{\tau}}^{\underline{\textsc{id}}}}\;\text{Simp} \tag{83}$$

Part 1 We can check that for every $\tau_1 = \_, \textsc{tn}(j_1, 0)$ such that $\tau_2 \prec_\tau \tau_1$:

$$\begin{array}{rcl} \mathsf{part\text{-}tr}_{\mathsf{u}:\tau_2, \tau}^{\mathsf{n}:\tau_1} \rightarrow \sigma_\tau(\mathsf{e\text{-}auth}_{\textsc{u}}^{\textsc{id}}) = \mathsf{n}^{j_1} & \qquad & \mathsf{part\text{-}tr}_{\mathsf{u}:\underline{\tau_2}, \underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} \rightarrow \sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}_{\textsc{u}}^{\underline{\textsc{id}}}) = \mathsf{n}^{j_1} \\ \neg\mathsf{accept}_{\tau}^{\textsc{id}} \rightarrow \sigma_\tau(\mathsf{e\text{-}auth}_{\textsc{u}}^{\textsc{id}}) = \mathsf{fail} & \qquad & \neg\mathsf{accept}_{\underline{\tau}}^{\underline{\textsc{id}}} \rightarrow \sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}_{\textsc{u}}^{\underline{\textsc{id}}}) = \mathsf{fail} \end{array}$$

And $(\mathsf{n}^{j_1}, \mathsf{n}^{j_1}) \in \text{reveal}_{\tau_0}$. Therefore we can decompose $\sigma_\tau(\text{e-auth}_{\text{U}}^{\text{ID}})$ and $\sigma_{\underline{\tau}}(\text{e-auth}_{\text{U}}^{\underline{\text{ID}}})$ using FA and get rid of the resulting terms using (82) and (83):

$$\dfrac{\dfrac{\dfrac{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0} \ \sim\ \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}}{\begin{array}{c}\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \text{accept}_\tau^{\text{ID}}, \left(\text{part-tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1}, \mathsf{n}^{j_1}\right)_{\substack{\tau_1 = \_, \text{TN}(j_1,0)\\ \tau_2 \prec_\tau \tau_1}}, \text{fail}\\ \sim\ \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \text{accept}_{\underline{\tau}}^{\underline{\text{ID}}}, \left(\text{part-tr}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}}, \mathsf{n}^{j_1}\right)_{\substack{\tau_1 = \_, \text{TN}(j_1,0)\\ \tau_2 \prec_\tau \tau_1}}, \text{fail}\end{array}}\ \text{Simp}}{\begin{array}{c}\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \text{if } \text{accept}_\tau^{\text{ID}} \text{ then } \underset{\substack{\tau_1 = \_, \text{TN}(j_1,0)\\ \tau_2 \prec_\tau \tau_1}}{\text{case}} (\text{part-tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} : \mathsf{n}^{j_1}) \text{ else fail}\\ \sim\ \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \text{if } \text{accept}_{\underline{\tau}}^{\underline{\text{ID}}} \text{ then } \underset{\substack{\tau_1 = \_, \text{TN}(j_1,0)\\ \tau_2 \prec_\tau \tau_1}}{\text{case}} (\text{part-tr}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} : \mathsf{n}^{j_1}) \text{ else fail}\end{array}}\ \text{Simp}}{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \sigma_\tau(\text{e-auth}_{\text{U}}^{\text{ID}}) \ \sim\ \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \sigma_{\underline{\tau}}(\text{e-auth}_{\text{U}}^{\underline{\text{ID}}})}\ R \qquad (84)$$

Part 2 Observe that for every $\tau_1 = \_, \text{TN}(j_1, 0)$ such that $\tau_2 \prec_\tau \tau_1$:

$$\text{part-tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \rightarrow \sigma_\tau(\text{SQN}_{\text{U}}^{\text{ID}}) - \sigma_\tau^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}}) = \mathbf{1} \qquad \text{part-tr}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} \rightarrow \sigma_{\underline{\tau}}(\text{SQN}_{\text{U}}^{\underline{\text{ID}}}) - \sigma_{\underline{\tau}}^{\text{in}}(\text{SQN}_{\text{U}}^{\underline{\text{ID}}}) = \mathbf{1}$$

$$\neg\text{accept}_\tau^{\text{ID}} \rightarrow \sigma_\tau(\text{SQN}_{\text{U}}^{\text{ID}}) - \sigma_\tau^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}}) = 0 \qquad \neg\text{accept}_{\underline{\tau}}^{\underline{\text{ID}}} \rightarrow \sigma_{\underline{\tau}}(\text{SQN}_{\text{U}}^{\underline{\text{ID}}}) - \sigma_{\underline{\tau}}^{\text{in}}(\text{SQN}_{\text{U}}^{\underline{\text{ID}}}) = 0$$

It is then easy to adapt the derivation in (84) to get a derivation of (we omit the details):

$$\dfrac{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0} \ \sim\ \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}}{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \sigma_\tau(\text{SQN}_{\text{U}}^{\text{ID}}) - \sigma_\tau^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}}) \ \sim\ \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \sigma_{\underline{\tau}}(\text{SQN}_{\text{U}}^{\underline{\text{ID}}}) - \sigma_{\underline{\tau}}^{\text{in}}(\text{SQN}_{\text{U}}^{\underline{\text{ID}}})}\ \text{Simp} \qquad (85)$$

Part 3 We finally take care of t_τ and the Mac^4 terms. First, we check that for every $\tau_1 = \_, \text{TN}(j_1, 0)$ such that $\tau_2 \prec_\tau \tau_1$:

$$\text{part-tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \rightarrow t_\tau = \text{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^4(\mathsf{n}^{j_0}) \qquad \text{part-tr}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} \rightarrow t_{\underline{\tau}} = \text{Mac}_{\mathsf{k}_{\mathsf{m}}^{\underline{\text{ID}}}}^4(\mathsf{n}^{j_0})$$

$$\neg\text{accept}_\tau^{\text{ID}} \rightarrow t_\tau = \text{error} \qquad \neg\text{accept}_{\underline{\tau}}^{\underline{\text{ID}}} \rightarrow t_{\underline{\tau}} = \text{error}$$

Similarly to what we did in (84), we decompose t_τ and $t_{\underline{\tau}}$ using (82) and (83). Omitting the detail of the derivation, this yield:

$$\dfrac{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \left(\text{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^4(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \ \sim\ \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \left(\text{Mac}_{\mathsf{k}_{\mathsf{m}}^{\underline{\text{ID}}}}^4(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}}}{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, t_\tau \ \sim\ \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, t_{\underline{\tau}}}\ \text{Simp}$$

Observe that the Mac^4 terms here are exactly the Mac^4 terms in $\text{l-reveal}_\tau \backslash \text{l-reveal}_{\tau_0}$. To conclude this proof, it only remains to give a derivation of:

$$\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \left(\text{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^4(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \ \sim\ \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \left(\text{Mac}_{\mathsf{k}_{\mathsf{m}}^{\underline{\text{ID}}}}^4(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}}$$

For every $\tau_1 = \_, \text{TN}(j_1, 0)$ such that $\tau_2 \prec_\tau \tau_1$, we are going to apply the PRF-MAC^4 axiom with key $\mathsf{k}_{\mathsf{m}}^{\text{ID}}$ to replace $\text{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^4(\mathsf{n}^{j_0})$ by a fresh nonce n_{τ_1}. Let $\psi \equiv \phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}$, observe that:

$$\text{set-mac}_{\text{ID}}^4(\psi) \ = \left\{\pi_1(g(\phi_{\tau_a}^{\text{in}})) \mid \tau_a = \_, \text{TU}_{\text{ID}}(j_a, 1) \prec \tau\right\} \cup \left\{\mathsf{n}^{j_n} \mid \tau_n = \_, \text{TN}(j_n, 1) \prec \tau\right\}$$

Let:

$$T = \left\{\mathsf{n}^{j_0} \mid \tau_1 = \_, \text{TN}(j_0, 0) \wedge \tau_2 \prec_\tau \tau_1\right\}$$

Our goal is to rewrite ψ into a vector of terms ψ_1 such that $\text{set-mac}_{\text{ID}}^4(\psi_1) \cap T = \emptyset$. This will allow us to apply the PRF-MAC^4 axiom. We are going to rewrite ψ as follows:

- Let $\tau_a = \_, \textsc{tu}_{\textsc{id}}(j_a, 1) \prec \tau$. By validity of τ, we know that $\tau_a \prec_\tau \tau_2$, and that there exists $\tau_b = \_, \textsc{tu}_{\textsc{id}}(j_a, 0) \prec_\tau \tau_a$. Using **(StrEqu2)**, we know that:

$$\mathsf{accept}^{\textsc{id}}_{\tau_a} \leftrightarrow \bigvee_{\substack{\tau_x = \_, \textsc{tn}(j_x, 0) \\ \tau_b \prec_\tau \tau_x \prec_\tau \tau_a}} \mathsf{part\text{-}tr}^{\mathsf{n}:\tau_x}_{\mathsf{u}:\tau_b, \tau_a}$$

We let $\alpha^{\textsc{id}}_{\tau_a}$ be the right-hand side of the equation above. Using this, we can check that:

$$t_{\tau_a} \;=\; \mathsf{if}\ \alpha^{\textsc{id}}_{\tau_a}\ \mathsf{then} \operatorname*{\mathsf{case}}_{\substack{\tau_x = \_, \textsc{tn}(j_x, 0) \\ \tau_b \prec_\tau \tau_x \prec_\tau \tau_a}} (\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_x}_{\mathsf{u}:\tau_b, \tau_a} : \mathsf{Mac}^4_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\mathsf{n}^{j_x}))\ \mathsf{else\ error}$$

Let $\kappa^{\textsc{id}}_{\tau_a}$ be the right-hand side of the equation above. For every $\tau_x = \_, \textsc{tn}(j_x, 0)$, if $\mathsf{n}^{j_x} \in \mathsf{set\text{-}mac}^4_{\textsc{id}}(\alpha^{\textsc{id}}_{\tau_a}, \kappa^{\textsc{id}}_{\tau_a})$ then $\tau_x \prec_\tau \tau_a$. Therefore:

$$\begin{aligned} & \mathsf{set\text{-}mac}^4_{\textsc{id}}\left(\alpha^{\textsc{id}}_{\tau_a}, \kappa^{\textsc{id}}_{\tau_a}\right) \cap T \\ \subseteq\ & \left\{\mathsf{n}^{j_x} \mid \tau_x = \_, \textsc{tn}(j_x, 0) \wedge \tau_x \prec_\tau \tau_a\right\} \cap \left\{\mathsf{n}^{j_0} \mid \tau_1 = \_, \textsc{tn}(j_0, 0) \wedge \tau_2 \prec_\tau \tau_1\right\} \\ =\ & \left\{\mathsf{n}^{j_x} \mid \tau_x = \_, \textsc{tn}(j_x, 0) \wedge \tau_x \prec_\tau \tau_a \wedge \tau_2 \prec_\tau \tau_x\right\} \end{aligned}$$

By validity of τ, we know that $\tau_a \prec_\tau \tau_2$. This implies that whenever $\tau_x \prec_\tau \tau_a$ and $\tau_2 \prec_\tau \tau_x$, we have $\tau_x \prec_\tau \tau_2 \prec_\tau \tau_x$. Hence:

$$\mathsf{set\text{-}mac}^4_{\textsc{id}}\left(\alpha^{\textsc{id}}_{\tau_a}, \kappa^{\textsc{id}}_{\tau_a}\right) \cap T \;=\; \emptyset \tag{86}$$

Let ψ_0 be ψ in which we replace, for every $\tau_a = \_, \textsc{tu}_{\textsc{id}}(j_a, 1) \prec \tau$, any occurrence of $\mathsf{accept}^{\textsc{id}}_{\tau_a}$ and t_{τ_a} by, respectively, $\alpha^{\textsc{id}}_{\tau_a}$ and $\kappa^{\textsc{id}}_{\tau_a}$, for every τ_a. We then have:

$$\mathsf{set\text{-}mac}^4_{\textsc{id}}(\psi_0) \;=\; \left\{\mathsf{n}^{j_n} \mid \tau_n = \_, \textsc{tn}(j_n, 1) \prec \tau\right\} \;\cup \bigcup_{\substack{\tau_a = \_, \textsc{tu}_{\textsc{id}}(j_a, 1) \\ \tau_a \prec \tau}} \mathsf{set\text{-}mac}^4_{\textsc{id}}\left(\alpha^{\textsc{id}}_{\tau_a}, \kappa^{\textsc{id}}_{\tau_a}\right)$$

And using (86), we know that:

$$\mathsf{set\text{-}mac}^4_{\textsc{id}}(\psi_0) \cap T = \left\{\mathsf{n}^{j_n} \mid \tau_n = \_, \textsc{tn}(j_n, 1) \prec \tau\right\} \tag{87}$$

- Let $\tau_n = \_, \textsc{tn}(j_n, 1)$ and $\tau_n{}' = \_, \textsc{tn}(j_n, 0)$ such that $\tau_n{}' \prec_\tau \tau_n$. Using **(StrEqu3)**, we know that:

$$\mathsf{accept}^{\textsc{id}}_{\tau_n} \;\leftrightarrow \bigvee_{\substack{\tau_i{}' = \_, \textsc{tu}_{\textsc{id}}(j_i, 0) \\ \tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1) \\ \tau_i{}' \prec_\tau \tau_n{}' \prec_\tau \tau_i \prec_\tau \tau_n}} \mathsf{full\text{-}tr}^{\mathsf{n}:\tau_n{}', \tau_n}_{\mathsf{u}:\tau_i{}', \tau_i}$$

Let $\lambda^{\textsc{id}}_{\tau_n}$ be the right-hand side of the equation above. We check that if $\mathsf{n}^{j_n} \in \mathsf{set\text{-}mac}^4_{\textsc{id}}(\lambda^{\textsc{id}}_{\tau_n})$ then there exists $\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1)$ such that $\tau_i \prec_\tau \tau_n$. Since $\tau_i \prec \tau$, we know that $j_i \neq j$. Therefore $\tau_i \prec_\tau \tau_2$, and we can show that:

$$\mathsf{set\text{-}mac}^4_{\textsc{id}}\left(\lambda^{\textsc{id}}_{\tau_n}\right) \cap T \;=\; \emptyset \tag{88}$$

Let ψ_1 be ψ_0 in which we replace, for every $\tau_n = \_, \textsc{tn}(j_n, 1)$ and $\tau_n{}' = \_, \textsc{tn}(j_n, 0)$ such that $\tau_n{}' \prec_\tau \tau_n$, any occurrence of $\mathsf{accept}^{\textsc{id}}_{\tau_n}$ by $\lambda^{\textsc{id}}_{\tau_n}$. Using (87) and (88), we can check that:

$$\mathsf{set\text{-}mac}^4_{\textsc{id}}(\psi_1) \cap T \;=\; \emptyset$$

Which is what we wanted to show.

Part 4 Let $\tau_1 = \_, \textsc{tn}(j_0, 0)$ be such that $\tau_2 \prec_\tau \tau_1$. For every $\tau_1{}' = \_, \textsc{tn}(j_0', 0)$ be such that $\tau_2 \prec_\tau \tau_1{}'$, if $j_0' \neq j_0$ then $(\mathsf{n}^{j_0'} = \mathsf{n}^{j_0}) \leftrightarrow \mathsf{false}$. Moreover, since $\mathsf{set\text{-}mac}^4_{\textsc{id}}(\psi_1) \cap T = \emptyset$, we know that for every $\mathsf{n} \in \mathsf{set\text{-}mac}^4_{\textsc{id}}(\psi_1)$, $(\mathsf{n} = \mathsf{n}^{j_0}) \leftrightarrow \mathsf{false}$.

