A Survey of Subscription Privacy on the 5G Radio Interface - The Past, Present and Future

Haibat Khan*, Keith M. Martin†
Information Security Group, Royal Holloway, University of London, Egham, Surrey, UK.
Email: *Haibat.Khan.2016@live.rhul.ac.uk (corresponding author), †Keith.Martin@rhul.ac.uk

***Abstract*—End-user privacy in mobile telephony systems is nowadays of great interest because of the envisaged hyper-connectivity and the potential of the unprecedented services (virtual reality, machine-type communication, vehicle-to-everything, IoT, etc.) being offered by the new 5G system. This paper reviews the state of subscription privacy in 5G systems. As the work on 5G Release 15 – the first full set of 5G standards – has recently been completed, this seems to be an appropriate occasion for such a review. The scope of the privacy study undertaken is limited to the wireless part of the 5G system which occurs between the service provider's base station and the subscriber's mobile phone. Although 5G offers better privacy guarantees than its predecessors, this work highlights that there still remain significant issues which need rectifying. We undertook an endeavor to (*i*) compile the privacy vulnerabilities that already existed in the previous mobile telephony generations. Thereafter, (*ii*) the privacy improvements offered by the recently finalized 5G standard were aggregated. Consequently, (*iii*) we were able to highlight privacy issues from previous generations that remain unresolved in 5G Release 15. For completeness, (*iv*) we also explore new privacy attacks which surfaced after the publication of the 5G standard. To address the identified privacy gaps, we also present future research directions in the form of proposed improvements.**

***Index Terms*—5G, anonymity, GSM, LTE, mobile networks, privacy, UMTS, unlinkability.**

I. Introduction

Mobile telephony subscribers' personal information has become an attractive target for online advertisements and other connected industries. Besides the commercial arena, the Edward Snowden revelations show that national intelligence agencies also collect telephony subscribers' personal information on an unprecedented scale [1]. Apart from the danger that this personal information is utilized for nefarious political agendas, it may also be misused for personal advantages. Thus, privacy has turned out to be a primary consideration for end users when selecting and using a telephony service today. From a regulatory compliance perspective, the EU General Data Protection Regulation (GDPR) [2] obligations for protecting personal data of subscribers are directly applicable to mobile telephony operators. With penalties that can reach as high as EUR 20 million or 4 percent of total worldwide annual turnover, there is a huge financial risk for mobile operators in the event of potential non-compliance. Hence, protecting end-user privacy is all the more important for the latest international mobile telephony standards such as 5G.

3rd Generation Partnership Project (3GPP), the de facto international body for mobile telephony standardization, released the first documents pertaining to 5G at the end of the year 2017. The development of the 5G system was planned in two phases: 5G Phase 1 (formally called Release 15) and 5G Phase 2 (formally Release 16). As 5G Release 15 – the first full set of 5G standards – was frozen [1] in June 2019 (see Figure 1), this seems to be an appropriate time to undertake a comprehensive review of one of the most prominent privacy aspects of 5G based mobile telephony, i.e., subscription privacy on the wireless channel. 5G security and privacy documentation [3] often refers to previous generations for elaboration of various security and privacy requirements. The same is true in the case of subscription privacy where Release 15 refers to 3GPP TS 33.102 [4] for the requirements which are listed below:

- **User Identity Privacy:** The permanent identity of a user to whom a service is delivered cannot be eavesdropped on the radio access link.
- **User Location Privacy:** The presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link.
- **User Untraceability:** An intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

An important point to note here is that the use of the phrase "cannot be eavesdropped" in the above statements should not be misinterpreted if it only refers to a passive adversary 'eavesdropping' on the radio interface. This certainly is not the case here and a few previously published papers [5] fell prey to this misnomer. 3GPP has always considered active adversaries for its security and privacy scenarios. A pertinent example of this is the 3GPP study TR 33.899 [6] which was conducted to collect, analyze and further investigate potential security threats and requirements for 5G systems and contains explicit references to active adversaries.

In this paper, we provide an overview of the state of subscription privacy on the 5G radio interface. Keeping the aforementioned privacy objectives in mind, this paper evaluates, systematizes, and contextualizes the requisite aspects of 5G subscription privacy in three chronological categories; past, present and the future. The *past* category looks at the state of subscription privacy before the advent of 5G Release 15. In *present*, the improvements provisioned to user privacy by Release 15 are explored. Finally, the *future* category

[1] After "freezing", no additional functionality can be added to a Release.

