*electronics*

MDPI

*Article*

# Formal Verification and Analysis of 5G AKA Protocol Using Mixed Strand Space Model

**Yuelei Xiao [1,2,*] and Shan Gao [3]**

[1] School of Modern Posts, Xi'an University of Post and Telecommunications, Xi'an 710061, China
[2] Shaanxi Provincial Information Engineering Research Institute, Xi'an 710121, China
[3] School of Computer, Xi'an University of Post and Telecommunications, Xi'an 710061, China; 18846821960@163.com
* Correspondence: xiaoyuelei@xupt.edu.cn; Tel.: +86-85383289

**Abstract:** The 5th generation mobile communication technology (5G) authentication and key management (AKA) protocol specified by the 3rd generation partnership project (3GPP) includes three cases because it introduces synchronization failure and message authentication code (MAC) failure procedures. Thus, there may be interactions between these cases, forming vulnerabilities that do not exist in any single case. However, this is not fully considered in the existing formal analysis and improvement of the 5G AKA protocol. To solve this problem, this paper formally analyzes the security of the latest version of the 5G AKA protocol based on the mixed strand space model for mixed protocols and finds many new attacks, including cross attacks for mixed cases. Then, a secure and efficient primary authentication and key agreement protocol for 5G networks is proposed, which is named the 5G-AKA'. In the 5G-AKA' protocol, the pre-shared key between the user equipment (UE) and the home network (HN) is replaced with a derivation key of the pre-shared key, the challenge–response mechanism between the serving network (SN) and the HN is added, the subscription permanent identifier (SUPI) of the UE is added to the second message between the SN and the HN, and the MAC failure is replaced with a timeout mechanism on the HN. Finally, the 5G-AKA' protocol is proved secure in the mixed strand space model and can overcome these attacks of the latest version of the 5G AKA protocol. Additionally, the comparative analysis shows that the 5G-AKA' protocol is better than the recently improved 5G AKA protocols in security, and the 5G-AKA' protocol is efficient and is backward compatible with the 5G AKA protocol.

**Keywords:** 5G-AKA'; mutual authentication; weak agreement; attack scenarios; location privacy; pre-shared key; perfect forward secrecy; challenge–response; timeout mechanism



**Citation:** Xiao, Y.; Gao, S. Formal Verification and Analysis of 5G AKA Protocol Using Mixed Strand Space Model. *Electronics* **2022**, *11*, 1333. https://doi.org/10.3390/electronics11091333

Academic Editors: Flavio Canavero and Diego Rivera Pinto

Received: 6 February 2022
Accepted: 14 April 2022
Published: 22 April 2022



## 1. Introduction

With the continuous popularization of the 5th generation mobile communication technology (5G), in the near future, the 5G network, as an important communication infrastructure, will penetrate into diversified vertical industries and fields such as transportation, medical treatment and industry, and support various information interactions between people, people and things, and things and things [1]. In the 5G network, three different primary authentication and key agreement protocols are defined in the related 3rd generation partnership project (3GPP) specifications [2–4], including the 5G authentication and key agreement (AKA) protocol, the improved extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA') protocol and the 5G extensible authentication protocol method for transport layer security (EAP-TLS) protocol. The first two protocols are based on the shared key cryptography, while the last one is based on the public key cryptography. These protocols all aim to provide mutual authentication of subscribers and networks. Currently, they are in the process of standardization.

The 5G AKA protocol [2–4] is developed directly from the evolution packet system (EPS)-AKA protocol of the long-term evolution (LTE)/4th generation mobile communication technology (4G) network [3], so it inherits certain security vulnerabilities from the EPS-AKA protocol such as impersonation attacks, man-in-the-middle attacks (MitM) and denial of service (DoS) attacks [5–11]. Dehnel-Wild et al. [12] analyzed the 5G AKA protocol of technical specification (TS) 33.501 v0.7.0. They discovered a protocol vulnerability that would enable the attacker to impersonate another user to a serving network (SN). Based on the Tamarin model checker [13], Basin et al. [14] investigated the security properties of the 5G AKA protocol of TS 33.501 v15.1.0, and several major issues were revealed, which are related to user localization, leakage of activity, the impact of active attackers and the presence of malicious SN while roaming. In [15], Liu et al. pointed out that the 5G AKA protocol suffers from link-ability attacks, and then proposed a new authentication scheme by making use of the Diffie–Hellman key exchange algorithm for generating the session key. This scheme was successful in preventing link-ability attacks along with a MitM attack.

For the more recent 5G AKA protocol, Borgaonkar et al. [16] found a new attack. They claimed that the protection mechanism of the sequence number (SQN) can be defeated under specific replay attacks due to its use of exclusive-or (XOR) and a lack of randomness. In [17], Cremers et al. modeled all the key components of the 5G AKA protocol (i.e., the user equipment, the serving network and the home network) according to the definition in the 3GPP specification document. They discovered an attack that exploits a potential race condition and additionally showed that solving the race condition for the honest case does not necessarily prevent the attack. In [18], Koutsos et al. investigated the privacy properties of the 5G AKA protocol using the Bana–Comon logic [19,20]. They discovered a novel de-synchronization attack and proved that their proposed protocol guarantees the privacy properties. In [21], Braeken et al. proposed a novel version of the 5G AKA protocol to prevent active attacks and gain resistance against malignant serving networks. Unfortunately, there is a possibility of having SN impersonation, so this scheme does not eliminate the vulnerability towards the MitM attack. Further, Gharsallah et al. [22] also attempted to launch a revised version of the 5G AKA protocol. However, their proposed protocol suffers from privacy preservation as the device identities are clearly transmitted in the air which leads to numerous security attacks.

As time goes on, more and more attacks of the 5G AKA protocol were found due to the insecure channel between different network domains in the legacy mobile network. In [23], Hu et al. discovered an attack exploiting the subscription concealed identifier (SUCI) to track a subscriber in the 5G network, which is directly caused by the insecure air channel. To cover this issue, they proposed a secure authentication scheme by utilizing the existing public key infrastructure (PKI) mechanism. Further, they found a location sniffing attack, which can be implemented by an attacker through inexpensive devices [24]. Similarly, they proposed a fix scheme based on the existing PKI mechanism. In [25], Edris et al. modeled the 5G AKA protocol with symbolic modeling using ProVerif based on three and four entities models, and then proposed their security consideration. Further, Mariya et al. [26] proposed an enhanced version of the authentication and key agreement protocol for the 5G system that surmounts the limitations existing in the 5G AKA protocol. Parne et al. [27] introduced a protocol that preserves the privacy of the user identity and overcomes the identified problems of the 5G AKA protocol. Similarly, 3GPP has also been enhancing the security of the 5G AKA protocol [2–4].

Because the 5G AKA protocol [2–4] introduces synchronization failure and message authentication code (MAC) failure procedures, it has three cases, so there may be interactions between these cases, forming vulnerabilities that do not exist in any single case. However, this is not fully considered in the above security analysis and improvement of the 5G AKA protocol. Therefore, we formally analyze the security of the latest version of the 5G AKA protocol considering three cases at the same time. Then, we propose a secure and efficient primary authentication and key agreement protocol for 5G networks, named

the 5G-AKA'. Finally, we prove that the 5G-AKA' protocol is secure, and it is efficient and backward compatible.

The main contributions of this paper are as follows:

- We formally analyze the security of the latest version of the 5G AKA protocol in the mixed strand space model for mixed protocols [28] and give twenty-one attack scenarios of the 5G AKA protocol. Based on these attack scenarios, we find many new attacks of the 5G AKA protocol, including cross attacks for mixed cases.
- We propose the 5G-AKA' protocol, and then formally analyze its security in the mixed strand space model for mixed protocols [28]. As a result, no attack scenario is obtained. By discussion and analysis, the 5G-AKA' protocol can overcome these attacks of the 5G AKA protocol, thus it is secure.
- Based on comparative analysis, the 5G-AKA' protocol is better than the 5G AKA protocol and the recently improved 5G AKA protocols in security, and is efficient and backward compatible.

The rest of this paper is organized as follows. Section 2 provides an overview of the latest version of the 5G AKA protocol. In Section 3, we formally analyze the security of the latest version of the 5G AKA protocol in the mixed strand space model. Section 4 describes our proposed 5G-AKA' protocol and gives the security analysis of the 5G-AKA' protocol in the mixed strand space model. In Section 5, we present some discussions and we conclude the paper in Section 6.

## 2. Overview of the 5G AKA Protocol

According to [2–4], the steps of the latest version of the 5G AKA protocol in the 3GPP standard version v17.4.0 of TS 33.501 are illustrated in Figure 1.

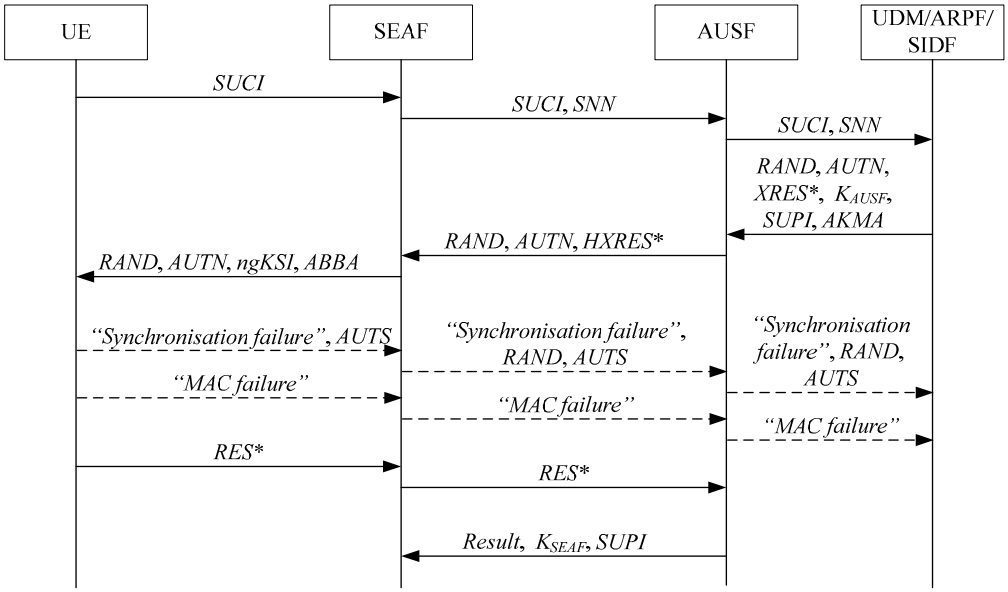


**Figure 1.** The steps of the latest version of the 5G AKA protocol. In the following notations, various fields in the figures have been described, including these fields marked with *. In detail, $XRES$ is an expected response, while $XRES^*$ is an expected response from $XRES$, then $HXRES^*$ is a hashing expected response from $XRES^*$. $RES$ is response, while $RES^*$ is a response from $RES$.

In Figure 1, the detailed steps of the latest version of the 5G AKA protocol are as follows:

1. When the security anchor function (SEAF) initiates authentication with the user equipment (UE), the UE sends $SUCI$ to the SEAF, where the UE includes mobile equipment (ME) and a universal subscriber identity module (USIM).

$$SUCI = x \cdot G || \{SUPI\}_{EK} || MAC_{UE} \tag{1}$$

$$EK || ICB || MK = KDF(x \cdot y \cdot G) \tag{2}$$

$$MAC_{UE} = HMAC(MK, \{SUPI\}_{EK}) \tag{3}$$

where $SUCI$ denotes a SUCI of the UE, $SUPI$ denotes the subscription permanent identifier (SUPI) of the UE, $x \cdot G$ and $x$ are an ephemeral public/private key pair of the UE for the Diffie–Hellman exchange, $y \cdot G$ and $y$ are an ephemeral public/private key pair of the home network (HN) for the Diffie–Hellman exchange, $EK$ is an encryption key, $ICB$ is an initial counter block (ICB), $MK$ is a MAC key, $MAC_{UE}$ is a MAC of the UE, $KDF()$ is a key derivation function and $HMAC()$ is a hash function for computing MAC, $||$ denotes a cascade of fields.

2. Upon receiving $SUCI$, the SEAF sends $SUCI$ and $SNN$ to the authentication server function (AUSF). $SNN$ denotes the serving network name (SNN) of the SN.
3. If the SEAF is entitled to use $SNN$, then the AUSF stores the receiving $SNN$ and sends $SUCI$ and $SNN$ to the unified data management (UDM).
4. The UDM invokes the subscriber identity de-concealing function (SIDF) whether $SUCI$ is received. Then, the SIDF de-conceals $SUCI$ to gain $SUPI$ before the UDM can process the request. Based on $SUPI$, the UDM/ARPF (authentication credential repository and processing function) chooses the authentication method.
5. When 5G AKA is selected, the UDM/ARPF generates $RAND$, calculates $AUTN$ and $XRES^*$, and derives $K_{AUSF}$, and then creates a 5G home environment authentication vector from $RAND$, $AUTN$, $XRES^*$ and $K_{AUSF}$. $RAND$ is an unpredictable challenge of the HN.

$$AUTN = SQN \oplus AK || AMF || MAC \tag{4}$$

$$MAC = f_1(K, SQN || RAND || AMF) \tag{5}$$

$$XRES = f_2(K, RAND) \tag{6}$$

$$CK = f_3(K, RAND) \tag{7}$$

$$IK = f_4(K, RAND) \tag{8}$$

$$AK = f_5(K, RAND) \tag{9}$$

$$K_{AUSF} = KDF(CK || IK, SNN || SQN \oplus AK) \tag{10}$$

$$XRES* = KDF(CK || IK, SNN || RAND || XRES) \tag{11}$$

where $AUTN$ is an authentication token of the HN, $SQN$ is a fresh sequence number generated by the HN, $AK$ is an anonymity key, $AMF$ is the authentication management field (AMF) and the separation bit of the AMF is set 1, $MAC$ is a MAC of the HN, $K$ is a long-term key between the UE and the HN, $f_1()$ and $f_2()$ are two message authentication functions, $f_3()$, $f_4()$ and $f_5()$ is three key generating functions, $CK$ is a cipher key, $IK$ is an integrity key, $K_{AUSF}$ is a key derived from $CK$ and $IK$, $XRES$ is an expected response and $XRES^*$ is an expected response derived from $CK$ and $IK$.

6. The UDM sends the 5G home environment authentication vector to the AUSF together with $SUPI$. When an authentication and key management for applications (AKMA) subscription is used, the UDM also sends $AKMA$ to the AUSF. $AKMA$ denotes the AKMA indication and routing indicator.
7. The AUSF stores the $XRES^*$ temporarily together with the received $SUPI$.
8. The AUSF generates a 5G authentication vector from the 5G home environment authentication vector received from the UDM/ARPF by computing $HXRES^*$ from

$XRES^*$, computing $K_{SEAF}$ from $K_{AUSF}$, replacing $XRES^*$ with $HXRES^*$, and replacing $K_{AUSF}$ with $K_{SEAF}$ in the 5G home environment authentication vector.

$$HXRES^* = SHA256(RAND||XRES^*) \tag{12}$$

$$K_{SEAF} = KDF(K_{AUSF}, SNN) \tag{13}$$

where $HXRES^*$ is a hashing $XRES^*$, $SHA256()$ is a hash function.

9. The ASUF creates a 5G serving environment authentication vector by removing $K_{SEAF}$ from the 5G authentication vector, and then sends the 5G serving environment authentication vector (i.e., $RAND$, $AUTN$ and $HXRES^*$) to the SEAF.
10. The SEAF stores $HXRES^*$, and then sends $RAND$, $AUTN$, $ngKSI$ and $ABBA$ to the UE. $ngKSI$ is used by the UE and the access and mobility management function to identify the $K_{AMF}$ and the partial native security context that is created if the authentication is successful. $ABBA$ denotes the anti-bidding down between architectures (ABBA) parameter.
11. In the UE, the ME forwards $RAND$ and $AUTN$ to the USIM. Upon receipt of $RAND$ and $AUTN$, the USIM first computes the anonymity key $AK$ and retrieves the sequence number $SQN$. Next, the USIM computes $XMAC$ and compares this with $MAC$ which is included in $AUTN$. Then, the USIM verifies that the received $SQN$ is in the correct range. If $XMAC$ is the same as $MAC$ and $SQN$ is in the correct range (i.e., $SQN_{UE} < SQN$, where $SQN_{UE}$ denotes the highest sequence number the USIM has accepted), then the USIM computes a response $RES$, $CK$ and $IK$, and then returns $RES$, $CK$ and $IK$ to the ME. The ME then computes $RES^*$, $K_{AUSF}$ and $K_{SEAF}$.

$$XMAC = f_1(K, SQN||RAND||AMF) \tag{14}$$

$$RES = f_2(K, RAND) \tag{15}$$

$$RES* = KDF(CK||IK, SNN||RAND||RES) \tag{16}$$

where $RES$ is a response and $RES^*$ is a response derived from $CK$ and $IK$.

12. The UE sends $RES^*$ to the SEAF.
13. The SEAF computes $HRES^*$ and compares this with $HXRES^*$. If they coincide, then the SEAF considers the authentication as successful from the serving network's point of view. If not, then the SEAF considers the authentication as unsuccessful.

$$HRES^* = SHA256(RAND||RES^*) \tag{17}$$

where $HRES^*$ is a hashing $RES^*$.

14. The SEAF sends the received $RES^*$ to the AUSF.
15. The AUSF compares the received $RES^*$ with the stored $XRES^*$. If $RES^*$ and $XRES^*$ are equal, then the AUSF considers the authentication as successful from the home network point of view. Then, the AUSF informs the UDM about the authentication result.
16. The AUSF indicates to the SEAF whether the authentication was successful or not from the home network point of view (i.e., *Result*). If the authentication was successful, then the ASUF also sends $K_{SEAF}$ and $SUPI$ to the SEAF.

In step 11, if $XMAC$ and $MAC$ are different, then the USIM indicates to the ME a MAC failure of $AUTN$. Then, the UE sends the "MAC failure" indication to the SEAF. Further, the SEAF sends the "MAC failure" indication to the AUSF. Finally, the ASUF sends the "MAC failure" indication to the UDM/ARPF.

In step 11, if $SQN$ is not in the correct range (i.e., $SQN_{UE} \geq SQN$), then the USIM computes $AUTS$, and then sends $AUTS$ with a "Synchronization failure" indication to the ME. Then, the UE sends $AUTS$ with the "Synchronization failure" indication to the SEAF. Further, the SEAF sends $RAND$ and $AUTS$ with the "Synchronization failure" indication

to the AUSF. Finally, the ASUF sends $RAND$ and $AUTS$ with the "Synchronization failure" indication to the UDM/ARPF.

$$AUTS = SQN_{UE} \oplus AK^*||MAC - S \tag{18}$$

$$MAC - S = f_1^*(K, SQN_{UE}||RAND||AMF_0) \tag{19}$$

$$AK^* = f_5^*(K, RAND) \tag{20}$$

where $AK^*$ is an anonymity key, $MAC - S$ is a MAC of the UE, $AMF_0$ is a dummy value of all zeros, $f_1^*()$ is a message authentication function and $f_5^*()$ is a key generating function.

Upon receiving the "MAC failure" indication or the "Synchronization failure" indication, the UDM/ARPF creates a new 5G home environment authentication vector and runs a new authentication procedure with the UE, i.e., go to step 5 to continue the 5G AKA protocol. Under normal communication conditions, these failures do not often occur [2–4]. However, they can often be used by the penetrator to perform many attacks on the 5G AKA protocol (see Section 3). In [14,15,18,24], the authors also exploited the usage of the different types of failures, MAC-based or synchronization-based, to track a specific subscriber, and then given the corresponding revised schemes.

## 3. Formal Verification and Analysis of the 5G AKA Protocol

To simplify the formal verification and analysis, we assume that:

- The parties of the 5G AKA protocol shown in Figure 1 are simplified as the UE, the SN and the HN. The USIM and the ME are located in the UE, and the SEAF is located in the SN. The AUSF, the UDM, the ARPE and the SIDF are located in the HN.
- There is a session key between the SN and the HN, and it is secure.
- $ngKSI$ and $ABBA$ do not affect the security of the 5G AKA protocol, so they are ignored here.

According to these assumptions, the 5G AKA protocol shown in Figure 1 can be summarized into three cases as follows:

Case (I): the verification of $AUTN$ succeeds and the authentication is successful. The steps of this case are as follows:

1. $UE \rightarrow SN: SUCI;$
2. $SN \rightarrow HN: \{SUCI||SNN\}_{K_{SN,HN}};$
3. $HN \rightarrow SN: \{RAND||AUTN||HXRES^*\}_{K_{SN,HN}};$
4. $SN \rightarrow UE: RAND||AUTN;$
5. $UE \rightarrow SN: RES^*;$
6. $SN \rightarrow HN: \{RES^*\}_{K_{SN,HN}};$
7. $HN \rightarrow SN: \{Result||K_{SEAF}||SUPI\}_{K_{SN,HN}}.$

where $SUCI$, $RAND||AUTN$ and $RES^*$ are three messages exchanged between the UE and SN, $\{SUCI||SNN\}_{K_{SN,HN}}$, $\{RAND||AUTN||HXRES*\}_{K_{SN,HN}}$, $\{RES*\}_{K_{SN,HN}}$ and $\{Result||K_{SEAF}||SUPI\}_{K_{SN,HN}}$ are four messages exchanged between the SN and the HN.

