IMSI-based Routing and Identity Privacy in 5G

Mohsin Khan, Valtteri Niemi
University of Helsinki and
Helsinki Institute for Information Technology
Helsinki, Finland
mohsin.khan, valtteri.niemi@helsinki.fi

Philip Ginzboorg
Huawei Technologies and
Aalto University
Finland
philip.ginzboorg@huawei.com

***Abstract*—In 5G, identity privacy of a user is proposed to be protected by concealing the identifier of the user. In order to route the concealed identifier to the appropriate destination, certain information about the international mobile subscriber identity (IMSI) - country code and network code, need to be revealed. But, as was recently pointed out, the routing of requests for authentication information between visited and home network and also within the home network, needs more information about the IMSI to be revealed. Recently it was also revealed that the serving network needs to be able to identify a user with IMSI without relying on the home network for lawful interception purposes. In this new context, we re-examine published alternative solutions of identity privacy. We find the previously promising solutions e.g., solution based on public key of home network become less promising. We find the solution based on identity based encryption becomes more promising than it was before.**

I. Introduction

In a mobile computing environment, the privacy of a user's current physical location is desirable [16], [31]. This is because lack of the location privacy enables third parties to track a user. To achieve location privacy, we need the privacy of the users' identities. In the 3GPP-defined mobile networks, a user has many identities, e.g., international mobile subscriber identity (IMSI), international mobile equipment identity (IMEI), mobile station international subscriber directory number (MSISDN), and many more. Privacy of all of these identities need to be protected. Among all of these identities, IMSI is the most difficult to protect. This is because IMSI is used for the identification of a user that is unknown (e.g., when connecting for the first time) to the network [3], hence have no confidentiality protection. Serious effort has been put to solve this problem by the academic and 3GPP community. However, IMSI privacy is still not achieved, the so called IMSI catchers are still in existence [18], [17], [25] and have become very cheap (in the order of hundreds of Euros) off-the-shelf [30], [27] technology. The alarming news is that the IMSI catchers are no more only an idle threat but have become a reality to the extent of mass surveillance [28].

Identity privacy is a major requirement in 5G [8]. Many solutions have been proposed to defeat IMSI catchers [6]. Most of the solutions are based on some cryptographic techniques. Comparative analysis between the competitive solutions have been published [23]. There are pros and cons in every solution. 3GPP community is now at the verge of finalizing the specification for the first phase of 5G technology. A solution based on public key cryptography has been chosen to protect the privacy of IMSI [8] (in Section 6.12.2). In this solution, the home network (HN) owns the public-private key pair. The user equipment (UE) shall generate a concealed identity with the raw public key that was securely provisioned to the user in control of the HN. We call this solution as root-key based solution.

An issue about routing authentication information has surfaced recently [11]. We will explain this issue in Section IV. To solve this issue, the root-key based solution needs to reveal more information about the identity of a user. This reduces the effectiveness of root-key based solution. Another issue around lawful interception (LI) has been noticed recently [11]. We will explain the issue in Section V. In Section III, we categorize the promising solutions based on the cryptographic techniques used. In Section VI, we will present a comparative analysis of the alternative categories of solutions in the light of these two new concerns as well as the relevant old concerns [23], [22]. We will see that the balance of pros and cons between different solutions changes significantly. The root-key based solution which appeared to be quite straightforward and effective solution [23] becomes less effective and requires more implementation effort. On the other hand, a solution based on identity based encryption (IBE) [23], [22] which had its own cons, solves both of the concerns of IMSI-based routing and LI. In this light we will argue that solution based on identity based encryption could be the most effective and also fairly straightforward solution to protect the privacy of IMSI.

In order to present a smooth discussion, we need to first explain some background. We will present an abstract view of a mobile network. This view is abstract enough to cover both LTE and 5G, even earlier generations. We will discuss how IMSI is used, how privacy of IMSI is vulnerable in the legacy networks. We will also discuss the principles of different categories of solutions very briefly.

