Concealing IMSI in 5G Network Using Identity Based Encryption

Mohsin Khan and Valtteri Niemi
mohsin.khan@helsinki.fi, valtteri.niemi@helsinki.fi

University of Helsinki, Department of Computer Science

Abstract. Subscription privacy of a user has been a historical concern with all the previous generation mobile networks, namely, GSM, UMTS, and LTE. While a little improvement have been achieved in securing the privacy of the long-term identity of a subscriber, the so called IMSI catchers are still in existence even in the LTE and advanced LTE networks. Proposals have been published to tackle this problem in 5G based on pseudonyms, and different public-key technologies. This paper looks into the problem of concealing long-term identity of a subscriber and presents a technique based on identity based encryption (IBE) to tackle it. The proposed solution can be extended to a mutual authentication and key agreement protocol between a serving network (SN) and a user equipment (UE). This mutual authentication and key agreement protocol does not need to connect with the home network (HN) on every run. A qualitative comparison of the advantages and disadvantages of different techniques show that our solution is competitive for securing the long-term identity privacy of a user in the 5G network.

1 Introduction

The NGMN Alliance has pointed out the privacy of a user as a requirement of the 5G network [13]. When a user equipment (UE) tries to connect to a network, the UE has to identify itself using an identifier. Once the UE is identified, an authentication protocol is run between the UE and the network. There are two types of attackers against the user privacy. A passive attacker just listens to the radio communication and tries to figure out identity of the user. An active attacker may transmit some radio messages itself. It is easier to protect against a passive attacker than an active attacker. Since 2G (GSM) the network has used temporary identities to protect against passive attackers. However, even in the LTE network the permanent identity is not protected against active attackers.

We discuss solutions to conceal the long-term identifier known as international mobile subscriber identity (IMSI) during the identification phase. These solutions are based on pseudonyms and public-key encryption. The pseudonym based approaches require to maintain a synchronization of pseudonyms between the UE and the HN. We discuss solutions based on certificates and root-key for the category of public key. Public-key based solutions do not require any synchronization. However, the public-key based solutions have higher cost both in terms of communication and computation.

We propose a novel solution based on identity based encryption (IBE). One additional advantage of our solution is that, it also works as a mutual authentication protocol between SN and UE without the involvement of the HN every time the authentication is needed. This advantage can not be achieved using root-key based approach. This advantage can be achieved using certificate based approach, but it is the heaviest in terms of communication and computation. We evaluate our solutions based on the following criteria: (1) Immunity to attackers, (2) Parts of the IMSI concealed, (3) Signalling overhead, (4) Latency, (5) PKI complexity, (6) Public-key revocation, etc. The choice of the solution depends on how much we want to achieve. Our solution based on IBE becomes a competitive one by meeting most of the important requirements.

2   3GPP-defined Aspects of Mobile Networks

In 3GPP TR 33.899 [8], subscribers' privacy is captured as one of the high level security requirements of the 5G network. In the context of diversified devices and the complex business and service model of 5G, it is important to define who is a subscriber and what subscriber privacy means. According to 3GPP TR 21.905 [3], a subscriber is an entity (associated with one or more users) that is engaged in a subscription with a service provider. A subscription describes the commercial relationship between the subscriber and the service provider, cf. 3GPP TR 21.905 [3]. A subscription identifier uniquely identifies a subscription in the 3GPP system and is used to access networks based on 3GPP specifications. Subscription privacy refers to the right to protect any information that can be used to identify a subscription to whom such information relates. This definition of privacy suggests to protect any personally identifiable information (PII) from an attacker. While it may be difficult to draw a clear boundary between PII and non-PII, the long-term identifier is surely a PII.

2.1   System Overview

In the case of GSM, 3G (UMTS) and 4G (LTE) networks, IMSI is a long-term identity of a subscriber. An IMSI is usually presented as a 15 digit number but can be shorter. The first 3 digits are the mobile country code (MCC), followed by the mobile network code (MNC), either 2 digits 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 [4].

In order to present an easily comprehensible discussion, we need to know what are the entities and communication interfaces are involved in this identification process. We also need to know which entities can be entrusted with the IMSI of a subscriber. As the architecture of 5G is yet to be finalized, we present an abstraction of the involved entities and assume that whatever the architecture of 5G will eventually be, it will contain something for each of these entities and something for each of these interfaces. Figure 1 shows the abstraction. The abstraction involves the UE, SN and HN. Note that in a non-roaming situation,

the SN and HN are the same network. 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 catcher (PIC) and active IMSI cather (AIC).