We can therefore apply simultaneously the $\textsc{prf-mac}^4$ axiom with key $\mathsf{k}_{\mathsf{m}}^{\textsc{id}}$ for every $\tau_1 = \_, \textsc{tn}(j_0, 0)$ such that $\tau_2 \prec_\tau \tau_1$, to replace $\mathsf{Mac}^4_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\mathsf{n}^{j_0})$ by a fresh nonce n_{τ_1}. We then rewrite back ψ_1 into ψ. This yield the derivation:

$$\dfrac{\dfrac{\dfrac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, (\mathsf{n}_{\tau_1})_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \sim \zeta}{\psi_1, (\mathsf{n}_{\tau_1})_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \sim \zeta}\,R}{\psi_1, \left(\mathsf{Mac}^4_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \sim \zeta}\,\textsc{prf-mac}^4}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^4_{\mathsf{k}_{\mathsf{m}}^{\textsc{id}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \sim \zeta}\,R$$

where:

$$\zeta \equiv \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left((\mathsf{Mac}^4_{\mathsf{k}_{\mathsf{m}}^{\underline{\textsc{id}}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}}$$

Observe that we never used the fact that τ was a *basic* trace of actions above, but only the fact that τ is a *valid* trace of actions. Therefore the same reasoning applies to ζ, and for every $\tau_1 = \_, \textsc{tn}(j_0, 0)$ such that $\tau_2 \prec_\tau \tau_1$, we replace $\mathsf{Mac}^4_{\mathsf{k}_{\mathsf{m}}^{\underline{\textsc{id}}}}(\mathsf{n}^{j_0})$ by a fresh nonce n'_{τ_1}. We conclude using Fresh:

$$\dfrac{\dfrac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, (\mathsf{n}_{\tau_1})_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{n}'_{\tau_1}\right)_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}}}\,\mathsf{Fresh}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, (\mathsf{n}_{\tau_1})_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left((\mathsf{Mac}^4_{\mathsf{k}_{\mathsf{m}}^{\underline{\textsc{id}}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \textsc{tn}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}}}\,R + \textsc{prf-mac}^4$$

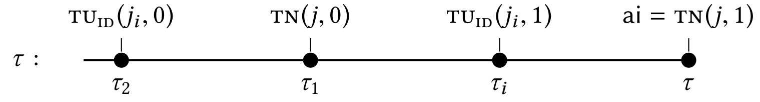
Which concludes this proof.

G.11 Case ai = $\textsc{tn}(j, 1)$

We know that $\underline{\mathsf{ai}} = \textsc{tn}(j, 1)$. Here $\mathsf{l\text{-}reveal}_\tau$ and $\mathsf{l\text{-}reveal}_{\tau_0}$ coincides everywhere except on:

$$\mathsf{net\text{-}e\text{-}auth}_\tau(\textsc{id}, j) \sim \underline{\mathsf{net\text{-}e\text{-}auth}}_{\underline{\tau}}(\textsc{id}, j) \qquad\qquad \mathsf{sync\text{-}diff}_\tau^{\textsc{id}} \sim \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\textsc{id})}$$

Let $\textsc{id} \in \mathcal{S}_{\mathsf{id}}$, $\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1)$, $\tau_1 = \_, \textsc{tn}(j, 0)$, $\tau_2 = \_, \textsc{tu}_{\textsc{id}}(j_i, 0)$ such that $\tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i$:


$\textsc{tu}_{\textsc{id}}(j_i, 0)$
$\textsc{tn}(j, 0)$
$\textsc{tu}_{\textsc{id}}(j_i, 1)$
$\mathsf{ai} = \textsc{tn}(j, 1)$
τ :
τ_2
τ_1
τ_i
τ

Let $\mathsf{f} \equiv \mathsf{full\text{-}tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i}$ and $\underline{\mathsf{f}} \equiv \mathsf{full\text{-}tr}^{\mathsf{n}:\underline{\tau_1},\underline{\tau}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau_i}}$. Using **(Der4)** we know that we have the following derivation:

$$\dfrac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{f} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{\mathsf{f}}}\,\mathsf{Simp} \tag{89}$$

Since $\mathsf{f} \rightarrow \mathsf{accept}_\tau^{\textsc{id}}$, we have:

$$[\mathsf{f} \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\textsc{u}}^{\textsc{id}})]\mathsf{sync\text{-}diff}_\tau^{\textsc{id}} = [\mathsf{f} \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\textsc{u}}^{\textsc{id}})] \begin{pmatrix} \text{if } \sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\textsc{n}}^{\textsc{id}}) = \mathsf{n}^j \text{ then } \mathsf{suc}(\mathsf{sync\text{-}diff}_{\tau_0}^{\textsc{id}}) \\ \hfill \text{else } \mathsf{sync\text{-}diff}_{\tau_0}^{\textsc{id}} \end{pmatrix}$$

Case 1 Assume that $\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1) \prec_\tau \textsc{ns}_{\textsc{id}}(\_)$. Let $\tau_{\textsc{ns}} = \_, \textsc{ns}_{\textsc{id}}(j_{\textsc{ns}})$ be the latest session reset in τ, i.e. $\tau_{\textsc{ns}} \prec_\tau \tau$ and $\tau_{\textsc{ns}} \not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)$. We show by induction that for every τ' such that $\tau_{\textsc{ns}} \preceq \tau'$ we have:

$$f \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\textsc{n}}^{\textsc{id}}) = \mathsf{n}^j \;\rightarrow\; \sigma_{\tau_{\textsc{ns}}}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) = \sigma_{\tau'}(\textsc{sqn}_{\textsc{n}}^{\textsc{id}}) \tag{90}$$

Let τ' be such that $\tau_{\textsc{ns}} \preceq \tau'$:

- If $\tau' = \tau_{\textsc{ns}}$ then the property trivially holds.
- If $\tau_{\textsc{ns}} \prec_\tau \tau'$. The only cases where $\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}$ is updated are $\textsc{pn}(j', 1)$ and $\textsc{tn}(j', 1)$:
  - If $\tau' = \_, \textsc{pn}(j', 1)$: since $\tau = \textsc{tn}(j, 1)$ we know by validity of τ that $j' \neq j$. Therefore:

$$\mathsf{inc\text{-}accept}_{\tau'}^{\mathrm{ID}} \;\rightarrow\; \sigma_{\tau'}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j'} \;\rightarrow\; \sigma_{\tau'}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) \neq \mathsf{n}^{j} \;\rightarrow\; \sigma_{\tau}^{\mathsf{in}}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) \neq \mathsf{n}^{j}$$

    It follows that:

$$\sigma_{\tau}^{\mathsf{in}}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j} \;\rightarrow\; \neg\mathsf{inc\text{-}accept}_{\tau'}^{\mathrm{ID}} \;\rightarrow\; \sigma_{\tau'}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) = \sigma_{\tau'}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$$

    And we conclude by applying the induction hypothesis.
  - If $\tau' = \_, \textsc{tn}(j', 1)$: since $\tau = \textsc{tn}(j, 1)$ and $\tau' \prec \tau$, we know that $j' \neq j$ (by validity of τ). Therefore:

$$\sigma_{\tau}^{\mathsf{in}}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j} \;\rightarrow\; \neg\mathsf{inc\text{-}accept}_{\tau'}^{\mathrm{ID}} \;\rightarrow\; \sigma_{\tau'}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) = \sigma_{\tau'}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$$

    And we conclude by applying the induction hypothesis.

This concludes the proof of (90). We prove by induction over τ' in $\textsc{ns}_{\mathrm{ID}}(j_{\textsc{ns}}) \leq \tau' \leq \tau$ that:

$$f \wedge \sigma_{\tau}^{\mathsf{in}}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j} \;\rightarrow\; \neg\sigma_{\tau'}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \tag{91}$$

Let ai' be such that $\tau' = \_, \mathsf{ai}'$.

- The case $\mathsf{ai}' = \textsc{ns}_{\mathrm{ID}}(j_{\textsc{ns}})$ is trivial since we then have $\sigma_{\tau'}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{false}$.
- If $\mathsf{ai}' \neq \textsc{pu}_{\mathrm{ID}}(\_, 2)$, then since $\textsc{ns}(j_{\textsc{ns}}) \not\prec_\tau \textsc{ns}(\_)$ we know that $\mathsf{ai}' \neq \textsc{ns}(\_)$. Hence $\sigma_{\tau'}^{\mathsf{up}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) = \bot$, which implies $\sigma_{\tau'}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \sigma_{\tau'}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})$. By induction hypothesis we know that:

$$f \wedge \sigma_{\tau}^{\mathsf{in}}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j} \;\rightarrow\; \neg\sigma_{\tau'}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})$$

  which concludes this case.
- If $\mathsf{ai}' = \textsc{pu}_{\mathrm{ID}}(j', 2)$. Let $\tau''' = \_, \textsc{pu}_{\mathrm{ID}}(j', 1) \leq \tau$. By validity of τ we know that $\tau_{\textsc{ns}} \prec_\tau \tau'''$. Using **(Equ2)** we know that:

$$\mathsf{accept}_{\tau'}^{\mathrm{ID}} \;\leftrightarrow\; \bigvee_{\substack{\tau''=\_,\textsc{pn}(j'',1)\\ \tau''' \prec_\tau \tau'' \prec_\tau \tau'}} \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau''',\tau'}^{\mathsf{n}:\tau''}$$

  And using **(StrEqu4)**:

$$\neg\sigma_{\tau'}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau''',\tau'}^{\mathsf{n}:\tau''} \;\rightarrow\; \sigma_{\tau'}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau'}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) = 0$$

  Using (90), we know that:

$$f \wedge \sigma_{\tau}^{\mathsf{in}}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j} \;\rightarrow\; \sigma_{\tau_{\textsc{ns}}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) = \sigma_{\tau'''}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \wedge \sigma_{\tau_{\textsc{ns}}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) = \sigma_{\tau'}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$$

  Therefore:

$$f \wedge \sigma_{\tau}^{\mathsf{in}}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j} \;\rightarrow\; \sigma_{\tau'''}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) = \sigma_{\tau'}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$$

  Using **(B5)** we know that $\sigma_{\tau'''}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \leq \sigma_{\tau'''}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}})$, and by **(B1)** we know that $\sigma_{\tau'''}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) \leq \sigma_{\tau'}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}})$. Moreover $\sigma_{\tau'''}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{suc}(\sigma_{\tau'''}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})) < \sigma_{\tau'''}^{\mathsf{in}}(\textsc{sqn}_{\mathrm{N}}^{\mathrm{ID}})$. We summarize all of this graphically in Figure 27. Putting everything together we get that:

$$\mathsf{f} \wedge \neg\sigma_{\tau'}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau''',\tau'}^{\mathsf{n}:\tau''} \;\rightarrow\; \sigma_{\tau'}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau'}(\textsc{sqn}_{\mathrm{U}}^{\mathrm{ID}}) \;\rightarrow\; \mathsf{false}$$

  We deduce that:

$$\mathsf{f} \wedge \neg\sigma_{\tau'}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{accept}_{\tau'}^{\mathrm{ID}} \;\rightarrow\; \bigvee_{\substack{\tau''=\_,\textsc{pn}(j'',1)\\ \textsc{pu}_{\mathrm{ID}}(j',1) \prec_\tau \tau'' \prec_\tau \tau'}} \mathsf{f} \wedge \neg\sigma_{\tau'}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\_,\tau'}^{\mathsf{n}:\tau''} \;\rightarrow\; \mathsf{false}$$

  Moreover, using the induction hypothesis we know that:

$$f \wedge \sigma_{\tau}^{\mathsf{in}}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j} \;\rightarrow\; \neg\sigma_{\tau'}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})$$

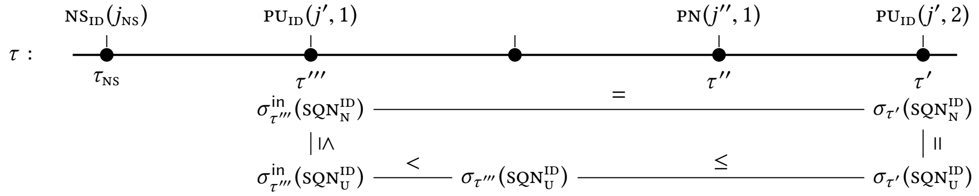

τ :
$\textsc{ns}_{\textsc{id}}(j_{\textsc{ns}})$
$\textsc{pu}_{\textsc{id}}(j', 1)$
$\textsc{pn}(j'', 1)$
$\textsc{pu}_{\textsc{id}}(j', 2)$
$\tau_{\textsc{ns}}$
τ'''
τ''
τ'
$\sigma^{\mathsf{in}}_{\tau'''}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$
$=$
$\sigma_{\tau'}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$
$\leq$
$=$
$\sigma^{\mathsf{in}}_{\tau'''}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$<$
$\sigma_{\tau'''}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$\leq$
$\sigma_{\tau'}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$

Fig. 27. First Graphical Representation Used in the Proof of the Case $\textsc{tn}(j, 1)$ of Lemma 15.

Therefore:

$$f \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\textsc{id}}_{\textsc{n}}) = \mathsf{n}^{j} \;\rightarrow\; \neg\mathsf{accept}_{\tau'} \;\rightarrow\; \neg\sigma_{\tau'}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}})$$

This concludes the proof of (91). Using (91) we get that $\mathsf{f} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \rightarrow \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\textsc{id}}_{\textsc{n}}) \neq \mathsf{n}^{j}$. Hence:

$$[\mathsf{f}]\mathsf{sync\text{-}diff}^{\textsc{id}}_{\tau} = [\mathsf{f} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}})]\mathsf{sync\text{-}diff}^{\textsc{id}}_{\tau_0}$$

We know that $\underline{\mathsf{f}} \rightarrow \mathsf{accept}^{\nu_{\tau_2}(\textsc{id})}_{\underline{\tau}}$. Moreover, $\nu_{\tau_2}(\textsc{id}) \neq \nu_{\tau}(\textsc{id})$, hence using **(A5)** we know that $\underline{\mathsf{f}} \rightarrow \neg\mathsf{accept}^{\nu_{\tau}(\textsc{id})}_{\underline{\tau}}$. Hence:

$$[\underline{\mathsf{f}}]\mathsf{sync\text{-}diff}^{\nu_{\tau}(\textsc{id})}_{\underline{\tau}} = [\underline{\mathsf{f}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_{\tau}(\textsc{id})}_{\textsc{u}})]\mathsf{sync\text{-}diff}^{\nu_{\tau}(\textsc{id})}_{\underline{\tau_0}}$$

Using the derivation in (89) and the fact that:

$$\left(\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}), \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_{\tau}(\textsc{id})}_{\textsc{u}})\right) \in \mathsf{reveal}_{\tau_0} \qquad \left(\mathsf{sync\text{-}diff}^{\textsc{id}}_{\tau_0}, \mathsf{sync\text{-}diff}^{\nu_{\tau}(\textsc{id})}_{\underline{\tau_0}}\right) \in \mathsf{reveal}_{\tau_0}$$

We can build the derivation:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{f}, \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}), \quad \mathsf{sync\text{-}diff}^{\textsc{id}}_{\tau_0} \\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{\mathsf{f}}, \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_{\tau}(\textsc{id})}_{\textsc{u}}), \mathsf{sync\text{-}diff}^{\nu_{\tau}(\textsc{id})}_{\underline{\tau_0}}\end{array}}\,\mathsf{Simp}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, [\mathsf{f}]\mathsf{sync\text{-}diff}^{\textsc{id}}_{\tau} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, [\underline{\mathsf{f}}]\mathsf{sync\text{-}diff}^{\nu_{\tau}(\textsc{id})}_{\underline{\tau}}}\,\mathsf{Simp} \tag{92}$$

Case 2 Assume that $\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1) \not<_{\tau} \textsc{ns}_{\textsc{id}}(\_)$. We introduce the term $\theta_{\textsc{pn}}$ (resp. $\theta_{\textsc{tn}}$) which states that no $\textsc{supi}$ (resp. $\textsc{guti}$) network session has been initiated which $\textsc{id}$ between τ_1 and τ:

$$\theta_{\textsc{pn}} \;\equiv \bigwedge_{\substack{\tau' = \_, \textsc{pn}(\_, 1) \\ \tau_1 <_{\tau} \tau'}} \neg\mathsf{inc\text{-}accept}^{\textsc{id}}_{\tau'} \qquad\qquad \theta_{\textsc{tn}} \;\equiv \bigwedge_{\substack{\tau' = \textsc{tn}(\_, 0) \\ \tau_1 <_{\tau} \tau'}} \neg\mathsf{accept}^{\textsc{id}}_{\tau'}$$

It is easy to show that:

$$\left(\mathsf{f} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\textsc{id}}_{\textsc{n}}) = \mathsf{n}^{j}\right) \;\leftrightarrow\; (\mathsf{f} \wedge \theta_{\textsc{pn}} \wedge \theta_{\textsc{tn}})$$

We are now going to show that for every $\tau_1 \leq \tau'$, $P(\tau')$ holds where $P(\tau')$:

$$P(\tau') \;\equiv\; (\mathsf{f} \wedge \theta_{\textsc{pn}}) \;\rightarrow\; \left(\sigma_{\tau'}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) = \mathsf{UnSet} \wedge \sigma_{\tau'}(\mathsf{session}^{\textsc{id}}_{\textsc{n}}) = \mathsf{n}^{j} \wedge \bigwedge_{\substack{\tau_1 <_{\tau} \tau'' \leq \tau' \\ \tau'' = \textsc{tn}(\_, 0)}} \neg\mathsf{accept}^{\textsc{id}}_{\tau''}\right) \tag{93}$$

Since $\mathsf{f} \rightarrow \mathsf{accept}_{\tau_1}$, we know that $\mathsf{f} \rightarrow \sigma_{\tau_1}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) = \mathsf{UnSet}$. This shows that $P(\tau_1)$ holds. Let $\tau_1 <_{\tau} \tau'$, where $\tau' = \tau'_0, \mathsf{ai}'$, and assume $P(\tau'_0)$ holds by induction. We have four cases:

- If $\mathsf{ai}' \notin \{\textsc{tn}(\_, 0), \textsc{tn}(\_, 1), \textsc{pn}(\_, 1)\}$ then $P(\tau') \equiv P(\tau'_0)$, which concludes this case.