II. Background

1) IMSI: A unique International Mobile Subscriber Identity (IMSI) shall be allocated to each mobile subscriber in the GSM/UMTS/EPS system [2]. An IMSI is usually presented as a 15 digit number but can be shorter. The first 3 digits are the mobile country code (MCC), which are followed by the mobile network code (MNC), either 2 or 3 digits. The length of the MNC depends on the value of the MCC. The remaining digits are the mobile subscription identification number (MSIN) within the network's customer base [2].

In the legacy networks – e.g., LTE, when a user equipment (UE) tries to connect to a network for the first time, the UE has

to identify itself using IMSI [3]. Once the UE is identified, an authentication protocol (e.g., EPS AKA [3]) is run in between the UE and the network. If the authentication protocol runs successfully, the network serves the UE with the services the UE is authorized to avail.

2) Mobile Network: A mobile network consists of UE, serving network (SN) and HN. Both of the SN and HN consist of radio access network (RAN) and core network (CN). The RAN of SN provides the connectivity in between UE and CN of SN. On the other hand, the CN of SN connects itself with the CN of HN via IPX. Note that in a non-roaming situation, the SN and HN are the same network. See Figure 1.

3) IMSI Catchers: There are two more entities which are not part of the network but relevant in our discussion, because they attack the network. They are passive IMSI catchers and active IMSI catchers [22]. The interface UE-SN is a logical interface in between UE and SN. This interface is initially unprotected. The logical interface SN-HN between SN and HN is protected and the security of this interface is out of the scope of this paper. The passive IMSI catchers eavesdrop on the UE-RAN interface when it is unprotected to extract an IMSI. The active IMSI catchers impersonate a legitimate SN and run a legitimate-looking protocol with the UE in order to find out the IMSI. The HN and UE both know the IMSI and they are trusted. Both passive IMSI catchers and active IMSI catchers are untrusted.

4) Solutions Against IMSI catchers: In legacy networks, the approach of protecting IMSI privacy is to use a temporary identifier instead of the actual IMSI and keep changing the temporary identifier at a feasible frequency. Note that the temporary identifier has to be assigned over a confidentiality protected channel and different entities of the network may assign different temporary identifiers to the UE. In the LTE network, the temporary identifier assigned by serving network (SN) is called globally unique temporary identity (GUTI) [2] and the home network (HN) does not assign any temporary identifier to the UE. However, during the initial attachment of a UE to the SN, the UE has neither a GUTI nor a security context with the SN that can assign it with a GUTI. Besides, GUTI can be lost by either one or both of the UE and the SN. This would force the UE to reveal its IMSI to the SN to keep itself from permanently locked out of the network. This problem gives an opportunity to an active IMSI catcher who impersonates a legitimate SN and forces the UE to run the initial attachment protocol. This also gives an opportunity to a passive IMSI catcher to eavesdrop the IMSI sent in clear text. To fight against these active IMSI catchers in 5G, different solutions [19], [26], [29], [24], [21], [20], [23], [22] have been proposed.

III. Categories of Solutions

All the solutions that we are aware of to defeat IMSI catchers are based on cryptographic encryption techniques. In this section we will look into different categories of solutions. The categories are drawn based on different cryptographic encryption techniques.

5) Pseudonym Based: The pseudonym based solutions as proposed in [26], [19], [29], [24], [20] fall in the category of symmetric key encryption. In this kind of solutions, temporary