The logical interface between UE and SN is initially unprotected. The logical interface between SN and HN is protected. The PICs eavesdrop on the UE-RAN interface when it is unprotected to extract an IMSI. The AICs impersonate a legitimate SN and run a legitimate looking protocol with the UE in order to find out the IMSI.

HN and UE both know the IMSI and they are trusted. Both of PIC and AIC are untrusted. It is in principle possible not to trust SN. However, by other specifications in 3GPP TS 33.106 [5] and TS 33.107 [6], it is required to reveal IMSI to the SN to enable lawful interception (LI) without involving HN.
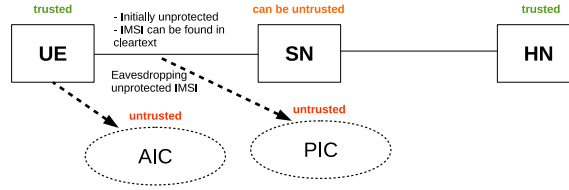

Fig. 1. High-level security architecture

2.2   Current Solution Approach and its Weakness

One approach of protecting IMSI privacy is to use a temporary identifier instead of the actual IMSI and keep changing the temporary identifier frequently. Note that the temporary identifier has to be assigned confidentially. Different entities of the network may assign different temporary identifiers to the UE.

In the LTE network, the temporary identifier assigned by an SN is called globally unique temporary identity (GUTI) and the 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 AIC who impersonates a legitimate SN and forces the UE to run the initial attachment protocol. This also gives an opportunity to a PIC to eavesdrop the IMSI sent in cleartext. Solutions [11, 14, 16, 12] have been proposed by using temporary IMSI known as pseudonym. While these solutions solve the cases of lost and unsynchronised GUTI, they still have the problem of lost or unsynchronised pseudonyms. Public-key technologies have also been considered as potential approach to solve this problem.

3   Discussion on Different Proposed Solutions

Before delving into different proposed those solutions, let us introduce some notation.

1. $hnid, snid = MCC||MNC$ identifies the HN and SN respectively
2. e_A, d_A is the public and private key of entity A respectively
3. $\mathcal{X}_{A,B}(e_A, e_B)$ is the certificate of the public key e_A of A. The certificate can be verified by anyone who considers B as a root CA using the public key e_B. The certificate is a guarantee from B that the public key e_A is owned by A .
4. E, D are encryption and decryption functions so that $D(E(M, K), K) = M$.
5. $S(M, K)$ is the signature of message M signed by the key K

3.1   Solution Based on Pseudonyms:

Pseudonym based solutions have been proposed in [14, 11, 16, 12]. In this kind of solutions, temporary 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. One such opportunity could be when the HN sends the authentication vector to an SN.

3.2   Solution Based on Certificate Based Public-key Cryptography

Use of certificate based public-key encryption to conceal long-term identity has been suggested in 3GPP TR 33.821 [7]. To use certificate based public-key cryptography, we need to figure out who are the root CAs and who else can be a CA, who own 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. We provide a high-level description for few variants of certificate based solution.

Variant 1: It uses a global root of trust. There is a global entity trusted by everyone. Using this trusted global entity, a chain of trust can be established. The SN presents the certificate to a UE trying to attach. The UE verifies the certificate. If the verification result is positive, the UE encrypts its IMSI using the public key of the SN and sends to the SN.

Variant 2: In this variant the HN of a subscriber is the root CA. The HN generates a public-private key pair and generates a certificate of the public key signed by the HN itself. A UE is provisioned with this self signed certificate. An SN interested to serve a UE obtains a certificate $\mathcal{X}_{snid,hnid}(e_{snid}, e_{hnid})$. The UE sends $hnid, e_{hnid}$ to the SN. The SN looks up for the certificate $\mathcal{X}_{snid,hnid}(e_{snid}, e_{hnid})$. In case it exists at the disposal of the SN, the SN sends it to the UE. The UE verifies the certificate. If the certificate is verified as valid, then the UE sends the IMSI to the SN encrypted by the public key e_{snid} of the SN.