- If $\mathrm{ai}' = \textsc{tn}(\_, 0)$, then using the induction hypothesis $P(\tau_0')$ we know that $\mathsf{f} \wedge \theta_{\textsc{pn}} \rightarrow \sigma^{\mathsf{in}}_{\tau'}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) = \mathsf{UnSet}$. Therefore $\mathsf{f} \wedge \theta_{\textsc{pn}} \rightarrow \neg\mathrm{accept}^{\textsc{id}}_{\tau'}$. We know that $\mathsf{f} \wedge \theta_{\textsc{pn}} \rightarrow \sigma^{\mathsf{in}}_{\tau'}(\mathsf{session}^{\textsc{id}}_{\textsc{n}}) = \mathsf{n}^{j}$. We conclude by observing that:

$$\neg\mathrm{accept}^{\textsc{id}}_{\tau'} \wedge \sigma^{\mathsf{in}}_{\tau'}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) = \mathsf{UnSet} \wedge \sigma^{\mathsf{in}}_{\tau'}(\mathsf{session}^{\textsc{id}}_{\textsc{n}}) = \mathsf{n}^{j} \rightarrow \\ \Big(\sigma_{\tau'}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) = \mathsf{UnSet} \wedge \sigma_{\tau'}(\mathsf{session}^{\textsc{id}}_{\textsc{n}}) = \mathsf{n}^{j}\Big)$$

- If $\mathrm{ai}' = \textsc{tn}(j', 1)$. Since $\tau' \prec \tau$, we know that $j \neq j'$. Therefore $\sigma^{\mathsf{in}}_{\tau'}(\mathsf{session}^{\textsc{id}}_{\textsc{n}}) = \mathsf{n}^{j} \rightarrow \sigma^{\mathsf{in}}_{\tau'}(\mathsf{session}^{\textsc{id}}_{\textsc{n}}) \neq \mathsf{n}^{j'}$. We deduce that $\mathsf{f} \wedge \theta_{\textsc{pn}} \rightarrow \neg\mathrm{accept}^{\textsc{id}}_{\tau'}$. This concludes this case.
- If $\mathrm{ai}' = \_, \textsc{pn}(\_, 1)$. We know that $\mathsf{f} \wedge \theta_{\textsc{pn}} \rightarrow \neg\mathrm{inc\text{-}accept}^{\textsc{id}}_{\tau'}$. We conclude using the facts that:

$$\neg\mathrm{inc\text{-}accept}^{\textsc{id}}_{\tau'} \rightarrow \sigma_{\tau'}(\mathsf{session}^{\textsc{id}}_{\textsc{n}}) = \sigma^{\mathsf{in}}_{\tau'}(\mathsf{session}^{\textsc{id}}_{\textsc{n}})$$

$$\neg\mathrm{inc\text{-}accept}^{\textsc{id}}_{\tau'} \rightarrow \sigma_{\tau'}(\textsc{guti}^{\textsc{id}}_{\textsc{n}}) = \sigma^{\mathsf{in}}_{\tau'}(\textsc{guti}^{\textsc{id}}_{\textsc{n}})$$

By applying (93) at instant τ_0, we get that:

$$\Big(\mathsf{f} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\textsc{id}}_{\textsc{n}}) = \mathsf{n}^{j}\Big) \;\leftrightarrow\; (\mathsf{f} \wedge \theta_{\textsc{pn}} \wedge \theta_{\textsc{tn}}) \;\leftrightarrow\; (\mathsf{f} \wedge \theta_{\textsc{pn}}) \tag{94}$$

Part 1 Let $\tau' = \_, \textsc{pn}(j', 1)$, with $\tau_1 \prec_{\tau} \tau'$. Let $\tau_0' = \textsc{pn}(j', 0)$. Using **(Equ3)** we know that:

$$\mathrm{accept}^{\textsc{id}}_{\tau'} \;\leftrightarrow\; \bigvee_{\substack{\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1) \\ \tau_0' \prec_{\tau} \tau_a \prec_{\tau} \tau'}} \underbrace{\begin{pmatrix} g(\phi^{\mathsf{in}}_{\tau_a}) = \mathsf{n}^{j'} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau'})) = \{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\rangle\}^{\mathsf{n}_{\mathsf{e}}^{j_a}}_{\mathsf{pk}_{\textsc{n}}} \\ \wedge\ \pi_2(g(\phi^{\mathsf{in}}_{\tau'})) = \mathsf{Mac}^{1}_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\langle\{\langle \textsc{id}\,,\, \sigma^{\mathsf{in}}_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\rangle\}^{\mathsf{n}_{\mathsf{e}}^{j_a}}_{\mathsf{pk}_{\textsc{n}}}\,,\, g(\phi^{\mathsf{in}}_{\tau_a})\rangle) \end{pmatrix}}_{\lambda^{\tau'}_{\tau_a}} \tag{95}$$

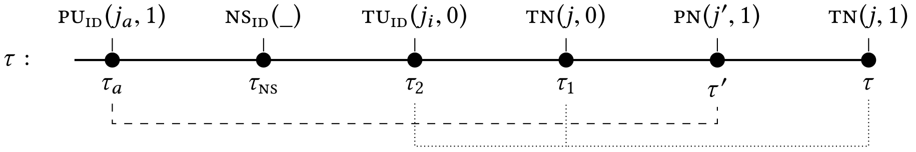
We define:

$$\tau_{\textsc{ns}} = \begin{cases} \textsc{ns}_{\textsc{id}}(j_{\textsc{ns}}) & \text{if there exists } j_{\textsc{ns}} \text{ s.t. } \textsc{ns}_{\textsc{id}}(j_{\textsc{ns}}) \prec_{\tau} \tau \text{ and } \textsc{ns}_{\textsc{id}}(j_{\textsc{ns}}) \not\prec_{\tau} \textsc{ns}_{\textsc{id}}(\_). \\ \epsilon & \text{otherwise} \end{cases}$$

Let $\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1)$ such that $\tau_0' \prec_{\tau} \tau_a \prec_{\tau} \tau'$. Since $\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1) \not\prec_{\tau} \textsc{ns}_{\textsc{id}}(\_)$, we have only three interleavings possible: $\tau_a \prec_{\tau} \tau_{\textsc{ns}}$, $\tau_{\textsc{ns}} \prec_{\tau} \tau_a \prec_{\tau} \tau_2$, $\tau_i \prec_{\tau} \tau_a$. First, we are going to show that in the first two cases we have:

$$\mathsf{f} \wedge \lambda^{\tau'}_{\tau_a} \;\rightarrow\; \neg\mathrm{inc\text{-}accept}^{\textsc{id}}_{\tau'}$$

- If $\tau_a \prec_{\tau} \tau_{\textsc{ns}}$, we have the following interleaving:



By definition of $\mathrm{inc\text{-}accept}^{\textsc{id}}_{\tau'}$, and using the fact that $\lambda^{\tau'}_{\tau_a} \rightarrow \mathrm{accept}^{\textsc{id}}_{\tau'}$ we know that:

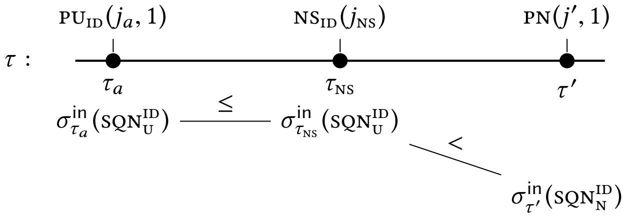
$$\lambda^{\tau'}_{\tau_a} \wedge \mathrm{inc\text{-}accept}^{\textsc{id}}_{\tau'} \;\;\rightarrow\;\; \sigma^{\mathsf{in}}_{\tau'}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \leq \sigma^{\mathsf{in}}_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$$

To conclude this case, we only need to show that:

$$\lambda^{\tau'}_{\tau_a} \wedge \mathrm{inc\text{-}accept}^{\textsc{id}}_{\tau'} \;\;\rightarrow\;\; \sigma^{\mathsf{in}}_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) < \sigma^{\mathsf{in}}_{\tau'}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) \tag{96}$$

From which we obtain directly a contradiction, implies that:

$$\mathsf{f} \wedge \lambda^{\tau'}_{\tau_a} \;\rightarrow\; \neg\mathrm{inc\text{-}accept}^{\textsc{id}}_{\tau'} \qquad\qquad \text{when } \tau_a \prec_{\tau} \tau_{\textsc{ns}} \tag{97}$$

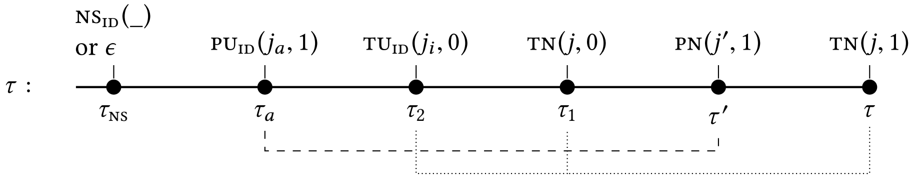


$\textsc{pu}_{\textsc{id}}(j_a, 1)$
$\textsc{ns}_{\textsc{id}}(j_{\textsc{ns}})$
$\textsc{pn}(j', 1)$
τ :
τ_a
$\tau_{\textsc{ns}}$
τ'
$\sigma^{\mathsf{in}}_{\tau_a}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$\leq$
$\sigma^{\mathsf{in}}_{\tau_{\textsc{ns}}}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$<$
$\sigma^{\mathsf{in}}_{\tau'}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$

Fig. 28. Second Graphical Representation Used in the Proof of the Case $\textsc{tn}(j, 1)$ of Lemma 15.

The proof of (96) is by **(B1)** and **(B6)**[8]. We give a graphical representation in Figure 28.

- If $\tau_{\textsc{ns}} \prec_\tau \tau_a \prec_\tau \tau_2$, we have the following interleaving:



We know that $\lambda^{\tau'}_{\tau_a} \rightarrow \sigma_{\tau_a}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) = \mathsf{UnSet}$, and that $\mathsf{f} \rightarrow \sigma^{\mathsf{in}}_{\tau_2}(\textsc{guti}^{\textsc{id}}_{\textsc{u}})$. By **(B3)**, we get $\mathsf{f} \rightarrow \sigma^{\mathsf{in}}_{\tau_2}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) \neq \mathsf{UnSet}$. This means that $\textsc{guti}^{\textsc{id}}_{\textsc{u}}$ is unset at τ_a, but set at τ_2. Therefore there was a successful run of the protocol ($\textsc{supi}$ or $\textsc{guti}$) between τ_a and τ_2. More precisely, using Proposition 22 we have:

$$\begin{aligned} \mathsf{f} \wedge \lambda^{\tau'}_{\tau_a} &\rightarrow \sigma_{\tau_a}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) = \mathsf{UnSet} \wedge \sigma^{\mathsf{in}}_{\tau_2}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) \neq \mathsf{UnSet} \\ &\rightarrow \bigvee_{\substack{\tau''=\_,\textsc{fu}_{\textsc{id}}(j'') \\ \tau_a \prec_\tau \tau'' \prec_\tau \tau_2}} \mathsf{accept}^{\textsc{id}}_{\tau''} \end{aligned} \tag{98}$$

Let $\tau'' = \_, \textsc{fu}_{\textsc{id}}(j'')$ such that $\tau_a \prec_\tau \tau'' \prec_\tau \tau_2$. We then have two cases:

- Assume $j'' = j_a$. In order to have $\mathsf{accept}^{\textsc{id}}_{\tau''}$, we need the $\textsc{supi}$ or $\textsc{guti}$ session j'' to have been executed before τ''. Intuitively, this cannot happen if $j'' = j_a$ because the user session j_a is interacting with the network session j', and $\tau'' \prec_\tau \tau'$. Formally, using the fact that $j'' = j_a$ we are going to show that:

$$\neg\left(\lambda^{\tau'}_{\tau_a} \wedge \mathsf{accept}^{\textsc{id}}_{\tau''}\right) \tag{99}$$

First, by **(Equ1)** we know that:

$$\begin{aligned} \mathsf{accept}^{\textsc{id}}_{\tau''} &\rightarrow \bigvee_{\textsc{fn}(j_x) \not\prec_{\tau''} \textsc{ns}_{\textsc{id}}(\_)} \mathsf{inj\text{-}auth}_{\tau''}(\textsc{id}, j_x) \\ &\rightarrow \bigvee_{\textsc{fn}(j_x) \not\prec_{\tau''} \textsc{ns}_{\textsc{id}}(\_)} \sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{j_x}_{\textsc{n}}) = \textsc{id} \wedge \sigma^{\mathsf{in}}_{\tau''}(\mathsf{e\text{-}auth}^{\textsc{id}}_{\textsc{u}}) = \mathsf{n}^{j_x} \end{aligned}$$

By **(A8)** we get:

$$\rightarrow \bigvee_{\textsc{fn}(j_x) \not\prec_{\tau''} \textsc{ns}_{\textsc{id}}(\_)} \sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{j_x}_{\textsc{n}}) = \textsc{id} \wedge \sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{\textsc{id}}_{\textsc{u}}) = \mathsf{n}^{j_x} \tag{100}$$

[8] Using the fact that $\mathsf{f} \rightarrow \sigma^{\mathsf{in}}_{\tau_2}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}})$ and $\sigma^{\mathsf{in}}_{\tau_2}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \rightarrow \sigma_{\tau'}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}})$

We know that $\lambda_{\tau_a}^{\tau'} \rightarrow \sigma_{\tau_a}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{n}^{j'}$. Moreover, using the validity of τ we know that $\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}$ is not updated between τ_a and τ'', therefore $\lambda_{\tau_a}^{\tau'} \rightarrow \sigma_{\tau''}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{n}^{j'}$. Putting this together with (100), and using the fact that:

$$\left(\sigma_{\tau''}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{n}^{j_x} \wedge \sigma_{\tau''}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{n}^{j'}\right) \rightarrow \mathsf{false} \qquad \text{if } j_x \neq j'$$

We get:

$$\mathsf{accept}_{\tau''}^{\mathrm{ID}} \wedge \lambda_{\tau_a}^{\tau'} \quad \rightarrow \quad \sigma_{\tau''}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\mathrm{N}}^{j'}) = \mathrm{ID} \wedge \sigma_{\tau''}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{n}^{j'}$$

Since $\tau'' \prec_\tau \tau'$, we know that $\sigma_{\tau''}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\mathrm{N}}^{j'}) = \mathsf{fail}$. Hence:

$$\rightarrow \quad \sigma_{\tau''}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\mathrm{N}}^{j'}) = \mathrm{ID} \wedge \sigma_{\tau''}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\mathrm{N}}^{j'}) = \mathsf{fail} \quad \rightarrow \quad \mathsf{false}$$

Which concludes the proof of (99).

- Assume $j'' \neq j_a$. Intuitively, we know that $\mathsf{accept}_{\tau''}^{\mathrm{ID}}$ implies that $\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}$ and $\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}$ have been incremented and synchronized between τ_a and τ'. Therefore we know that the test $\mathsf{inc\text{-}accept}_{\tau'}^{\mathrm{ID}}$ fails. Formally, we show that:

$$\mathsf{accept}_{\tau''}^{\mathrm{ID}} \quad \rightarrow \quad \sigma_{\tau_a}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau''}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \tag{101}$$

  We give the outline of the proof. First, we apply **(StrEqu1)** to τ''. Then, we take $\tau_0'' = \_, \mathrm{FN}(j_e) \prec \tau''$. We let $\tau_1'' = \_, \mathrm{PN}(j_e, 1)$ or $\_, \mathrm{TN}(j_e, 1)$ such that $\tau_1'' \prec \tau_0''$, and we do a case disjunction on τ_1'':
  * If $\tau_1'' = \_, \mathrm{PN}(j_e, 1)$, then we use **(StrEqu4)** on it, and we show that $\sigma_{\tau_a}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau''}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})$ by doing a case disjunction on $\mathsf{inc\text{-}accept}_{\tau_1''}^{\mathrm{ID}}$.
  * If $\tau_1'' = \_, \mathrm{TN}(j_e, 1)$, then we use **(StrEqu2)** on it, and we show that $\sigma_{\tau_a}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau''}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})$ using **(B4)**

  We omit the details.