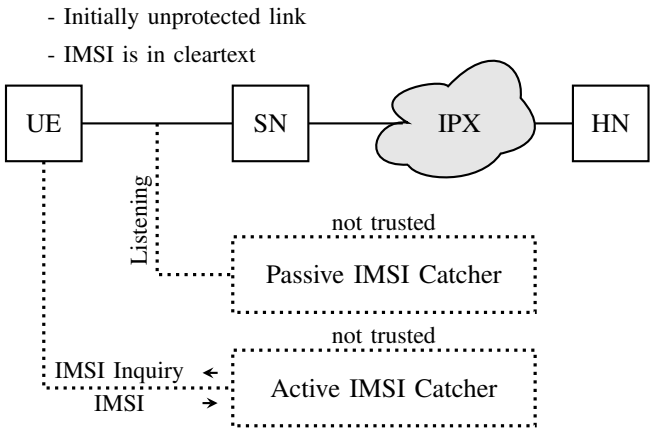

Fig. 1. High-level Security Architecture

identifiers called pseudonyms are assigned to a UE. Next time when the UE tries to identify itself to an SN, it uses a pseudonym instead of IMSI. Periodically, whenever there is an opportunity, the HN sends a new pseudonym to the UE with confidentiality and integrity protection using a symmetric key – that is why it falls under the category of symmetric key encryption. One such opportunity is when the HN sends the authentication vector to an SN.

6) Certificate based: In the certificate based encryption, the public key is signed by a trusted third party. The sender has to be pre-provisioned with the root certificate so that the sender can authenticate the public key of the receiver. Use of certificate based public-key encryption to conceal long-term identity has been suggested in 3GPP TR 33.821 [1]. The UE encrypts the IMSI using the public key of the SN before sending. To use certificate based public-key cryptography, we need to figure out who are the root certificate authorities (CA) and who else can be a CA, who owns a public key, how a certificate can be revoked, and how the UE can be re-provisioned with a new root certificate if needed. Different solutions can be devised based on the choice of root CAs and other CAs.

7) Root-key Based: In the root-key based encryption, no runtime authentication of the public key is required, because a very limited number of public keys are used in the system and all the senders are pre-provisioned with all the existing public keys. Use of root-key has been proposed in 3GPP TR 33.899 in solution #7.3. In this approach only one pair of public-private key pair exists. This key pair is owned by the HN and we call it the root-key. The HN provisions the public key to all its UEs. Instead of sending the IMSI, the UE encrypts the IMSI with the public root key and sends the result to the SN along with MCC and MNC. The SN sends the encrypted IMSI to the HN. The HN decrypts the IMSI and sends the IMSI back to the SN along with an authentication vector (AV).

8) Identity Based: In IBE, the public key of a receiver is computed from the identity of the receiver and the public key of a trusted third party known as private key generator (PKG). The public key of the trusted third party has to be provisioned to the sender. The private key of the receiver is computed as a function of the identity of the receiver and the private key of

the PKG. The private key of the receiver has to be provisioned to the receiver by the PKG. In IBE based solution [22], [23], the HN is the PKG. The HN has a public-private key pair. The UEs are provisioned with the public key of the HN. The SNs which have a roaming agreements with the HN are also provisioned with their respective private keys by the HN. When a UE identifies itself with IMSI, it encrypts the IMSI using the public key of the SN. The UE computes the public key of the SN as function of the identity of the SN and the public key of the HN. The most interesting aspect of this solution is that there is no certificate involved and the SN can decrypt the encrypted IMSI.

All these solutions try to defeat the IMSI catchers by concealing the permnanent identity – IMSI. The concealed identity is known as subscription concealed identifier (SUCI) and the permanent idenity is known as subscription permanent identifier (SUPI) [8]. In the next two sections we will explain the issues around IMSI-based routing and LI that impacts the effectiveness of different categories of solutions.

IV. IMSI-based Routing

First aspect of the issue is the routing of authentication information requests inside one mobile network. Subscribers' database of the mobile network operator is typically divided into several parts to increase lookup efficiency. In today's cellular systems, serving network's request for authentication information is routed to the correct database partition based on typically the first one to three digits of the MSIN [4].

Subscribers' database in 5G system is called Unified Data Management (UDM), and similarly to the previous generations of cellular systems, there are likely to be several UDM entities in the mobile network (in order to increase lookup efficiency).