Variant 3: In this variant, there is no other CA than the root CA. Hence the chain of certificates is very short. Only an HN can be a CA. The certificates of all the SNs a UE might visit are pre-provisioned to the UE by the HN. When a UE attempts to attach to an SN, the UE encrypts the IMSI with the public key of the SN which is already provisioned to the UE. If the public key of an SN is revoked, the HN has to provision the revocation to the UE.

3.3   Solution Based on Root-key based Encryption

We use only one pair of public-private key pair in this approach. Such a technique has been proposed in 3GPP TR 33.899 in solution #7.3. This key pair is owned by the HN and we call it to be 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 the *hnid*. 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).

3.4   Solution Based on IBE

In the next section we discuss the basic principles of IBE and present a solution of the identity privacy using IBE.

4   Details of the IBE Based Solution

4.1   How IBE works

The idea of IBE was proposed by Adi Shamir in 1984 [15]. In IBE, the public and private keys of a receiver are computed from the identity of the receiver in conjunction with the public and private key of a trusted third party respectively. A sender does not need to authenticate the public key of a receiver each time the sender and the receiver agree on a security context. The authenticity of the public key in IBE is guaranteed by the trusted third party.

Usually in IBE, the trusted third party is known as the private key generator (PKG). The private key of the receiver has to be provisioned to the receiver by the PKG. It is impossible to revoke the public key in IBE unless the identity itself is revoked. Please note that a PKG knows the private keys of all the receivers. As a result a PKG can decrypt any message sent by any sender to any receiver. This implies that there must be a very high level of trust in the PKG.

Dan Boneh and Matthew Franklin published a fully functional IBE scheme in 2003 [9]. The security of this scheme was based on a natural analogue of the computational Diffie-Hellman assumption. Based on this assumption they showed that the new system has chosen ciphertext security in the random oracle model. To make the revocation of public keys easier, this scheme also suggests to use an expiry time as part of the identity of a receiver. We use this suggestion in our solution. Clifford Cocks present an implementation in 2001 [10] and show that the security of the implementation is related to the difficulty of solving the quadratic residuosity problem.

4.2 Existing proposals of Using IBE in 5G Network

RFC 6508 [2] presents an algorithm SAKKE for establishment of a secret shared value. Applications of SAKKE may include a date-time component in their identity to ensure that identities and hence the corresponding private-keys are only valid for a fixed period of time. Solution #7.11 in 3GPP TR 33.899 [8] uses IBE to protect the long-term identity according to RFC 6508. However, the solution does not address the issue of revocation of the identity based public-keys. RFC 6507 [1] describes a certificate-less signature scheme based on IBE. In this scheme a string called public validation token (PVT) randomly chosen by the PKG is assigned to an identity. Both the public and private key of a receiver are computed using the PVT along with the receiver's identity. So, the public key associated with an identity can be revoked by revoking the PVT. Solution #2.14 in 3GPP TR 33.899 presents an authentication framework based on the signature scheme of RFC 6507 and the authentication protocol EAP-TLS. This solution uses the PVT to revoke the public key associated with an identity. However, in this solution it is not clear how a UE can check if the public key of an SN has been revoked or not.

4.3 The Proposed Solution

Next we present a protocol that serves the purposes of both privacy protected identification of UE and mutual authentication between UE and SN. This mutual authentication does not require a contact with the HN each time the protocol is run between a UE and an SN. In our solution we do not use PVT but instead use an expiry time with pre-agreed format. This expiry time can act as the PVT. If the public key of an identity needs to be revoked, the expiry time along with the identity is added to the revocation list. If the identity requires a new public key, the PKG uses another expiry time to compute the private key of the identity. The newly computed private key is then provisioned to the identity along with the the new expiry time. When the expiry time comes, all the public keys computed using the expiry time are automatically revoked. So, the revocation list does not need to include revocations whose expiry time is in the past.