Case (II): the verification of $AUTN$ fails and it is a synchronization failure. The steps of this case are as follows:

1. $UE \rightarrow SN: SUCI;$
2. $SN \rightarrow HN: \{SUCI||SNN\}_{K_{SN,HN}};$
3. $HN \rightarrow SN: \{RAND||AUTN||HXRES^*\}_{K_{SN,HN}};$
4. $SN \rightarrow UE: RAND||AUTN;$
5. $UE \rightarrow SN: Syncf||AUTS;$
6. $SN \rightarrow HN: \{Syncf||RAND||AUTS\}_{K_{SN,HN}}.$

where $SUCI$, $RAND||AUTN$ and $Syncf||AUTS$ are three messages exchanged between the UE and SN, $\{SUCI||SNN\}_{K_{SN,HN}}$, $\{RAND||AUTN||HXRES^*\}_{K_{SN,HN}}$ and $\{Syncf||RAND||AUTS\}_{K_{SN,HN}}$ are three messages exchanged between the SN and the HN.

Case (III): the verification of $AUTN$ fails and it is a MAC failure. The steps of this case are as follows:

1. $UE \rightarrow SN$: $SUCI$;
2. $SN \rightarrow HN$: $\{SUCI||SNN\}_{K_{SN,HN}}$;
3. $HN \rightarrow SN$: $\{RAND||AUTN||HXRES^*\}_{K_{SN,HN}}$;
4. $SN \rightarrow UE$: $RAND||AUTN$;
5. $UE \rightarrow SN$: $MACf$;
6. $SN \rightarrow HN$: $\{MACf\}_{K_{SN,HN}}$.

where $SUCI$, $RAND||AUTN$ and $MACf$ are three messages exchanged between the UE and SN, $\{SUCI||SNN\}_{K_{SN,HN}}$, $\{RAND||AUTN||HXRES^*\}_{K_{SN,HN}}$ and $\{MACf\}_{K_{SN,HN}}$ are three messages exchanged between the SN and the HN.

In the above cases, $K_{SN,HN}$ denotes the session key between the SN and the HN, $Syncf$ denotes the "Synchronization failure" indication and $MACf$ denotes the "MAC failure" indication.

The strand space model [28–30] is a well-studied formal analysis method for security protocols. In [28], Fábrega et al. studied the case of mixed protocols, where principals use secret material in more than one protocol. In such cases, the two protocols can potentially interact, forming vulnerabilities not present in either protocol alone. To find these vulnerabilities, they proposed a mixed strand space model for such cases.

As mentioned above, there are three cases in the 5G AKA protocol, so there may be interactions between these cases, forming vulnerabilities that do not exist in any single case. In order to find these vulnerabilities, we use the mixed strand space model [28] to analyze the security of the 5G AKA protocol as follows.

### *3.1. Mixed Strand Space for the 5G AKA Protocol*

**Definition 1.** *A regular strand space* $\sum_{\mathrm{I}}$ *is a space for case I of the 5G AKA protocol if* $\sum_{\mathrm{I}}$ *is the union of three kinds of strands: (1) Initiator strands* $s \in \mathrm{Init_I}[UE, SN, HN, SUCI, RAND, AUTN, RES^*]$ *with trace:* $< +SUCI, -RAND||AUTN, +RES^* >$. *The principal associated with this strand is UE. XMAC computed locally is equal to* $MAC \subset AUTN$ *and* $SQN \subset AUTN$ *is in the correct range (i.e.,* $SQN_{UE} < SQN$*); (2) Responder strands* $r \in \mathrm{Resp_I}[UE, SN, HN, SUCI, SNN, RAND, H_1, H_2, H_3, Result, K_{SEAF}, SUPI]$ *with trace:* $< -SUCI, +\{SUCI||SNN\}_{K_{SN,HN}}, -\{RAND||H_1||H_2\}_{K_{SN,HN}}, +RAND||H_1, -H_3, +\{H_3\}_{K_{SN,HN}}, -\{Result||K_{SEAF}||SUPI\}_{K_{SN,HN}} >$. *The principal associated with this strand is* $SN$. $H_1$, $H_2$ *and* $H_3$ *are three messages that are not inspected by* $SN$, *where* $H_2 = SHA256(RAND||H_3)$; *(3) Server strands* $t \in \mathrm{Serv_I}[UE, SN, HN, SUCI, SNN, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$ *with trace:* $< -\{SUCI||SNN\}_{K_{SN,HN}}, +\{RAND||AUTN||HXRES^*\}_{K_{SN,HN}}, -\{RES^*\}_{K_{SN,HN}}, +\{Result||K_{SEAF}||SUPI\}_{K_{SN,HN}} >$. *The principal associated with this strand is* $HN$.

**Definition 2.** *A regular strand space* $\sum_{\mathrm{II}}$ *is a space for case II of the 5G AKA protocol if* $\sum_{\mathrm{II}}$ *is the union of three kinds of strands: (1) Initiator strands* $s \in \mathrm{Init_{II}}[UE, SN, HN, SUCI, RAND, AUTN, Syncf, AUTS]$ *with trace:* $< +SUCI, -RAND||AUTN, +Syncf||AUTS >$. *The principal associated with this strand is UE. XMAC computed locally is equal to* $MAC \subset AUTN$, *but* $SQN \subset AUTN$ *is not in the correct range (i.e.,* $SQN_{UE} \geq SQN$*); (2) Responder strands* $r \in \mathrm{Resp_{II}}[UE, SN, HN, SUCI, SNN, RAND, H_1, H_2, Syncf, H_4]$ *with trace:* $< -SUCI, +\{SUCI||SNN\}_{K_{SN,HN}}, -\{RAND||H_1||H_2\}_{K_{SN,HN}}, +RAND||H_1, -Syncf||H_4, +\{Syncf||RAND||H_4\}_{K_{SN,HN}} >$. *The principal associated with this strand is SN.* $H_1$, $H_2$ *and* $H_4$ *are three messages that are not inspected by SN; (3) Server strands* $t \in \mathrm{Serv_{II}}[UE, SN, HN, SUCI, SNN,$

$RAND$, $AUTN$, $HXRES^*$, $Syncf$, $AUTS$] *with trace:* $< -\{SUCI||SNN\}_{K_{SN,HN}}$, $+\{RAND||AUTN||HXRES^*\}_{K_{SN,HN}}$, $-\{Syncf||RAND||AUTS\}_{K_{SN,HN}} >$. *The principal associated with this strand is* $HN$.

**Definition 3.** *A regular strand space* $\sum_{\text{III}}$ *is a space for case III of the 5G AKA protocol if* $\sum_{\text{III}}$ *is the union of three kinds of strands: (1) Initiator strands* $s \in \text{Init}_{\text{III}}[UE, SN, HN, SUCI, RAND, AUTN, MACf]$ *with trace:* $< +SUCI, -RAND||AUTN, +MACf >$. *The principal associated with this strand is* $UE$. $XMAC$ *computed locally is not equal to* $MAC \subset AUTN$. *(2) Responder strands* $r \in \text{Resp}_{\text{III}}[UE, SN, HN, SUCI, SNN, RAND, H_1, H_2, MACf]$ *with trace:* $< -SUCI, +\{SUCI||SNN\}_{K_{SN,HN}}, -\{RAND||H_1||H_2\}_{K_{SN,HN}}, +RAND||H_1, -MACf, +\{MACf\}_{K_{SN,HN}} >$. *The principal associated with this strand is* $SN$. $H_1$ *and* $H_2$ *are two messages that are not inspected by* $SN$. *(3) Server strands* $t \in \text{Serv}_{\text{III}}[UE, SN, HN, SUCI, SNN, RAND, AUTN, HXRES^*, MACf]$ *with trace:* $< -\{SUCI||SNN\}_{K_{SN,HN}}, +\{RAND||AUTN||HXRES^*\}_{K_{SN,HN}}, -\{MACf\}_{K_{SN,HN}} >$. *The principal associated with this strand is* $HN$.

**Definition 4.** *An infiltrated mixed strand space* $\sum, \mathcal{P}$ *is a space for the 5G AKA protocol if* $\sum = \sum_{\text{I}} \cup \sum_{\text{II}} \cup \sum_{\text{III}} \cup \mathcal{P}$, *where penetrator strands* $p \in \mathcal{P}$ [28–30].

Definition 1 gives a regular strand space for case I of the 5G AKA protocol (i.e., $\sum_{\text{I}}$), including initiator strands, responder strands and server strands for case I of the 5G AKA protocol. Definition 2 gives a regular strand space for case II of the 5G AKA protocol (i.e., $\sum_{\text{II}}$), including initiator strands, responder strands and server strands for case II of the 5G AKA protocol. Definition 3 gives a regular strand space for case III of the 5G AKA protocol (i.e., $\sum_{\text{III}}$), including initiator strands, responder strands and server strands for case III of the 5G AKA protocol. Definition 4 gives an infiltrated mixed strand space for the 5G AKA protocol, including $\sum_{\text{I}}$, $\sum_{\text{II}}$, $\sum_{\text{III}}$ and penetrator strands (i.e., $\mathcal{P}$).

### *3.2. The Initiator's Guarantee of the 5G AKA Protocol*

**Theorem 1.** *Suppose: (1)* $\sum$ *is a space for the 5G AKA protocol, and* $\mathcal{C}$ *is a bundle containing an initiator strand* $s \in \text{Init}_{\text{I}}[UE, SN, HN, SUCI, RAND, AUTN, RES^*]$; *(2)* $K \notin \mathcal{K}_P$ *and* $K_{SN^*,HN} \notin \mathcal{K}_P$, *where* $SN^*$ *denotes any authorized SN; (3)* $RAND$ *is uniquely originating in* $\sum$. *Then,* $\mathcal{C}$ *contains a unique server strand* $t \in \text{Serv}_{\text{I}}[UE, SN', HN, SUCI', SNN', RAND, AUTN, (HXRES^*)', (RES*)', Result, K'_{SEAF}, SUPI]$ *and a responder strand* $r \in \text{Resp}_{\text{I}}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES*)', (RES^*)', Result, K''_{SEAF}, SUPI'']$, *where* $x' \subset SUCI'$, $SNN' \subset (HXRES^*)'$, $SNN' \subset (RES^*)'$, $SNN' \subset K'_{SEAF}$, $SUPI'' \subset SUCI''$ *and* $K''_{SEAF}$ *is generated for* $SUPI''$. *Alternatively,* $\mathcal{C}$ *contains a unique server strand* $t \in \text{Serv}_{\text{III}}[UE, SN', HN, SUCI', SNN', RAND, AUTN, (HXRES^*)', MACf]$ *and a responder strand* $r \in \text{Resp}_{\text{I}}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', (RES^*)', Result, K''_{SEAF}, SUPI'']$, $r \in \text{Resp}_{\text{II}}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', Syncf, H''_4]$ *or* $r \in \text{Resp}_{\text{III}}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', MACf]$, *where* $x' \subset SUCI'$, $SNN' \subset (HXRES^*)'$, $SNN' \subset (RES^*)'$, $SUPI'' \subset SUCI''$ *and* $K''_{SEAF}$ *is generated for* $SUPI''$.

**Proof of Theorem 1.** By assumptions (2) and (3), $K \notin \mathcal{K}_P$ and $RAND$ are uniquely originating in $\sum$, so $MAC = f_1(K, SQN||RAND||AMF) \subset AUTN \subset term(< s, 2 >)$ must uniquely originate on a server strand $t$ according to Definitions 1 to 4.

(1) If $t$ is a server strand of Definition 1, then $t \in \text{Serv}_{\text{I}}[UE, SN', HN, SUCI', SNN', RAND, AUTN, (HXRES^*)', (RES^*)', Result, K'_{SEAF}, SUPI]$, where $x' \subset SUCI'$, $SNN' \subset (HXRES^*)'$, $SNN' \subset (RES^*)'$ and $SNN' \subset K'_{SEAF}$. By assumption (2), $K_{SN',HN} \notin \mathcal{K}_P$, so $\{(RES^*)'\}_{K_{SN',HN}} = term(< t, 3 >)$ must originate on a responder strand $r \in \text{Resp}_{\text{I}}[UE'', SN', HN, SUCI'', SNN', RAND, H''_1, (HXRES^*)', (RES^*)',$

$Result$, $K''_{SEAF}$, $SUPI''$], where $SUPI'' \subset SUCI''$ and $K''_{SEAF}$ is generated for $SUPI''$. Since $K_{SN',HN} \notin \mathcal{K}_P$, $\{RAND||H''_1||(HXRES^*)'\}_{K_{SN',HN}} = term(<r,3>)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $H''_1 = AUTN$. Hence, $r \in \text{Resp}_\text{I}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', (RES^*)', Result, K''_{SEAF}, SUPI'']$.

(2) If $t$ is a server strand of Definition 2, then $t \in \text{Serv}_\text{II}[UE, SN', HN, SUCI', SNN', RAND, AUTN, (HXRES^*)', Syncf, AUTS']$, where $x' \subset SUCI'$, $SNN' \subset (HXRES^*)'$ and $SQN'_{UE} \subset AUTS'$. By assumption (2), $K \notin \mathcal{K}_P$, so $(MAC - S)' = f_1(K, SQN'_{UE}||RAND||AMF_0) \subset AUTS' \subset term(<t,3>)$ must originate on an initiator strand $s' \in \text{Init}_\text{II}[UE, SN'', HN, SUCI'', RAND, AUTN'', Syncf, AUTS']$, where $AUTN'' = SQN'' \oplus AK||AMF||MAC''$ and $MAC'' = f_1(K, SQN''||RAND||AMF)$. Since $K \notin \mathcal{K}_P$, $MAC'' \subset AUTN'' \subset term(<s',2>)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SQN'' = SQN$ and $AUTN'' = AUTN$. By assumption (1) and Definition 1, $SQN_{UE} < SQN$ on $s$. However, $SQN_{UE} \geq SQN$ on $s'$ according to Definition 2. Therefore, $s$ and $s'$ cannot be in the same run of the protocol, so $s'$ must exist in the past run of the protocol. However, it is impossible from $SQN_{UE} \geq SQN$ to $SQN_{UE} < SQN$ because $SQN_{UE}$ increases. That is to say, it is impossible that $s'$ exists in the past run of the protocol and $s$ exists in the current run of the protocol. Hence, $t$ is not a server strand of Definition 2.

(3) If $t$ is a server strand of Definition 3, then $t \in \text{Serv}_\text{III}[UE, SN', HN, SUCI', SNN', RAND, AUTN, (HXRES^*)', MACf]$, where $x' \subset SUCI'$ and $SNN' \subset (HXRES^*)'$. Since $RAND$ is uniquely originating in $\sum$, $RAND$ originates at $n_0 =< t,2 >$, where $v_0 = term(<t,2>) = \{RAND||AUTN||(HXRES^*)'\}_{K_{SN',HN}}$. Let $S = \{n \in \mathcal{C} : RAND \subset term(n) \wedge v_0 term(n)\}$. Since $term(<s,2>) = RAND||AUTN \in \mathcal{C}$, $S$ is non-empty. Hence, $S$ has at least one $\leq$-minimal element $n_2$ and the sign of $n_2$ is positive. $n_2$ does not lie on a penetrator strand but must lie on a regular strand instead (Lemma 5.4 in [29]). By inspection, $n_1$ precedes $n_2$ on the regular strand and $term(n_1) = v_0$, and the regular strand containing $n_1$ and $n_2$ is a responder strand $r$. If $r$ is a responder strand of Definition 1, then $r \in \text{Resp}_\text{I}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', (RES^*)', Result, K''_{SEAF}, SUPI'']$, where $SNN' \subset (RES^*)'$, $SUPI'' \subset SUCI''$ and $K''_{SEAF}$ is generated for $SUPI''$. If $r$ is a responder strand of Definition 2, then $r \in \text{Resp}_\text{II}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', Syncf, H''_4]$. If $r$ is a responder strand of Definition 3, then $r \in \text{Resp}_\text{III}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', MACf]$. □

According to Theorem 1, the corresponding attack scenarios can be obtained as shown in Figures 2–5, where the messages between the HN and the authorized SN are protected by their session key.

In Figures 2–5, the green dashed box represents the initiator strand of Theorem 1, while the blue dashed boxes represent the server strands and the responder strands of Theorem 1. The fields marked in red on the server strand and the responder strand are some fields that cannot be agreed with the UE, which are caused by MitM attacks.

According to Figures 2–5, some specific attacks can be found as follows.

(1) $UE$ cannot find that $SUCI'$ and $SUCI''$ are replayed because $AUTN$ does not contain the challenge of the UE (i.e., $x$), which is included in $SUCI$. That is to say, the replay attacks on the SN and the HN can be formed, resulting in the energy consumption ion of the SN and the HN.

(2) $UE$ successfully authenticates $HN$, but does not authenticate $SN$ because $AUTN$ does not contain $SNN$, which makes that $SNN'$ is included in $(HXRES*)'$, $(RES*)'$ and $K'_{SEAF}$, and the principal associated with the responder strand is $SN'$. In [14], the

authors also pointed out this security issue. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(3) Both $K'_{SEAF}$ and $K''_{SEAF}$ cannot be agreed with the UE because $SNN'$ is included in them. That is to say, the key agreement fails, resulting in a new authentication and key agreement process.

(4) In Figures 3–5, there are interactions between different cases of the 5G AKA protocol, named cross attacks. They are caused by the penetrator taking advantage of $Syncf$ and $MACf$. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(5) In Figures 3 and 4, the penetrator replays an encrypted $MACf$ between the SN and the HN to make authentication failure. In Figure 5, the penetrator directly sends $MACf$ to the SN to make authentication failure. They are called MAC failure attacks. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(6) The server strand and the responder strand of Theorem 1 may exist in the past run of the protocol because they do not contain the challenge of the UE (i.e., $x$), which is included in $SUCI$. That is to say, $RAND||AUTN$ on the UE may be a replayed message and $SQN \subset AUTN$ is still in the correct range. As a result, the location privacy of the UE can be compromised by reidentifying $RES^*$. That is to say, the location privacy of the UE can be compromised.