If the MSIN in the authentication information request message is encrypted, then either, (i) MSIN has to be decrypted before routing, or (ii) the routing of the message to the correct UDM is based on another part in the message. The second of these options is more attractive than the first, because the decryption entity may become a new bottleneck in the 5G system. Therefore, 3GPP SA3 is moving towards option (ii). (One solution proposed in 3GPP SA3 uses home network's public key identifier for routing purposes; another solution proposes leave required SUCI routing information unencrypted as part of the SUCI [5].)

Another aspect of the issue is the routing of authentication information requests between different mobile networks. Mobile network operators interconnect their networks via IP exchanges (IPXs). Typically MCC and MNC are sufficient for routing visited network's requests for authentication information to the home network. But, if a mobile virtual network operator (MVNO) has (i) the same MCC and MNC as the MNO from whom it purchases networking services in bulk; and (ii) subscribers' database in a completely different location from that of MNO, then knowing only MCC and MNC is not enough to identify the home network. In that case, an IPx uses part of MSIN, in addition to MCC and MNC, for routing visited network's requests to the home network.

All in all, authentication information requests in 5G system should include some cleartext routing information, in addition to MCC and MNC. Please note that this extra information may be used for tracking the user: for example, if information equivalent of four MSIN digits is revealed, then the probability of identifying a user becomes ten thousand times bigger. On the other hand, solutions in which the MSIN is decrypted at SN, e.g., IBE based solution do not have this weakness.

V. Lawful Interception

According to 3GPP specification [7], LI requirement is: the SN should be able to identify a user with the IMSI without relying on the HN. However, if the SN can not decrypt the MSIN coming from the UE (because it may be encrypted by the public key of the home network or be a pseudonym known to HN only), then the SN has to learn the MSIN from the HN. This is the case for both the root-key based or pseudonym based solution.

In root-key and pseudonym based solutions, the SN has to learn the IMSI from the HN. Apparently it means that the SN is relying on the HN to resolve the IMSI of a user. However, to be confident that the HN gave the original IMSI of a user, several ways have been proposed in 3GPP SA3 [12], [13], [14], [9], [10]. In [12], [13], the SN receives the SUCI and a hash computed on the SUCI and SUPI from the UE. The SN also receives the SUPI from the HN. So the SN can compute the hash on SUCI and SUPI. If the HN gave a fake SUPI to the SN then the hash computed by the SN would not match with the hash the SN received from the UE. In [14], the UE sends its SUPI to SN using the NAS security mode command procedure. Since NAS security mode command procedure is usually confidentiality protected, SUPI privacy is also protected. The SN does not provide service to UE, if SUPI indication from UE and HN do not match. In [9], the combination of NAS security mode command procedure and the hash based technique is used. The hash based technique is used when the NAS encryption is not active. All these solutions add overhead by adding new signalling messages or parameters to the messages of the authentication and key agreement or of NAS security mode command. However, the solution in [10] vouch for binding SUPI in generating the anchor key in the VPLMN as mentioned in [15]. So, if the HN gave a fake SUPI to the SN, the SN would generate a different key than that of the UE. Thus, the UE will not be able to get any service if the HN gives the SN a fake SUPI.

Nevertheless, the solutions in which MSIN can be decrypted in the SN do not have the concern of HN telling the truth or lie. This is because, the SN does not need the HN for resolving the MSIN – the SN would learn the MSIN directly from the UE. This is the case for certificate based and IBE based solution. Unless the HN and the UE collude to fool the LI entity in the SN, the LI entity can trust that the identity given by the UE is correct after authentication of the UE has succeeded.

VI. Qualitative Comparison of Different Categories of Solutions

Qualitative comparison of different solutions based on different criteria was presented in [23], [22]. In this paper we take the same approach. For smoother reading, we present only those criteria which we have found to make a difference

between solutions. We only compare according to the solution categories. We have discussed two different categories of solutions: pseudonym based and public-key based. We have categorized the different public-key technologies into three categories: certificate based, root-key based and identity based. In Table I, we present a comparison among the different solutions based on different criteria. We indicate the performance of the solutions based on each criteria according the following symbols : ++ very good, + good, +- somewhat okay, - not good.