  Using **(B1)** we know that $\sigma_{\tau''}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \leq \sigma_{\tau'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})$ and $\sigma_{\tau_a}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \leq \sigma_{\tau_a}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})$. Hence, we deduce from (101) that:

$$\mathsf{accept}_{\tau''}^{\mathrm{ID}} \quad \rightarrow \quad \sigma_{\tau_a}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})$$

  Moreover, by definition of $\mathsf{inc\text{-}accept}_{\tau'}^{\mathrm{ID}}$, and using the fact that $\lambda_{\tau_a}^{\tau'} \rightarrow \mathsf{accept}_{\tau'}^{\mathrm{ID}}$ we know that:

$$\lambda_{\tau_a}^{\tau'} \wedge \mathsf{inc\text{-}accept}_{\tau'}^{\mathrm{ID}} \quad \rightarrow \quad \sigma_{\tau'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \leq \sigma_{\tau_a}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})$$

  Putting the two equations above together:

$$\lambda_{\tau_a}^{\tau'} \wedge \mathsf{inc\text{-}accept}_{\tau'}^{\mathrm{ID}} \wedge \mathsf{accept}_{\tau''}^{\mathrm{ID}} \quad \rightarrow \quad \mathsf{false}$$

  Hence:

$$\lambda_{\tau_a}^{\tau'} \wedge \mathsf{accept}_{\tau''}^{\mathrm{ID}} \quad \rightarrow \quad \neg\mathsf{inc\text{-}accept}_{\tau'}^{\mathrm{ID}}$$

From (98), (99) and the equation above, we deduce that:

$$\mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \quad \rightarrow \quad \bigvee_{\substack{\tau'' = \_, \mathrm{FU}_{\mathrm{ID}}(j'') \\ \tau_a \prec_\tau \tau'' \prec_\tau \tau_2}} \mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \wedge \mathsf{accept}_{\tau''}^{\mathrm{ID}} \quad \rightarrow \quad \bigvee_{\substack{\tau'' = \_, \mathrm{FU}_{\mathrm{ID}}(j'') \\ \tau_a \prec_\tau \tau'' \prec_\tau \tau_2}} \neg\mathsf{inc\text{-}accept}_{\tau'}^{\mathrm{ID}}$$

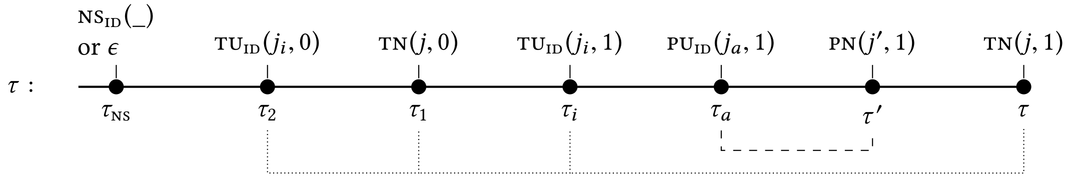
Hence:

$$\mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \quad \rightarrow \quad \neg\mathsf{inc\text{-}accept}_{\tau'}^{\mathrm{ID}} \qquad\qquad \text{when } \tau_{\mathrm{NS}} \prec_\tau \tau_a \prec_\tau \tau_2 \tag{102}$$

Part 2 Using (97) and (102), we know that we can focus on the (partial) $\textsc{supi}$ sessions that started after τ_i, i.e. the sessions with transcript of the from $\lambda_{\tau_a}^{\tau'}$, where $\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1)$, $\tau' = \_, \textsc{pn}(j', 1)$ and $\tau_i \prec_\tau \tau_a \prec_\tau \tau'$. Formally, we have:

$$\begin{aligned}
(\mathsf{f} \wedge \theta_{\textsc{pn}}) \quad &\leftrightarrow \quad \mathsf{f} \wedge \bigwedge_{\substack{\tau' = \_, \textsc{pn}(\_, 1) \\ \tau_1 \prec_\tau \tau'}} \neg \mathsf{inc\text{-}accept}_{\tau'}^{\textsc{id}} \\
&\leftrightarrow \quad \mathsf{f} \wedge \bigwedge_{\substack{\tau' = \_, \textsc{pn}(\_, 1) \\ \tau_1 \prec_\tau \tau'}} \mathsf{accept}_{\tau'}^{\textsc{id}} \rightarrow \neg \mathsf{inc\text{-}accept}_{\tau'}^{\textsc{id}} \\
&\leftrightarrow \quad \mathsf{f} \wedge \bigwedge_{\substack{\tau' = \_, \textsc{pn}(j', 1) \\ \tau_0' = \_, \textsc{pn}(j', 0) \\ \tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1) \\ \tau_1 \prec_\tau \tau' \\ \tau_0' \prec_\tau \tau_a \prec_\tau \tau'}} \lambda_{\tau_a}^{\tau'} \rightarrow \neg \mathsf{inc\text{-}accept}_{\tau'}^{\textsc{id}} && \text{(By (95))} \\
&\leftrightarrow \quad \mathsf{f} \wedge \bigwedge_{\substack{\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1) \\ \tau' = \_, \textsc{pn}(j', 1) \\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \lambda_{\tau_a}^{\tau'} \rightarrow \neg \mathsf{inc\text{-}accept}_{\tau'}^{\textsc{id}} && \text{(By (97) and (102))}
\end{aligned}$$

We represent graphically the shape of the interleavings that we need to consider:



Part 3 We are now going to show that if at least one partial $\textsc{supi}$ session that started after τ_i accepts (i.e. $\mathsf{f} \wedge \lambda_{\tau_a}^{\tau'}$ holds), then we have $\sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\textsc{n}}^{\textsc{id}}) \neq \mathsf{n}^j$. First, from what we showed in **Part 2**, and using (94) we know that:

$$\begin{aligned}
\neg \left(\mathsf{f} \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\textsc{n}}^{\textsc{id}}) = \mathsf{n}^j \right) \quad &\leftrightarrow \quad \neg \mathsf{f} \vee \bigvee_{\substack{\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1) \\ \tau' = \_, \textsc{pn}(j', 1) \\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \wedge \mathsf{inc\text{-}accept}_{\tau'}^{\textsc{id}} \\
&\rightarrow \quad \neg \mathsf{f} \vee \bigvee_{\substack{\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1) \\ \tau' = \_, \textsc{pn}(j', 1) \\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \mathsf{f} \wedge \lambda_{\tau_a}^{\tau'}
\end{aligned}$$

We know show that the converse implication holds. In a first time, assume that for every $\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1)$ and $\tau' = \_, \textsc{pn}(j', 1)$ such that $\tau_i \prec_\tau \tau_a \prec_\tau \tau'$ we have:

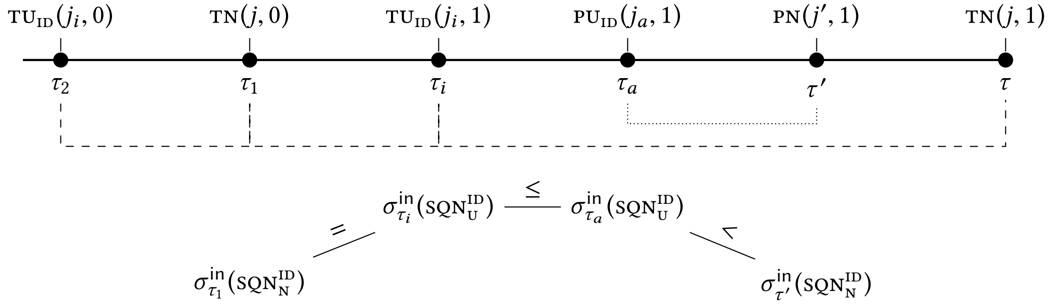
$$\mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \wedge \neg \mathsf{inc\text{-}accept}_{\tau'}^{\textsc{id}} \quad \rightarrow \quad \sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\textsc{n}}^{\textsc{id}}) \neq \mathsf{n}^j \tag{103}$$

Then we know that:

$$\neg \mathsf{f} \vee \bigvee_{\substack{\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1) \\ \tau' = \_, \textsc{pn}(j', 1) \\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \quad \rightarrow \quad \neg \left(\mathsf{f} \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\textsc{n}}^{\textsc{id}}) = \mathsf{n}^j \right)$$

Therefore:

$$\neg \left(\mathsf{f} \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\textsc{n}}^{\textsc{id}}) = \mathsf{n}^j \right) \quad \leftrightarrow \quad \neg \mathsf{f} \vee \bigvee_{\substack{\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1) \\ \tau' = \_, \textsc{pn}(j', 1) \\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \tag{104}$$



$\textsc{tu}_{\textsc{id}}(j_i, 0)$
$\textsc{tn}(j, 0)$
$\textsc{tu}_{\textsc{id}}(j_i, 1)$
$\textsc{pu}_{\textsc{id}}(j_a, 1)$
$\textsc{pn}(j', 1)$
$\textsc{tn}(j, 1)$
τ_2
τ_1
τ_i
τ_a
τ'
τ
$\sigma_{\tau_i}^{\text{in}}(\textsc{sqn}_{\text{U}}^{\textsc{id}})$
$\leq$
$\sigma_{\tau_a}^{\text{in}}(\textsc{sqn}_{\text{U}}^{\textsc{id}})$
$=$
$<$
$\sigma_{\tau_1}^{\text{in}}(\textsc{sqn}_{\text{N}}^{\textsc{id}})$
$\sigma_{\tau'}^{\text{in}}(\textsc{sqn}_{\text{N}}^{\textsc{id}})$

Fig. 29. Third Graphical Representation Used in the Proof of the Case $\textsc{tn}(j, 1)$ of Lemma 15.

We now give the proof of (103). Let $\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1)$ and $\tau' = \_, \textsc{pn}(j', 1)$ such that $\tau_i \prec_\tau \tau_a \prec_\tau \tau'$. We know that:

$$\lambda_{\tau_a}^{\tau'} \wedge \neg\text{inc-accept}_{\tau'}^{\textsc{id}} \;\rightarrow\; \sigma_{\tau_a}^{\text{in}}(\textsc{sqn}_{\text{U}}^{\textsc{id}}) < \sigma_{\tau'}^{\text{in}}(\textsc{sqn}_{\text{N}}^{\textsc{id}}) \qquad\qquad \text{f} \;\rightarrow\; \sigma_{\tau_1}^{\text{in}}(\textsc{sqn}_{\text{N}}^{\textsc{id}}) = \sigma_{\tau_i}^{\text{in}}(\textsc{sqn}_{\text{U}}^{\textsc{id}})$$

Moreover by **(B1)** we know that $\sigma_{\tau_i}^{\text{in}}(\textsc{sqn}_{\text{U}}^{\textsc{id}}) \leq \sigma_{\tau_a}^{\text{in}}(\textsc{sqn}_{\text{U}}^{\textsc{id}})$. We summarize this graphically in Figure 29. We deduce that:

$$\text{f} \wedge \lambda_{\tau_a}^{\tau'} \wedge \neg\text{inc-accept}_{\tau'}^{\textsc{id}} \;\rightarrow\; \sigma_{\tau_1}^{\text{in}}(\textsc{sqn}_{\text{N}}^{\textsc{id}}) < \sigma_{\tau'}^{\text{in}}(\textsc{sqn}_{\text{N}}^{\textsc{id}})$$

Moreover:

$$\sigma_{\tau_1}^{\text{in}}(\textsc{sqn}_{\text{N}}^{\textsc{id}}) < \sigma_{\tau'}^{\text{in}}(\textsc{sqn}_{\text{N}}^{\textsc{id}}) \;\rightarrow\; \bigvee_{\substack{\tau_x = \textsc{pn}(j_x, 1)\\ \tau_1 \prec_\tau \tau_x \prec_\tau \tau'}} \text{inc-accept}_{\tau_x}^{\textsc{id}} \vee \bigvee_{\substack{\tau_x = \textsc{tn}(j_x, 1)\\ \tau_1 \prec_\tau \tau_x \prec_\tau \tau'}} \text{inc-accept}_{\tau_x}^{\textsc{id}}$$

For every $\tau_x = \textsc{pn}(j_x, 1)$ such that $\tau_1 \prec_\tau \tau_x \prec_\tau \tau'$ we have $j_x \neq j$. Therefore:

$$\bigvee_{\substack{\tau_x = \textsc{pn}(j_x, 1)\\ \tau_1 \prec_\tau \tau_x \prec_\tau \tau'}} \text{inc-accept}_{\tau_x}^{\textsc{id}} \;\rightarrow\; \bigvee_{\substack{\tau_x = \textsc{pn}(j_x, 1)\\ \tau_1 \prec_\tau \tau_x \prec_\tau \tau'}} \sigma_{\tau_x}(\text{session}_{\text{N}}^{\textsc{id}}) = \text{n}^{j_x} \;\rightarrow\; \sigma_{\tau}^{\text{in}}(\text{session}_{\text{N}}^{\textsc{id}}) \neq \text{n}^{j}$$

And:

$$\bigvee_{\substack{\tau_x = \textsc{tn}(j_x, 1)\\ \tau_1 \prec_\tau \tau_x \prec_\tau \tau'}} \text{inc-accept}_{\tau_x}^{\textsc{id}} \;\rightarrow\; \bigvee_{\substack{\tau_x = \textsc{tn}(j_x, 1)\\ \tau_1 \prec_\tau \tau_x \prec_\tau \tau'}} \sigma_{\tau_x}^{\text{in}}(\text{session}_{\text{N}}^{\textsc{id}}) = \text{n}^{j_x} \;\rightarrow\; \sigma_{\tau}^{\text{in}}(\text{session}_{\text{N}}^{\textsc{id}}) \neq \text{n}^{j}$$

This concludes the proof of (103).

The proofs in **Part 1** to **3** only used the fact that τ is a valid action trace. We never used the fact that τ is a basic trace. Therefore, carrying out the same proof, we can show that:

$$\neg\left(\underline{\text{f}} \wedge \sigma_{\underline{\tau}}^{\text{in}}(\text{session}_{\text{N}}^{\nu_\tau(\textsc{id})}) = \text{n}^{j}\right) \;\leftrightarrow\; \neg\underline{\text{f}} \vee \bigvee_{\substack{\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1)\\ \tau' = \_, \textsc{pn}(j', 1)\\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \underline{\text{f}} \wedge \lambda_{\underline{\tau_a}}^{\tau'} \tag{105}$$

Part 4 Let $\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1)$ and $\tau' = \_, \textsc{pn}(j', 1)$ be such that $\tau_i \prec_\tau \tau_a \prec_\tau \tau'$. Observing that:

$$\left(\text{n}^{j'}, \text{n}^{j'}\right) \in \text{reveal}_{\tau_0} \qquad \left(\{\langle \textsc{id} \,,\, \sigma_{\tau_a}^{\text{in}}(\textsc{sqn}_{\text{U}}^{\textsc{id}})\rangle\}_{\text{pk}_{\text{N}}}^{\text{n}_{\text{e}}^{j_a}}, \{\langle \nu_\tau(\textsc{id}) \,,\, \sigma_{\underline{\tau_a}}^{\text{in}}(\textsc{sqn}_{\text{U}}^{\nu_\tau(\textsc{id})})\rangle\}_{\text{pk}_{\text{N}}}^{\text{n}_{\text{e}}^{j_a}}\right) \in \text{reveal}_{\tau_0}$$

$$\left(\text{Mac}_{\text{k}_{\text{m}}^{\textsc{id}}}^{1}(\langle\{\langle \textsc{id} \,,\, \sigma_{\tau_a}^{\text{in}}(\textsc{sqn}_{\text{U}}^{\textsc{id}})\rangle\}_{\text{pk}_{\text{N}}}^{\text{n}_{\text{e}}^{j_a}} \,,\, g(\phi_{\tau_a}^{\text{in}})\rangle), \text{Mac}_{\text{k}_{\text{m}}^{\nu_\tau(\textsc{id})}}^{1}(\langle\{\langle \nu_\tau(\textsc{id}) \,,\, \sigma_{\underline{\tau_a}}^{\text{in}}(\textsc{sqn}_{\text{U}}^{\nu_\tau(\textsc{id})})\rangle\}_{\text{pk}_{\text{N}}}^{\text{n}_{\text{e}}^{j_a}} \,,\, g(\phi_{\underline{\tau_a}}^{\text{in}})\rangle)\right) \in$$

$$\text{reveal}_{\tau_0}$$

It is straightforward to show that we have a derivation of:

$$\frac{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \lambda^{\tau'}_{\tau_a} \ \sim\ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \lambda^{\underline{\tau'}}_{\underline{\tau_a}}}\ \text{Simp}$$