Description of the proposed solution The UE's HN acts as the PKG. The solution is pictorially presented in Figure 2. It has two different phases. In the first phase, the key generations and provisioning take place. In the second phase the identification and authentication happens. The description follows:

- In step 1.1 the HN generates a public-private key pair e_{hnid}, d_{hnid}.
- In 1.2, the HN provisions the UE with e_{hnid} and d_{ue}. d_{ue} is generated using the private key d_{hnid}, $IMSI$, and a chosen expiry time ET_{eu}.
- In 1.3, the SN sends the $snid$ to HN.
- In 1.4 the HN chooses a suitable expiry time ET and the private key d_{snid} is computed considering $snid||ET$ as the identity of the SN.
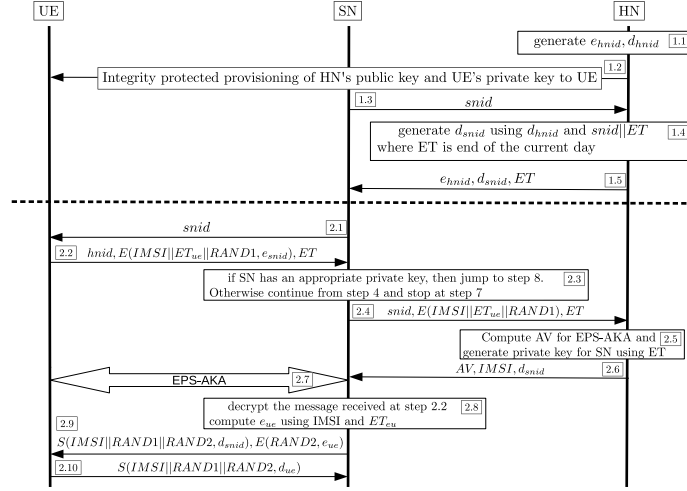
Fig. 2. Privacy protected UE identification and mutual authentication using IBE

- In 1.5, the HN sends d_{snid}, ET, e_{hnid} to the SN. The SN stores these information in its key-table.
- In 2.1, the SN broadcasts the $snid$.
- In 2.2, the UE sends $hnid, E(IMSI\|ET_{ue}\|RAND1, e_{snid}), ET$ to the SN.
- In 2.3, the SN looks for a private key d_{snid} compatible with ET.
- If SN has such a private key then it jumps to step 2.8. Otherwise it continues from step 2.4 and stop at step 2.7.
- In 2.4, SN sends $snid, E(IMSI\|ET_{ue}\|RAND1), ET$ to HN.
- In 2.5, HN computes the key d_{snid} using $d_{hnid}, snid$ and ET. Then HN decrypts the received encrypted message using the key d_{snid}. After extracting the the IMSI, HN prepares an AV.
- In 2.6, HN sends $AV, IMSI, d_{snid}$ to SN. The SN stores d_{snid}, ET.
- In 2.7, EPS-AKA is run between UE and SN and consequently mutual authentication and key agreement is achieved.
- In 2.8, SN decrypts the received encrypted message and compute e_{ue} using $IMSI\|ET_{ue}$ and e_{hnid}.
- In 2.9 HN sends the signature $S(IMSI\|RAND1\|RAND2, d_{snid})$ along with $E(RAND2, e_{ue})$ to the UE. The signature is verifiable by e_{snid} in the UE.
- In 2.10, the UE sends the signature $S(IMSI\|RAND1\|RAND2, d_{ue})$ to the SN which is verifiable by e_{ue}. If both UE and SN can verify the signatures as valid, the mutual authentication is completed successfully.

Note that UE and SN have successfully exchanged two randomly chosen values RAND1 and RAND2 with confidentiality protection. A symmetric key can be computed at both UE and SN using these random values and e_{hnid} using a function like key derivation function used in LTE security. There is also an alternative option of using ephemeral Diffie-Hellman key exchange protocol. The messages required for the ephemeral Diffie-Hellman key exchange can be transported along with the messages sent in step 2.9 and 2.10. In that case, confidentiality protection of $RAND2$ is not required. In solution #2.14 in 3GPP

TR 33.899, a static Diffie-Hellman key exchange have been proposed. In the static Diffie-Hellman technique the public key credentials used are the same as used in the IBE based solution. Consequently, static Diffie-Hellman does not require any extra communication for the symmetric key exchange.

Revocation of Public Keys The ET used to generate the public key d_{snid} is quite near in the future, e.g., the day end. So, if the public key needs to be revoked, it would automatically be revoked when the expiration time comes. In this way, a compromised SN would be able mount an attack only for a short period of time. However, the SN would need to get new d_{snid} from the HN before the old d_{snid} expires.