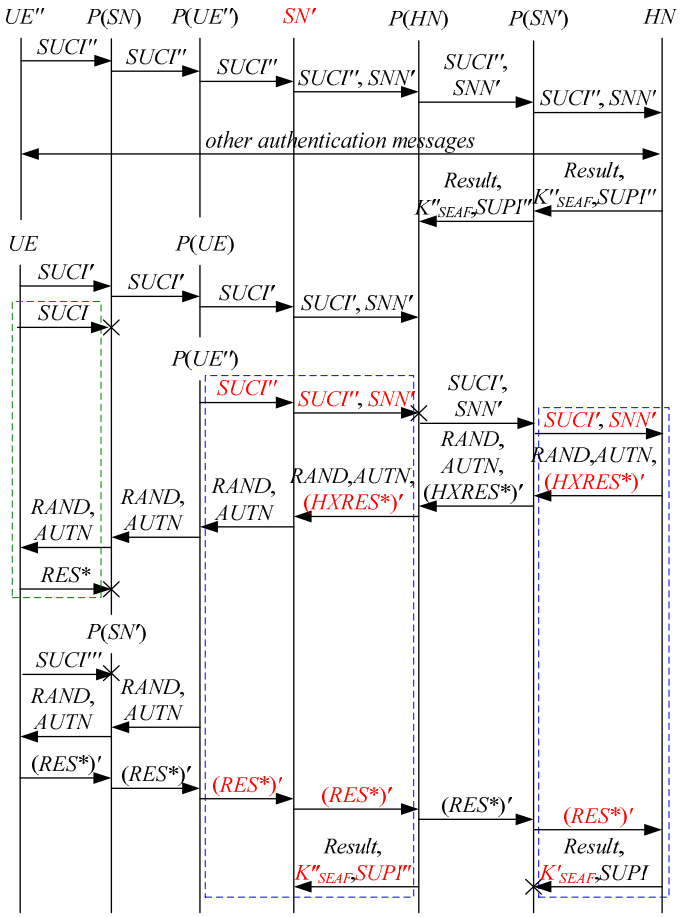


**Figure 2.** The first attack scenario of the 5G AKA protocol.

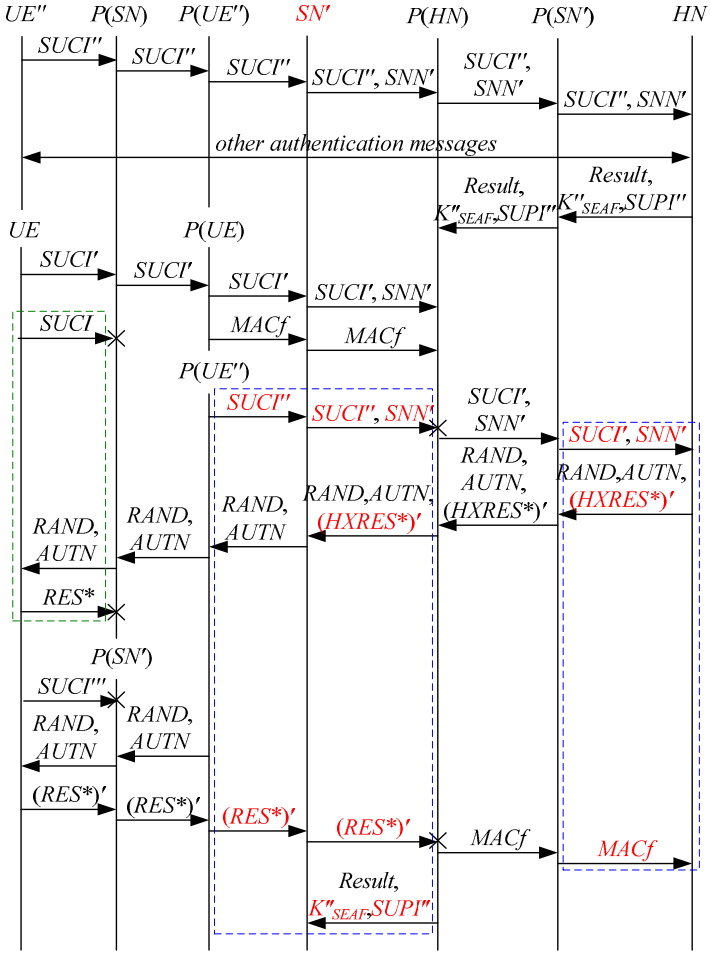


**Figure 3.** The second attack scenario of the 5G AKA protocol.

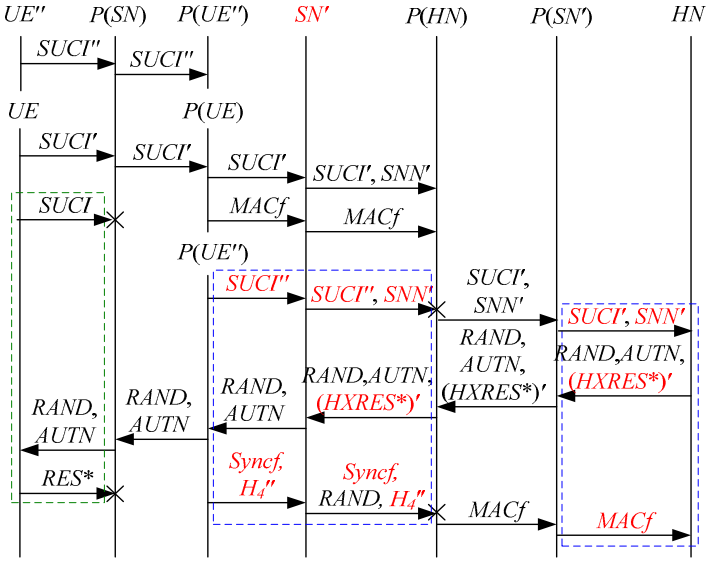


**Figure 4.** The third attack scenario of the 5G AKA protocol.

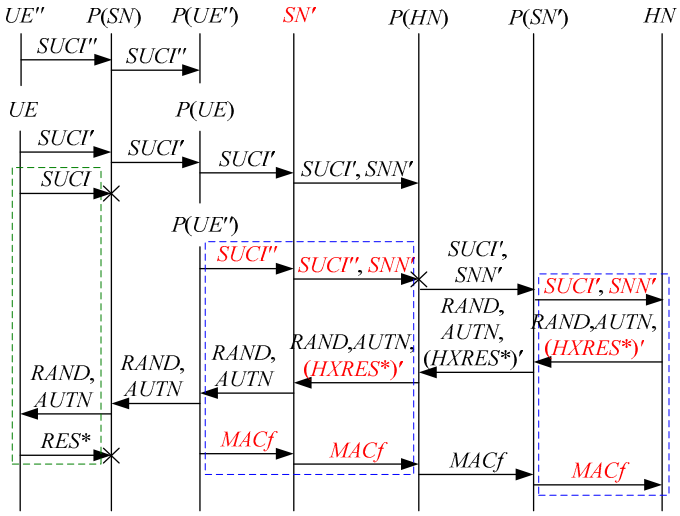


**Figure 5.** The fourth attack scenario of the 5G AKA protocol.

**Theorem 2.** *Suppose: (1) $\sum$ is a space for the 5G AKA protocol, and $\mathcal{C}$ is a bundle containing an initiator strand $s \in Init_{II}[UE, SN, HN, SUCI, RAND, AUTN, Syncf, AUTS]$; (2) $K \notin \mathcal{K}_P$ and $K_{SN^*,HN} \notin \mathcal{K}_P$, where $SN^*$ denotes any authorized SN; (3) $RAND$ is uniquely originating in $\sum$. Then, $\mathcal{C}$ contains a unique server strand $t \in Serv_I[UE, SN', HN, SUCI', SNN', RAND, AUTN, (HXRES^*)', (RES^*)', Result, K'_{SEAF}, SUPI]$ and a responder strand $r \in Resp_I[UE''', SN', HN, SUCI''', SNN', RAND, AUTN, (HXRES^*)', (RES^*)', Result, K'''_{SEAF}, SUPI''']$, and both $t$ and $r$ must exist in the past run of the protocol, where $x' \subset SUCI'$, $SNN' \subset (HXRES^*)'$, $SNN' \subset (RES^*)'$, $SNN' \subset K'_{SEAF}$, $SUPI''' \subset SUCI'''$ and $K'''_{SEAF}$ is generated for $SUPI'''$. Alternatively, $\mathcal{C}$ contains a unique server strand $t \in Serv_{II}[UE, SN', HN, SUCI', SNN', RAND, AUTN, (HXRES^*)', Syncf, AUTS']$ and a responder strand $r \in Resp_{II}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', Syncf, AUTS']$, where $x' \subset SUCI'$, $SNN' \subset (HXRES^*)'$, $SQN'_{UE} \subset AUTS'$ and $SUPI'' \subset SUCI''$. Alternatively, $\mathcal{C}$ contains a unique server strand $t \in Serv_{III}[UE, SN', HN, SUCI', SNN', RAND, AUTN, (HXRES^*)', MACf]$ and a responder strand $r \in Resp_I[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', (RES^*)', Result, K''_{SEAF}, SUPI'']$, $r \in Resp_{II}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', Syncf, H''_4]$ or $r \in Resp_{III}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', MACf]$, where $x' \subset SUCI'$, $SNN' \subset (HXRES^*)'$, $SNN' \subset (RES^*)'$, $SUPI'' \subset SUCI''$ and $K''_{SEAF}$ is generated for $SUPI''$, and both $t$ and $r$ must exist in the past run of the protocol when $r \in Resp_I[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', (RES^*)', Result, K''_{SEAF}, SUPI'']$.*

**Proof of Theorem 2.** By assumptions (2) and (3), $K \notin \mathcal{K}_P$ and $RAND$ are uniquely originating in $\sum$, so $MAC = f_1(K, SQN||RAND||AMF) \subset AUTN \subset term(< s, 2 >)$ must uniquely originate on a server strand $t$ according to Definitions 1 to 4.

(1) If $t$ is a server strand of Definition 1, then $t \in \text{Serv}_\text{I}[UE, SN', HN, SUCI', SNN', RAND, AUTN, (HXRES^*)', (RES^*)', Result, K'_{SEAF}, SUPI]$, where $x' \subset SUCI'$, $SNN' \subset (HXRES^*)'$, $SNN' \subset (RES^*)'$ and $SNN' \subset K'_{SEAF}$. By assumption (2), $K \notin \mathcal{K}_P$. Since $CK = f_3(K, RAND)$ and $IK = f_4(K, RAND)$, $CK \notin \mathcal{K}_P$ and $IK \notin \mathcal{K}_P$, so $CK||IK \notin \mathcal{K}_P$. Hence, $(RES^*)' = KDF(CK||IK, SNN'||RAND||RES) \subset term(< t, 3 >)$ must originate on an initiator strand $s' \in \text{Init}_\text{I}[UE, SN', HN, SUCI'', RAND, AUTN'', (RES^*)']$, where $AUTN'' = SQN'' \oplus AK||AMF||MAC''$ and $MAC'' = f_1(K, SQN''||RAND||AMF)$. Since $K \notin \mathcal{K}_P$, $MAC'' \subset AUTN'' \subset term(< s', 2 >)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SQN'' = SQN$ and $AUTN'' = AUTN$. By assumption (1) and Definition 2, $SQN_{UE} \geq SQN$ on $s$. However, $SQN_{UE} < SQN$ on $s'$ according to Definition 1. Therefore, $s$ and $s'$ cannot be in the same run of the protocol, so $s'$ must exist in the past run of the protocol. Because $SQN_{UE}$ increases, it is possi-

ble from $SQN_{UE} < SQN$ to $SQN_{UE} \geq SQN$. That is to say, it is possible that $s'$ exists in the past run of the protocol and $s$ exists in the current run of the protocol. Hence, it is possible that $t$ is a server strand of Definition 1. By assumption (2), $K_{SN',HN} \notin \mathcal{K}_P$, so $\{(RES^*)'\}_{K_{SN',HN}} = term(<t,3>)$ must originate on a responder strand $r \in \text{Resp}_\text{I}[UE''', SN', HN, SUCI''', SNN', RAND, H'''_1, (HXRES^*)', (RES^*)', Result, K'''_{SEAF}, SUPI''']$, where $SUPI''' \subset SUCI'''$ and $K'''_{SEAF}$ is generated for $SUPI'''$. Since $K_{SN',HN} \notin \mathcal{K}_P$, $\{RAND||H'''_1||(HXRES^*)'\}_{K_{SN',HN}} = term(<r,3>)$ must originate on a server strand $t''$. Since $RAND$ is uniquely originating in $\sum$, $t'' = t$, so $H'''_1 = AUTN$. Hence, $r \in \text{Resp}_\text{I}[UE''', SN', HN, SUCI''', SNN', RAND, AUTN, (HXRES^*)', (RES^*)', Result, K'''_{SEAF}, SUPI''']$. From the above, $s'$ exists in the past run of the protocol and $MAC \subset AUTN \subset term(<s',2>)$ originates on $t$, so $t$ must exist in past run of the protocol. From the above, $\{(RES^*)'\}_{K_{SN',HN}} = term(<t,3>)$ originates on $r$, so $r$ also must exist in the past run of the protocol.

(2) If $t$ is a server strand of Definition 2, then $t \in \text{Serv}_\text{II}[UE, SN', HN, SUCI', SNN', RAND, AUTN, (HXRES^*)', Syncf, AUTS']$, where $x' \subset SUCI', SNN' \subset (HXRES^*)'$ and $SQN'_{UE} \subset AUTS'$. By assumption (2), $K_{SN',HN} \notin \mathcal{K}_P$, so $\{Syncf||RAND||AUTS'\}_{K_{SN',HN}} = term(<t,3>)$ must originate on a responder strand $r \in \text{Resp}_\text{II}[UE'', SN', HN, SUCI'', SNN', RAND, H''_1, H''_2, Syncf, AUTS']$, where $SUPI'' \subset SUCI''$. Since $K_{SN',HN} \notin \mathcal{K}_P$, $\{RAND||H''_1||H''_2\}_{K_{SN',HN}} = term(<$ r, $3>)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $H''_1 = AUTN$ and $H''_2 = (HXRES^*)'$. Hence, $r \in \text{Resp}_\text{II}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', Syncf, AUTS']$.

(3) If $t$ is a server strand of Definition 3, then $t \in \text{Serv}_\text{III}[UE, SN', HN, SUCI', SNN', RAND, AUTN, (HXRES^*)', MACf]$, where $x' \subset SUCI'$ and $SNN' \subset (HXRES^*)'$. Since $RAND$ is uniquely originating in $\sum$, $RAND$ originates at $n_0 =< t,2 >$, where $v_0 = term(<t,2>) = \{RAND||AUTN||(HXRES^*)'\}_{K_{SN',HN}}$. Let $S = \{n \in \mathcal{C} : RAND \subset term(n) \wedge v_0 term(n)\}$. Since $term(<s,2>) = RAND||AUTN \in \mathcal{C}$, $S$ is non-empty. Hence, $S$ has at least one $\leq$-minimal element $n_2$ and the sign of $n_2$ is positive. $n_2$ does not lie on a penetrator strand but must lie on a regular strand instead (Lemma 5.4 in [29]). By inspection, $n_1$ precedes $n_2$ on the regular strand and $term(n_1) = v_0$, and the regular strand containing $n_1$ and $n_2$ is a responder strand $r$. If $r$ is a responder strand of Definition 1, then $r \in \text{Resp}_\text{I}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', (RES^*)', Result, K''_{SEAF}, SUPI'']$, where $SNN' \subset (RES^*)', SUPI'' \subset SUCI''$ and $K''_{SEAF}$ is generated for $SUPI''$. From the above, it is possible that $r$ is a responder strand of Definition 1 because it is possible from $SQN_{UE} < SQN$ to $SQN_{UE} \geq SQN$, and both $r$ and $t$ must exist in the past run of the protocol. If $r$ is a responder strand of Definition 2, then $r \in \text{Resp}_\text{II}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', Syncf, H''_4]$. If $r$ is a responder strand of Definition 3, then $r \in \text{Resp}_\text{III}[UE'', SN', HN, SUCI'', SNN', RAND, AUTN, (HXRES^*)', MACf]$. □

According to Theorem 2, the corresponding attack scenarios can be obtained as shown in Figures 6–10, where the messages between the HN and the authorized SN are protected by their session key.

In Figures 6–10, the green dashed box represents the initiator strand of Theorem 2, while the blue dashed boxes represent the server strand and the responder strand of Theorem 2. The fields marked in red on the server strand and the responder strand are some fields that cannot be agreed with the UE, which are caused by MitM attacks.

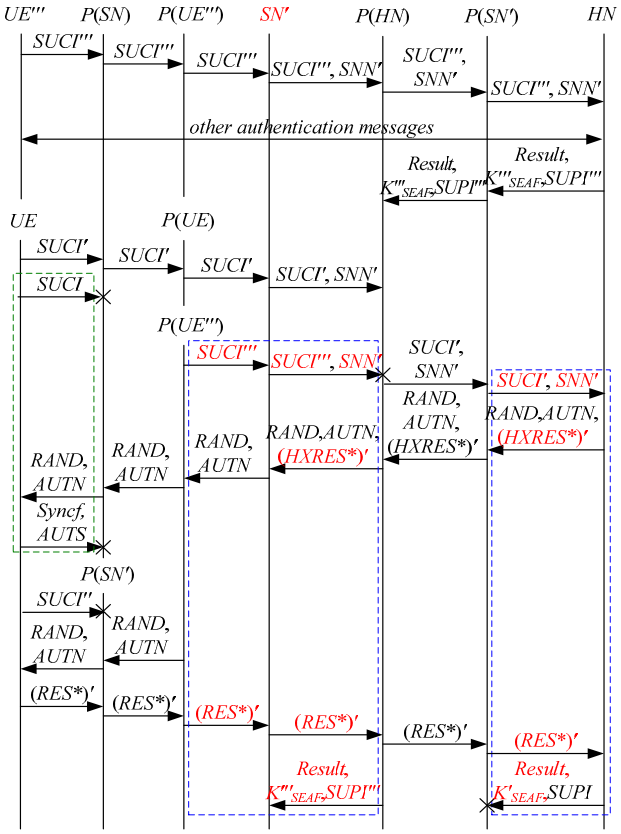


**Figure 6.** The fifth attack scenario of the 5G AKA protocol.

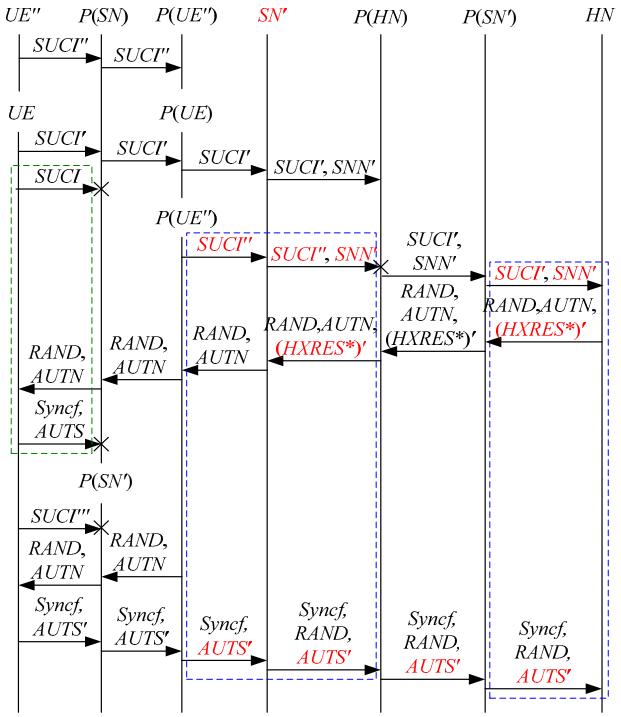


**Figure 7.** The sixth attack scenario of the 5G AKA protocol.

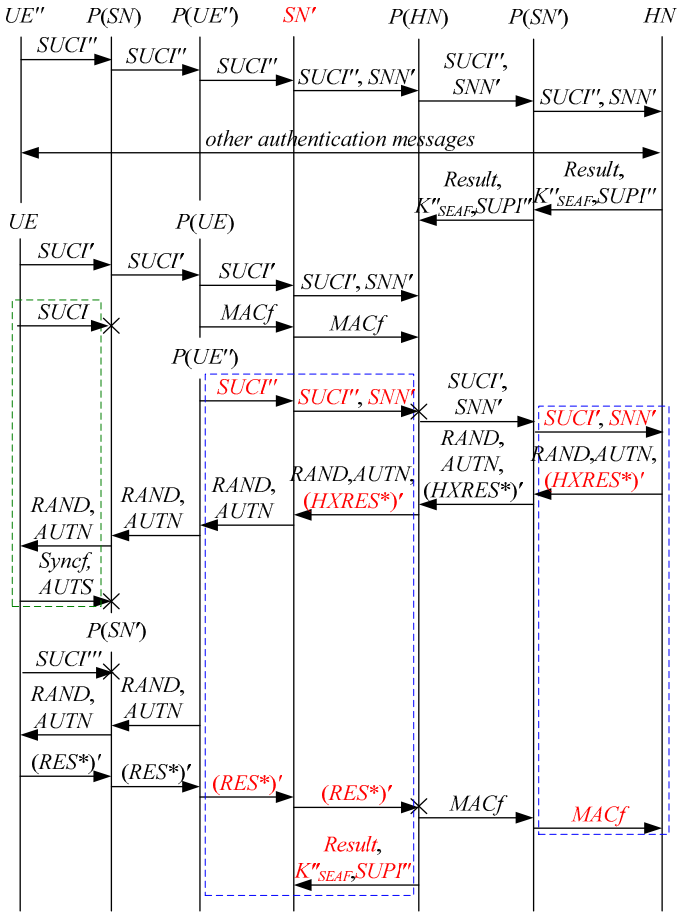


**Figure 8.** The seventh attack scenario of the 5G AKA protocol.

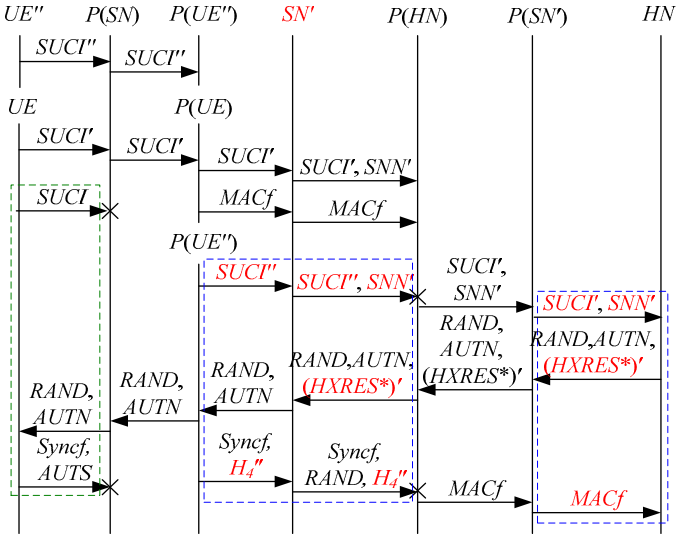


**Figure 9.** The eighth attack scenario of the 5G AKA protocol.

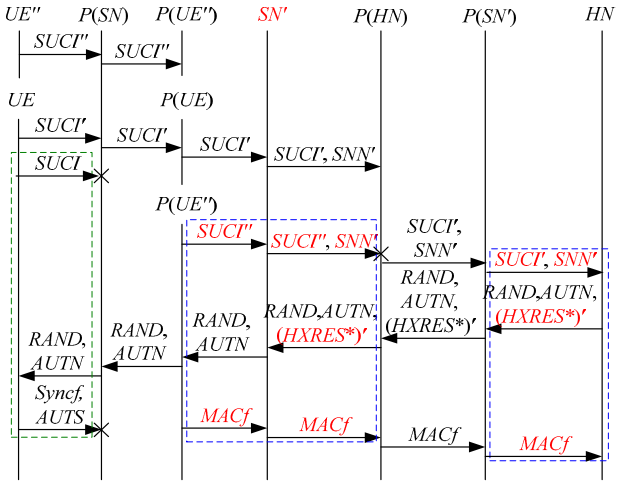


**Figure 10.** The ninth attack scenario of the 5G AKA protocol.

According to Figures 6–10, some specific attacks can be found as follows:

(1) $UE$ cannot find that $SUCI'$ and $SUCI''$ are replayed because $AUTN$ does not contain the challenge of the UE (i.e., $x$), which is included in $SUCI$. That is to say, the replay attacks on the SN and the HN can be formed, resulting in the energy consumption ion of the SN and the HN.