Using (104) and (105), and combining the derivation above with the derivation in (89), we can build the following derivation:

$$\dfrac{\dfrac{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0},}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{f} \land \neg \bigvee_{\substack{\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1) \\ \tau' = \_, \textsc{pn}(j', 1) \\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \text{f} \land \lambda^{\tau'}_{\tau_a} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \underline{\text{f}} \land \neg \bigvee_{\substack{\tau_a = \_, \textsc{pu}_{\textsc{id}}(j_a, 1) \\ \tau' = \_, \textsc{pn}(j', 1) \\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \underline{\text{f}} \land \lambda^{\underline{\tau'}}_{\underline{\tau_a}}}\ (\text{Dup}, \text{FA})^*}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{f} \land \sigma^{\text{in}}_{\tau}(\text{session}^{\textsc{id}}_{\textsc{n}}) = \text{n}^j \ \sim\ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \underline{\text{f}} \land \sigma^{\text{in}}_{\underline{\tau}}(\text{session}^{\nu_\tau(\textsc{id})}_{\textsc{n}}) = \text{n}^j}\ R \tag{106}$$

We know that:

$$\begin{aligned}
[\text{f}]\text{sync-diff}^{\textsc{id}}_{\tau} \ &= \ \text{if f} \land \sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}}) \land \sigma^{\text{in}}_{\tau}(\text{session}^{\textsc{id}}_{\textsc{n}}) = \text{n}^j \text{ then suc}(\text{sync-diff}^{\textsc{id}}_{\tau_0}) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{else sync-diff}^{\textsc{id}}_{\tau_0} \\
[\underline{\text{f}}]\text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau}} \ &= \ \text{if } \underline{\text{f}} \land \sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}}) \land \sigma^{\text{in}}_{\underline{\tau}}(\text{session}^{\nu_\tau(\textsc{id})}_{\textsc{n}}) = \text{n}^j \text{ then suc}(\text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau_0}}) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{else sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau_0}}
\end{aligned}$$

Hence, using (106) and the fact that:

$$\Big(\sigma^{\text{in}}_{\tau}(\text{sync}^{\textsc{id}}_{\textsc{u}}), \sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\textsc{id})}_{\textsc{u}})\Big) \in \text{reveal}_{\tau_0} \qquad\qquad \Big(\text{sync-diff}^{\textsc{id}}_{\tau_0}, \text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau_0}}\Big) \in \text{reveal}_{\tau_0}$$

We have a derivation of:

$$\frac{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, [\text{f}]\text{sync-diff}^{\textsc{id}}_{\tau} \ \sim\ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, [\underline{\text{f}}]\text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau}}}\ \text{Simp} \tag{107}$$

Part 5 Using **(StrEqu3)**, we know that:

$$\text{accept}^{\textsc{id}}_{\tau} \quad \leftrightarrow \quad \bigvee_{\substack{\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1) \\ \tau_1 = \_, \textsc{tn}(j, 0) \\ \tau_2 = \_, \textsc{tu}_{\textsc{id}}(j_i, 0) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i}} \text{full-tr}^{\text{n}:\tau_1, \tau}_{\text{u}:\tau_2, \tau_i}$$

We split between the cases $\tau_i \prec_\tau \tau_{\textsc{ns}}$ and $\tau_i \not\prec_\tau \tau_{\textsc{ns}}$:

$$\leftrightarrow \quad \bigvee_{\substack{\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1) \\ \tau_1 = \_, \textsc{tn}(j, 0) \\ \tau_2 = \_, \textsc{tu}_{\textsc{id}}(j_i, 0) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i \prec_\tau \tau_{\textsc{ns}}}} \text{full-tr}^{\text{n}:\tau_1, \tau}_{\text{u}:\tau_2, \tau_i} \ \lor \ \bigvee_{\substack{\tau_i = \_, \textsc{tu}_{\textsc{id}}(j_i, 1) \\ \tau_1 = \_, \textsc{tn}(j, 0) \\ \tau_2 = \_, \textsc{tu}_{\textsc{id}}(j_i, 0) \\ \tau_{\textsc{ns}} \prec_\tau \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i}} \text{full-tr}^{\text{n}:\tau_1, \tau}_{\text{u}:\tau_2, \tau_i}$$

If $\tau_i \prec_\tau \tau_{\textsc{ns}}$ then $\nu_{\tau_2}(\textsc{id}) = \nu_{\tau_i}(\textsc{id}) \neq \nu_\tau(\textsc{id})$, and if $\tau_i \not\prec_\tau \tau_{\textsc{ns}}$ then $\nu_{\tau_2}(\textsc{id}) = \nu_{\tau_i}(\textsc{id}) = \nu_\tau(\textsc{id})$. It follows, using **(StrEqu3)** on $\underline{\tau}$, that:

$$\bigvee_{\substack{\underline{\textsc{id}} \in \text{copies-id}_{C}(\textsc{id}) \\ \underline{\textsc{id}} \neq \nu_\tau(\textsc{id})}} \text{accept}^{\underline{\textsc{id}}}_{\underline{\tau}} \ \leftrightarrow \ \bigvee_{\substack{\tau_i = \_, \textsc{tu}_{\underline{\textsc{id}}}(j_i, 1) \\ \tau_1 = \_, \textsc{tn}(j, 0) \\ \tau_2 = \_, \textsc{tu}_{\underline{\textsc{id}}}(j_i, 0) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i \prec_\tau \tau_{\textsc{ns}}}} \text{full-tr}^{\text{n}:\underline{\tau_1}, \underline{\tau}}_{\text{u}:\underline{\tau_2}, \underline{\tau_i}} \qquad \text{accept}^{\nu_\tau(\textsc{id})}_{\underline{\tau}} \ \leftrightarrow \ \bigvee_{\substack{\tau_i = \_, \textsc{tu}_{\nu_\tau(\textsc{id})}(j_i, 1) \\ \tau_1 = \_, \textsc{tn}(j, 0) \\ \tau_2 = \_, \textsc{tu}_{\nu_\tau(\textsc{id})}(j_i, 0) \\ \tau_{\textsc{ns}} \prec_\tau \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i}} \text{full-tr}^{\text{n}:\underline{\tau_1}, \underline{\tau}}_{\text{u}:\underline{\tau_2}, \underline{\tau_i}}$$

Hence, using (92) if $\tau_i \prec_\tau \textsc{ns}_{\textsc{id}}$, and (107) if $\tau_i \not\prec_\tau \textsc{ns}_{\textsc{id}}$, we can build the following derivation:

$$\frac{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{sync-diff}^{\textsc{id}}_{\tau} \ \sim\ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{sync-diff}^{\nu_\tau(\textsc{id})}_{\underline{\tau}}}\ \text{Simp}$$

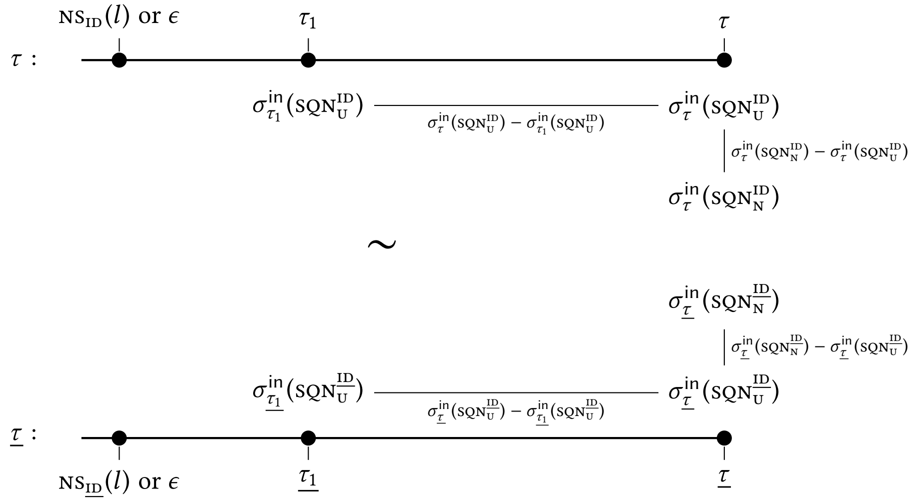

$\textsc{ns}_{\textsc{id}}(l)$ or ϵ
τ_1
τ
τ :
$\sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$\sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) - \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$\sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$\sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) - \sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})$
$\sigma^{\mathsf{in}}_{\tau}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}})$
$\sim$
$\sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{n}})$
$\sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{n}}) - \sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}})$
$\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}})$
$\sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}}) - \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}})$
$\sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}})$
$\underline{\tau}$:
$\textsc{ns}_{\underline{\textsc{id}}}(l)$ or ϵ
$\underline{\tau_1}$
$\underline{\tau}$

Fig. 30. First Graphical Representation of the Proof of **(Der1)**

Part 6 Observe that:

$$\mathsf{net\text{-}e\text{-}auth}_{\tau}(\textsc{id}, j) \;\leftrightarrow\; \mathsf{accept}^{\textsc{id}}_{\tau} \qquad \underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\textsc{id}, j) \;\leftrightarrow\; \bigvee_{\underline{\textsc{id}} \in \mathsf{copies\text{-}id}_{C}(\textsc{id})} \mathsf{accept}^{\underline{\textsc{id}}}_{\underline{\tau}}$$

We therefore easily obtain the derivation:

$$\frac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{net\text{-}e\text{-}auth}_{\tau}(\textsc{id}, j) \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\textsc{id}, j)}$$

Finally, we know that:

$$\bigvee\nolimits_{\textsc{id} \in \mathcal{S}_{\mathsf{id}}} \mathsf{accept}^{\textsc{id}}_{\tau} \;\leftrightarrow\; \bigvee\nolimits_{\textsc{id} \in \mathcal{S}_{\mathsf{id}}} \mathsf{accept}^{\textsc{id}}_{\tau}\mathsf{net\text{-}e\text{-}auth}_{\tau}(\textsc{id}, j)$$

$$\bigvee\nolimits_{\textsc{id} \in \mathcal{S}_{\mathsf{id}}, \underline{\textsc{id}} \in \mathsf{copies\text{-}id}_{C}(\textsc{id})} \mathsf{accept}^{\underline{\textsc{id}}}_{\underline{\tau}} \;\leftrightarrow\; \bigvee\nolimits_{\textsc{id} \in \mathcal{S}_{\mathsf{id}}} \underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\textsc{id}, j)$$

It follows that:

$$\cfrac{\cfrac{\cfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \bigvee_{\textsc{id} \in \mathcal{S}_{\mathsf{id}}} \mathsf{net\text{-}e\text{-}auth}^{\textsc{id}}_{\tau} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \bigvee_{\textsc{id} \in iddom} \underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\textsc{id}, j)}\;\mathsf{Simp}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \bigvee_{\textsc{id} \in \mathcal{S}_{\mathsf{id}}} \mathsf{accept}^{\textsc{id}}_{\tau} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \bigvee_{\textsc{id} \in \mathcal{S}_{\mathsf{id}}, \underline{\textsc{id}} \in \mathsf{copies\text{-}id}_{C}(\textsc{id})} \mathsf{accept}^{\underline{\textsc{id}}}_{\underline{\tau}}}\;R}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_{\tau} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}}}\;\mathsf{FA}^{*}$$

H PROOF OF PROPOSITION 29

Proof of **(Der1)**. We have two cases:

- either there exists l such that $\textsc{ns}_{\textsc{id}}(l) \prec \tau$ and $\textsc{ns}_{\textsc{id}}(l) \not\prec_{\tau} \textsc{ns}_{\textsc{id}}(\_)$. In that case we have $\textsc{ns}_{\textsc{id}}(l) \prec_{\tau} \tau_1$.
- or for every i, $\textsc{ns}_{\textsc{id}}(i) \not\prec_{\tau} \tau_1$.

Let $\underline{\textsc{id}} = \nu_\tau(\textsc{id})$. We summarize this graphically in Figure 30. In both case, for every $\tau_1 \preceq \tau' \prec \tau$:

$$\Big(\sigma_{\tau'}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}), \sigma_{\underline{\tau}'}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\Big) \in \mathsf{reveal}_{\tau_0}$$

$$\Big([\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})]\big(\sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) - \sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\big), [\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}})]\big(\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\big)\Big) \in \mathsf{reveal}_{\tau_0}$$

We know that:

$$\sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \ = \ \sigma_{\tau_0}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \ = \ \sum_{\tau_1 \preceq \tau'} \sigma_{\tau'}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})$$

And:

$$\begin{aligned} & \sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \\ \leftrightarrow \quad & \sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \Big(\big(\sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\big) + [\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})]\big(\sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) - \sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\big) < 0\Big) \end{aligned}$$

Similarly:

$$\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) = \sum_{\tau_1 \preceq \tau'} \sigma_{\underline{\tau}'}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})$$

And:

$$\begin{aligned} & \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) \wedge \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\underline{\mathrm{ID}}}) < \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) \\ \leftrightarrow \quad & \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) \wedge \Big(\Big(\big(\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\big) + [\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}})]\big(\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\big)\Big) < 0\Big) \end{aligned}$$

Putting everything together, we get:

$$\frac{\dfrac{\mathsf{l\text{-}reveal}_{\tau_0} \ \sim \ \mathsf{r\text{-}reveal}_{\tau_0}}{\begin{array}{c} \mathsf{l\text{-}reveal}_{\tau_0}, \sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}), [\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})]\big(\sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) - \sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\big), \big(\sigma_{\tau'}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}),\big)_{\tau_1 \preceq \tau'} \\ \sim \ \mathsf{r\text{-}reveal}_{\tau_0}, \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}}), [\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}})]\big(\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\big), \big(\sigma_{\underline{\tau}'}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}),\big)_{\tau_1 \preceq \tau'} \end{array}}\ \mathsf{Dup}^*}{\begin{array}{c} \mathsf{l\text{-}reveal}_{\tau_0}, \sigma_{\tau_1}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \\ \sim \ \mathsf{r\text{-}reveal}_{\tau_0}, \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) \wedge \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\underline{\mathrm{ID}}}) < \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) \end{array}}\ \mathsf{Simp}$$

The derivation of (29) is very similar. We omit the details, and only give the graphical representation of its proof in Figure 31. ■

Proof of **(Der3)**. Since τ is valid, we know that for every τ', if $\tau_2 \prec_\tau \tau'$ then $\tau' \neq \textsc{ns}_{\textsc{id}}(\_)$. It follows that $\underline{\tau_2} = \_, \textsc{tu}_{\nu_\tau(\textsc{id})}(j, 0)$ and $\underline{\tau} = \_, \textsc{tu}_{\nu_\tau(\textsc{id})}(j, 1)$. The fact that $\underline{\tau_2} \prec_{\underline{\tau}} \underline{\tau_1}$ is then straightforward. Letting $\underline{\textsc{id}} = \nu_\tau(\textsc{id})$, we can then check that $\mathsf{part\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1}$ and $\mathsf{part\text{-}tr}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}}$ are as described in Figure 32.

We have two cases. **Case 1** Assume that for all $\tau' \prec_\tau \tau_1$ such that $\tau' \not\preceq_\tau \textsc{ns}_{\textsc{id}}(\_)$ we have $\tau' \neq \_, \textsc{fu}_{\textsc{id}}(\_)$.