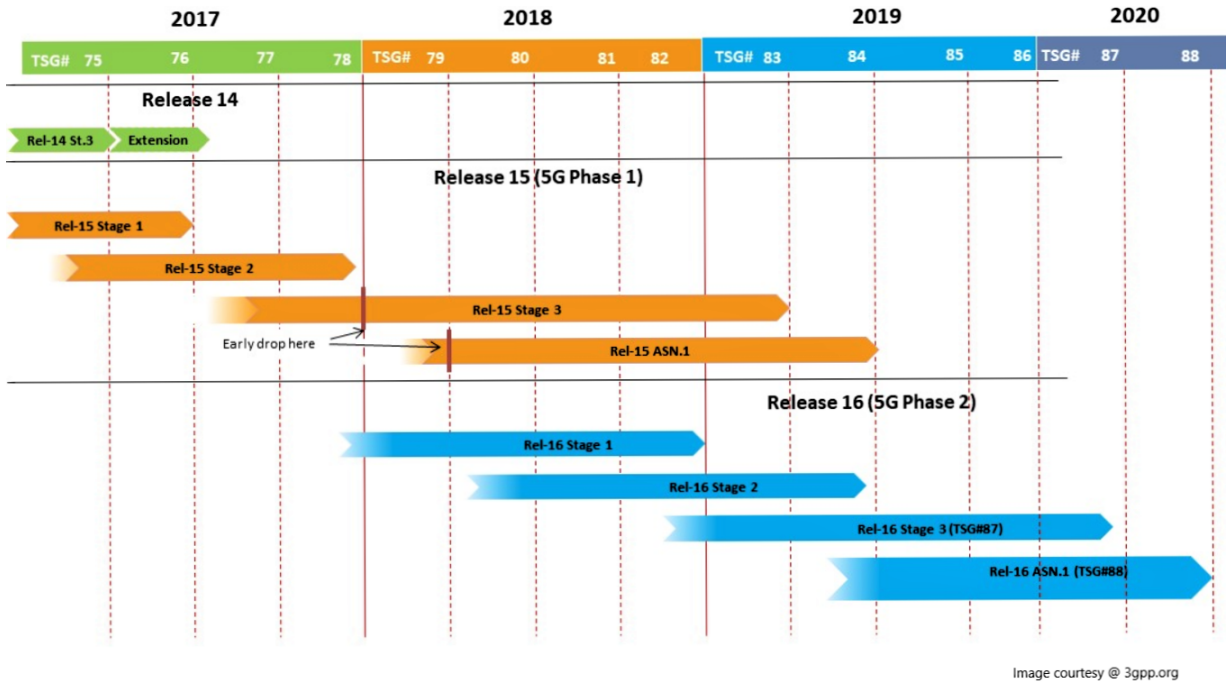


Fig. 1: 3GPP time-lines pertaining to various Releases.

discusses the privacy aspects which still could be improved in subsequent Releases.

A. Scope of the Study

There are three aspects which play a pivotal role in defining the scope of the study undertaken in this paper:

- We confine the privacy study undertaken in this paper to the wireless part of the 5G system. This is primarily because this medium is open and can easily be exploited by any malicious party and, as a result, is the most vulnerable.
- In this manuscript only those aspects of subscription privacy are discussed which come under the purview of 3GPP. Modern-day smart phones have evolved into powerful devices with functionality that goes beyond just telecommunications. These multitasking devices are now being utilized for all sorts of computational purposes which may or may not affect the end-user privacy that 3GPP is trying to protect. There are numerous other sources of leakage affecting user privacy such as Wi-Fi [7], Bluetooth [8], etc. which do not fall under the purview of 3GPP. We do not consider privacy leakages via these other sources in this work.
- Lastly, as work on 3GPP Release 16 (Phase 2 of 5G) is still under active development, we do not consider the ever-evolving Release 16.

B. Contributions

To our knowledge, this paper presents the first work on 5G subscription privacy after the completion of the first phase (Release 15) of the standard. Unlike other survey papers whose ambit of 5G security and privacy exploration has been very wide, we focus on one particular and very critical aspect, i.e., subscription privacy on the 5G wireless interface. In summary, the main contributions of this paper are as follows:

- **Comprehensive Overview:** This paper categorizes the privacy from the viewpoint of mobile users. To do so in a comprehensive manner, we study around 50 published papers and 20 3GPP publications to sift and sort the appropriate aspects of subscription privacy in 5G.
- **Chronological Context:** In this work, various aspects of subscription privacy are contextualized in a chronological order which gives an insight into the standards' development cycle and provides the reader with an opportunity to appreciate how things evolve in the real world.
- **Identification of Future Challenges:** Based on our study of the evolution of subscription privacy in 5G, we highlight possible issues that are yet to be addressed and, where appropriate, the impediments faced in resolving such challenges.