(2) $UE$ successfully authenticates $HN$, but does not authenticate $SN$ because $AUTN$ does not contain $SNN$, which means that $SNN'$ is included in $(HXRES^*)'$, $(RES^*)'$ and $K'_{SEAF}$, and the principal associated with the responder strand is $SN'$. In [14], the authors also pointed out this security issue. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(3) In Figures 6 and 8–10, there are interactions between different cases of the 5G AKA protocol, i.e., cross attacks. They are caused by the penetrators taking advantage of $Syncf$ and $MACf$. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(4) In Figures 8 and 9, the penetrator replays an encrypted $MACf$ between the SN and the HN to make authentication failure. In Figure 10, the penetrator directly sends $MACf$ to the SN to make authentication failure. They are called MAC failure attacks. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(5) The server strand and the responder strand of Theorem 2 in Figures 6 and 8 only exist in the past run of the protocol according to Theorem 2, i.e., $RAND||AUTN$ on the initiator strand of Theorem 2 in Figures 6 and 8 is a replayed message and $SQN \subset AUTN$ is not in the correct range. As a result, the location privacy of the UE can be compromised by identifying $Syncf$. Further, the server strand and the responder strand of Theorem 2 in Figures 7, 9 and 10 may exist in the past run of the protocol because they do not contain the challenge of the UE (i.e., $x$), which is included in $SUCI$. That is to say, $RAND||AUTN$ on the UE in Figures 7, 9 and 10 can be a replayed message and $SQN \subset AUTN$ is not in the correct range. As a result, the location privacy of the UE can be compromised by identifying $Syncf$. In [14,15,18,24], the authors also exploited this attack. That is to say, the location privacy of the UE can be compromised.

**Theorem 3.** *Suppose: $\sum$ is a space for the 5G AKA protocol, and $\mathcal{C}$ is a bundle containing an initiator strand $s \in Init_{III}[UE, SN, HN, SUCI, RAND, AUTN, MACf]$. Then, the penetrator can complete the entire message exchange without any responder strand or server strand.*

**Proof of Theorem 3.** By the above assumption and Definition 3, $XMAC$ computed locally is not equal to $MAC \subset AUTN \subset term(< s, 2 >)$, so $MAC$ does not originate on any responder strand and server strand. □

According to Theorem 3, the corresponding attack scenario can be obtained as shown in Figure 11.

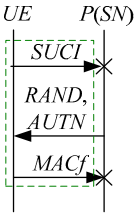


**Figure 11.** The tenth attack scenario of the 5G AKA protocol.

In Figure 11, the green dashed box represents the initiator strand of Theorem 3. According to Figure 11, $UE$ does not authenticate $SN$ and $HN$. The penetrator $P$ can perform a masquerading attack, where $RAND||AUTN$ is forged or tampered by $P$. In the other words, the penetrator can forge or tamper with $RAND||AUTN$ to make the UE respond to a "MAC failure" indication, resulting in authentication failure. This is also called MAC failure attacks. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

### *3.3. The Server's Guarantee of the 5G AKA Protocol*

**Theorem 4.** *Suppose: (1) $\sum$ is a space for the 5G AKA protocol, and $\mathcal{C}$ is a bundle containing a server strand $t \in Serv_I[UE, SN, HN, SUCI, SNN, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$; (2) $K \notin \mathcal{K}_P$ and $K_{SN^*,HN} \notin \mathcal{K}_P$, where $SN^*$ denotes any authorized SN; (3) $RAND$ is uniquely originating in $\sum$. Then, $\mathcal{C}$ contains an initiator strand $s \in Init_I[UE, SN, HN, SUCI', RAND, AUTN, RES^*]$ and a responder strand $r \in Resp_I[UE'', SN, HN, SUCI'', SNN, RAND, AUTN, HXRES^*, RES^*, Result, K''_{SEAF}, SUPI'']$, where $x' \subset SUCI'$, $SUPI'' \subset SUCI''$ and $K''_{SEAF}$ is generated for $SUPI''$.*

**Proof of Theorem 4.** By assumption (2), $K \notin \mathcal{K}_P$. Since $CK = f_3(K, RAND)$ and $IK = f_4(K, RAND)$, $CK \notin \mathcal{K}_P$ and $IK \notin \mathcal{K}_P$, so $CK||IK \notin \mathcal{K}_P$. Hence, $RES^* = KDF(CK||IK, SNN||RAND||RES) \subset term(< t, 3 >)$ must originate on an initiator strand $s \in \text{Init}_\text{I}[UE, SN, HN, SUCI', RAND, AUTN', RES^*]$, where $x' \subset SUCI'$ and $SQN' \subset AUTN'$. Since $K \notin \mathcal{K}_P$, $MAC' = f_1(K, SQN'||RAND||AMF) \subset AUTN' \subset term(< s, 2 >)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SQN' = SQN$ and $AUTN' = AUTN$. Hence, $s \in \text{Init}_\text{I}[UE, SN, HN, SUCI', RAND, AUTN, RES^*]$. By assumption (2), $K_{SN,HN} \notin \mathcal{K}_P$, so $\{RES^*\}_{K_{SN,HN}} = term(< t, 3 >)$ must originate on a responder strand $r \in \text{Resp}_\text{I}[UE'', SN, HN, SUCI'', SNN, RAND, H''_1, HXRES^*, RES^*, Result, K''_{SEAF}, SUPI'']$, where $SUPI'' \subset SUCI''$ and $K''_{SEAF}$ is generated for $SUPI''$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND||H''_1||HXRES^*\}_{K_{SN,HN}} = term(< r, 3 >)$ must originate on a server strand $t''$. Since $RAND$ is uniquely originating in $\sum$, $t'' = t$, so $H''_1 = AUTN$. Hence, $r \in \text{Resp}_\text{I}[UE'', SN, HN, SUCI'', SNN, RAND, AUTN, HXRES^*, RES^*, Result, K''_{SEAF}, SUPI'']$. □

According to Theorem 4, the corresponding attack scenario can be obtained as shown in Figure 12, where the messages between the HN and the authorized SN are protected by their session key.

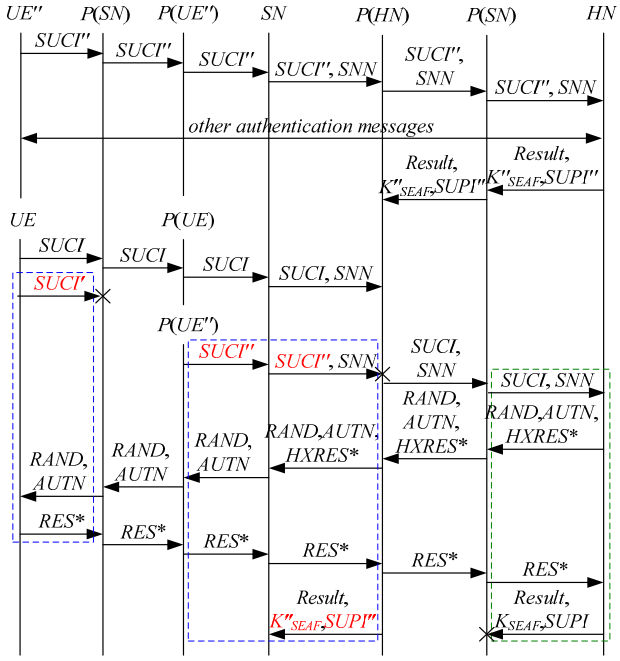


**Figure 12.** The eleventh attack scenario of the 5G AKA protocol.

In Figure 12, the green dashed box represents the server strand of Theorem 4, while the blue dashed boxes represent the initiator strand and the responder strand of Theorem 4. The fields marked in red on the initiator strand and the responder strand are some fields that cannot be agreed with the HN, which are caused by MitM attacks.

According to Figure 12, $HN$ successfully authenticates $UE$ and $SN$, but some specific attacks can be found as follows:

(1) $HN$ cannot find that $SUCI$ is replayed, which is not equal to $SUCI'$ and $SUCI''$. This is because $SUCI$ does not contain the challenge of the HN (i.e., $RAND$). That is to say, the replay attacks on the HN can be formed, resulting in the energy consumption ion of the HN.

(2) $K''_{SEAF}$ and $SUPI''$ cannot be agreed with the HN because the HN does not send $K''_{SEAF}$ and $SUPI''$ together with $RAND$, which makes that $K''_{SEAF}$ and $SUPI''$ can be a replayed key and a replayed SUPI, respectively. That is to say, the key agreement fails, resulting in a new authentication and key agreement process.

**Theorem 5.** *Suppose: (1) $\sum$ is a space for the 5G AKA protocol, and $\mathcal{C}$ is a bundle containing a server strand $t \in Serv_{II}[UE, SN, HN, SUCI, SNN, RAND, AUTN, HXRES^*, Syncf, AUTS]$; (2) $K \notin \mathcal{K}_P$ and $K_{SN*,HN} \notin \mathcal{K}_P$, where $SN^*$ denotes any authorized SN; (3) $RAND$ is uniquely originating in $\sum$. Then, $\mathcal{C}$ contains an initiator strand $s \in Init_{II}[UE, SN', HN, SUCI', RAND, AUTN, Syncf, AUTS]$ and a responder strand $r \in Resp_{II}[UE'', SN, HN, SUCI'', SNN, RAND, AUTN, HXRES^*, Syncf, AUTS]$, where $x' \subset SUCI'$ and $SUPI'' \subset SUCI''$.*

**Proof of Theorem 5.** By assumption (2), $K \notin \mathcal{K}_P$, so $MAC - S = f_1^*(K, SQN_{UE}||RAND||AMF_0) \subset AUTS \subset term(< t, 3 >)$ must originate on an initiator strand $s \in \text{Init}_{\text{II}}[UE, SN', HN, SUCI', RAND, AUTN', Syncf, AUTS]$, where $x' \subset SUCI'$ and $SQN' \subset AUTN'$. Since $K \notin \mathcal{K}_P$, $MAC' = f_1(K, SQN'||RAND||AMF) \subset AUTN' \subset term(< s, 2 >)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SQN' = SQN$ and $AUTN' = AUTN$. Hence, $s \in \text{Init}_{\text{II}}[UE, SN', HN, SUCI', RAND, AUTN, Syncf, AUTS]$. By assumption (2), $K_{SN,HN} \notin \mathcal{K}_P$, so $\{Syncf||RAND||AUTS\}_{K_{SN,HN}} = term(< t, 3 >)$ must originate on a responder strand $r \in \text{Resp}_{\text{II}}[UE'', SN, HN, SUCI'', SNN, RAND, H''_1, H''_2, Syncf, AUTS]$, where $SUPI'' \subset SUCI''$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND||H''_1||H''_2\}_{K_{SN,HN}} = term(< r, 3 >)$ must originate on a server strand $t''$. Since

$RAND$ is uniquely originating in $\sum$, $t'' = t$, so $H''_1 = AUTN$ and $H''_2 = HXRES^*$. Hence, $r \in \text{Resp}_{\text{II}}[UE'', SN, HN, SUCI'', SNN, RAND, AUTN, HXRES^*, Syncf, AUTS]$. □

According to Theorem 5, the corresponding attack scenario can be obtained as shown in Figure 13, where the messages between the HN and the authorized SN are protected by their session key.

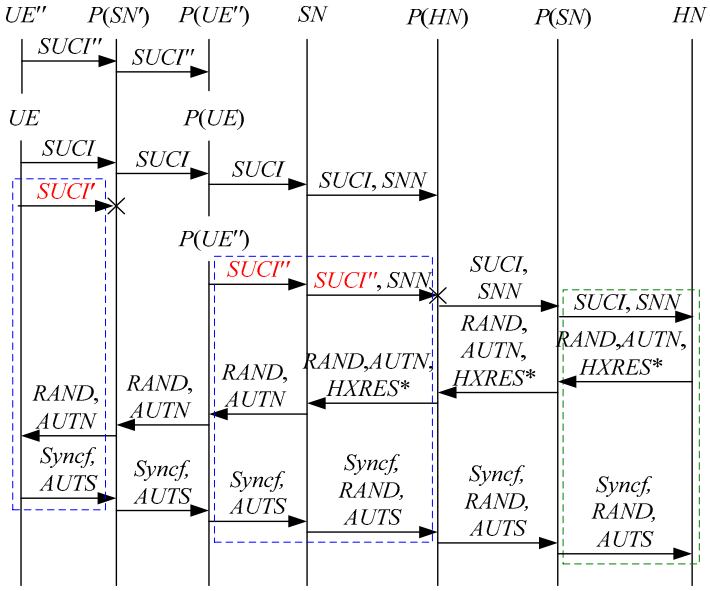


**Figure 13.** The twelfth attack scenario of the 5G AKA protocol.

In Figure 13, the green dashed box represents the server strand of Theorem 5, while the blue dashed boxes represent the initiator strand and the responder strand of Theorem 5. The fields marked in red on the initiator strand and the responder strand are some fields that cannot be agreed with the HN, which are caused by MitM attacks.

According to Figure 13, $HN$ successfully authenticates $UE$ and $SN$. However, $HN$ cannot find that $SUCI$ is replayed, which is not equal to $SUCI'$ and $SUCI''$. This is because $SUCI$ does not contain the challenge of the HN (i.e., $RAND$). That is to say, the replay attacks on the HN can be formed, resulting in the energy consumption ion of the HN.

**Theorem 6.** *Suppose: (1) $\sum$ is a space for the 5G AKA protocol, and $\mathcal{C}$ is a bundle containing a server strand $t \in Serv_{III}[UE, SN, HN, SUCI, SNN, RAND, AUTN, HXRES^*, MACf]$; (2) $K_{SN^*,HN} \notin \mathcal{K}_P$, where $SN^*$ denotes any authorized SN. Then, $\mathcal{C}$ contains a responder strand $r \in Resp_{III}[UE', SN, HN, SUCI', SNN, RAND', H'_1, H'_2, MACf]$, where $SUPI' \subset SUCI'$.*

**Proof of Theorem 6.** By assumption (2), $K_{SN,HN} \notin \mathcal{K}_P$, so $\{MACf\}_{K_{SN,HN}} = term(< s, 3 >)$ must originate on a responder strand $r \in \text{Resp}_{\text{III}}[UE', SN, HN, SUCI', SNN, RAND', H'_1, H'_2, MACf]$, where $SUPI' \subset SUCI'$. □

According to Theorem 6, the corresponding attack scenario can be obtained as shown in Figure 14, where the messages between the HN and the authorized SN are protected by their session key.

In Figure 14, the green dashed box represents the server strand of Theorem 6, while the blue dashed box represents the responder strand of Theorem 6. The fields marked in red on the responder strand are some fields that cannot be agreed with the HN, which are caused by MitM attacks.

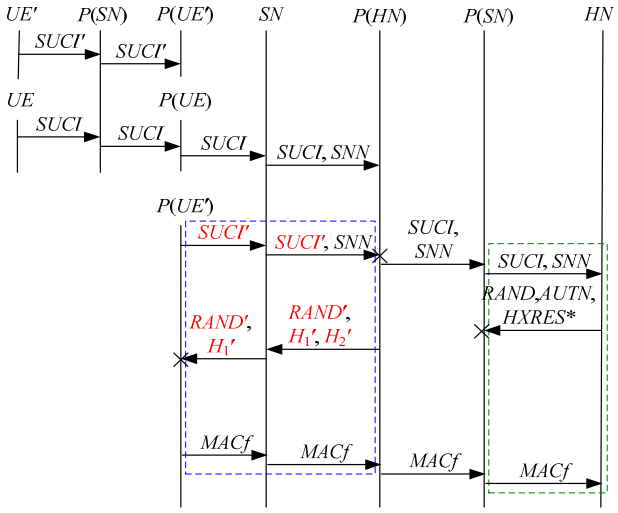


**Figure 14.** The thirteenth attack scenario of the 5G AKA protocol.

According to Figure 14, $HN$ successfully authenticates $SN$, but only authenticates $UE$ based on $SUCI$, and some specific attacks can be found as follows.

(1) $HN$ cannot find that $SUCI$ is replayed, which is not equal to $SUCI'$. This is because $SUCI$ does not contain the challenge of the HN (i.e., $RAND$). That is to say, the replay attacks on the HN can be formed, resulting in the energy consumption ion of the HN.

(2) The penetrator directly sends $MACf$ to the SN to make authentication failure. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(3) The responder strand of Theorem 6 may exist in the past run of the protocol because it does not contain the challenge of the HN, i.e., $\{MACf\}_{K_{SN,HN}}$ on the HN of Theorem 6 can be a replayed message, resulting in a replay attack. In the other words, the penetrator replays an encrypted $MACf$ between the SN and the HN to make an authentication failure. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

### *3.4. The Responder's Guarantee of the 5G AKA Protocol*

**Theorem 7.** *Suppose: (1) $\sum$ is a space for the 5G AKA protocol, and $\mathcal{C}$ is a bundle containing a responder strand $r \in Resp_I[UE, SN, HN, SUCI, SNN, RAND, H_1, H_2, H_3, Result, K_{SEAF}, SUPI]$; (2) $K^* \notin \mathcal{K}_P$ and $K_{SN^*,HN} \notin \mathcal{K}_P$, where $SN^*$ denotes any authorized SN and $K^*$ denotes a pre-shared key between HN and any authorized UE; (3) $RAND$ is uniquely originating in $\sum$. Then, $\mathcal{C}$ contains a unique server strand $t \in Serv_I[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', (RES^*)', Result, K'_{SEAF}, SUPI']$ and an initiator strand $s \in Init_I[UE', SN, HN, SUCI'', RAND, AUTN', (RES^*)']$, where $SUPI' \subset SUCI'$, $SUPI' \subset SUCI''$, $K' \subset AUTN'$, $K' \subset (HXRES^*)'$, $K' \subset (RES^*)'$, $K' \subset K'_{SEAF}$ and $K'_{SEAF}$ is generated for $SUPI'$. Alternatively, $\mathcal{C}$ contains a unique server strand $t \in Serv_{III}[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', MACf]$ and an initiator strand $s \in Init_I[UE', SN, HN, SUCI'', RAND, AUTN', (RES^*)']$, where $SUPI' \subset SUCI'$, $SUPI' \subset SUCI''$, $K' \subset AUTN'$ and $K' \subset (HXRES^*)'$.*

**Proof of Theorem 7.** By assumptions (2) and (3), $K_{SN,HN} \notin \mathcal{K}_P$ and $RAND$ are uniquely originating in $\sum$, so $\{RAND||H_1||H_2\}_{K_{SN,HN}} = term(< r, 3 >)$ must uniquely originate on a server strand $t$ according to Definitions 1 to 4.

(1) If $t$ is a server strand of Definition 1, then $t \in \text{Serv}_\text{I}[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', (RES^*)', Result, K'_{SEAF}, SUPI']$, where $SUPI' \subset SUCI'$, $K' \subset AUTN'$, $K' \subset (HXRES^*)'$, $K' \subset (RES^*)'$, $K' \subset K'_{SEAF}$ and $K'_{SEAF}$ is generated for $SUPI'$. By assumption (2), $K' \notin \mathcal{K}_P$. Since $CK' = f_3(K', RAND)$ and $IK' =$

$f_4(K', RAND)$, $CK' \notin \mathcal{K}_P$ and $IK' \notin \mathcal{K}_P$, so $CK'||IK' \notin \mathcal{K}_P$. Hence, $(RES^*)' = KDF(CK'||IK', SNN||RAND||RES') \subset term(< t, 3 >)$ must originate on an initiator strand $s \in \text{Init}_\text{I}[UE', SN, HN, SUCI'', RAND, AUTN'', (RES^*)']$, where $SUPI' \subset SUCI''$ and $SQN'' \subset AUTN''$. Since $K' \notin \mathcal{K}_P$, $MAC'' = f_1(K', SQN''||RAND||AMF) \subset AUTN'' \subset term(< s, 2 >)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SQN'' = SQN$ and $AUTN'' = AUTN'$. Hence, $s \in \text{Init}_\text{I}[UE', SN, HN, SUCI'', RAND, AUTN', (RES^*)']$.

(2) If $t$ is a server strand of Definition 2, then $t \in \text{Serv}_\text{II}[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', Syncf, AUTS']$, where $SUPI' \subset SUCI'$, $K' \subset AUTN'$, $K' \subset (HXRES^*)'$, $K' \subset AUTS'$ and $SQN_{UE'} \subset AUTS'$. By Definition 1, $(RES^*)' = KDF(CK'||IK', SNN||RAND||RES') = term(< r, 5 >)$. By assumption (2), $K' \notin \mathcal{K}_P$. Since $CK' = f_3(K', RAND)$ and $IK' = f_4(K', RAND)$, $CK' \notin \mathcal{K}_P$ and $IK' \notin \mathcal{K}_P$, so $CK'||IK' \notin \mathcal{K}_P$. Hence, $(RES^*)' = term(< r, 5 >)$ must originate on an initiator strand $s \in \text{Init}_\text{I}[UE', SN, HN, SUCI'', RAND, AUTN'', (RES^*)']$, where $SUPI' \subset SUCI''$ and $SQN'' \subset AUTN''$. Since $K' \notin \mathcal{K}_P$, $MAC'' = f_1(K', SQN''||RAND||AMF) \subset AUTN'' \subset term(< s, 2 >)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SQN'' = SQN$ and $AUTN'' = AUTN'$. Hence, $s \in \text{Init}_\text{I}[UE', SN, HN, SUCI'', RAND, AUTN', (RES^*)']$. By assumption (2), $K' \notin \mathcal{K}_P$, so $(MAC - S)' = f_1^*(K', SQN_{UE'}||RAND||AMF_0) \subset AUTS \subset term(< t, 3 >)$ must originate on an initiator strand $s' \in \text{Init}_\text{II}[UE', SN''', HN, SUCI''', RAND, AUTN''', Syncf, AUTS']$, where $SUPI' \subset SUCI'''$ and $SQN''' \subset AUTN'''$. Since $K' \notin \mathcal{K}_P$, $MAC''' = f_1(K', SQN'''||RAND||AMF) \subset AUTN''' \subset term(< s', 2 >)$ must originate on a server strand $t''$. Since $RAND$ is uniquely originating in $\sum$, $t'' = t$, so $SQN''' = SQN$ and $AUTN''' = AUTN'$. Hence, $s' \in \text{Init}_\text{II}[UE', SN''', HN, SUCI''', RAND, AUTN', Syncf, AUTS']$. By Definition 1, $SQN_{UE'} < SQN$ on $s$. However, $SQN_{UE'} \geq SQN$ on $s'$ according to Definition 2. Therefore, $s$ and $s'$ cannot be in the same run of the protocol, so $s$ or $s'$ must exist in the past run of the protocol. Since $s$ or $s'$ exists in the past run of the protocol, $t$ must exist in the past run of the protocol. Because $(MAC - S)' \subset AUTS' \subset term(< t, 3 >)$ originates on $s'$, $s'$ must exist in the past run of the protocol, so $s$ must exist in the current run of the protocol. However, it is impossible from $SQN_{UE'} \geq SQN$ to $SQN_{UE'} < SQN$ because $SQN_{UE'}$ increases. That is to say, it is impossible that $s'$ exists in the past run of the protocol and $s$ exists in the current run of the protocol. Hence, $t$ is not a server strand of Definition 2.