When the public key of a UE is revoked, the IMSI and relevant ET is stored in a revocation list in the HN. An SN serving UEs of an HN has a copy of the list. The SN also periodically checks with the HN if there is any new revocations. Before computing the public key of the UE in step 2.8, the SN checks the revocation list. If it is revoked, the SN discards the message received from the UE and the authentication fails.

All the entries with expiry time older than current date-time can be removed from the revocation list, hence the revocation list will not grow to a very large size. This frequent private key exchange and refreshing the revocation list would create a bit increased traffic between an SN and HN. On the other hand, this increased traffic is not in the air interface but in the back haul network, which apparently is not very critical.

5   Comparison of Solutions

In this paper we have discussed two different categories of solutions. One is pseudonym based and the other is public-key based. We have discussed the pseudonym based approach on a high level. Different solutions could be devised following this approach. It is reasonable to assume that all those soulutions would require the UE and the HN to synchronize their states and the used pseudonyms.

We have looked into different kinds of public-key technologies that serve the purpose of concealing long-term identity of a user. We have categorized the different public-key technologies into three categories: certificate based, root-key based and identity based. We have discussed three variants of certificate based solutions from a high level. We also have discussed one root-key based solution. One good side of all of these solutions is that, none of them require to maintain synchronization of states between a UE and the HN. But these solutions have some downsides also. All public key based technologies need comparatively heavier computational resources and the ciphertexts are longer. This heavier computation and longer ciphertexts affect the latency. Solutions based on public-key technologies also require a mechanism of key revocation. Apart from the common downsides, there are other downsides in these public-key based solutions.

In certificate based solutions there is a need of a global PKI. However, in some variants of certificate based solutions, the effort to manage a PKI can be

reduced significantly. Certificate based solutions require an extra round trip between the UE and SN to exchange and verify the certificate. In a variant of a certificate based solution, this extra round trip could be removed at the expense of provisioning the certificate of an SN to a UE before the UE goes roaming to the SN. All the certificate based solutions have the requirement of exchanging certificates and verifying them. This creates signalling and computational overhead which consequently affect the latency.

The root-key based solution does not require any extra round trips or certificates, hence it has better signalling and computational overhead compared to certificate based. However, the root-key based solution still suffers from the increased latency in a roaming situation because every authentication needs to travel all the way to the HN. This is because no one else except the HN can decrypt the message sent by the UE. The solution creates also computational pressure in the HN.

We have proposed a novel solution based on IBE that can both accomplish the identification and mutual authentication. The solution does not need to maintain synchronized states between a UE and the HN. The solution does not require a global PKI and does not need certificates. Unlike the root-key based approach, our solution does not need to involve HN each time authentication is needed. The aforementioned argument makes the IBE based solution a potential candidate to solve the problem in question. In Table 1, we present a comparison among the different solutions based on different criteria.

Apparently pseudonym based solution is very good in most of the criteria. One downside of pseudonym based approach is, if the pseudonym is unsynchronized between UE and HN, the user has to visit the HN physically and get back to synchronized state by giving the IMSI in a trusted environment. The need of visiting the HN physically might make the pseudonym based solution a little clumsy. Variant 1 of certificate based approach is good in preventing AIC and also conceals *hnid*. But this is bad in many other important criteria because of exhanging and verifying certificates. Considering the concealment of *hnid* with a bit less priority, the variant1 of certificate based solution is outperformed by both root-key based and IBE based solution. CertV2 and CertV3 can not even conceal *hnid*. So, the extra overhead of using Certv2 and CertV3 is not worth comparing to root-key and IBE. When comparing IBE and root-key, both of them are almost similar except that IBE based solution is extendable to a mutual authentication protocol between UE and HN. However, Cert1V can also be extended to a mutual authentication protocol.

The above discussion leads to the conclusion that, if concealing *hnid* is essential, then the only applicable solution is Certv1, the certficate based solution with global root of trust. If conclealmeant of *hnid* can be compromised, then the choice of the solution depends on the requirement of mututal authentication. If mutual authentication of UE and SN without involving HN is considered important and useful then IBE based solution is the winner. Otherwise, root-key based solution is just enough.