C. Paper Outline

The remainder of this paper is organized as follows: Section II provides the requisite background. Section III discusses the privacy vulnerabilities that existed before 5G, while improvements to subscription privacy provisioned by 5G are detailed in Section IV. In Section V, outstanding privacy issues of 5G and future research directions are discussed. Section VI describes the related work. Finally, Section VII concludes the paper and provides recommendations.

II. Technical Background

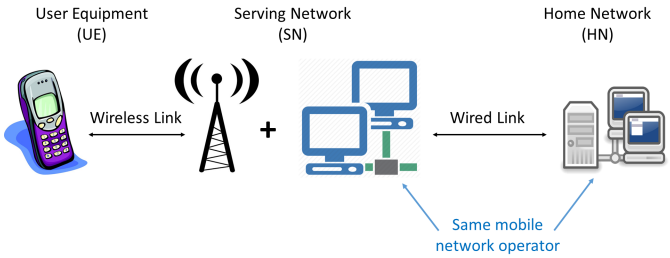
Before we delve further into the subscription privacy aspects of 5G, we outline the mobile telephony ecosystem and its pertinent security and privacy mechanisms

A. System Architecture

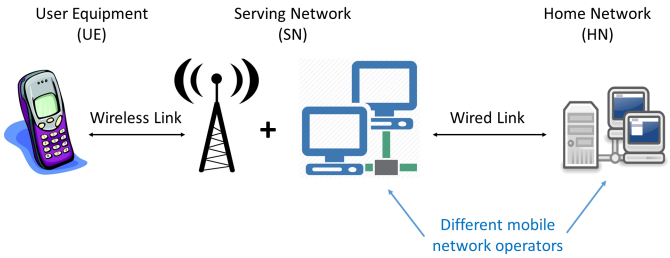
The mobile telephony architecture consists of three main domains; Home Network (HN), Serving Network (SN) and User Equipment (UE) (see Figure 2). The *subscribers* carry UE, which typically refers to Mobile Equipment (ME) (the phone) containing a Universal Integrated Circuit Card (UICC) (the SIM card). The HN domain represents the network functions that are conducted at a permanent location regardless of the location of the subscriber. The HN is where a subscription initially gets registered. It stores the subscribers' credentials and is responsible for management of subscription information. The SN domain is the part which provides the subscribers access to the telephony network and its services. It represents the network functions that are local to the user's access point and thus their location changes when the user moves. The SN is responsible for routing calls and transport of user data/information from source to destination. It has the ability to interact with the HN to cater for user-specific data/services.

Often UEs may have to operate in areas where their operators have no network coverage (i.e., base stations). In such scenarios called *roaming*, other service providers, who have a roaming agreement with the subscriber's operator, provide SN services. Hence, in this paper, we treat SN as a semi-trusted entity to whom a subscriber's long-term credentials can not be exposed (barring a few exceptions). Note that according to the 3GPP standard [3], HNs and SNs are further divided into logical sub-entities. The security and privacy properties being discussed in this paper do not require this level of granularity.

It is within the UICC that the application Universal Subscriber Identity Module (USIM) runs. The USIM represents the relationship between a subscriber and its issuing HN. During a subscription registration, the HN stores the subscriber's long-term identifier, Mobile Station International Subscriber Directory Number (MSISDN) (the telephone number) and other subscriber related data, including a 128-bit secret key K and 48-bit monotonically increasing counters called Sequence Numbers (SQNs), within the USIM. These SQNs are utilized for the purpose of replay prevention. While an SQN should be synchronized between the UE and HN, sometimes it may become out-of-sync due to the loss of messages on the wireless channel. We therefore use SQN_{UE} and SQN_{HN} to refer to the state of SQN in UE and HN respectively. These subscription parameters are also stored within the HN's database and form the basis of a security context between UEs and HNs and by extension (during roaming) between UEs and SNs. The SNs provision services to UEs after establishment of a secure channel between them with help of the HNs.



(a) When not roaming, both HN and SN belong to the same mobile network operator.



(b) When roaming, the SN and HN belong to distinct mobile network operators.

Fig. 2: The mobile network architecture. The channel between UE and SN is initially unprotected while that between SN and HN is assumed to be protected.