(3) If $t$ is a server strand of Definition 3, then $t \in \text{Serv}_\text{III}[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', MACf]$, where $SUPI' \subset SUCI'$, $K' \subset AUTN'$ and $K' \subset (HXRES^*)'$. By Definition 1, $(RES^*)' = KDF(CK'||IK', SNN||RAND||RES') = term(< r, 5 >)$. By assumption (2), $K' \notin \mathcal{K}_P$. Since $CK' = f_3(K', RAND)$ and $IK' = f_4(K', RAND)$, $CK' \notin \mathcal{K}_P$ and $IK' \notin \mathcal{K}_P$, so $CK'||IK' \notin \mathcal{K}_P$. Hence, $(RES^*)' = term(< r, 5 >)$ must originate on an initiator strand $s \in \text{Init}_\text{I}[UE', SN, HN, SUCI'', RAND, AUTN'', (RES^*)']$, where $SUPI' \subset SUCI''$ and $SQN'' \subset AUTN''$. Since $K' \notin \mathcal{K}_P$, $MAC'' = f_1(K', SQN''||RAND||AMF) \subset AUTN'' \subset term(< s, 2 >)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SQN'' = SQN$ and $AUTN'' = AUTN'$. Hence, $s \in \text{Init}_\text{I}[UE', SN, HN, SUCI'', RAND, AUTN', (RES^*)']$. □

According to Theorem 7, the corresponding attack scenarios can be obtained as shown in Figures 15 and 16, where the messages between the HN and the authorized SN are protected by their session key.

In Figures 15 and 16, the green dashed box represents the responder strand of Theorem 7, while the blue dashed boxes represent the initiator strand and the server strand of Theorem 7. The fields marked in red on the initiator strand and the server strand are some fields that cannot be agreed with the SN, which are caused by MitM attacks.

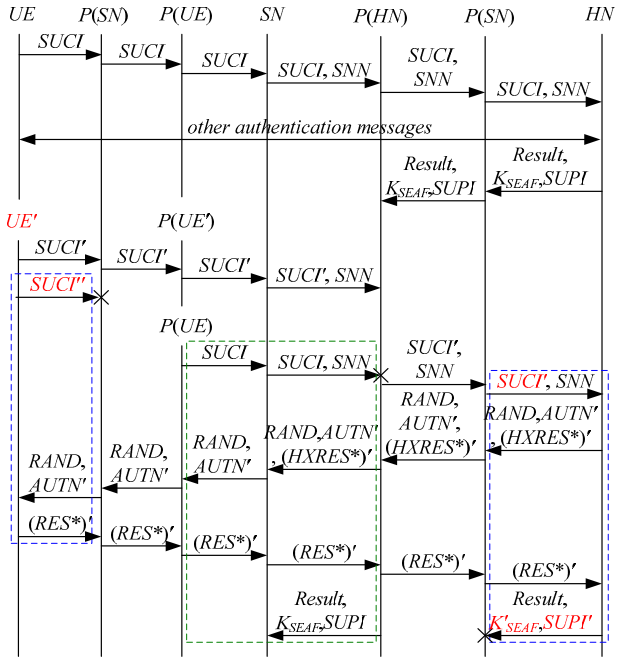


**Figure 15.** The fourteenth attack scenario of the 5G AKA protocol.

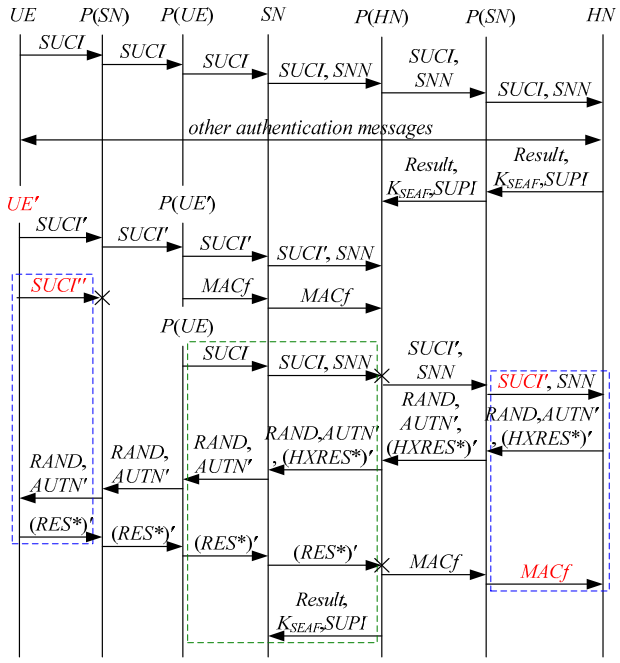


**Figure 16.** The fifteenth attack scenario of the 5G AKA protocol.

According to Figures 15 and 16, some specific attacks can be found as follows:

(1) $SN$ successfully authenticates $HN$, but does not authenticate $UE$. This is because $SN$ cannot inspect $AUTN'$, $(HXRES^*)'$ and $(RES^*)'$, and $SUPI$ is not sent with $RAND$, which means that $AUTN'$, $(HXRES^*)'$ and $(RES^*)'$ can be related to $SUPI'$ rather than $SUPI$. Accordingly, $SUPI'$ is included in $SUCI'$ and $SUCI''$, and is related to $K'_{SEAF}$. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(2) In Figure 16, there are interactions between different cases of the 5G AKA protocol, i.e., cross attacks. They are caused by the penetrators taking advantage of $MACf$. The penetrator replays an encrypted $MACf$ between the SN and the HN to make

authentication failure, i.e., MAC failure attacks. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(3) The initiator strand and the server strand of Theorem 7 may exist in the past run of the protocol because they do not contain the challenge of the SN, i.e., the messages received by the SN can be replayed messages. As a result, the penetrator can impersonate the UE and the HN to complete the entire 5G AKA protocol with the SN, forming DoS attacks on the SN. This results in the energy consumption ion of the SN.

**Theorem 8.** *Suppose: (1) $\sum$ is a space for the 5G AKA protocol, and $\mathcal{C}$ is a bundle containing a responder strand $r \in Resp_{II}[UE, SN, HN, SUCI, SNN, RAND, H_1, H_2, Syncf, H_4]$; (2) $K^* \notin \mathcal{K}_P$ and $K_{SN^*,HN} \notin \mathcal{K}_P$, where $SN^*$ denotes any authorized SN and $K^*$ denotes a pre-shared key between HN and any authorized UE; (3) $RAND$ is uniquely originating in $\sum$. Then, $\mathcal{C}$ contains a unique server strand $t \in Serv_I[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', (RES^*)', Result, K'_{SEAF}, SUPI']$ and an initiator strand $s \in Init_I[UE', SN, HN, SUCI'', RAND, AUTN', (RES^*)']$, where $SUPI' \subset SUCI'$, $SUPI' \subset SUCI''$, $K' \subset AUTN'$, $K' \subset (HXRES^*)'$, $K' \subset (RES^*)'$, $K' \subset K'_{SEAF}$ and $K'_{SEAF}$ is generated for $SUPI'$. Alternatively, $\mathcal{C}$ contains a unique server strand $t \in Serv_{II}[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', Syncf, AUTS']$ and an initiator strand $s \in Init_{II}[UE', SN'', HN, SUCI'', RAND, AUTN', Syncf, AUTS']$, where $SUPI' \subset SUCI'$, $SUPI' \subset SUCI''$, $K' \subset AUTN'$, $K' \subset (HXRES^*)'$, $K' \subset AUTS'$ and $SQN_{UE'} \subset AUTS'$. Alternatively, $\mathcal{C}$ contains a unique server strand $t \in Serv_{III}[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', MACf]$, where $SUPI' \subset SUCI'$, $K' \subset AUTN'$ and $K' \subset (HXRES^*)'$.*

**Proof of Theorem 8.** By assumptions (2) and (3), $K_{SN,HN} \notin \mathcal{K}_P$ and $RAND$ are uniquely originating in $\sum$, so $\{RAND||H_1||H_2\}_{K_{SN,HN}} = term(<r,3>)$ must uniquely originate on a server strand $t$ according to Definitions 1 to 4.

(1) If $t$ is a server strand of Definition 1, then $t \in \text{Serv}_\text{I}[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', (RES^*)', Result, K'_{SEAF}, SUPI']$, where $SUPI' \subset SUCI'$, $K' \subset AUTN'$, $K' \subset (HXRES^*)'$, $K' \subset (RES^*)'$, $K' \subset K'_{SEAF}$ and $K'_{SEAF}$ is generated for $SUPI'$. By assumption (2), $K' \notin \mathcal{K}_P$. Since $CK' = f_3(K', RAND)$ and $IK' = f_4(K', RAND)$, $CK' \notin \mathcal{K}_P$ and $IK' \notin \mathcal{K}_P$, so $CK'||IK' \notin \mathcal{K}_P$. Hence, $(RES^*)' = KDF(CK'||IK', SNN||RAND||RES') \subset term(<t,3>)$ must originate on an initiator strand $s \in \text{Init}_\text{I}[UE', SN, HN, SUCI'', RAND, AUTN'', (RES^*)']$, where $SUPI' \subset SUCI''$ and $SQN'' \subset AUTN''$. Since $K' \notin \mathcal{K}_P$, $MAC'' = f_1(K', SQN''||RAND||AMF) \subset AUTN'' \subset term(<s,2>)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SQN'' = SQN$ and $AUTN'' = AUTN'$. Hence, $s \in \text{Init}_\text{I}[UE', SN, HN, SUCI'', RAND, AUTN', (RES^*)']$.

(2) If $t$ is a server strand of Definition 2, then $t \in \text{Serv}_\text{II}[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', Syncf, AUTS']$, where $SUPI' \subset SUCI'$, $K' \subset AUTN'$, $K' \subset (HXRES^*)'$, $K' \subset AUTS'$ and $SQN_{UE'} \subset AUTS'$. By assumption (2), $K' \notin \mathcal{K}_P$, so $(MAC-S)' = f_1^*(K', SQN_{UE'}||RAND||AMF_0) \subset AUTS \subset term(<t,3>)$ must originate on an initiator strand $s \in \text{Init}_\text{II}[UE', SN'', HN, SUCI'', RAND, AUTN'', Syncf, AUTS']$, where $SUPI' \subset SUCI''$ and $SQN'' \subset AUTN''$. Since $K' \notin \mathcal{K}_P$, $MAC'' = f_1(K', SQN''||RAND||AMF) \subset AUTN'' \subset term(<s,2>)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SQN'' = SQN$ and $AUTN'' = AUTN'$. Hence, $s \in \text{Init}_\text{II}[UE', SN'', HN, SUCI'', RAND, AUTN', Syncf, AUTS']$.

(3) If $t$ is a server strand of Definition 3, then $t \in \text{Serv}_\text{III}[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', MACf]$, where $SUPI' \subset SUCI'$, $K' \subset AUTN'$ and $K' \subset (HXRES^*)'$. □

According to Theorem 8, the corresponding attack scenarios can be obtained, as shown in Figures 17–19, where the messages between the HN and the authorized SN are protected by their session key.

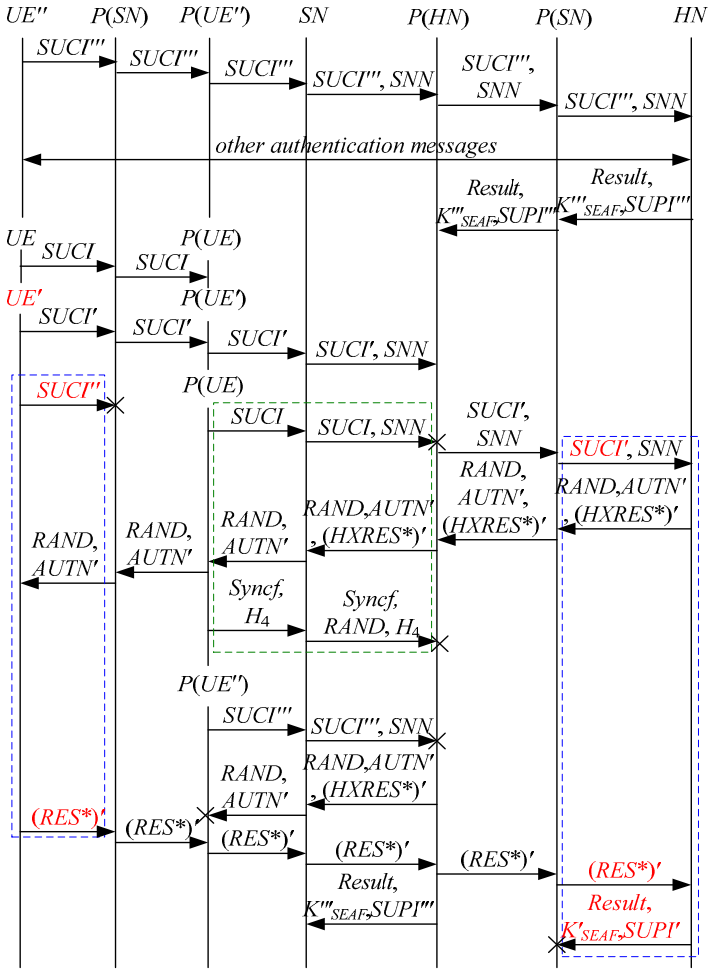


**Figure 17.** The sixteenth attack scenario of the 5G AKA protocol.

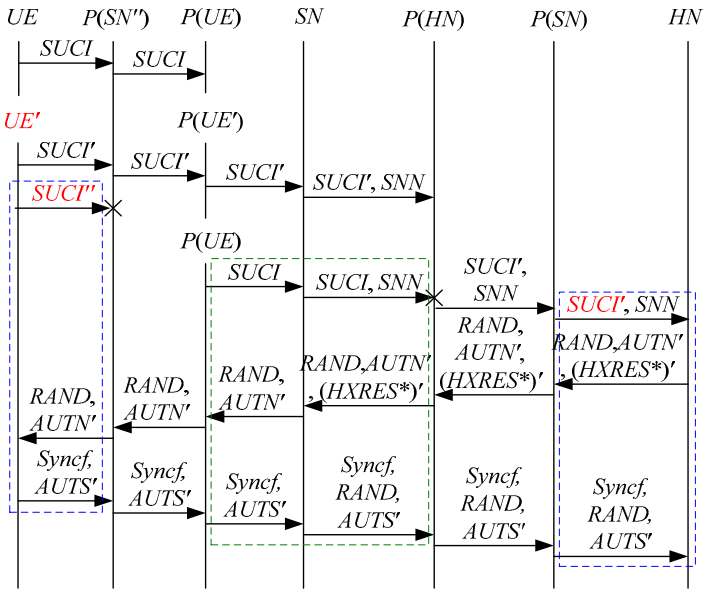


**Figure 18.** The seventeenth attack scenario of the 5G AKA protocol.

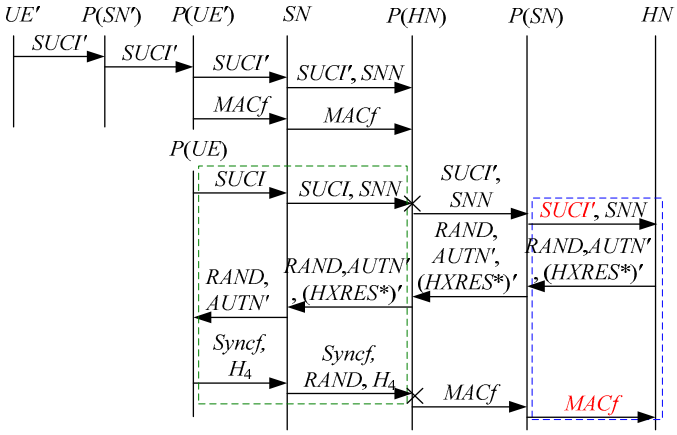


**Figure 19.** The eighteenth attack scenario of the 5G AKA protocol.

In Figures 17–19, the green dashed box represents the responder strand of Theorem 8, while the blue dashed boxes represent the initiator strand and the server strand of Theorem 8. The fields marked in red on the initiator strand and the server strand are some fields that cannot be agreed with the SN, which are caused by MitM attacks.

According to Figures 17–19, some specific attacks can be found as follows.

(1) $SN$ successfully authenticates $HN$, but does not authenticate $UE$. This is because $SN$ cannot inspect $AUTN'$, $(HXRES^*)'$ and $(RES^*)'$, which means that $AUTN'$, $(HXRES^*)'$ and $(RES^*)'$ can be related to $SUPI'$ rather than $SUPI$. Accordingly, $SUPI'$ is included in $SUCI'$ and $SUCI''$, and is related to $K'_{SEAF}$. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(2) In Figures 17 and 19, there are interactions between different cases of the 5G AKA protocol, i.e., cross attacks. They are caused by the penetrators taking advantage of $Syncf$ and $MACf$. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(3) In Figure 19, the penetrator replays an encrypted $MACf$ between the SN and the HN to make authentication failure, i.e., MAC failure attacks. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(4) The initiator strand and the server strand of Theorem 8 may exist in the past run of the protocol, i.e., the messages received by the SN can be replayed messages. As a result, the penetrator can impersonate the UE and the HN to complete the entire 5G AKA protocol with the SN, forming DoS attacks on the SN. This results in the energy consumption ion of the SN.

**Theorem 9.** *Suppose: (1)* $\sum$ *is a space for the 5G AKA protocol, and* $\mathcal{C}$ *is a bundle containing a responder strand* $r \in Resp_{III}[UE, SN, HN, SUCI, SNN, RAND, H_1, H_2, MACf]$*; (2)* $K^* \notin \mathcal{K}_P$ *and* $K_{SN^*,HN} \notin \mathcal{K}_P$*, where* $SN^*$ *denotes any authorized SN and* $K^*$ *denotes a pre-shared key between HN and any authorized UE; (3)* $RAND$ *is uniquely originating in* $\sum$*. Then,* $\mathcal{C}$ *contains a unique server strand* $t \in Serv_I[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', (RES^*)', Result, K'_{SEAF}, SUPI']$ *and an initiator strand* $s \in Init_I[UE', SN, HN, SUCI'', RAND, AUTN', (RES^*)']$*, where* $SUPI' \subset SUCI'$, $SUPI' \subset SUCI''$, $K' \subset AUTN'$, $K' \subset (HXRES^*)'$, $K' \subset (RES^*)'$, $K' \subset K'_{SEAF}$ *and* $K'_{SEAF}$ *is generated for* $SUPI'$*. Alternatively,* $\mathcal{C}$ *contains a unique server strand* $t \in Serv_{II}[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', Syncf, AUTS']$ *and an initiator strand* $s \in Init_{II}[UE', SN'', HN, SUCI'', RAND, AUTN', Syncf, AUTS']$*, where* $SUPI' \subset SUCI'$, $SUPI' \subset SUCI''$, $K' \subset AUTN'$, $K' \subset (HXRES^*)'$, $K' \subset AUTS'$ *and* $SQN_{UE'} \subset AUTS'$*. Alternatively,* $\mathcal{C}$ *contains a unique server strand* $t \in Serv_{III}[UE', SN, HN, SUCI', SNN, RAND, AUTN', (HXRES^*)', MACf]$*, where* $SUPI' \subset SUCI'$, $SUPI' \subset SUCI''$, $K' \subset AUTN'$, $K' \subset (HXRES^*)'$, $K' \subset AUTS'$ *and* $SQN_{UE'} \subset AUTS'$.

**Proof of Theorem 9.** It is the same as Theorem 8. □

According to Theorem 9, the corresponding attack scenarios can be obtained as shown in Figures 20–22, where the messages between the HN and the authorized SN are protected by their session key.

In Figures 20–22, the green dashed box represents the responder strand of Theorem 9, while the blue dashed boxes represent the initiator strand and the server strand of Theorem 9. The fields marked in red on the initiator strand and the server strand are some fields that cannot be agreed with the SN, which are caused by MitM attacks.

According to Figures 20–22, some specific attacks can be found as follows.

(1) $SN$ successfully authenticates $HN$, but does not authenticate $UE$. This is because $SN$ cannot inspect $AUTN'$, $(HXRES^*)'$ and $(RES^*)'$, which makes that $AUTN'$, $(HXRES^*)'$ and $(RES^*)'$ can be related to $SUPI'$ rather than $SUPI$. Accordingly, $SUPI'$ is included in $SUCI'$ and $SUCI''$, and is related to $K'_{SEAF}$. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(2) In Figures 20 and 21, there are interactions between different cases of the 5G AKA protocol, i.e., cross attacks. They are caused by the penetrators taking advantage of $Syncf$ and $MACf$. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(3) In Figures 20–22, the penetrator directly sends $MACf$ to the SN to make an authentication failure, i.e., MAC failure attacks. That is to say, the authentication fails, resulting in a new authentication and key agreement process.