Criteria	Pseudo	CertV1	CertV2	CertV3	Root-key	IBE
Immunity to AIC	+ -	+	+	+	+	+
Concealing *hnid*	-	+	-	-	-	-
Signalling overhead	+ +	-	-	-	+	+
Computational overhead	+	-	-	-	+	+
Latency while roaming	-	-	-	-	-	+
Latency while at home	+ +	-	-	-	+	+
PKI effort	+ +	-	+	+	+	+
Key revocation	++	-	-	-	+	-
Provisioning effort	+	+	+	-	+	+
Using existing gear	+	-	+	+	+	+
Maturity	-	+	+	-	+	-
Mutual Authentication between UE and SN	-	+	+	+	-	+

Table 1. Comparative evaluation of the solutions

6   Conclusion

We have explained the requirement of subscription privacy and found that concealment of IMSI is needed to meet this requirement. In this paper we have discussed different known approaches to conceal the IMSI. The solutions are based on pseudonyms and public-key encryption. We have proposed a novel solution based on identity based encryption that serves the purposes of both identification and mutual authentication. We have used expiry time as part of the identity of the entities in the system. We have presented a rigorous comparison between different discussed and proposed solutions. We argue that identity based encryption is a competitive solution when concealing the home network identity is not necessary and mutual authentication in between a user equipment and a serving network is useful without connecting with the home network. Note that our comparison between different solutions is not quantified with experimental results. The comparison is based on qualitative analysis based on known facts of public-key cryptography.

7   Acknowledgement

Bibliography

[1] RFC 6507 Category: Informational. In *https://tools.ietf.org/html/rfc6507*, 2012.

[2] RFC 6508 Category: Informational. In *https://tools.ietf.org/html/rfc6508*, 2012.

[3] 3GPP. 3GPP TR 21.905. In *https://portal.3gpp.org/desktopmodules/ Specifications/SpecificationDetails.aspx?specificationId=558*. 3GPP.

[4] 3GPP. 3GPP TS 23.003, 14.2.0. In *https://portal.3gpp.org/desktopmodules/ Specifications/SpecificationDetails.aspx?specificationId=729*. 3GPP.

[5] 3GPP. 3GPP TS 33.106. In *https://portal.3gpp.org/desktopmodules/ Specifications/SpecificationDetails.aspx?specificationId=2265*. 3GPP.

[6] 3GPP. 3GPP TS 33.107. In *https://portal.3gpp.org/desktopmodules/ Specifications/SpecificationDetails.aspx?specificationId=2266*. 3GPP.

[7] 3GPP. 3GPP TR 33.821, 9.0.0. In *https://portal.3gpp.org/desktopmodules/ Specifications/SpecificationDetails.aspx?specificationId=2311*. 3GPP, 2009.

[8] 3GPP. 3GPP TR 33.899, 1.1.0. In *https://portal.3gpp.org/desktopmodules/ Specifications/SpecificationDetails.aspx?specificationId=3045*. 3GPP, 2016.

[9] Dan Boneh and Matthew Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 1923, 2001 Proceedings*, pages 213–219. Springer Berlin Heidelberg, 2001.

[10] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, pages 360–363, London, UK, UK, 2001. Springer-Verlag.

[11] Philip Ginzboorg and Valtteri Niemi. Privacy of the long-term identities in cellular networks. In *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, MobiMedia '16, pages 167–175. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016.

[12] Mohammed Shafiul Alam Khan and Chris J. Mitchell. Improving Air Interface User Privacy in Mobile Telephony. In *Security Standardisation Research: Second International Conference, SSR 2015, Tokyo, Japan, December 15-16, 2015, Proceedings*, pages 165–184. Springer International Publishing, 2015.

[13] NGMN. NGMN 5G White Paper. In *https://www.ngmn.org/uploads/ media/NGMN_5G_White_Paper_V1_0.pdf*. NGMN.

[14] Karl Norrman, Mats Näslund, and Elena Dubrova. Protecting IMSI and User Privacy in 5G Networks. In *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, MobiMedia '16, pages 159–166. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016.

[15] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology: Proceedings of CRYPTO 84*, pages 47–53. Springer Berlin Heidelberg, 1985.

[16] Fabian van den Broek, Roel Verdult, and Joeri de Ruiter. Defeating IMSI Catchers. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, pages 340–351. ACM, 2015.