a) Immunity Against Active IMSI Catchers: This is the most important criterion because the whole effort is to defeat the active IMSI catchers. Before the concern around IMSI-based routing surfaced, in pseudonym based and root-key based solution, it was sufficient to reveal MCC and MNC to route the SUCI to the appropriate destination. So, an active IMSI catcher could learn the MCC and MNC only. However, because of the concerns around IMSI-based routing, pseudonym based and root-key based solutions have to reveal more information from MSIN. It makes them less immune against active IMSI catchers. However, these solutions can still achieve certain degree of anonymity. So, we evaluate them with +-. Note that, in [23], these two solutions were evaluated with +. The certificate based solution with global PKI can conceal even MCC and MNC. So, we evaluate them with ++. In IBE based solution, only MCC and MNC needs to be revealed. So we evaluate it with +.

b) Lawful Interception: The LI requirement is that the SN should be able to identify a user with the IMSI without relying on the HN. Both in pseudonym based and root-key based solutions, the SN has to rely on the HN to identify a user with the IMSI – HN sends the IMSI to the SN. To be confident that the HN gave the real IMSI some extra effort is required as mentioned in [12], [13], [14], [9], [10]. Before the concern around LI surfaced, this extra effort was not required. Besides, in both of these solutions, it has to be assumed that the HN and UE are not colluding. Only under such assumption, the SN can trust that the IMSI given by the HN is correct. Since it needs the assumption, we evaluate these two solutions as +-. In certificate and IBE based solutions, the SUCI can be decrypted in the SN. So, these two categories of solutions do not have the concern of the HN telling the truth or lie. This is because, the SN does not need the HN for resolving the MSIN. The MSIN can be decrypted out of the SUCI by the SN itself. So, we evaluate both of these solutions with +.

c) Deployment and Maintenance Effort: Pseudonym based approach does not require standardization. Changes in the SIM and HN – operated by the same entity, is sufficient. So, it is relatively easy to deploy. However, it makes the subscription database very sensitive to any changes, hence the maintenance becomes difficult. So, we rate this with +-. Certificate based solutions require setting up PKI and maintaining it. That is a lot of effort. So we rate certificate based solution with -. Root-key based and IBE based solutions are fairly easy to deploy and maintain. So we rate them with +.

d) Transparency to the Legacy SNs: To enable the SN to identify a user with IMSI – the LI requirement, the pseudonym based solutions require similar solutions as mentioned in [12], [13], [14], [9], [10]. These solutions need the SN to understand extra message fields sent by the HN. This means the pseudonym based solutions are not transparent to the legacy SNs. However, pseudonym based solution would be transparent to the SNs if identifying a user using pseudonyms would become a sufficient LI requirement. So we evaluate them with +-. Consequently, even though previously it was a very important advantage of pseudonym based approach, it becomes a just okay solution now in this regard. So we rate this with +-. However, no other solutions are transparent to SNs. Because in all the other solutions, the SN has to receive ciphertext produced by public key – none of the legacy SNs has to do that. So we rate all of them with -.

e) Signalling overhead: In pseudonym based solution, the SN needs to know the IMSI of a user from the HN. To be confident that the IMSI given by the HN is correct, similar measures as mentioned in [12], [13], [14], [9], [10] have to be implemented. This adds some extra signalling overhead on top of what exists in the legacy networks. However, pseudonym based solution does not use public key encryption. The use of only symmetric key encryption produces shorter ciphertext which keeps the signalling overhead significantly low. So we rate it with +. Certificate based solutions require an extra round trip between the UE and the SN to exchange the certificate. This creates signalling overhead. Certificate based solution does not require the HN to give the IMSI to the SN. So, certificate based solution does not require the added signalling overhead as it requires in pseudonym based solution. This may sound that pseudonym based and certificate based solutions are equally good/bad in this criteria – both of them need added signalling for different purposes. However, the added signalling overhead in pseudonym based solution is in the core network, whereas the added signalling overhead to exchange the certificates is in the radio network. Besides certificates can be quite long. So we rate certificate based solution with -. The root-key based solution requires the similar extra signalling as the pseudonym based solution requires. Besides it has to route the SUCI all the way to the HN. The SUCI is generated using public key encryption – quite longer than pseudonyms. However, it does not need to exchange certificates – a significant relieve. So we rate it with +-. IBE based solutions do not require any extra round trips or certificates – less signalling overhead compared to certificate based solutions. IBE based solution does not require the HN to give the IMSI to the SN. For this reason, IBE based solution does not require the extra signalling overhead as the pseudonym based or root-key based solution require. However, IBE based solution produces SUCI which are quite longer than pseudonyms. So we rate them with +.