(4) The initiator strand and the server strand of Theorem 9 may exist in the past run of the protocol, i.e., the messages received by the SN can be replayed messages. As a result, the penetrator can impersonate the UE and the HN to complete the entire 5G AKA protocol with the SN, thus forming DoS attacks on the SN. This results in the energy consumption ion of the SN.

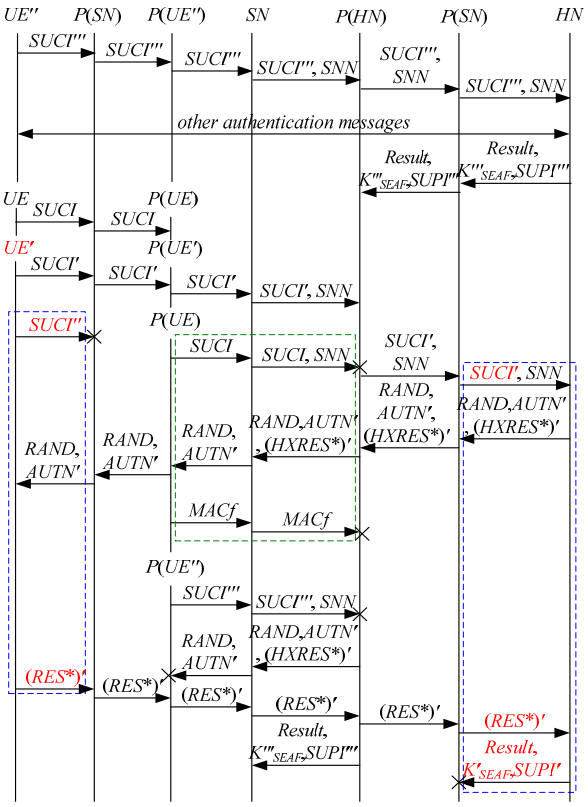


**Figure 20.** The nineteenth attack scenario of the 5G AKA protocol.

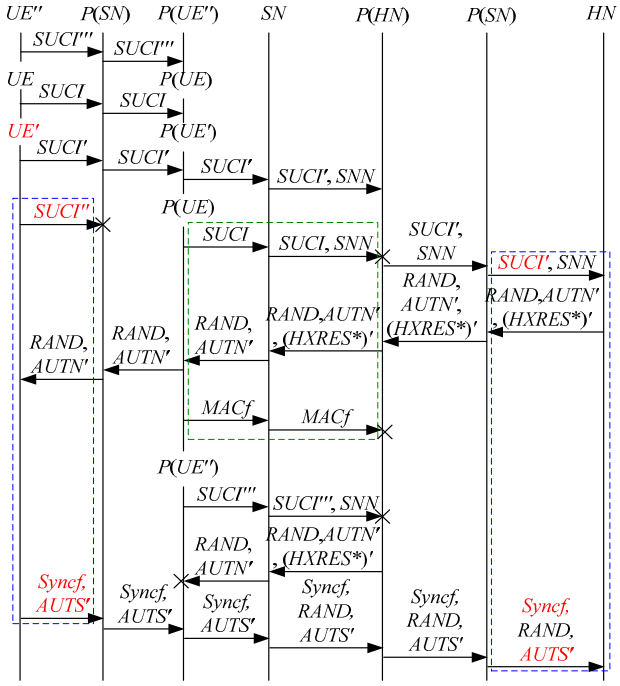


**Figure 21.** The twentieth attack scenario of the 5G AKA protocol.

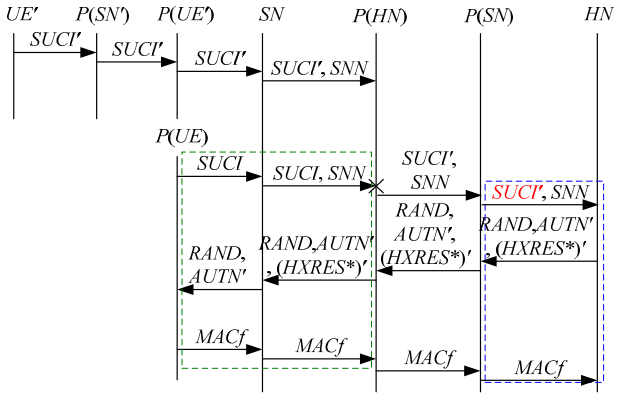


**Figure 22.** The twenty-first attack scenario of the 5G AKA protocol.

## 4. Our Proposed 5G-AKA′ Protocol and Its Security Analysis

### *4.1. The 5G-AKA′ Protocol*

In order to overcome the above security problems of the latest version of the 5G AKA protocol, we propose a 5G-AKA′ protocol, which is illustrated in Figure 23.

Compared with the latest version of the 5G AKA protocol, the main improvements of our proposed 5G-AKA′ protocol are as follows:

- To cryptographically bind $x \cdot y \cdot G$ and $SNN$ to $K$, and protect $K$, we replace $K$ with $BK$ on the UE and the HN.

$$BK = KDF(K, x \cdot y \cdot G||SNN) \tag{21}$$

  where $BK$ is a base key derived from $K$.
- To prevent DoS attacks on the SN, we add the challenge–response mechanism between the SN and the HN. In detail, we add $RAND_{SN}$ to the first three messages between the SEAF (located in the SN) and the AUSF (located in the HN) and add $RAND$ to the fourth message between the SEAF and the AUSF, where $RAND_{SN}$ is an unpredictable challenge of the SEAF;

- Add $SUPI$ to the second message between the SEAF and the AUSF, matching with $SUCI$ in the first message between them;
- In the latest version of the 5G AKA protocol, $MACf$ is used to initiate a new authentication procedure for the UE. However, it causes a large number of attacks according to the above security analysis. Hence, we use a timeout mechanism on the HN instead of $MACf$ to initiate a new authentication procedure towards the UE. That is to say, if $XMAC$ and $MAC$ are different, then the UE directly discards the receives $RAND||AUTN$, and the HN will initiate a new authentication procedure towards the UE when the HN does not receive an authentication response message or a synchronization failure message within a certain period of time.

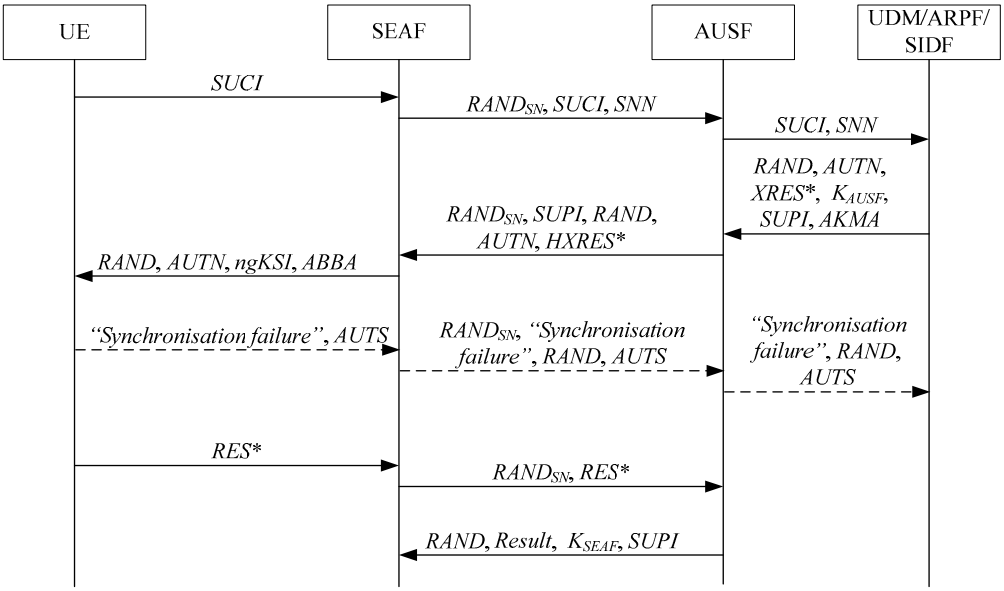


**Figure 23.** Our proposed 5G-AKA' protocol.

According to the above descriptions, our proposed 5G-AKA' protocol can be summarized into two cases as follows:

Case (I): the verification of $AUTN$ succeeds and the authentication is successful. The steps of this case are as follows:

1. $UE \rightarrow SN: SUCI;$
2. $SN \rightarrow HN: \{RAND_{SN}||SUCI||SNN\}_{K_{SN,HN}};$
3. $HN \rightarrow SN: \{RAND_{SN}||SUPI||RAND||AUTN||HXRES^*\}_{K_{SN,HN}};$
4. $SN \rightarrow UE: RAND||AUTN;$
5. $UE \rightarrow SN: RES^*;$
6. $SN \rightarrow HN: \{RAND_{SN}||RES^*\}_{K_{SN,HN}};$
7. $HN \rightarrow SN: \{RAND||Result||K_{SEAF}||SUPI\}_{K_{SN,HN}}.$

where $SUCI$, $RAND||AUTN$ and $RES^*$ are three messages exchanged between the UE and SN, $\{RAND_{SN}||SUCI||SNN\}_{K_{SN,HN}}$, $\{RAND_{SN}||SUPI||RAND||AUTN||HXRES^*\}_{K_{SN,HN}}$, $\{RAND_{SN}||RES^*\}_{K_{SN,HN}}$ and $\{RAND||Result||K_{SEAF}||SUPI\}_{K_{SN,HN}}$ are four messages exchanged between the SN and the HN.

Case (II): the verification of $AUTN$ fails and it is a synchronization failure. The steps of this case are as follows:

1. $UE \rightarrow SN: SUCI;$
2. $SN \rightarrow HN: \{RAND_{SN}||SUCI||SNN\}_{K_{SN,HN}};$
3. $HN \rightarrow SN: \{RAND_{SN}||SUPI||RAND||AUTN||HXRES^*\}_{K_{SN,HN}};$
4. $SN \rightarrow UE: RAND||AUTN;$

5. $UE \rightarrow SN: Syncf||AUTS;$
6. $SN \rightarrow HN: \{RAND_{SN}||Syncf||RAND||AUTS\}_{K_{SN,HN}}.$

where $SUCI$, $RAND||AUTN$ and $Syncf||AUTS$ are three messages exchanged between the UE and SN, $\{RAND_{SN}||SUCI||SNN\}_{K_{SN,HN}}$, $\{RAND_{SN}||SUPI||RAND||AUTN||HXRES^*\}_{K_{SN,HN}}$ and $\{RAND_{SN}||Syncf||RAND||AUTS\}_{K_{SN,HN}}$ are three messages exchanged between the SN and the HN.

In the above cases, $K$ is replaced with $BK$. Similarly, we use the mixed strand space model [28] to analyze the security of our proposed 5G-AKA′ protocol as follows.

### *4.2. Mixed Strand Space for the 5G-AKA′ Protocol*

**Definition 5.** *A regular strand space $\sum_I$ is a space for case I of the 5G-AKA′ protocol if $\sum_I$ is the union of three kinds of strands: (1) Initiator strands $s \in Init_I[UE, SN, HN, SUCI, RAND, AUTN, RES^*]$ with trace: $< +SUCI, -RAND||AUTN, +RES^* >$. The principal associated with this strand is UE. XMAC computed locally is equal to $MAC \subset AUTN$ and $SQN \subset AUTN$ is in the correct range (i.e., $SQN_{UE} < SQN$); (2) Responder strands $r \in Resp_I[UE, SN, HN, SUCI, SNN, RAND_{SN}, RAND, H_1, H_2, H_3, Result, K_{SEAF}, SUPI]$ with trace: $< -SUCI, +\{RAND_{SN}||SUCI||SNN\}_{K_{SN,HN}}, -\{RAND_{SN}||SUPI||RAND||H_1||H_2\}_{K_{SN,HN}}, +RAND||H_1, -H_3, +\{RAND_{SN}||H_3\}_{K_{SN,HN}}, -\{RAND||Result||K_{SEAF}||SUPI\}_{K_{SN,HN}} >$. The principal associated with this strand is SN. $H_1$, $H_2$ and $H_3$ are three messages that are not inspected by SN, where $H_2 = SHA256(RAND||H_3)$; (3) Server strands $t \in Serv_I[UE, SN, HN, SUCI, SNN, RAND_{SN}, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$ with trace: $< -\{RAND_{SN}||SUCI||SNN\}_{K_{SN,HN}}, +\{RAND_{SN}||SUPI||RAND||AUTN||HXRES^*\}_{K_{SN,HN}}, -\{RAND_{SN}||RES^*\}_{K_{SN,HN}}, +\{RAND||Result||K_{SEAF}||SUPI\}_{K_{SN,HN}} >$. The principal associated with this strand is HN.*

**Definition 6.** *A regular strand space $\sum_{II}$ is a space for case II of the 5G-AKA′ protocol if $\sum_{II}$ is the union of three kinds of strands: (1) Initiator strands $s \in Init_{II}[UE, SN, HN, SUCI, RAND, AUTN, Syncf, AUTS]$ with trace: $< +SUCI, -RAND||AUTN, +Syncf||AUTS >$. The principal associated with this strand is UE. XMAC computed locally is equal to $MAC \subset AUTN$, but $SQN \subset AUTN$ is not in the correct range (i.e., $SQN_{UE} \geq SQN$); (2) Responder strands $r \in Resp_{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND_{SN}, RAND, H_1, H_2, Syncf, H_4]$ with trace: $< -SUCI, +\{RAND_{SN}||SUCI||SNN\}_{K_{SN,HN}}, -\{RAND_{SN}||SUPI||RAND||H_1||H_2\}_{K_{SN,HN}}, +RAND||H_1, -Syncf||H_4, +\{RAND_{SN}||Syncf||RAND||H_4\}_{K_{SN,HN}} >$. The principal associated with this strand is SN. $H_1$, $H_2$ and $H_4$ are three messages that are not inspected by SN; (3) Server strands $t \in Serv_{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND_{SN}, RAND, AUTN, HXRES^*, Syncf, AUTS]$ with trace: $< -\{RAND_{SN}||SUCI||SNN\}_{K_{SN,HN}}, +\{RAND_{SN}||SUPI||RAND||AUTN||HXRES^*\}_{K_{SN,HN}}, -\{RAND_{SN}||Syncf||RAND||AUTS\}_{K_{SN,HN}} >$. The principal associated with this strand is HN.*

**Definition 7.** *An infiltrated strand space $\sum, \mathcal{P}$ is a space for the 5G-AKA′ protocol if $\sum = \sum_I \cup \sum_{II} \cup \mathcal{P}$, where penetrator strands $p \in \mathcal{P}$ [28–30].*

Definition 5 gives a regular strand space for case I of the 5G-AKA′ protocol (i.e., $\sum_I$), including initiator strands, responder strands and server strands for case I of the 5G-AKA′ protocol. Definition 6 gives a regular strand space for case II of the 5G-AKA′ protocol (i.e., $\sum_{II}$), including initiator strands, responder strands and server strands for case II of the 5G AKA protocol. Definition 7 gives an infiltrated mixed strand space for the 5G-AKA′ protocol, including $\sum_I$, $\sum_{II}$ and penetrator strands (i.e., $\mathcal{P}$).

*4.3. The Initiator's Guarantee of the 5G-AKA' Protocol*

**Theorem 10.** *Suppose: (1) $\sum$ is a space for the 5G-AKA' protocol, and $\mathcal{C}$ is a bundle containing an initiator strand $s \in Init_I[UE, SN, HN, SUCI, RAND, AUTN, RES^*]$; (2) $K \notin \mathcal{K}_P$ and $K_{SN,HN} \notin \mathcal{K}_P$; (3) $x$, $RAND$, $RAND'_{SN}$ is uniquely originating in $\sum$. Then, $\mathcal{C}$ contains a unique server strand $t \in Serv_I[UE, SN, HN, SUCI, SNN, RAND'_{SN}, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$ and a unique responder strand $r \in Resp_I[UE, SN, HN, SUCI, SNN, RAND'_{SN}, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$.*

**Proof of Theorem 10.** Since $BK = KDF(K, x \cdot y \cdot G||SNN)$, $BK \notin \mathcal{K}_P$ according to assumption (2). Because $MAC = f_1(BK, SQN||RAND||AMF)$ and $RAND$ is uniquely originating in $\sum$, $MAC \subset AUTN \subset term(< s, 2 >)$ must uniquely originate on a server strand $t$ according to Definitions 5 to 7.

(1) If $t$ is a server strand of Definition 5, then $t \in \text{Serv}_\text{I}[UE, SN, HN, SUCI, SNN, RAND'_{SN}, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$. By assumptions (2) and (3), $K_{SN,HN} \notin \mathcal{K}_P$ and $RAND'_{SN}$ are uniquely originating in $\sum$, so $\{RAND'_{SN}||RES^*\}_{K_{SN,HN}} = term(< t, 3 >)$ must originate on a unique responder strand $r \in \text{Resp}_\text{I}[UE'', SN, HN, SUCI'', SNN, RAND'_{SN}, RAND, H''_1, HXRES^*, RES^*, Result, K''_{SEAF}, SUPI'']$, where $SUPI'' \subset SUCI''$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND'_{SN}||SUPI''||RAND||H''_1||HXRES^*\}_{K_{SN,HN}} = term(< r, 3 >)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $H''_1 = AUTN$, $SUPI'' = SUPI$ and $UE'' = UE$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND||Result||K''_{SEAF}||SUPI\}_{K_{SN,HN}} = term(< r, 7 >)$ must originate on a server strand $t''$. Since $RAND$ is uniquely originating in $\sum$, $t'' = t$, so $K''_{SEAF} = K_{SEAF}$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND'_{SN}||SUCI||SNN\}_{K_{SN,HN}} = term(< t, 1 >)$ must originate on a responder strand $r'$. Since $RAND'_{SN}$ is uniquely originating in $\sum$, $r' = r$, so $SUCI'' = SUCI$. Hence, $r \in \text{Resp}_\text{I}[UE, SN, HN, SUCI, SNN, RAND'_{SN}, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$.

(2) If $t$ is a server strand of Definition 6, then $t \in \text{Serv}_\text{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND'_{SN}, RAND, AUTN, HXRES^*, Syncf, AUTS']$, where $SQN'_{UE} \subset AUTS'$. Since $BK \notin \mathcal{K}_P$, $MAC - S' = f_1^*(BK, SQN'_{UE}||RAND||AMF_0) \subset AUTS' \subset term(< t, 3 >)$ must originate on an initiator strand $s' \in \text{Init}_\text{II}[UE, SN, HN, SUPI, SUCI, RAND, AUTN'', Syncf, AUTS']$, so $x$ originates on $term(< s', 1 >)$. By assumptions (1) and (2), $x$ originates on $term(< s, 1 >)$. Since $x$ is uniquely originating in $\sum$, $s' = s$. However, $s' \in \text{Init}_\text{II}$ and $s \in \text{Init}_\text{I}$, $s' \neq s$. Hence, $t$ is not a server strand of Definition 6. □

**Theorem 11.** *Suppose: (1) $\sum$ is a space for the 5G-AKA' protocol, and $\mathcal{C}$ is a bundle containing an initiator strand $s \in Init_{II}[UE, SN, HN, SUCI, RAND, AUTN, Syncf, AUTS]$; (2) $K \notin \mathcal{K}_P$ and $K_{SN,HN} \notin \mathcal{K}_P$; (3) $x$, $RAND$, $RAND'_{SN}$ is uniquely originating in $\sum$. Then, $\mathcal{C}$ contains a unique server strand $t \in Serv_{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND'_{SN}, RAND, AUTN, HXRES^*, Syncf, AUTS]$ and a unique responder strand $r \in Resp_{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND'_{SN}, RAND, AUTN, HXRES^*, Syncf, AUTS]$.*

**Proof of Theorem 11.** Since $BK = KDF(K, x \cdot y \cdot G||SNN)$, $BK \notin \mathcal{K}_P$ according to assumption (2). Because $MAC = f_1(BK, SQN||RAND||AMF)$ and $RAND$ are uniquely originating in $\sum$, $MAC \subset AUTN \subset term(< s, 2 >)$ must uniquely originate on a server strand $t$ according to Definitions 5 to 7.

(1) If $t$ is a server strand of Definition 5, then $t \in \text{Serv}_\text{I}[UE, SN, HN, SUCI, SNN, RAND'_{SN}, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$. Since $BK \notin \mathcal{K}_P$, $CK = f_3(BK, RAND) \notin \mathcal{K}_P$ and $IK = f_4(BK, RAND) \notin \mathcal{K}_P$, so $CK||IK \notin \mathcal{K}_P$. Hence, $RES^* = KDF(CK||IK, SNN||RAND||RES) \subset term(< t, 3 >)$ must originate on an initiator strand $s' \in \text{Init}_\text{I}[UE, SN, HN, SUCI, RAND, AUTN'', RES^*]$, so $x$ orig-

inates on $term(< s', 1 >)$. By assumptions (1) and (2), $x$ originates on $term(< s, 1 >)$. Since $x$ is uniquely originating in $\sum$, $s' = s$. However, $s' \in \text{Init}_\text{I}$ and $s \in \text{Init}_\text{II}$, $s' \neq s$. Hence, $t$ is not a server strand of Definition 5.