Then we know that for all $\underline{\tau}' <_{\underline{\tau}} \underline{\tau_1}$ such that $\underline{\tau}' \not\preceq_{\underline{\tau}} \textsc{ns}_{\nu_\tau(\textsc{id})}(\_)$ we have $\underline{\tau}' \neq \_, \textsc{fu}_{\nu_\tau(\textsc{id})}(\_)$. Therefore using **(B7)** twice we get:

$$\mathsf{part\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \ \to \ \mathsf{false} \qquad\qquad \mathsf{part\text{-}tr}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} \ \to \ \mathsf{false}$$

Therefore we have a trivial derivation:

$$\frac{\dfrac{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{false} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{false}}\ \mathsf{FA}}{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{part\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \ \sim \ \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{part\text{-}tr}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}}}\ R \tag{108}$$

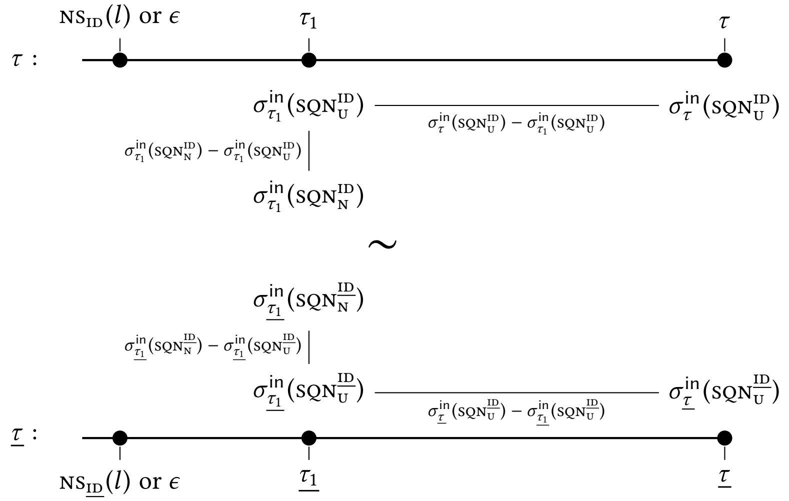

$\mathrm{NS}_{\mathrm{ID}}(l)$ or ϵ
τ_1
τ
τ :
$\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$
$\sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) - \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$
$\sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$
$\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) - \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$
$\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$
$\sim$
$\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{N}})$
$\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{N}}) - \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{U}})$
$\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{U}})$
$\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) - \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{U}})$
$\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{U}})$
$\underline{\tau}$:
$\mathrm{NS}_{\underline{\mathrm{ID}}}(l)$ or ϵ
$\underline{\tau_1}$
$\underline{\tau}$

Fig. 31. Second Graphical Representation for the Proof of **(Der1)**

$$\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \equiv \left(\begin{array}{l} \quad \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_1} \ \wedge\ \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \underline{\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f}_{\mathsf{k}^{\mathrm{ID}}}(\mathsf{n}^{j_1})} \\ \wedge\ \pi_3(g(\phi^{\mathsf{in}}_{\tau})) = \underline{\mathsf{Mac}^3_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}, \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}), \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})\rangle)} \\ \wedge\ g(\phi^{\mathsf{in}}_{\tau_1}) = \underline{\sigma^{\mathsf{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})} \ \wedge\ \underline{\sigma^{\mathsf{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}})} \ \wedge\ \underline{\sigma^{\mathsf{in}}_{\tau_2}(\mathsf{valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}})} \\ \wedge\ \underline{\mathsf{range}(\sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}))} \end{array}\right)$$

$$\mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}} \equiv \left(\begin{array}{l} \quad \pi_1(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \mathsf{n}^{j_1} \ \wedge\ \pi_2(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \underline{\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{N}}) \oplus \mathsf{f}_{\mathsf{k}^{\underline{\mathrm{ID}}}}(\mathsf{n}^{j_1})} \\ \wedge\ \pi_3(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \underline{\mathsf{Mac}^3_{\mathsf{k}^{\underline{\mathrm{ID}}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}, \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{N}}), \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{U}})\rangle)} \\ \wedge\ g(\phi^{\mathsf{in}}_{\underline{\tau_1}}) = \underline{\sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{U}})} \ \wedge\ \underline{\sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{N}})} \ \wedge\ \underline{\sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathsf{valid\text{-}guti}^{\underline{\mathrm{ID}}}_{\mathrm{U}})} \\ \wedge\ \underline{\mathsf{range}(\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{N}}))} \end{array}\right)$$

Fig. 32. Terms $\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}$ and $\mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}$ in the Proof of **(Der3)**.

Case 2 First, we are going to introduce various instants corresponding to previous sessions of the protocol. Eventually, we will be in the situation depicted in Figure 33.

Assume that there exists $\tau_3 = \_, \mathrm{FU}_{\mathrm{ID}}(j_0)$ such that $\tau_3 \prec_\tau \tau_1$, $\tau_3 \not\prec_\tau \mathrm{NS}_{\mathrm{ID}}(\_)$ and $\tau_3 \not\prec_\tau \mathrm{FU}_{\mathrm{ID}}(\_)$. Then $\underline{\tau_3} = \_, \mathrm{FU}_{\nu_\tau(\mathrm{ID})}(\_)$, $\underline{\tau_3} \prec_{\underline{\tau}} \underline{\tau_1}$, $\underline{\tau_3} \not\prec_{\underline{\tau}} \mathrm{NS}_{\nu_\tau(\mathrm{ID})}(\_)$ and $\underline{\tau_3} \not\prec_{\underline{\tau}} \mathrm{FU}_{\nu_\tau(\mathrm{ID})}(\_)$.

Assume that $j_0 = j$, then we know that $\tau \prec_\tau \tau_3$, which is absurd. Therefore $j_0 \neq j$. Using the validity of τ, we know that τ_3 cannot occur between $\tau_2 = \_, \textsc{tu}_{\textsc{id}}(j, 0)$ and $\tau = \_, \textsc{tu}_{\textsc{id}}(j, 0)$. Hence $\tau_3 \prec_\tau \tau_2$.

Let $\tau_{\textsc{ns}}$ be the latest $\textsc{ns}_{\textsc{id}}(\_)$, if it exists, or ϵ otherwise: $\tau_{\textsc{ns}} = \_, \textsc{ns}_{\textsc{id}}(\_)$ or ϵ and $\tau_{\textsc{ns}} \not\prec_\tau \textsc{ns}_{\textsc{id}}(\_)$. Let τ_x be $\_, \textsc{tu}_{\textsc{id}}(j_0, 0)$ or $\_, \textsc{pu}_{\textsc{id}}(j_0, 1)$ be the beginning of the *UE* session associated to τ_3. We know that $\tau_{\textsc{ns}} \prec_\tau \tau_x \prec_\tau \tau_3$.

We know that $\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \sigma^{\text{in}}_{\tau_2}(\text{valid-guti}^{\textsc{id}}_{\textsc{u}})$. As $\tau_3 \not\prec_\tau \textsc{fu}_{\textsc{id}}(\_)$, we know that there are no $\textsc{fu}_{\textsc{id}}(\_)$ action between τ_3 and τ_2. If there exists an action by user $\textsc{id}$ between τ_3 and τ_2, then we have either $\tau_3 \prec_\tau \textsc{pu}_{\textsc{id}}(\_, 1) \prec_\tau \tau_2$ or $\tau_3 \prec_\tau \textsc{tu}_{\textsc{id}}(\_, 0) \prec_\tau \tau_2$. In both case, $\text{valid-guti}^{\textsc{id}}_{\textsc{u}}$ is set to false, and cannot be set back to something else without a $\textsc{fu}_{\textsc{id}}(\_)$ action. It follows that if there exists a user action between τ_3 and τ_2 then $\neg\sigma^{\text{in}}_{\tau_2}(\text{valid-guti}^{\textsc{id}}_{\textsc{u}})$. Using the same reasoning we have $\neg\sigma^{\text{in}}_{\underline{\tau_2}}(\text{valid-guti}^{\underline{\textsc{id}}}_{\textsc{u}})$ if there exists a user action between τ_3 and τ_2. Hence in that case the derivation (108) works.

By consequence we now assume that:

$$\{\_, \textsc{tu}_{\textsc{id}}(\_), \_, \textsc{pu}_{\textsc{id}}(\_, \_), \textsc{fu}_{\textsc{id}}(\_)\} \cap \{\tau' \mid \tau_3 \prec_\tau \tau' \prec_\tau \tau_2\} = \emptyset$$

It follows that $\neg\text{accept}^{\textsc{id}}_{\tau_3} \rightarrow \neg\sigma^{\text{in}}_{\tau_2}(\text{valid-guti}^{\textsc{id}}_{\textsc{u}})$, hence $\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \text{accept}^{\textsc{id}}_{\tau_3}$. Also, we deduce that $\sigma_{\tau_3}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) \equiv \sigma^{\text{in}}_{\tau_2}(\textsc{guti}^{\textsc{id}}_{\textsc{u}})$. Applying **(StrEqu1)**, we know that:

$$\text{accept}^{\textsc{id}}_{\tau_3} \quad \leftrightarrow \quad \bigvee_{\tau_x \prec_\tau \tau_a = \_, \textsc{fn}(j_a) \prec_\tau \tau_3} \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3}$$

Therefore:

$$\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \quad \leftrightarrow \quad \bigvee_{\tau_x \prec_\tau \tau_a = \_, \textsc{fn}(j_a) \prec_\tau \tau_3} \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \wedge \text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau}$$

Similarly, we show that $\sigma_{\underline{\tau_3}}(\textsc{guti}^{\underline{\textsc{id}}}_{\textsc{u}}) \equiv \sigma^{\text{in}}_{\underline{\tau_2}}(\textsc{guti}^{\underline{\textsc{id}}}_{\textsc{u}})$ and that:

$$\text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}} \quad \leftrightarrow \quad \bigvee_{\tau_x \prec_\tau \tau_a = \_, \textsc{fn}(j_a) \prec_\tau \tau_3} \text{fu-tr}^{\text{n}:\underline{\tau_a}}_{\text{u}:\underline{\tau_3}} \wedge \text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}}$$

We can start building the wanted derivation:

$$\dfrac{\dfrac{\begin{array}{c}\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \left(\text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \wedge \text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau}\right)_{\tau_x \prec_\tau \tau_a = \_, \textsc{fn}(j_a) \prec_\tau \tau_3} \\ \sim\ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \left(\text{fu-tr}^{\text{n}:\underline{\tau_a}}_{\text{u}:\underline{\tau_3}} \wedge \text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}}\right)_{\tau_x \prec_\tau \tau_a = \_, \textsc{fn}(j_a) \prec_\tau \tau_3}\end{array}}{\begin{array}{c}\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \displaystyle\bigvee_{\tau_x \prec_\tau \tau_a = \_, \textsc{fn}(j_a) \prec_\tau \tau_3} \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \wedge \text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \\ \sim\ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \displaystyle\bigvee_{\tau_x \prec_\tau \tau_a = \_, \textsc{fn}(j_a) \prec_\tau \tau_3} \text{fu-tr}^{\text{n}:\underline{\tau_a}}_{\text{u}:\underline{\tau_3}} \wedge \text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}}\end{array}}\ \text{FA}^*}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \ \sim\ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}}}\ R$$

Let $\tau_a = \_, \textsc{fn}(j_a)$ be such that $\tau_x \prec_\tau \tau_a \prec_\tau \tau_3$. Let τ_b be $\_, \textsc{tn}(j_a, 1)$ or $\_, \textsc{pn}(j_a, 1)$ such that $\tau_b \prec_\tau \tau_a$. To conclude, we just need to build a derivation of:

$$\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \wedge \text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \ \sim\ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{fu-tr}^{\text{n}:\underline{\tau_a}}_{\text{u}:\underline{\tau_3}} \wedge \text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}}$$

The proof consist in rewriting $\text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \wedge \text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau}$ and $\text{fu-tr}^{\text{n}:\underline{\tau_a}}_{\text{u}:\underline{\tau_3}} \wedge \text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}}$ such that they can be decomposed (using FA) into corresponding parts appearing in reveal_{τ_0}. We do this piece by piece: the waved underlined part first, the dotted underlined and the dashed underlined part. We represent graphically the protocols executions in Figure 33.

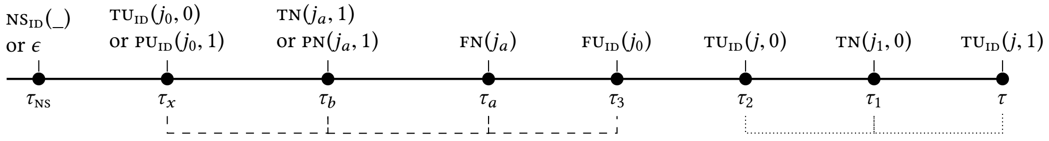

$\mathrm{NS}_{\mathrm{ID}}(\_)$ or ϵ
$\mathrm{TU}_{\mathrm{ID}}(j_0, 0)$ or $\mathrm{PU}_{\mathrm{ID}}(j_0, 1)$
$\mathrm{TN}(j_a, 1)$ or $\mathrm{PN}(j_a, 1)$
$\mathrm{FN}(j_a)$
$\mathrm{FU}_{\mathrm{ID}}(j_0)$
$\mathrm{TU}_{\mathrm{ID}}(j, 0)$
$\mathrm{TN}(j_1, 0)$
$\mathrm{TU}_{\mathrm{ID}}(j, 1)$
τ_{NS}
τ_x
τ_b
τ_a
τ_3
τ_2
τ_1
τ

Fig. 33. Graphical Representation of the Protocol Executions

Part 1 (Waves) We are going to give a derivation of:

$$\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\underline{\tau_3}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}})$$

Recall that $\sigma_{\tau_3}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) \equiv \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})$ and $\sigma_{\underline{\tau_3}}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) \equiv \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})$. Hence it is sufficient to prove that:

$$\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\underline{\tau_3}} \wedge \sigma_{\underline{\tau_3}}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}})$$

We know that:

$$[\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3}]\sigma_{\tau_3}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = [\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3}]\mathrm{GUTI}^{j_a}$$

Hence:

$$\left(\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}})\right) \leftrightarrow \left(\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) = \mathrm{GUTI}^{j_a}\right)$$

Intuitively, the only way we can have $\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) = \mathrm{GUTI}^{j_a}$ is:

- if the SUPI or GUTI network session j_a accepts with the increasing sequence number condition.
- and if $\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}})$ was not over-written between τ_b and τ_1.

It is actually straightforward to show by induction that:

$$\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathrm{GUTI}^{j_a} \leftrightarrow \left(\neg\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_b} \vee \bigvee_{\substack{\tau'=\_,\mathrm{TN}(j',1) \\ \text{or } \tau'=\_,\mathrm{PN}(j',1) \\ \tau_b <_\tau \tau' <_\tau \tau_1}} \mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau'} \vee \bigvee_{\substack{\tau'=\_,\mathrm{TN}(j',0) \\ \tau_b <_\tau \tau' <_\tau \tau_1}} \mathsf{accept}^{\mathrm{ID}}_{\tau'}\right)$$

Hence:

$$\begin{aligned}
& \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \\
\leftrightarrow\ & \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_b} \wedge \bigwedge_{\substack{\tau'=\_,\mathrm{TN}(j',1) \\ \text{or } \tau'=\_,\mathrm{PN}(j',1) \\ \tau_b <_\tau \tau' <_\tau \tau_1}} \neg\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau'} \wedge \bigwedge_{\substack{\tau'=\_,\mathrm{TN}(j',0) \\ \tau_b <_\tau \tau' <_\tau \tau_1}} \neg\mathsf{accept}^{\mathrm{ID}}_{\tau'} \\
\leftrightarrow\ & \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_b} \wedge \bigwedge_{\substack{\tau'=\_,\mathrm{TN}(j',1) \\ \text{or } \tau'=\_,\mathrm{PN}(j',1) \\ \tau_b <_\tau \tau' <_\tau \tau_1}} \neg\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau'} \wedge \bigwedge_{\substack{\tau'=\_,\mathrm{TN}(j',0) \\ \tau_b <_\tau \tau' <_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\tau'}) \neq \mathrm{GUTI}^{j_a}
\end{aligned}$$

For every $\tau_n = \_, \mathrm{TN}(\_, 1)$ or $\_, \mathrm{PN}(\_, 1)$, we know that $\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}$ is incremented at τ_n if and only if $\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_n}$ is true. Therefore:

$$\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_n} \leftrightarrow \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) < \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$$

Using the fact that $\sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$, we can rewrite this as:

$$\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_n} \leftrightarrow \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) - \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) < \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) - \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$$

Using this remark we can show that:

$$\begin{aligned}
&\text{fu-tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) = \sigma^{\mathsf{in}}_{\tau_1}(\textsc{guti}^{\textsc{id}}_{\textsc{n}})\\
\leftrightarrow\ &\text{fu-tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \begin{pmatrix} \sigma^{\mathsf{in}}_{\tau_b}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) - \sigma^{\mathsf{in}}_{\tau_b}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\\ < \ \sigma_{\tau_b}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) - \sigma_{\tau_b}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\end{pmatrix} \wedge \begin{pmatrix} \sigma_{\tau_b}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) - \sigma_{\tau_b}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\\ = \ \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{n}}) - \sigma^{\mathsf{in}}_{\tau_1}(\textsc{sqn}^{\textsc{id}}_{\textsc{u}})\end{pmatrix} \wedge \bigwedge_{\substack{\tau'=\_,\textsc{tn}(j',0)\\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\tau'}) \neq \textsc{guti}^{j_a}
\end{aligned}$$

Doing exactly the same reasoning, we show that:

$$\begin{aligned}
&\text{fu-tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\underline{\tau_3}} \wedge \sigma_{\underline{\tau_3}}(\textsc{guti}^{\underline{\textsc{id}}}_{\textsc{u}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{guti}^{\underline{\textsc{id}}}_{\textsc{n}})\\
\leftrightarrow\ &\text{fu-tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\underline{\tau_3}} \wedge \begin{pmatrix} \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{n}}) - \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}})\\ < \ \sigma_{\underline{\tau_b}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{n}}) - \sigma_{\underline{\tau_b}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}})\end{pmatrix} \wedge \begin{pmatrix} \sigma_{\underline{\tau_b}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{n}}) - \sigma_{\underline{\tau_b}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}})\\ = \ \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{n}}) - \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}})\end{pmatrix} \wedge \bigwedge_{\substack{\tau'=\_,\textsc{tn}(j',0)\\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\underline{\tau'}}) \neq \textsc{guti}^{j_a}
\end{aligned}$$

We introduce some notation that will be used later: for every action trace $\tau = \tau_0, \mathsf{ai}$ and identity $\textsc{id}$, we let $\text{sync-diff-in}^{\textsc{id}}_{\tau} \equiv \text{sync-diff}^{\textsc{id}}_{\tau_0}$.