f) Computational overhead: Pseudonym based solutions require some extra computation in the HN to generate next pseudonym of a user randomly. However, this is quite less complex in comparison with public key encryption. So, we rate it with ++. Certificate based solutions require to exchange and verify the certificate and compute public key encryption/decryption. This creates computational overhead. So, we rate it with -. However, both root-key and IBE based solutions require public key encryption and decryption but do not require verifying certificates. So we rate them with +.

g) Latency: In pseudonym based solution, some extra signalling overhead is needed to add to enable the SN to serve

the LI requirement. However, since pseudonym based solution uses symmetric key encryption and does not use public key encryption, the signalling and computational overhead is comparatively low. However, when the user is roaming, to resolve the IMSI, the pseudonym has to travel all the way to the HN – increases latency. So we rate it with -. Certificate based solutions require an extra round trip between the UE and SN to exchange and verify the certificates, computes public key encryption and have longer message length. All these affect the latency. So we rate certificate based solution too with -. In the root-key based solution, when the user is roaming, to resolve the IMSI, the pseudonym has to travel all the way to the HN – increases latency. So we evaluate it with -. The IBE based solutions do not require any extra round trips or certificates. However, they compute public key encryption and have longer message length. Hence the latency is affected. However, So we rate them with +-.

h) Key revocation: Pseudonym based solution is a symmetric-key based solution. So it does not require any key revocation. So, we rate it with ++. However, all the public key based solutions require a mechanism of key revocation. In certificate based solution, to access the revocation list, a user has to connect to an SN. How a UE may know that the public key of the SN has already been revoked? On the other hand, in IBE based solutions, revocation is inherently complicated. One solution around this is to use short expiry time for the public keys of the SNs. By doing so, key revocation increases some overhead. So we rate both of them with -. In root key based solution no revocation is required because there is only one public key. If the corresponding private key is compromised, the UE has to be re-provisioned with the new public key. So we rate it with +.

i) Maturity: We also look at the solutions from the point of view of the maturity of the technology. Use of pseudonyms for privacy purpose is not yet a very matured technology. Use of IBE is not yet widespread. So we rate both of them with -. However, certificate based public-key encryption technology is widespread and matured. Use of root-key can be viewed as a special case of certificate based public-key. So, we rate both of certificate based and root-key based solutions with +.

j) Mutual authentication: It is possible that in future there might be a need of mutual authentication between the UE and the SN without the intervention of the HN. In this respect we notice that pseudonym based and root-key based solution can not be used for mutual authentication. This is because, in these cases the IMSI is not visible to the SN without consulting with the HN. So, we rate these two categories with -. However, Certificate based and IBE based solutions can be extended into a mutual authentication protocol between UE and SN. One example can be found in [23]. So, we rate both of these two categories with +.

k) Summary of the Comparison: Looking at the table, it seems evident that IBE based solution is the most promising solution. Certificate based approach is good in preventing active IMSI catchers and handling the requirement of lawful interception. But the solution is costly in almost all other aspects. Maybe, the industry is not yet ready to spend such expenses to provide user identity privacy. Even though pseudonym based approach is inexpensive from almost all the aspects, it becomes a bit less effective to achieve its original purpose - immunity against active IMSI catchers. Because of the LI issues, it also loses its most important merit - transparency with legacy SNs. The root-key based approach is also a bit less effective in serving its original purpose - immunity against active IMSI catchers. It also makes the lawful interception a bit more complicated than that of IBE based solution. However, key revocation in IBE may have some latency whereas no key revocation is required in root-key. But still, considering the effectiveness of the solution, we would like to conclude that IBE based solution is a better choice than the root-key based solution.