(2) If $t$ is a server strand of Definition 6, then $t \in \text{Serv}_\text{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND'_{SN}, RAND, AUTN, HXRES^*, Syncf, AUTS']$, where $SQN'_{UE} \subset AUTS'$. Since $BK \notin \mathcal{K}_P$, $MAC - S' = f_1^*(BK, SQN'_{UE}||RAND||AMF_0) \subset AUTS' \subset term(< t, 3 >)$ must originate on an initiator strand $s'$. Since $x$ is uniquely originating in $\sum$, $s' = s$, so $SQN'_{UE} = SQN_{UE}$ and $AUTS' = AUTS$. Hence, $t \in \text{Serv}_\text{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND'_{SN}, RAND, AUTN, HXRES^*, Syncf, AUTS]$. By assumptions (2) and (3), $K_{SN,HN} \notin \mathcal{K}_P$ and $RAND'_{SN}$ are uniquely originating in $\sum$, so $\{RAND'_{SN}||Syncf||RAND||AUTS\}_{K_{SN,HN}} = term(< t, 3 >)$ must originate on a unique responder strand $r \in \text{Resp}_\text{II}[UE'', SN, HN, SUPI'', SUCI'', SNN, RAND'_{SN}, RAND, H''_1, H''_2, Syncf, AUTS]$, where $SUPI'' \subset SUCI''$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND'_{SN}||SUPI''||RAND||H''_1||H''_2\}_{K_{SN,HN}} = term(< r, 3 >)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SUPI'' = SUPI$, $UE'' = UE$, $H''_1 = AUTN$ and $H''_2 = HXRES^*$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND'_{SN}||SUCI||SNN\}_{K_{SN,HN}} = term(< t, 1 >)$ must originate on a responder strand $r'$. Since $RAND'_{SN}$ is uniquely originating in $\sum$, $r' = r$, so $SUCI'' = SUCI$. Hence, $r \in \text{Resp}_\text{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND'_{SN}, RAND, AUTN, HXRES^*, Syncf, AUTS]$. □

According to Theorems 10 and 11, $UE$ successfully authenticates $HN$ and $SN$, and all fields except $RAND'_{SN}$ on the sever strand and the responder are agreed with the UE. $RAND'_{SN}$ is unknowable to the UE because it is mainly used for the challenge–response mechanism between the SN and the HN, which does not affect the security of the 5G-AKA′ protocol. Hence, MitM attacks are prevented.

In addition, those attacks in Section 3.2 are overcome as follows:

(1) Since $BK = KDF(K, x \cdot y \cdot G||SNN)$ is used to calculate $AUTN$, the challenge of the UE (i.e., $x$), the pre-shared key between the UE and the HN (i.e., $K$) and $SNN$ are included in $AUTN$. As a result, $UE$ can find whether $SUCI$ is replayed, $UE$ successfully authenticates $HN$ and $SN$, and $RAND||AUTN$ on the UE cannot be replayed, making that the location privacy of the UE cannot be compromised.

(2) Since $MACf$ is replaced with a timeout mechanism on the HN, MAC failure attacks are prevented. Further, $RAND||AUTN$ on the UE cannot be replayed maliciously to generate $Syncf$. As a result, the penetrator cannot take advantage of $Syncf$ and $MACf$ to performed cross attacks.

### *4.4. The Server's Guarantee of the 5G-AKA′ Protocol*

**Theorem 12.** *Suppose: (1) $\sum$ is a space for the 5G-AKA′ protocol, and $\mathcal{C}$ is a bundle containing a server strand $t \in Serv_I[UE, SN, HN, SUCI, SNN, RAND_{SN}, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$; (2) $K \notin \mathcal{K}_P$ and $K_{SN,HN} \notin \mathcal{K}_P$; (3) $x$, $RAND$, $RAND_{SN}$ is uniquely originating in $\sum$. Then, $\mathcal{C}$ contains a unique initiator strand $s \in Init_I[UE, SN, HN, SUCI, RAND, AUTN, RES^*]$ and a unique responder strand $r \in Resp_I[UE, SN, HN, SUCI, SNN, RAND_{SN}, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$.*

**Proof of Theorem 12.** Since $BK = KDF(K, x \cdot y \cdot G||SNN)$, $BK \notin \mathcal{K}_P$ according to assumption (2). Because $CK = f_3(BK, RAND)$ and $IK = f_4(BK, RAND)$, $CK \notin \mathcal{K}_P$ and $IK \notin \mathcal{K}_P$, so $CK||IK \notin \mathcal{K}_P$. By assumption (3), $x$ is uniquely originating in $\sum$, so $RES^* = KDF(CK||IK, SNN||RAND||RES) \subset term(< t, 3 >)$ must originate on a unique initiator strand $s \in \text{Init}_\text{I}[UE, SN, HN, SUCI, RAND, AUTN', RES^*]$, where $SQN' \subset AUTN'$. Since $BK \notin \mathcal{K}_P$, $MAC' = f_1(BK, SQN'||RAND||AMF) \subset AUTN' \subset term(< s, 2 >)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SQN' = SQN$ and $AUTN' = AUTN$. Hence, $s \in \text{Init}_\text{I}[UE, SN, HN,$

$SUCI$, $RAND$, $AUTN$, $RES^*$]. By assumptions (2) and (3), $K_{SN,HN} \notin \mathcal{K}_P$ and $RAND_{SN}$ are uniquely originating in $\sum$, so $\{RAND_{SN}||RES^*\}_{K_{SN,HN}} = term(<t,3>)$ must originate on a unique responder strand $r \in \text{Resp}_\text{I}[UE'', SN, HN, SUCI'', SNN, RAND_{SN}, RAND, H''_1, HXRES^*, RES^*, Result, K''_{SEAF}, SUPI'']$, where $SUPI'' \subset SUCI''$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND_{SN}||SUPI''||RAND||H''_1||HXRES^*\}_{K_{SN,HN}} = term(<r,3>)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $H''_1 = AUTN$, $SUPI'' = SUPI$ and $UE'' = UE$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND||Result||K''_{SEAF}||SUPI\}_{K_{SN,HN}} = term(<r,7>)$ must originate on a server strand $t''$. Since $RAND$ is uniquely originating in $\sum$, $t'' = t$, so $K''_{SEAF} = K_{SEAF}$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND_{SN}||SUCI||SNN\}_{K_{SN,HN}} = term(<t,1>)$ must originate on a responder strand $r'$. Since $RAND_{SN}$ is uniquely originating in $\sum$, $r' = r$, so $SUCI'' = SUCI$. Hence, $r \in \text{Resp}_\text{I}[UE, SN, HN, SUCI, SNN, RAND_{SN}, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$. □

**Theorem 13.** *Suppose: (1) $\sum$ is a space for the 5G-AKA′ protocol, and $\mathcal{C}$ is a bundle containing a server strand $t \in Serv_{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND_{SN}, RAND, AUTN, HXRES^*, Syncf, AUTS]$; (2) $K \notin \mathcal{K}_P$ and $K_{SN,HN} \notin \mathcal{K}_P$; (3) $x$, $RAND$, $RAND_{SN}$ is uniquely originating in $\sum$. Then, $\mathcal{C}$ contains a unique initiator strand $s \in Init_{II}[UE, SN, HN, SUCI, RAND, AUTN, Syncf, AUTS]$ and a unique responder strand $r \in Resp_{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND_{SN}, RAND, AUTN, HXRES^*, Syncf, AUTS]$.*

**Proof of Theorem 13.** Since $BK = KDF(K, x \cdot y \cdot G||SNN)$, $BK \notin \mathcal{K}_P$ according to assumption (2). By assumption (3), $x$ is uniquely originating in $\sum$, so $MAC - S = f_1^*(BK, SQN_{UE}||RAND||AMF_0) \subset AUTS \subset term(<t,3>)$ must originate on a unique initiator strand $s \in \text{Init}_\text{II}[UE, SN, HN, SUCI, RAND, AUTN', Syncf, AUTS]$, where $SQN' \subset AUTN'$. Since $BK \notin \mathcal{K}_P$, $MAC' = f_1(BK, SQN'||RAND||AMF) \subset AUTN' \subset term(<s,2>)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SQN' = SQN$ and $AUTN' = AUTN$. Hence, $s \in \text{Init}_\text{II}[UE, SN, HN, SUCI, RAND, AUTN, Syncf, AUTS]$. By assumptions (2) and (3), $K_{SN,HN} \notin \mathcal{K}_P$ and $RAND_{SN}$ are uniquely originating in $\sum$, so $\{RAND_{SN}||Syncf||RAND||AUTS\}_{K_{SN,HN}} = term(<t,3>)$ must originate on a unique responder strand $r \in \text{Resp}_\text{II}[UE'', SN, HN, SUPI'', SUCI'', SNN, RAND_{SN}, RAND, H''_1, H''_2, Syncf, AUTS]$, where $SUPI'' \subset SUCI''$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND_{SN}||SUPI''||RAND||H''_1||H''_2\}_{K_{SN,HN}} = term(<r,3>)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SUPI'' = SUPI$, $UE'' = UE$, $H''_1 = AUTN$ and $H''_2 = HXRES^*$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND_{SN}||SUCI||SNN\}_{K_{SN,HN}} = term(<t,1>)$ must originate on a responder strand $r'$. Since $RAND_{SN}$ is uniquely originating in $\sum$, $r' = r$, so $SUCI'' = SUCI$. Hence, $r \in \text{Resp}_\text{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND_{SN}, RAND, AUTN, HXRES^*, Syncf, AUTS]$. □

According to Theorems 12 and 13, $HN$ successfully authenticates $UE$ and $SN$, and all fields on the initiator strand and the responder are agreed with the HN, so MitM attacks are prevented.

In addition, those attacks in Section 3.3 are overcome as follows:

(1) Although $HN$ cannot find that $SUCI$ is replayed because $SUCI$ does not contain the challenge of the HN (i.e., $RAND$), $UE$ can find whether $SUCI$ is replayed because $BK = KDF(K, x \cdot y \cdot G||SNN)$ is used to calculate $AUTN$. Hence, this does not affect the security of the 5G-AKA′ protocol.
(2) Since $MACf$ is replaced with a timeout mechanism on the HN, MAC failure attacks are prevented.
(3) Since the HN sends $K_{SEAF}$ and $SUPI$ together with $RAND$, they can be agreed with the HN.

*4.5. The Responder's Guarantee of the 5G-AKA′ Protocol*

**Theorem 14.** *Suppose: (1) $\sum$ is a space for the 5G-AKA′ protocol, and $\mathcal{C}$ is a bundle containing a responder strand $r \in Resp_I[UE, SN, HN, SUCI, SNN, RAND_{SN}, RAND, H_1, H_2, H_3, Result, K_{SEAF}, SUPI]$; (2) $K \notin \mathcal{K}_P$ and $K_{SN,HN} \notin \mathcal{K}_P$; (3) $x$, $RAND$, $RAND_{SN}$ is uniquely originating in $\sum$. Then, $\mathcal{C}$ contains a unique server strand $t \in Serv_I[UE, SN, HN, SUCI, SNN, RAND_{SN}, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$ and a unique initiator strand $s \in Init_I[UE, SN, HN, SUCI, RAND, AUTN, RES*]$.*

**Proof of Theorem 14.** By assumptions (2) and (3), $K_{SN,HN} \notin \mathcal{K}_P$ and $RAND$ are uniquely originating in $\sum$, so $\{RAND_{SN}||SUPI||RAND||H_1||H_2\}_{K_{SN,HN}} = term(< r,3 >)$ must uniquely originate on a server strand $t$ according to Definitions 5 to 7.

(1) If $t$ is a server strand of Definition 5, then $t \in \text{Serv}_\text{I}[UE, SN, HN, SUCI', SNN, RAND_{SN}, RAND, AUTN', (HXRES^*)', (RES^*)', Result, K'_{SEAF}, SUPI]$, where $SUPI \subset SUCI'$, $x' \subset AUTN'$, $x' \subset (HXRES^*)'$, $x' \subset (RES^*)'$, $x' \subset K'_{SEAF}$ and $K'_{SEAF}$ is generated for $SUPI$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND||Result||K_{SEAF}||SUPI\}_{K_{SN,HN}} = term(< r,7 >)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $K'_{SEAF} = K_{SEAF}$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND_{SN}||SUCI'||SNN\}_{K_{SN,HN}} = term(< t,1 >)$ must originate on a responder strand $r'$. Since $RAND_{SN}$ is uniquely originating in $\sum$, $r' = r$, so $SUCI' = SUCI$ and $x' = x$ according to assumption (1). As a result, $AUTN' = AUTN$, $(HXRES^*)' = HXRES^*$ and $(RES^*)' = RES^*$. Hence, $t \in \text{Serv}_\text{I}[UE, SN, HN, SUCI, SNN, RAND_{SN}, RAND, AUTN, HXRES^*, RES^*, Result, K_{SEAF}, SUPI]$. Since $BK = KDF(K, x \cdot y \cdot G||SNN)$, $BK \notin \mathcal{K}_P$ according to assumption (2). Because $CK = f_3(BK, RAND)$ and $IK = f_4(BK, RAND)$, $CK \notin \mathcal{K}_P$ and $IK \notin \mathcal{K}_P$, so $CK||IK \notin \mathcal{K}_P$. By assumption (3), $x$ is uniquely originating in $\sum$, so $RES^* = KDF(CK||IK, SNN||RAND||RES) \subset term(< t,3 >)$ must originate on a unique initiator strand $s \in \text{Init}_\text{I}[UE, SN, HN, SUCI, RAND, AUTN'', RES^*]$, where $SQN'' \subset AUTN''$. Since $BK \notin \mathcal{K}_P$, $MAC'' = f_1(BK, SQN''||RAND||AMF) \subset AUTN'' \subset term(< s,2 >)$ must originate on a server strand $t''$. Since $RAND$ is uniquely originating in $\sum$, $t'' = t$, so $SQN'' = SQN$ and $AUTN'' = AUTN$. Hence, $s \in \text{Init}_\text{I}[UE, SN, HN, SUCI, RAND, AUTN, RES^*]$.

(2) If $t$ is a server strand of Definition 6, then $t \in \text{Serv}_\text{II}[UE, SN, HN, SUPI, SUCI', SNN, RAND_{SN}, RAND, AUTN', (HXRES^*)', Syncf, AUTS']$, where $SUPI \subset SUCI'$, $x' \subset AUTN'$, $x' \subset (HXRES^*)'$ and $x' \subset AUTS'$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND_{SN}||Syncf||RAND||AUTS'\}_{K_{SN,HN}} = term(< t,3 >)$ must originate on a responder strand $r' \in \text{Resp}_\text{II}[UE'', SN, HN, SUPI'', SUCI'', SNN, RAND_{SN}, RAND, H''_1, H''_2, Syncf, AUTS']$, so $RAND_{SN}$ originates on $term(< r',2 >)$. By assumptions (1) and (2), $RAND_{SN}$ originates on $term(< r,2 >)$. Since $RAND_{SN}$ is uniquely originating in $\sum$, $r' = r$. However, $r' \in \text{Resp}_\text{II}$ and $r \in \text{Resp}_\text{I}$, $r' \neq r$. Hence, $t$ is not a server strand of Definition 6. □

**Theorem 15.** *Suppose: (1) $\sum$ is a space for the 5G-AKA′ protocol, and $\mathcal{C}$ is a bundle containing a responder strand $r \in Resp_{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND_{SN}, RAND, H_1, H_2, Syncf, H_4]$; (2) $K \notin \mathcal{K}_P$ and $K_{SN,HN} \notin \mathcal{K}_P$; (3) $x$, $RAND$, $RAND_{SN}$ is uniquely originating in $\sum$. Then, $\mathcal{C}$ contains a unique server strand $t \in Serv_{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND_{SN}, RAND, AUTN, HXRES^*, Syncf, AUTS]$ and a unique initiator strand $s \in Init_{II}[UE, SN, HN, SUCI, RAND, AUTN, Syncf, AUTS]$.*

**Proof of Theorem 15.** By assumptions (2) and (3), $K_{SN,HN} \notin \mathcal{K}_P$ and $RAND$ and uniquely originating in $\sum$, so $\{RAND_{SN}||SUPI||RAND||H_1||H_2\}_{K_{SN,HN}} = term(< r,3 >)$ must uniquely originate on a server strand $t$ according to Definitions 5 to 7.

(1) If $t$ is a server strand of Definition 5, then $t \in \text{Serv}_\text{I}[UE, SN, HN, SUCI', SNN, RAND_{SN}, RAND, AUTN', (HXRES^*)', (RES^*)', Result, K'_{SEAF}, SUPI]$, where

$SUPI \subset SUCI'$, $x' \subset AUTN'$, $x' \subset (HXRES^*)'$, $x' \subset (RES^*)'$, $x' \subset K'_{SEAF}$ and $K'_{SEAF}$ is generated for $SUPI$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND_{SN}||(RES^*)'\}_{K_{SN,HN}} = term(< t,3 >)$ must originate on a unique responder strand $r' \in \text{Resp}_\text{I}[UE'', SN, HN, SUCI'', SNN, RAND_{SN}, RAND, H''_1, (HXRES^*)', (RES^*)', Result, K''_{SEAF}, SUPI'']$, so $RAND_{SN}$ originates on $term(< r',2 >)$. By assumptions (1) and (2), $RAND_{SN}$ originates on $term(< r,2 >)$. Since $RAND_{SN}$ is uniquely originating in $\sum$, $r' = r$. However, $r' \in \text{Resp}_\text{I}$ and $r \in \text{Resp}_\text{II}$, $r' \neq r$. Hence, $t$ is not a server strand of Definition 5.

(2) If $t$ is a server strand of Definition 6, then $t \in \text{Serv}_\text{II}[UE, SN, HN, SUPI, SUCI', SNN, RAND_{SN}, RAND, AUTN', (HXRES^*)', Syncf, AUTS']$, where $SUPI \subset SUCI'$, $x' \subset AUTN'$, $x' \subset (HXRES^*)'$ and $x' \subset AUTS'$. Since $K_{SN,HN} \notin \mathcal{K}_P$, $\{RAND_{SN}||SUCI'||SNN\}_{K_{SN,HN}} = term(< t,1 >)$ must originate on a responder strand $r'$. Since $RAND_{SN}$ is uniquely originating in $\sum$, $r' = r$, so $SUCI' = SUCI$ and $x' = x$ according to assumption (1). As a result, $AUTN' = AUTN$, $(HXRES^*)' = HXRES^*$ and $AUTS' = AUTS$. Hence, $t \in \text{Serv}_\text{II}[UE, SN, HN, SUPI, SUCI, SNN, RAND_{SN}, RAND, AUTN, HXRES^*, Syncf, AUTS]$. Since $BK = KDF(K, x \cdot y \cdot G||SNN)$, $BK \notin \mathcal{K}_P$ according to assumption (2). By assumption (3), $x$ is uniquely originating in $\sum$, so $MAC - S = f_1^*(BK, SQN_{UE}||RAND||AMF_0) \subset AUTS \subset term(< t,3 >)$ must originate on a unique initiator strand $s \in \text{Init}_\text{II}[UE, SN, HN, SUCI, RAND, AUTN'', Syncf, AUTS]$, where $SQN'' \subset AUTN''$. Since $BK \notin \mathcal{K}_P$, $MAC'' = f_1(BK, SQN''||RAND||AMF) \subset AUTN'' \subset term(< s,2 >)$ must originate on a server strand $t'$. Since $RAND$ is uniquely originating in $\sum$, $t' = t$, so $SQN'' = SQN$ and $AUTN'' = AUTN$. Hence, $s \in \text{Init}_\text{II}[UE, SN, HN, SUCI, RAND, AUTN, Syncf, AUTS]$. □

According to Theorems 14 and 15, $SN$ successfully authenticates $UE$ and $HN$, and all fields on the initiator strand and the responder are agreed with the HN, so MitM attacks are prevented.

In addition, those attacks in Section 3.4 are overcome as follows:

(1) Since $SUPI$ is added to the second message between the SN and the HN, and $RAND$ is added to the fourth message between the SN and the HN, both $K_{SEAF}$ and $SUPI$ on the HN can be agreed with the SN, which means that $SN$ successfully authenticates $UE$ and obtains the corresponding $K_{SEAF}$.

(2) Since $MACf$ is replaced with a timeout mechanism on the HN, MAC failure attacks are prevented. Further, $RAND||AUTN$ on the UE cannot be replayed maliciously to generate $Syncf$ because $BK = KDF(K, x \cdot y \cdot G||SNN)$. As a result, the penetrator cannot take advantage of $Syncf$ and $MACf$ to performed cross attacks.

(3) Since the challenge–response mechanism between the SN and the HN is added, the messages received by the SN cannot be replayed, preventing Dos attacks on the SN.

## 5. Discussion

### *5.1. Security of the 5G-AKA' Protocol*

According to the above security analysis of the latest version of the 5G AKA protocol, twenty-one attack scenarios can be obtained, where thirteen attack scenarios are related to $MACf$. In our proposed 5G-AKA' protocol, $MACf$ is replaced with a timeout mechanism on the HN, so the thirteen attack scenarios are eliminated. As a result, those attacks in the thirteen attack scenarios are eliminated, including MAC failure attacks.

Without considering $MACf$, the comparative analysis of authentication properties [28–30] between the latest version of the 5G AKA protocol and our proposed 5G-AKA' protocol is shown in Table 1.