We now split the proof in two, depending on whether $\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}})$ is true or false. Let $\psi \equiv \text{fu-tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma^{\mathsf{in}}_{\tau_2}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) = \sigma^{\mathsf{in}}_{\tau_1}(\textsc{guti}^{\textsc{id}}_{\textsc{n}})$ and $\underline{\psi} \equiv \text{fu-tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\underline{\tau_3}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\textsc{guti}^{\underline{\textsc{id}}}_{\textsc{u}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{guti}^{\underline{\textsc{id}}}_{\textsc{n}})$. Using the fact that:

$$\left(\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}), \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}})\right) \in \mathsf{reveal}_{\tau_0}$$

We can build the derivation:

$$\dfrac{\dfrac{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \psi, \neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \psi\\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}}) \wedge \underline{\psi}, \neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}}) \wedge \underline{\psi}\end{array}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}), \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \psi, \neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \psi\\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}}), \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}}) \wedge \underline{\psi}, \neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}}) \wedge \underline{\psi}\end{array}}\,\mathsf{Dup}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \psi\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{\psi}}\,\mathsf{Simp}$$

We now build a derivation of $\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \psi$ and of $\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \psi$:

- Using the fact that we have $\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}})$,we know that:

$$\begin{aligned}
&\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \text{fu-tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\textsc{guti}^{\textsc{id}}_{\textsc{u}}) = \sigma^{\mathsf{in}}_{\tau_1}(\textsc{guti}^{\textsc{id}}_{\textsc{n}})\\
\leftrightarrow\ &\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\textsc{id}}_{\textsc{u}}) \wedge \text{fu-tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \begin{pmatrix} \text{sync-diff-in}^{\textsc{id}}_{\tau_b}\\ < \ \text{sync-diff}^{\textsc{id}}_{\tau_b}\end{pmatrix} \wedge \begin{pmatrix} \text{sync-diff}^{\textsc{id}}_{\tau_b}\\ = \ \text{sync-diff-in}^{\textsc{id}}_{\tau_1}\end{pmatrix} \wedge \bigwedge_{\substack{\tau'=\_,\textsc{tn}(j',0)\\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\tau'}) \neq \textsc{guti}^{j_a}
\end{aligned}$$

Similarly we get that:

$$\begin{aligned}
&\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}}) \wedge \text{fu-tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\underline{\tau_3}} \wedge \sigma_{\underline{\tau_3}}(\textsc{guti}^{\underline{\textsc{id}}}_{\textsc{u}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\textsc{guti}^{\underline{\textsc{id}}}_{\textsc{n}})\\
\leftrightarrow\ &\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\textsc{id}}}_{\textsc{u}}) \wedge \text{fu-tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\underline{\tau_3}} \wedge \begin{pmatrix} \text{sync-diff-in}^{\underline{\textsc{id}}}_{\underline{\tau_b}}\\ < \ \text{sync-diff}^{\underline{\textsc{id}}}_{\underline{\tau_b}}\end{pmatrix} \wedge \begin{pmatrix} \text{sync-diff}^{\underline{\textsc{id}}}_{\underline{\tau_b}}\\ = \ \text{sync-diff-in}^{\underline{\textsc{id}}}_{\underline{\tau_1}}\end{pmatrix} \wedge \bigwedge_{\substack{\tau'=\_,\textsc{tn}(j',0)\\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\underline{\tau'}}) \neq \textsc{guti}^{j_a}
\end{aligned}$$

Moreover, we know that:

$$\left(\left(\textsc{guti}^{j_a}, \textsc{guti}^{j_a}\right) \in \mathsf{reveal}_{\tau_0}\right)_{\substack{\tau' = \_, \textsc{tn}(j',0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} \qquad \left(\mathsf{sync\text{-}diff\text{-}in}^{\mathrm{ID}}_{\tau_1}, \mathsf{sync\text{-}diff\text{-}in}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}}\right) \in \mathsf{reveal}_{\tau_0}$$

$$\left(\mathsf{sync\text{-}diff\text{-}in}^{\mathrm{ID}}_{\tau_b}, \mathsf{sync\text{-}diff\text{-}in}^{\underline{\mathrm{ID}}}_{\underline{\tau_b}}\right) \in \mathsf{reveal}_{\tau_0} \qquad \left(\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau_b}, \mathsf{sync\text{-}diff}^{\underline{\mathrm{ID}}}_{\underline{\tau_b}}\right) \in \mathsf{reveal}_{\tau_0}$$

$$\left(\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}})\right) \in \mathsf{reveal}_{\tau_0}$$

And using **(Der2)**, we know that we have a derivation of:

$$\frac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3}}\ \mathsf{Simp}$$

Using this, we can rewrite $\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi$ and $\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}$ as two terms that decompose, using FA, into matching part of reveal_{τ_0}. By consequence we can build the following derivation:

$$\frac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}\psi \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}}\ \mathsf{Simp} \tag{109}$$

- We now focus on the case where we have $\neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$.
First, assume that $\tau_b = \_, \textsc{tn}(j_a, 1)$. In that case, we know that $\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \rightarrow \mathsf{accept}^{\mathrm{ID}}_{\tau_b}$. Since $\mathsf{accept}^{\mathrm{ID}}_{\tau_b} \rightarrow \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$, we get that $(\neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi) \leftrightarrow \mathsf{false}$. Similarly $(\neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}) \leftrightarrow \mathsf{false}$. By consequence, we have a trivial derivation:

$$\frac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{false} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{false}}\ \mathsf{FA}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}}\ \mathsf{Simp}$$

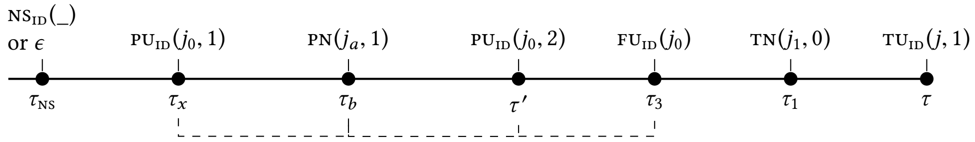
Now assume that $\tau_b = \_, \textsc{pn}(j_a, 1)$. Since $\tau_3 = \_, \textsc{fu}_{\textsc{id}}(j_0) \prec \tau$, we know by validity of τ there there exists $\tau' = \_, \textsc{pu}_{\textsc{id}}(j_0, 2)$ or $\_, \textsc{tu}_{\textsc{id}}(j_0, 1)$ such that $\tau' \prec_\tau \tau_3$. It is straightforward to check that if $\tau' = \_, \textsc{tu}_{\textsc{id}}(j_0, 1)$ then since $\tau_b = \_, \textsc{pn}(j_a, 1)$ we have $\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \leftrightarrow \mathsf{false}$ and $\mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \leftrightarrow \mathsf{false}$. Building the wanted derivation is then trivial.
Therefore assume that $\tau' = \_, \textsc{pu}_{\textsc{id}}(j_0, 2)$. Observe that $\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \rightarrow \mathsf{accept}^{\mathrm{ID}}_{\tau'}$. We have two cases:
  - Assume $\tau' \prec_\tau \tau_b$. Using **(Equ2)**, we know that:

$$\begin{aligned} \mathsf{accept}^{\mathrm{ID}}_{\tau'} \ &\rightarrow \bigvee_{\substack{\tau_n = \_, \textsc{pn}(j_n, 1) \\ \tau_x \prec_\tau \tau_n \prec_\tau \tau'}} \sigma^{\mathrm{ID}}_{\tau_x}(\mathsf{b\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^{j_n} \\ &\rightarrow \qquad \sigma^{\mathrm{ID}}_{\tau_x}(\mathsf{b\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}}) \neq \mathsf{n}^{j_a} && (\text{Since } \tau' \prec_\tau \tau_b) \end{aligned}$$

  Moreover:

$$\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \rightarrow \sigma^{\mathrm{ID}}_{\tau'}(\mathsf{e\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^{j_a} \rightarrow \sigma^{\mathrm{ID}}_{\tau_x}(\mathsf{b\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^{j_a}$$

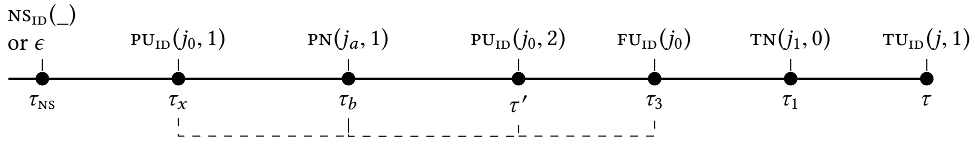
  Therefore $\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \rightarrow \mathsf{false}$. Similarly $\mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \rightarrow \mathsf{false}$. Hence we have a trivial derivation.
  - Assume $\tau_b \prec_\tau \tau'$. We summarize graphically the situation below:


$\textsc{ns}_{\textsc{id}}(\_)$ or ϵ
$\textsc{pu}_{\textsc{id}}(j_0, 1)$
$\textsc{pn}(j_a, 1)$
$\textsc{pu}_{\textsc{id}}(j_0, 2)$
$\textsc{fu}_{\textsc{id}}(j_0)$
$\textsc{tn}(j_1, 0)$
$\textsc{tu}_{\textsc{id}}(j, 1)$
$\tau_{\textsc{ns}}$
τ_x
τ_b
τ'
τ_3
τ_1
τ

First, since there are no ID actions between τ_b and τ', we know that $\neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \rightarrow \neg\sigma^{\mathsf{in}}_{\tau'}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$. Recall that $\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \rightarrow \mathsf{accept}^{\mathrm{ID}}_{\tau'}$. Using **(Equ2)**, it is simple to check that $\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \mathsf{accept}^{\mathrm{ID}}_{\tau'} \rightarrow \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_b}_{\mathsf{u}:\tau_x,\tau'}$. Therefore:

$$\begin{aligned}
\neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} &\rightarrow \neg\sigma^{\mathsf{in}}_{\tau'}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{accept}^{\mathrm{ID}}_{\tau'} \\
&\rightarrow \mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_b} \begin{array}{l} \wedge\ \sigma^{\mathsf{in}}_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma_{\tau_b}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \\ \wedge\ \sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \end{array} \qquad \text{(By } \textbf{(StrEqu4)}\text{)}
\end{aligned}$$

Using again the fact that there are no ID actions between τ_b and τ', we know that $\sigma^{\mathsf{in}}_{\tau_b}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \equiv \sigma^{\mathsf{in}}_{\tau'}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$. Moreover $\sigma^{\mathsf{in}}_{\tau'}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \equiv \sigma_{\tau'}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$, therefore $\sigma^{\mathsf{in}}_{\tau_b}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma_{\tau'}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$. Similarly, we know that $\sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \equiv \sigma^{\mathsf{in}}_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$. Summarizing:


$\textsc{ns}_{\textsc{id}}(\_)$ or ϵ
$\textsc{pu}_{\textsc{id}}(j_0, 1)$
$\textsc{pn}(j_a, 1)$
$\textsc{pu}_{\textsc{id}}(j_0, 2)$
$\textsc{fu}_{\textsc{id}}(j_0)$
$\textsc{tn}(j_1, 0)$
$\textsc{tu}_{\textsc{id}}(j, 1)$
$\tau_{\textsc{ns}}$
τ_x
τ_b
τ'
τ_3
τ_1
τ

$$\begin{tikzcd}
\sigma^{\mathsf{in}}_{\tau_b}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \arrow[r, dash, "="] & \sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \arrow[d, dash, "\parallel"] \\
\sigma^{\mathsf{in}}_{\tau_b}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \arrow[r, dash, "="] & \sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})
\end{tikzcd}$$

Therefore we get that:

$$\begin{aligned}
&\neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \\
\leftrightarrow\ &\neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \begin{pmatrix} & \sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) - \sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \\ = & \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) - \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \end{pmatrix} \wedge \bigwedge_{\substack{\tau' = \_,\textsc{tn}(j',0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\tau'}) \neq \mathrm{GUTI}^{j_a}
\end{aligned}$$

Besides, $\mathsf{accept}^{\mathrm{ID}}_{\tau'} \rightarrow \sigma_{\tau'}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$. Since $\tau' \prec_\tau \tau_1$ we know that $\sigma_{\tau'}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$. Hence:

$$\begin{aligned}
&\neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \\
\leftrightarrow\ &\neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau'} = \mathsf{sync\text{-}diff\text{-}in}^{\mathrm{ID}}_{\tau_1} \wedge \bigwedge_{\substack{\tau' = \_,\textsc{tn}(j',0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\tau'}) \neq \mathrm{GUTI}^{j_a}
\end{aligned}$$

Similarly:

$$\begin{aligned}
&\neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \sigma_{\underline{\tau_3}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{N}}) \\
\leftrightarrow\ &\neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \mathsf{sync\text{-}diff}^{\underline{\mathrm{ID}}}_{\underline{\tau'}} = \mathsf{sync\text{-}diff\text{-}in}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}} \wedge \bigwedge_{\substack{\tau' = \_,\textsc{tn}(j',0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\underline{\tau'}}) \neq \mathrm{GUTI}^{j_a}
\end{aligned}$$

And using **(Der2)**, we know that we have a derivation of:

$$\dfrac{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \sim \quad \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3}} \ \text{Simp}$$

Moreover, we know that:

$$\Big(\big(\mathrm{GUTI}^{j_a}, \mathrm{GUTI}^{j_a}\big) \in \text{reveal}_{\tau_0}\Big)_{\substack{\tau'=\_,\mathrm{TN}(j',0)\\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} \qquad \big(\text{sync-diff-in}^{\mathrm{ID}}_{\tau_1}, \text{sync-diff-in}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}}\big) \in \text{reveal}_{\tau_0}$$

$$\big(\text{sync-diff}^{\mathrm{ID}}_{\tau}, \text{sync-diff}^{\underline{\mathrm{ID}}}_{\underline{\tau'}}\big) \in \text{reveal}_{\tau_0} \qquad \Big(\sigma^{\text{in}}_{\tau_b}(\text{sync}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\text{in}}_{\underline{\tau_b}}(\text{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}})\Big) \in \text{reveal}_{\tau_0}$$

Similarly to what we did in (109), we can rewrite $\neg\sigma^{\text{in}}_{\tau_b}(\text{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi$ and $\neg\sigma^{\text{in}}_{\underline{\tau_b}}(\text{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}$ as two terms that decompose, using FA, into matching part of reveal_{τ_0}. By consequence we can build the following derivation:

$$\dfrac{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}\psi \ \sim \ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \neg\sigma^{\text{in}}_{\tau_b}(\text{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi \ \sim \ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \neg\sigma^{\text{in}}_{\underline{\tau_b}}(\text{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}} \ \text{Simp}$$

Part 2 (Dots)
Using **(StrEqu2)** we know that $\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \text{accept}^{\mathrm{ID}}_{\tau_1}$. Therefore, using **(A6)**, $\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \neg\text{accept}^{\mathrm{ID}'}_{\tau_1}$ for every $\mathrm{ID}' \neq \mathrm{ID}$. It follows that $\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow t_{\tau_1} = \text{msg}^{\mathrm{ID}}_{\tau_1}$, and therefore:

$$\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \ \rightarrow \ \pi_2(t_{\tau_1}) = \sigma^{\text{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f}_{\mathsf{k}^{\mathrm{ID}}}(\mathsf{n}^{j_1})$$

And:

$$\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \ \rightarrow \ \pi_3(t_{\tau_1}) = \text{Mac}^3_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}, \sigma^{\text{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}), \sigma^{\text{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})\rangle)$$

Since no action from agent ID occurs between τ_2 and τ_1, we know that $\sigma^{\text{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\text{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})$. Hence:

$$\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \ \rightarrow \ \pi_3(t_{\tau_1}) = \text{Mac}^3_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}, \sigma^{\text{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}), \sigma^{\text{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})\rangle)$$