VII. Conclusion

User identity privacy in 3GPP Release 15 – the first release of 5G system, will be based on what we call a ”root-key” solution. It impacts IMSI-based routing of messages and the legal interception (LI) entities in cellular networks. We have analyzed these and other impacts for several solution types for user identity privacy. It was found that IBE based solution is in several ways better than the root-key based solution. In conclusion, IBE based solution for user identity privacy could be proposed for future 3GPP releases of 5G system.

References

[1] 3GPP. TR 33.821 Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE).

[2] 3GPP. 3GPP TS 23.003 V 15.2.0 Numbering, addressing and identification. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729, December 2017.

[3] 3GPP. 3GPP TS 33.401 V 14.5.0 3GPP System Architecture Evolution (SAE); Security architecture. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729, December 2017.

[4] 3GPP. 3GPP S3-180761: discussion paper on embedded routing information in SUCI. http://www.3gpp.org/DynaReport/TDocExMtg--S3-90b--19778.htm, 2018.

[5] 3GPP. 3GPP S3-180763: pCR to 33.501 - addition of routing information into SUCI. http://www.3gpp.org/DynaReport/TDocExMtg--S3-90b--19778.htm, 2018.

[6] 3GPP. 3GPP TR 33.899 V 1.3.0: Study on the security aspects of the next generation system. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045, 2018.

[7] 3GPP. 3GPP TS 33.106: 3G security; Lawful interception requirements. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2265, 2018.

[8] 3GPP. 3GPP TS 33.501 v 1.0.0: Security architecture and procedures for 5G System. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169, 2018.

[9] 3GPP. 3GPP TSG SA WG3 (Security) Meeting #90-Bis: S3-180591, Solution for SUPI privacy and LI requirement. http://www.3gpp.org/DynaReport/TDocExMtg--S3-90b--19778.htm, 2018.

[10] 3GPP. 3GPP TSG SA WG3 (Security) Meeting #90-Bis: S3-180684, Proposal and Discussion for Privacy and LI solution. http://www.3gpp.org/DynaReport/TDocExMtg--S3-90b--19778.htm, 2018.

[11] 3GPP. 3GPP TSG SA WG3 (Security) Meeting #90-Bis: S3-180723, Requirement on routing SUCI. ftp://ftp.3gpp.org/TSG_SA/WG3_Security/TSGS3_90Bis_SanDiego/Docs/, 2018.

[12] 3GPP. 3GPP TSG SA WG3 (Security) Meeting #90-Bis: S3-180768, Discussion on LI conformity by verification hash with ppt attachment. http://www.3gpp.org/DynaReport/TDocExMtg--S3-90b--19778.htm, 2018.

TABLE I. COMPARATIVE EVALUATION OF THE SOLUTIONS

Criteria	Pseudonym	Certificate based	Root-key	IBE based
Immunity to Active IMSI Catchers	+-	++	+-	+
Lawful interception	+-	+	+-	+
Deployment and Maintenance Effort	+-	-	+	+
Transparency to the Legacy SNs	+-	-	-	-
Signalling overhead	+	-	+-	+
Computational overhead	++	-	+	+
Latency	-	-	-	+-
Key revocation	++	-	+	-
Maturity	-	+	+	-
Mutual Authentication	-	+	-	+

[13] 3GPP. 3GPP TSG SA WG3 (Security) Meeting #90-Bis: S3-180769, SUCI and LI verification hash integrated in 5G AKA. http://www.3gpp.org/DynaReport/TDocExMtg--S3-90b--19778.htm, 2018.