**Table 1.** The comparative analysis of authentication properties between the two protocols.

| Protocols | Authentication Properties | UE to SN | UE to HN | SN to UE | SN to HN | HN to UE | HN to SN |
|---|---|---|---|---|---|---|---|
| 5G AKA | Injection agreement | No | No | No | No | No | No |
| | Non-injection agreement | No | No | No | No | No | No |
| | Weaker agreement | No | Yes | No | Yes | Yes | Yes |
| 5G-AKA′ | Injection agreement | Yes | Yes | Yes | Yes | Yes | Yes |
| | Non-injection agreement | No | No | No | No | No | No |
| | Weaker agreement | No | No | No | No | No | No |

From Table 1, in the latest version of the 5G AKA protocol, only the weaker agreement can be established, and even weak agreement cannot be established in the cases of "UE to SN" and "SN to UE", because the UE cannot authenticate the SN, and the SN cannot authenticate the UE. However, in our proposed 5G-AKA′ protocol, mutual authentication and injection agreement among the UE, the SN and the HN can be established in all cases according to the security analysis of the 5G-AKA′ protocol.

According to the above security analysis of the latest version of the 5G AKA protocol, based on those missing agreements, the penetrator can perform MitM attacks and cross attacks. Additionally, based on replayed messages, replay attacks and masquerading attacks can be performed, the location privacy of the UE can be compromised and DoS attacks on the SN can be formed. However, according to the above security analysis of the 5G-AKA′ protocol, our proposed 5G-AKA′ protocol has overcome these attacks.

In terms of secrecy properties, the keys established in the latest version of the 5G AKA protocol are secret. However, if $K$ is leaked, then the attacker can calculate $K_{AUSF}$ and $K_{SEAF}$ based on those messages transmitted in the past run of the protocol. As a result, the attacker can decrypt those encrypted messages transmitted in the past run of the protocol. Therefore, the latest version of the 5G AKA protocol does not provide perfect forward secrecy. However, in our proposed 5G-AKA′ protocol, $K$ is replaced with $BK = KDF(K, x \cdot y \cdot G||SNN)$, providing perfect forward secrecy based on Diffie–Hellman exchange.

Therefore, our proposed 5G-AKA′ protocol is secure and can overcome those security problems of the latest version of the 5G AKA protocol. The comparative analysis of security properties between the 5G-AKA′ protocol and some recently improved 5G AKA protocols [22–24] is shown in Table 2.

**Table 2.** The comparative analysis of security properties between the 5G-AKA′ protocol and some recently improved 5G AKA protocols [22–24].

| Security Properties | 5G AKA | [22] | [23] | [24] | 5G-AKA′ |
|---|---|---|---|---|---|
| Implement mutual authentication | No | No | No | No | Yes |
| Prevent MitM attacks | No | No | No | No | Yes |
| Resistance against cross attacks | No | No | No | Yes | Yes |
| Compromise the location privacy of the UE | No | Yes | Yes | Yes | Yes |
| Prevent masquerading attacks | No | No | No | No | Yes |
| Resistance against replay attacks | No | No | No | No | Yes |
| Defend against DoS attacks on the SN | No | No | No | No | Yes |
| Prevent MAC failure attacks | No | No | No | Yes | Yes |
| Provide key secrecy | Yes | Yes | Yes | Yes | Yes |
| Provide perfect forward secrecy | No | No | No | No | Yes |

From Table 2, only some security properties can be guaranteed in the 5G AKA protocol and these recently improved 5G AKA protocols, but all security properties can be guaranteed in our proposed 5G-AKA′ protocol.

In [22], $AUTN$ contains the challenge of the UE (i.e., $r_{UE}$), so the first received message of the UE cannot be a replayed message, preventing the location privacy of the UE from being compromised. However, $AUTN$ does not contains $SNN$, so the UE cannot authenticate

the SN. Because the UE and the HN cannot reach an agreement in $SNN$, MitM attacks can be performed. Since the MAC failure is inherited from the 5G AKA protocol, cross attacks and MAC failure attacks still exist in the protocol of [22]. The received messages of the SN do not contain the challenge of the SN (i.e., $r_{SEAF}$), so these messages can be replayed messages, forming replay attacks, masquerading attacks and Dos attacks on the SN. In addition, $K_{AUSF}$ and $K_{SEAF}$ are encrypted, so key secrecy is provided, but perfect forward secrecy cannot be provided because $K_{AUSF}$ and $K_{SEAF}$ can be calculated when $K$ is leaked.

In [23], the Eph Private key and Eph Public key of the UE, the public/private key pair of the SN and the public/private key pair of the HN are used to ensure the security of the channel between the UE and the SN, the security of channel between the UE and the HN, and the security of channel between the SN and the HN. Since the first received message of the UE is encrypted by the Eph Public key of the UE, this means that the message can only be decrypted by the Eph Private key of the UE, so it cannot be a replayed message, preventing the location privacy of the UE being compromised. However, the other parts fully inherit the 5G AKA protocol, so the other attacks of the 5G AKA protocol still exist in the protocol of [23]. Similarly, perfect forward secrecy cannot be provided.

In [24], both the synchronization failure and the MAC failure are constructed as the format of $RES^*$, making it impossible to distinguish them, so as to prevent the location privacy of the UE from being compromised and prevent cross attacks and MAC failure attacks. However, the other parts fully inherit the 5G AKA protocol, so the other attacks of the 5G AKA protocol still exist in the protocol of [24]. Similarly, perfect forward secrecy cannot be provided.

Therefore, our proposed 5G-AKA' protocol is better than the 5G AKA protocol, and these recently improved 5G AKA protocols in security.

### *5.2. Performance of the 5G-AKA' Protocol*

The comparative analysis between the 5G-AKA' protocol and some recently improved 5G AKA protocols [22–24] in the number of messages, the number of fields, the amount of calculation and backward compatibility is shown in Table 3.

**Table 3.** The comparative analysis between the 5G-AKA' protocol and some recently improved 5G AKA protocols [22–24] in the number of messages, the number of fields, the amount of calculation and backward compatibility.

| Comparative Items | 5G AKA | [22] | [23] | [24] | 5G-AKA' |
|---|---|---|---|---|---|
| The number of messages | *MN* | *MN* | *MN* | *MN* | *MN*-2 |
| The number of fields | *FN* | *FN* + 9 | *FN*-1 | *FN* + 2 | *FN* + 4 |
| The amount of calculation | *CA* | *CA* + 2*F* | *CA* + 4*PED*-1*ECDH*-2*F* | *CA* + 2*PED* + 1*F* | *CA* + 1*F* |
| Backward compatibility | – | Yes | No | No | Yes |

In Table 3, *MN* denotes the number of messages of the 5G AKA protocol. *FN* denotes the number of fields of the 5G AKA protocol. *CA* denotes the amount of calculation of the 5G AKA protocol. Note that the number of messages and the number of fields in Table 3 are the number of messages and the number of fields among the UE, the SN and the HN. *ECDH* denotes the generation and verification of an elliptic curve Diffie–Hellman (ECDH) exchange. *PED* denotes the encryption and decryption based on a public and private key pair. *F* denotes the generation and verification of a key function, a key derivation function, a MAC function or a hash function, which are grouped into one category because they have a similar amount of calculation [27]. According to [26], the computation overhead of the generation or verification of an ECDH exchange is 1290 us, the computation overhead of the encryption based on a public key is 2580 us, the computation overhead of the decryption based on a private key is 1750 us, the computation overhead of the hash function based on SHA-256 is 3.8 us, and the computation overhead of the MAC function based on HMAC-SHA256 is 67 us.

In our proposed 5G-AKA′ protocol, two messages related to $MACf$ are cut down because $MACf$ is replaced with a timeout mechanism on the HN. Four $RAND_{SN}$, one $RAND$, and one $SUPI$ are added to the messages between the SN and the HN, while two $MACf$ are cut down, so four fields are added. Since $K$ is replaced with $BK = KDF(K, x \cdot y \cdot G||SNN)$ on the UE and the HN, the calculation amount of one $F$ is added. From Table 3, compared with other protocols, our proposed 5G-AKA′ protocol reduces two messages. The 5G-AKA′ protocol adds more fields than the protocols in [23] and [24], but less than the protocol in [22]. In the amount of calculation, our proposed 5G-AKA′ protocol increases the least, while the protocols in [23] and [24] increase the most because they introduce multiple public-key encryption and decryption. Hence, our proposed 5G-AKA′ protocol is efficient. Especially for the UE, only a key derivation function is added, but one field and one message are reduced.

In addition, the protocols in [23] and [24] destroys the structure of the messages instead of adding fields to the messages or extending fields in the messages, so they are not backward compatible. Our proposed 5G-AKA′ protocol only extends $K$ and adds some fields to the messages between the SN and the HN, so it is forward compatible.

## 6. Conclusions

In this paper, we summarize the 5G AKA protocol into three cases according to the overview of the latest version of the 5G AKA protocol and then use the mixed strand space model for mixed protocols to formally analyze the security of the 5G AKA protocol. As a result, twenty-one attack scenarios of the 5G AKA protocol are obtained, where thirteen attack scenarios are related to the MAC failure, including MAC failure attacks. Based on these attack scenarios, we find that the mutual authentication between the UE and the SN cannot be established, and only the weaker agreement can be established among the UE, the SN and the HN, resulting in MitM attacks and cross attacks. Further, by replaying some message to the UE and the SN, replay attacks and masquerading attacks can be performed, the location privacy of the UE can be compromised and DoS attacks on the SN can be formed. In addition, the 5G AKA protocol cannot provide perfect forward secrecy.

To overcome these attacks, we propose a 5G-AKA′ protocol, in which the pre-shared key between the UE and the HN is replaced with a derivation key of the pre-shared key, the challenge–response mechanism between the SN and the HN is added, the SUPI of the UE is added to the second message between the SN and the HN, and the MAC failure procedure is replaced with a timeout mechanism on the HN. According to the 5G-AKA′ protocol, we summarize the 5G-AKA′ protocol into two cases and then use the mixed strand space model for mixed protocols to formally analyze the security of the 5G-AKA′ protocol. As a result, no attack scenario is obtained.

By discussion and analysis, the 5G-AKA′ protocol can establish mutual authentication and injection agreement among the UE, the SN and the HN, and can overcome the above security problems of the latest version of the 5G AKA protocol. Therefore, the 5G-AKA′ protocol is secure. The comparative analysis of security properties between the 5G-AKA′ protocol and some recently improved 5G AKA protocols shows that the 5G-AKA′ protocol is better than these recently improved 5G AKA protocols in security. The comparative analysis between the 5G-AKA′ protocol and some recently improved 5G AKA protocols in the number of messages, the number of fields, the amount of calculation and backward compatibility shows that the 5G-AKA′ protocol is efficient, and is backward compatible with the 5G AKA protocol.

Recently, some authors also point out that the protection mechanism of SQN can be defeated due to its use of XOR in the 5G AKA protocol. This paper does not consider this security problem, and we will further study this security problem in the future.

**Author Contributions:** Methodology, Y.X.; formal analysis, S.G. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the National Natural Science Foundation of China (No.61741216, 61402367), Shaanxi Science and Technology Co-ordination & Innovation Project (No.2016KTTSGY01-03), National Key Research and Development Program (No. 2018YFC08242-04) and New Star Team Project of Xi'an University of Posts and Telecommunications.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Abbreviations

| | |
|---|---|
| 3GPP | 3rd generation partnership project |
| 4G | 4th generation mobile communication technology |
| 5G | 5th generation mobile communication technology |
| ABBA | anti-bidding down between architectures |
| AKA | authentication and key agreement |
| AKMA | authentication and key management for applications |
| AMF | authentication management field |
| ARPF | authentication credential repository and processing function |
| AUSF | authentication server function |
| DoS | denial of service |
| EAP-AKA' | improved extensible authentication protocol method for 3rd generation authentication and key agreement |
| EAP-TLS | extensible authentication protocol method for transport layer security |
| ECDH | elliptic curve Diffie–Hellman |
| EPS | evolution packet system |
| HN | home network |
| ICB | initial counter block |
| LTE | long-term evolution |
| MAC | message authentication code |
| ME | mobile equipment |
| MitM | man-in-the-middle attacks |
| PKI | public key infrastructure |
| SEAF | security anchor function |
| SIDF | subscriber identity de-concealing function |
| SN | serving network |
| SNN | serving network name |
| SQN | sequence number |
| SUCI | subscription concealed identifier |
| SUPI | subscription permanent identifier |
| TS | technical specification |
| UDM | unified data management |
| UE | user equipment |
| USIM | universal subscriber identity module |
| XOR | exclusive-or |

## Notations

| | |
|---|---|
| $ABBA$ | the ABBA parameter |
| $AK$, $AK^*$ | two anonymity keys |
| $AKMA$ | the AKMA indication and routing indicator |
| $AMF$ | the authentication management field |
| $AMF_0$ | a dummy value of all zeros |
| $AUTN$ | an authentication token of the HN |
| $AUTS$ | a resynchronization parameter |
| $BK$ | a base key derived from $K$ |

| | |
|---|---|
| $CA$ | the amount of calculation of the 5G AKA protocol |
| $CK$ | a cipher key |
| $ECDH$ | the generation and verification of an ECDH exchange |
| $EK$ | an encryption key |
| $f_1()$, $f_1^*()$, $f_2()$ | three message authentication functions |
| $f_3()$, $f_4()$, $f_5()$, $f_5^*()$ | four key generating functions |
| $F$ | the generation and verification of a key function or a key derivation function or a MAC function or a hash function |
| $FN$ | the number of fields (among the UE, the SN and the HN) of the 5G AKA protocol |
| $HMAC()$ | a hash function for computing MAC |
| $H_1$, $H_2$, $H_3$, $H_4$ | four messages that are not inspected by the SN |
| $HN$ | the HN |
| $HRES^*$ | a hashing response from $RES^*$ |
| $HXRES^*$ | a hashing expected response from $XRES^*$ |
| $ICB$ | an initial counter block |
| $IK$ | an integrity key |
| $K$ | a long-term key between the UE and the HN |
| $K_{AMF}$ | a key between the UE and the access and mobility management function |
| $K_{AUSF}$ | a key derived from $CK$ and $IK$ |
| $\mathcal{K}_P$ | the key set of the penetrator |
| $K_{SEAF}$ | a key derived from $K_{AUSF}$ |
| $K_{SN,HN}$ | the session key between the SN and the HN |
| $KDF()$ | a key derivation function |
| $MAC$ | a MAC of the HN |
| $MACf$ | the "MAC failure" indication |
| $MAC_{UE}$ | a MAC of the UE |
| $MK$ | a MAC key |
| $MN$ | the number of messages (among the UE, the SN and the HN) of the 5G AKA protocol |
| $ngKSI$ | identifying the $K_{AMF}$ and the partial native security context |
| $PED$ | the encryption and decryption based on a public and private key pair |
| $RAND$ | an unpredictable challenge of the HN |
| $RAND_{SN}$, $r_{SEAF}$ | two unpredictable challenges of the SEAF |
| $RES$ | a response |
| $RES^*$ | a response from $RES$ |
| $Result$ | the authentication result |
| $r_{UE}$ | an unpredictable challenge of the UE |
| $SHA256()$ | a hash function |
| $SN$ | the SN |
| $SNN$ | the serving network name of the SN |
| $SQN$ | a fresh sequence number generated by the HN |
| $SQN_{UE}$ | the highest sequence number the USIM has accepted |
| $SUCI$ | a SUCI of the UE |
| $SUPI$ | a SUPI of the UE |
| $Syncf$ | the "Synchronization failure" indication |
| $UE$ | the UE |
| $x$ | an ephemeral private key of the UE for Diffie-Hellman exchange |
| $x \cdot G$ | an ephemeral public key of the UE for Diffie-Hellman exchange |
| $XMAC$ | a MAC locally computed by the UE |
| $XRES$ | an expected response |
| $XRES^*$ | an expected response from $XRES$ |
| $y$ | an ephemeral private key of the HN for Diffie-Hellman exchange |
| $y \cdot G$ | an ephemeral public key of the HN for Diffie-Hellman exchange |

## References


1. Xu, S.; Gan, Z. Review and trends of 5G security technology. *Radio Commun. Technol.* **2020**, *46*, 133–138.
2. 3GPP TS 33.102: 3G Security; Security Architecture. Available online: https://www.3gpp.org/DynaReport/33102.htm (accessed on 26 January 2022).
3. 3GPP TS 33.401: 3GPP System Architecture Evolution (SAE); Security Architecture. Available online: https://www.3gpp.org/DynaReport/33401.htm (accessed on 26 January 2022).
4. 3GPP TS 33.501: 3GPP System Architecture Evolution (SAE); Security Architecture. Available online: https://www.3gpp.org/DynaReport/33501.htm (accessed on 26 January 2022).
5. Ferrag, M.A.; Maglaras, L.; Argyriou, A.; Kosmano, D.; Janicke, H. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *J. Netw. Comput. Appl.* **2018**, *101*, 55–82. [CrossRef]
6. Jover, R.P.; Marojevic, V. Security and protocol exploit analysis of the 5G specifications. *IEEE Access* **2019**, *7*, 24956–24963. [CrossRef]
7. Ahmad, I.; Shahabuddin, S.; Kumar, T.; Okwuibe, J.; Ylianttila, M. Security for 5G and beyond. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3682–3722. [CrossRef]
8. Khan, R.; Kumar, P.; Jayakody, D.N.K.; Liyanage, M. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 196–248. [CrossRef]
9. Hussain, S.R.; Echeverria, M.; Karim, I.; Chowdhury, O.; Berino, E. 5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 669–684.
10. Hussain, S.R.; Echeverria, M.; Chowdhury, O.; Li, N.; Bertino, E. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information. In Proceedings of the 26th Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 24–27 February 2019; pp. 1–15.
11. Khan, H.; Martin, K.M. A survey of subscription privacy on the 5G radio interface-the past, present and future. *J. Informat. Secur. Appl.* **2020**, *53*, 102537. [CrossRef]
12. Security Vulnerability in 5G-AKA Draft. Available online: https://www.cs.ox.ac.uk/5G-analysis/5G-AKA-draft-vulnerability.pdf (accessed on 23 February 2022).
13. Meier, S.; Schmidt, B.; Cremers, C.; Basin, D. The Tamarin prover for the symbolic analysis of security protocols. In Proceedings of the 25th International Conference on Computer Aided Verification, Saint Petersburg, Russia, 13–19 July 2013; pp. 696–701.
14. Basin, D.; Dreier, J.; Hirschi, L.; Radomirovic, S.; Sasse, R.; Stettler, V. A formal analysis of 5G authentication. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, 15–19 October 2018; pp. 1383–1396.
15. Liu, F.; Peng, J.; Zuo, M. Toward a secure access to 5G network. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1121–1128.
16. Borgaonkar, R.; Hirschi, L.; Park, S.; Shaik, A. New privacy threat on 3G, 4G, and upcoming 5G AKA Protocols. *Proc. Priv. Enhancing Technol.* **2019**, *3*, 108–127. [CrossRef]
17. Cremers, C.; Dehnel-Wild, M. Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion. In Proceedings of the 26th Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 24–27 February 2019; pp. 1–15.
18. Koutsos, A. The 5G-AKA authentication protocol privacy. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS & P), Stockholm, Sweden, 17–19 June 2019; pp. 464–479.
19. Bana, G.; Comon-Lundh, H. Towards unconditional soundness: Computationally complete symbolic attacker. In Proceedings of the First International Conference on Principles of Security and Trust (ETAPS), Tallinn, Estonia, 24 March–1 April 2012; pp. 189–208.
20. Bana, G.; Comon-Lundh, H. A computationally complete symbolic attacker for equivalence properties. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 609–620.
21. Braeken, A.; Liyanage, M.; Kumar, P.; Murphy, J. Novel 5G authentication protocol to improve the resistance against active attacks and malicious serving networks. *IEEE Access* **2019**, *7*, 64040–64052. [CrossRef]
22. Gharsallah, I.; Smaoui, S.; Zarai, F. A secure efficient and lightweight authentication protocol for 5G cellular networks: SEL-AKA. In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 1311–1316.
23. Hu, X.; Liu, C.; Liu, S.; Cheng, X. A security enhanced 5G authentication scheme for insecure channel. *IEICE Trans. Inf. Syst.* **2020**, *103*, 711–713. [CrossRef]
24. Hu, X.; Liu, C.; Liu, S.; Li, J.; Cheng, X. A vulnerability in 5G authentication protocols and its Countermeasure. *IEICE Trans. Inf. Syst.* **2020**, *103*, 1806–1809. [CrossRef]
25. Edris, E.K.K.; Aiash, M.; Loo, J.K. Formal verification and analysis of primary authentication based on 5G-AKA protocol. In Proceedings of the 2020 7th International Conference on Software Defined Systems (SDS), Paris, France, 20–23 April 2020; pp. 256–261.
26. Ouaissa, M.; Ouaissa, M. An improved privacy authentication protocol for 5G mobile networks. In Proceedings of the 2020 International Conference on Advances in Computing, Communication & Materials (ICACCM), Dehradun, India, 21–22 August 2020; pp. 136–143.

27. Parne, B.L.; Gupta, S.; Gandhi, K.; Meena, S. PPSE: Privacy preservation and security efficient AKA protocol for 5G communication networks. In Proceedings of the 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), New Delhi, India, 14–17 December 2020; pp. 1–6.
28. Fábrega, F.J.T.; Herzog, J.C.; Guttman, J.D. Mixed strand spaces. In Proceedings of the 12th IEEE Computer Security Foundations Workshop, Mordano, Italy, 30–30 June 1999; pp. 72–82.
29. Fábrega, F.J.T.; Herzog, J.C.; Guttman, J.D. Strand space: Proving security protocols correct. *J. Comput. Secur.* **1999**, *7*, 191–230. [CrossRef]
30. Herzog, J.C. The Diffie-Hellman key-agreement scheme in the strand-space model. In Proceedings of the 16th IEEE Computer Security Foundation Workshop, Pacific Grove, CA, USA, 30 June–2 July 2003; pp. 234–247.