Hence we can rewrite $\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau}$ as follows:

$$\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \ = \left(\begin{array}{l} \quad \pi_1(g(\phi^{\text{in}}_{\tau})) = \mathsf{n}^{j_1} \ \wedge \ \pi_2(g(\phi^{\text{in}}_{\tau})) = \underset{\cdots\cdots}{\pi_2(t_{\tau_1})} \ \wedge \ \pi_3(g(\phi^{\text{in}}_{\tau})) = \underset{\cdots\cdots}{\pi_3(t_{\tau_1})} \\ \wedge \ g(\phi^{\text{in}}_{\tau_1}) = \underset{-\,-\,-\,-}{\sigma^{\text{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})} \ \wedge \ \underset{\sim\sim\sim\sim}{\sigma^{\text{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\text{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}})} \ \wedge \ \underset{-\,-\,-\,-}{\sigma^{\text{in}}_{\tau_2}(\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}})} \\ \wedge \ \underset{-\,-\,-\,-\,-\,-}{\text{range}(\sigma^{\text{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\text{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}))} \end{array}\right)$$

By a similar reasoning we rewrite $\text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}}$ as follows:

$$\text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}} \ = \left(\begin{array}{l} \quad \pi_1(g(\phi^{\text{in}}_{\underline{\tau}})) = \mathsf{n}^{j_1} \ \wedge \ \pi_2(g(\phi^{\text{in}}_{\underline{\tau}})) = \underset{\cdots\cdots}{\pi_2(t_{\underline{\tau_1}})} \ \wedge \ \pi_3(g(\phi^{\text{in}}_{\underline{\tau}})) = \underset{\cdots\cdots}{\pi_3(t_{\underline{\tau_1}})} \\ \wedge \ g(\phi^{\text{in}}_{\underline{\tau_1}}) = \underset{-\,-\,-\,-}{\sigma^{\text{in}}_{\underline{\tau_2}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{U}})} \ \wedge \ \underset{\sim\sim\sim\sim}{\sigma^{\text{in}}_{\underline{\tau_2}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) = \sigma^{\text{in}}_{\underline{\tau_1}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{N}})} \ \wedge \ \underset{-\,-\,-\,-}{\sigma^{\text{in}}_{\underline{\tau_2}}(\text{valid-guti}^{\underline{\mathrm{ID}}}_{\mathrm{U}})} \\ \wedge \ \underset{-\,-\,-\,-\,-\,-}{\text{range}(\sigma^{\text{in}}_{\underline{\tau}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{U}}), \sigma^{\text{in}}_{\underline{\tau_1}}(\mathrm{SQN}^{\underline{\mathrm{ID}}}_{\mathrm{N}}))} \end{array}\right)$$

Part 3 (Dash) Since $\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \sigma^{\text{in}}_{\tau_2}(\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}})$ we know that:

$$\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \ \rightarrow \ \sigma^{\text{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) \ = \ \text{m-suci}^{\ \mathrm{ID}}_{\ \tau}$$

Besides, as $\sigma^{\text{in}}_{\tau_2}(\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}}) \rightarrow \sigma^{\text{in}}_{\tau_2}(\text{sync}^{\mathrm{ID}}_{\mathrm{U}})$, and since $\sigma^{\text{in}}_{\tau_2}(\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}}) \rightarrow \sigma^{\text{in}}_{\tau_1}(\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}})$ (because $\tau_2 \prec_\tau \tau_1$ and $\tau_2 \not\prec_\tau \textsc{ns}_{\mathrm{ID}}(\_)$), we know that:

$$\text{part-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow \Big(\text{range}(\sigma^{\text{in}}_{\tau}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\text{in}}_{\tau_1}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}})) \leftrightarrow \Big(\sigma^{\text{in}}_{\tau_1}(\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \sigma^{\text{in}}_{\tau}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\text{in}}_{\tau_1}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}})\Big)\Big)$$

Similarly we have:

$$\text{part-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}} \;\rightarrow\; \sigma^{\text{in}}_{\underline{\tau_2}}(\textsc{guti}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \;=\; \text{m-suci}^{\,\underline{\mathrm{ID}}}_{\underline{\tau}}$$

$$\text{part-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}} \rightarrow \Big(\text{range}(\sigma^{\text{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\mathrm{ID}}}_{\mathrm{U}}), \sigma^{\text{in}}_{\underline{\tau_1}}(\textsc{sqn}^{\underline{\mathrm{ID}}}_{\mathrm{N}})) \leftrightarrow \Big(\sigma^{\text{in}}_{\underline{\tau_1}}(\text{valid-guti}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \sigma^{\text{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) = \sigma^{\text{in}}_{\underline{\tau_1}}(\textsc{sqn}^{\underline{\mathrm{ID}}}_{\mathrm{N}})\Big)\Big)$$

Moreover:

$$\Big(\text{m-suci}^{\,\mathrm{ID}}_{\tau} \;\sim\; \text{m-suci}^{\,\underline{\mathrm{ID}}}_{\underline{\tau}}\Big) \in \text{reveal}_{\tau_0} \qquad \Big(\sigma^{\text{in}}_{\tau_2}(\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}}) \;\sim\; \sigma^{\text{in}}_{\underline{\tau_2}}(\text{valid-guti}^{\underline{\mathrm{ID}}}_{\mathrm{U}})\Big) \in \text{reveal}_{\tau_0}$$

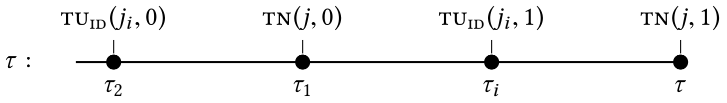
Finally, using **(Der1)**, we know that we have a derivation of:

$$\dfrac{\text{l-reveal}_{\tau_0} \;\sim\; \text{r-reveal}_{\tau_0}}{\begin{array}{c}\text{l-reveal}_{\tau_0}, \sigma^{\text{in}}_{\tau_1}(\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \sigma^{\text{in}}_{\tau}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\text{in}}_{\tau_1}(\textsc{sqn}^{\mathrm{ID}}_{\mathrm{N}}) \\ \sim\; \text{r-reveal}_{\tau_0}, \sigma^{\text{in}}_{\underline{\tau_1}}(\text{valid-guti}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \sigma^{\text{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) = \sigma^{\text{in}}_{\underline{\tau_1}}(\textsc{sqn}^{\underline{\mathrm{ID}}}_{\mathrm{N}})\end{array}}\;\text{Simp}$$

Part 4 (conclusion) To conclude, we combine the derivations of Part 1, Part 2 and Part 3. ■

Proof of **(Der4)**. Recall that:

$$\text{full-tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i} \;\equiv\; \text{part-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau_i} \wedge g(\phi^{\text{in}}_{\tau}) = \text{Mac}^4_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\mathsf{n}^j)$$



The fact that $\underline{\tau_2} = \_, \textsc{tu}_{\nu_{\tau_1}(\mathrm{ID})}(j_i, 0)$, $\underline{\tau_i} = \_, \textsc{tu}_{\nu_{\tau_1}(\mathrm{ID})}(j_i, 1)$ and $\underline{\tau_2} <_{\underline{\tau}} \underline{\tau_1} <_{\underline{\tau}} \underline{\tau_i}$ is straightforward from **(Der3)**. It is easy to check that:

$$\text{full-tr}^{\mathsf{n}:\underline{\tau_1},\underline{\tau}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau_i}} \;\equiv\; \text{part-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau_i}} \wedge g(\phi^{\text{in}}_{\underline{\tau}}) = \text{Mac}^4_{\mathsf{k}^{\nu_{\tau_1}(\mathrm{ID})}_{\mathsf{m}}}(\mathsf{n}^j)$$

Moreover, $(\text{Mac}^4_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\mathsf{n}^j), \text{Mac}^4_{\mathsf{k}^{\nu_{\tau_1}(\mathrm{ID})}_{\mathsf{m}}}(\mathsf{n}^j)) \in \text{reveal}_{\tau_0}$. By **(Der3)**, there exists a derivation using FA and Dup of:

$$\dfrac{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{part-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \sim \;\; \phi^{\text{in}}_{\tau}, \text{r-reveal}_{\tau_0}, \text{part-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\tau}}$$

It is therefore easy to built the wanted derivation using only FA and Dup. ■

Proof of **(Der2)**. We recall that:

$$\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \;\equiv\; \left(\begin{array}{l}\quad \text{inj-auth}_{\tau}(\textsc{id}, j_0) \wedge \sigma^{\text{in}}_{\tau}(\text{e-auth}^{j_0}_{\mathrm{N}}) \neq \text{UnknownId} \\ \wedge\; \pi_1(g(\phi^{\text{in}}_{\tau})) = \textsc{guti}^{j_0} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0}) \wedge\; \pi_2(g(\phi^{\text{in}}_{\tau})) = \text{Mac}^5_{\mathsf{k}_{\mathsf{m}}}(\langle \textsc{guti}^{j_0}\,,\, \mathsf{n}^{j_0}\rangle)\end{array}\right)$$

$$\text{fu-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau}} \;\equiv\; \left(\begin{array}{l}\quad \text{inj-auth}_{\underline{\tau}}(\nu_{\tau}(\textsc{id}), j_0) \wedge \sigma^{\text{in}}_{\underline{\tau}}(\text{e-auth}^{j_0}_{\mathrm{N}}) \neq \text{UnknownId} \\ \wedge\; \pi_1(g(\phi^{\text{in}}_{\underline{\tau}})) = \textsc{guti}^{j_0} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0}) \wedge\; \pi_2(g(\phi^{\text{in}}_{\underline{\tau}})) = \text{Mac}^5_{\mathsf{k}_{\mathsf{m}}}(\langle \textsc{guti}^{j_0}\,,\, \mathsf{n}^{j_0}\rangle)\end{array}\right)$$

Let $j_0 \in \mathbb{N}$, and τ_0 be such that $\tau = \tau_0, \mathsf{ai}$. It is straightforward to check that for any $n \in \mathbb{N}$:

$$\underbrace{\sigma_{\tau_0}(\text{e-auth}_{\mathrm{N}}^{j_0}) = \text{UnknownId}}_{\text{unk}} \;\leftrightarrow\; \bigwedge_{1\le i\le B} \neg\text{net-e-auth}_{\tau}(\mathrm{A}_i, j_0)$$

$$\underbrace{\sigma_{\underline{\tau_0}}(\text{e-auth}_{\mathrm{N}}^{j_0}) = \text{UnknownId}}_{\underline{\text{unk}}} \;\leftrightarrow\; \bigwedge_{1\le i\le B} \neg\underline{\text{net-e-auth}}_{\underline{\tau}}(\mathrm{A}_i, j_0)$$

Since for all $1 \le i \le B$:

$$(\text{net-e-auth}_{\tau}(\mathrm{A}_i, j_0) \sim \underline{\text{net-e-auth}}_{\underline{\tau}}(\mathrm{A}_i, j_0)) \in \text{reveal}_{\tau_0}$$

and since $\text{fu-tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \wedge \text{unk} \;\rightarrow\; \text{false}$ and $\text{fu-tr}_{\mathsf{u}:\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} \wedge \underline{\text{unk}} \;\rightarrow\; \text{false}$, we deduce that:

$$\dfrac{\dfrac{\dfrac{\phi_{\tau}^{\text{in}}, \text{l-reveal}_{\tau_0}, b_{j_i} \wedge \neg\text{unk} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \text{fu-tr}_{\mathsf{u}:\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} \wedge \neg\underline{\text{unk}}}{\phi_{\tau}^{\text{in}}, \text{l-reveal}_{\tau_0}, \text{unk}, \text{false}, \text{fu-tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \wedge \neg\text{unk} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \underline{\text{unk}}, \text{false}, \text{fu-tr}_{\mathsf{u}:\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} \wedge \neg\underline{\text{unk}}}\;\text{Dup}^*}{\begin{array}{c}\phi_{\tau}^{\text{in}}, \text{l-reveal}_{\tau_0}, \text{unk}, \text{fu-tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \wedge \text{unk}, \text{fu-tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \wedge \neg\text{unk}\\ \sim\phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \underline{\text{unk}}, \text{fu-tr}_{\mathsf{u}:\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} \wedge \underline{\text{unk}}, \text{fu-tr}_{\mathsf{u}:\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} \wedge \neg\underline{\text{unk}}\end{array}}\;R}{\phi_{\tau}^{\text{in}}, \text{l-reveal}_{\tau_0}, \text{fu-tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \text{fu-tr}_{\mathsf{u}:\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}}}\;R + \text{FA}^*$$

From the definitions, we get that:

$$\sigma_{\tau}^{\text{in}}(\text{b-auth}_{\mathrm{N}}^{j_0}) = \textsc{id} \;\rightarrow\; \left(\sigma_{\tau}^{\text{in}}(\text{e-auth}_{\mathrm{N}}^{j_0}) = \textsc{id} \vee \sigma_{\tau}^{\text{in}}(\text{e-auth}_{\mathrm{N}}^{j_0}) = \text{UnknownId}\right)$$

Therefore:

$$\text{fu-tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \wedge \neg\text{unk} \;\rightarrow\; \sigma_{\tau}^{\text{in}}(\text{e-auth}_{\mathrm{N}}^{j_0}) = \textsc{id} \;\rightarrow\; \text{net-e-auth}_{\tau}(\textsc{id}, j_0)$$

Moreover:

$$\text{net-e-auth}_{\tau}(\textsc{id}, j_0) \;\rightarrow\; \begin{pmatrix} \textsc{guti}^{j_0} \oplus \mathsf{f}_{\mathsf{k}}^{\mathsf{r}}(\mathsf{n}^{j_0}) = [\text{net-e-auth}_{\tau}(\textsc{id}, j_0)]\text{t-suci-}\oplus_{\tau}(\textsc{id}, j_0) \\ \wedge\ \text{Mac}_{\mathsf{k}_{\mathsf{m}}}^{5}(\langle \textsc{guti}^{j_0}\,,\ \mathsf{n}^{j_0}\rangle) = [\text{net-e-auth}_{\tau}(\textsc{id}, j_0)]\text{t-mac}_{\tau}(\textsc{id}, j_0) \end{pmatrix}$$

Using Proposition 24 on τ:

$$\text{inj-auth}_{\tau}(\textsc{id}, j_0) \;\leftrightarrow\; \mathsf{n}^{j_0} = \sigma_{\tau}^{\text{in}}(\text{e-auth}_{\mathrm{U}}^{\textsc{id}})$$

Using the observations above, we can rewrite $\text{fu-tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \wedge \neg\text{unk}$ as follows:

$$\text{fu-tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \wedge \neg\text{unk} \;=\; \begin{pmatrix} \mathsf{n}^{j_0} = \sigma_{\tau}^{\text{in}}(\text{e-auth}_{\mathrm{U}}^{\textsc{id}}) \;\wedge\; \neg\text{unk} \\ \wedge\ \pi_1(g(\phi_{\tau}^{\text{in}})) = [\text{net-e-auth}_{\tau}(\textsc{id}, j_0)]\text{t-suci-}\oplus_{\tau}(\textsc{id}, j_0) \\ \wedge\ \pi_2(g(\phi_{\tau}^{\text{in}})) = [\text{net-e-auth}_{\tau}(\textsc{id}, j_0)]\text{t-mac}_{\tau}(\textsc{id}, j_0) \end{pmatrix}$$

Similarly, we can rewrite $\text{fu-tr}_{\mathsf{u}:\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} \wedge \neg\underline{\text{unk}}$ as follows:

$$\text{fu-tr}_{\mathsf{u}:\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} \wedge \neg\underline{\text{unk}} \;=\; \begin{pmatrix} \mathsf{n}^{j_0} = \sigma_{\underline{\tau}}^{\text{in}}(\text{e-auth}_{\mathrm{U}}^{\nu_{\tau}(\textsc{id})}) \;\wedge\; \neg\underline{\text{unk}} \\ \wedge\ \pi_1(g(\phi_{\underline{\tau}}^{\text{in}})) = [\underline{\text{net-e-auth}}_{\underline{\tau}}(\textsc{id}, j_0)]\underline{\text{t-suci-}\oplus}_{\underline{\tau}}(\textsc{id}, j_0) \\ \wedge\ \pi_2(g(\phi_{\underline{\tau}}^{\text{in}})) = [\underline{\text{net-e-auth}}_{\underline{\tau}}(\textsc{id}, j_0)]\underline{\text{t-mac}}_{\underline{\tau}}(\textsc{id}, j_0) \end{pmatrix}$$

We can now conclude the proof:

$$\dfrac{\phi_{\tau}^{\text{in}}, \text{l-reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}}{\phi_{\tau}^{\text{in}}, \text{l-reveal}_{\tau_0}, \text{fu-tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \wedge \neg\text{unk} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \text{fu-tr}_{\mathsf{u}:\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}} \wedge \neg\underline{\text{unk}}}\;R + \text{FA}^* + \text{Dup}^* \qquad \blacksquare$$