[14] 3GPP. 3GPP TSG SA WG3 (Security) Meeting #90-Bis: S3-180818, Clause 6.7.2 (NAS SMC, SUPI from UE for LI). http://www.3gpp.org/DynaReport/TDocExMtg--S3-90b--19778.htm, 2018.

[15] 3GPP. SA3 #88-Bis (Adhoc on 5G) #88-Bis: S3-172488, pCR to 33.501 6.1.3.1, 6.1.3.2 - SUPI assurance in SEAF. http://www.3gpp.org/DynaReport/TDocExMtg--S3-90b--19778.htm, 2018.

[16] ASOKAN, N. Anonymity in a Mobile Computing Environment. In *1994 First Workshop on Mobile Computing Systems and Applications* (1994), pp. 200–204.

[17] DABROWSKI, A., PETZL, G., AND WEIPPL, E. R. The Messenger Shoots Back: Network Operator Based IMSI Catcher Detection. In *Research in Attacks, Intrusions, and Defenses. RAID 2016* (2016), Lecture Notes in Computer Science, vol 9854. Springer.

[18] DABROWSKI, A., PIANTA, N., KLEPP, T., MULAZZANI, M., AND WEIPPL, E. IMSI-Catch Me If You Can: IMSI-Catcher-Catchers. In *Proceedings of the 30th Annual Computer Security Applications Conference* (New York, NY, USA, 2014), ACSAC '14, ACM, pp. 246–255.

[19] GINZBOORG, P., AND NIEMI, V. Privacy of the Long-term Identities in Cellular Networks. In *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications* (2016), MobiMedia '16, ICST.

[20] KHAN, M., JÄRVINEN, K., GINZBOORG, P., AND NIEMI, V. On De-synchronization of User Pseudonyms in Mobile Networks. In *Information Systems Security* (2017), Springer International Publishing, pp. 347–366.

[21] KHAN, M., AND MITCHELL, C. Trashing IMSI Catchers in Mobile Networks. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2017), Boston, USA, July 18-20, 2017* (United States, 05 2017), Association for Computing Machinery (ACM).

[22] KHAN, M., AND NIEMI, V. Concealing IMSI in 5G Network Using Identity Based Encryption. In *Network and System Security* (2017), Springer International Publishing, pp. 544–554.

[23] KHAN, M., AND NIEMI, V. Privacy Enhanced Fast Mutual Authentication in 5G Network Using Identity Based Encryption. *Journal of ICT Standardization*, 1 (2017).

[24] KHAN, M. S. A., AND MITCHELL, C. J. Improving Air Interface User Privacy in Mobile Telephony. In *Second International Conference, SSR 2015, Proceedings* (2015), Springer International Publishing.

[25] NEY, P., SMITH, J., GABRIEL, C., AND TADAYOSHI, K. SeaGlass: Enabling City-Wide IMSI-Catcher Detection. In *Proceedings on Privacy Enhancing Technologies* (2017), PoPETs.

[26] NORRMAN, K., NÄSLUND, M., AND DUBROVA, E. Protecting IMSI and User Privacy in 5G Networks. In *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications* (2016), MobiMedia'16, ICST.

[27] SHAIK, A., SEIFERT, J., BORGAONKAR, R., ASOKAN, N., AND NIEMI, V. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. In *23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016* (2016).

[28] SOLTANI, A., AND TIMBERG, C. Tech firm tries to pull back curtain on surveillance efforts in Washington. https://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html?utm_term=.96e31aa4440b, 09 2014. [Online; Was available until 14-July-2017].

[29] VAN DEN BROEK, F., VERDULT, R., AND DE RUITER, J. Defeating IMSI Catchers. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (2015), CCS '15, ACM.

[30] VAN DEN BROEK, F., AND WICHERS SCHREUR, R. Femtocell Security in Theory and Practice. In *Secure IT Systems* (2013).

[31] VARADHARAJAN, V., AND MU, Y. Preserving privacy in mobile communications: a hybrid method. In *1997 IEEE International Conference on Personal Wireless Communications (Cat. No.97TH8338)* (12 1997), pp. 532–536.