B. Identifier Types and Terminologies

In mobile telephony systems, networks allocate to each subscriber a unique long-term identifier, known up to 4G as the International Mobile Subscriber Identity (IMSI) and since 5G as the Subscription Permanent Identifier (SUPI). A SUPI as defined in 3GPP TS 23.501 [9] is usually a string of 15 decimal digits and acts as the long-term identifier of an individual subscriber. The first three digits represent the Mobile Country Code (MCC), while the next two or three form the Mobile Network Code (MNC) that identifies the network operator. The length of the MNC field is a national affair. The remaining (nine or ten) digits are known as the Mobile Subscriber Identification Number (MSIN) and represent the individual user of that particular operator. Each decimal digit of the SUPI is represented in binary by using the Telephony Binary Coded Decimal (TBCD) encoding [10].

Authentication between a user and its service provider is based on a shared symmetric key (details in Section II-E), thus can only take place after an initial user identification. However, if the IMSI/SUPI values are sent in plaintext over the radio link for this purpose then subscribers can be identified, located and tracked using these permanent identifiers. To avoid this privacy breach, subscribers are assigned temporary identifiers called Globally Unique Temporary User Equipment Identity (GUTI) by the SNs. A GUTI uniquely and globally identifies a particular subscriber. These frequently-changing temporary identifiers are then used for identification purposes

over the wireless link before the establishment of a secure channel. The International Mobile Equipment Identity (IMEI), which uniquely identifies the ME, is a string of 15 digits. If the IMEI is sent in plaintext over the radio interface then it could compromise user privacy as it is also uniquely identifying from a subscription viewpoint. However, the 3GPP specifications prohibit a UE from transmitting the IMEI until after establishment of a secure channel with the network [11].

C. Security Assumptions

1) Assumptions on Channels: According to 3GPP TS 33.501 (sub-clause 5.9.3) [3], the channel between SN and HN should provide confidentiality, integrity, authentication and replay prevention. The channel between UE and SN essentially being a wireless one is subject to eavesdropping, interception and injection of messages by malicious third parties.

2) Assumptions on Parties: The UE and its associated HN are fully trusted entities. The shared secret data being stored by these two entities is assumed to be protected from third parties. Specifically, the UICC is considered to be a tamper-resistant security module whose contents cannot be read by a malicious entity. SNs are semi-trusted entities in the sense that during the secure channel establishment the long-term shared secret key K and sequence numbers SQN should not be revealed to them while the SUPI is provisioned to them. The provisioning of SUPI is essential for accurate billing purposes.

3) Assumptions on Cryptographic Functions: All the cryptographic functions (detailed in Section II-E) are assumed to provide both confidentiality and integrity protection to their respective inputs.

D. Initialization of Authentication

As we will see in Section II-E, secure channel establishment between subscribers and their service providers is conducted via challenge-response protocols based upon the shared secret key K. Thus, before such protocols can be executed it is imperative that the service provider correctly identifies the subscriber with whom this channel needs to be established. 3GPP TS 33.501 (sub-clause 6.1.2) [3] details the procedures for this subscription identification and selection of the subsequent authentication method (see Figure 3).

The SN may initiate an authentication with the UE during any procedure establishing a connection with the UE. The UE sends the SN either the 5G-GUTI in a *registration request* message or the Subscription Concealed Identifier (SUCI) as a response to an *identifier request* message. The SUCI is a randomized public-key encryption of the SUPI (see Section IV-A for details). In the case of a 5G-GUTI, the SN extracts the corresponding SUPI from its database and forwards it along with its global identity *Serving Network Name* (SN_{name}) to the HN in an *authenticate request* message. Otherwise the SUCI is sent instead of the SUPI. Upon receipt of the *authenticate request* message, the HN checks whether the SN is entitled to use the serving network name in the request message by comparing the incoming serving network name with the expected serving network name. The HN stores the received serving network name temporarily. If the SN is not authorized to use the serving network name, the HN responds with a *serving network not authorized* message. If the SUCI is received in an *authenticate request* message by HN, it deconceals the SUPI from it and chooses the authentication method based upon its policy.

E. The 5G-AKA

The security of communication between telephony subscribers and their service providers requires mutual authentication and key agreement. In 5G systems, these requirements are fulfilled by either EAP-AKA' or 5G-AKA, both Authenticated Key Agreement (AKA) protocols. EAP-AKA' and 5G-AKA are quite similar with identical message flows but with minor differences in the way various keys get derived. We therefore consider only 5G-AKA in this paper. 3GPP TS 33.501 (sub-clause 6.1.3.2) [3] defines the details of the 5G-AKA protocol. The security of 5G-AKA is based upon the shared symmetric key K, while SQN provisions replay protection. To initiate authentication, the UE sends the SN either the 5G-GUTI in a *registration request* message or the SUCI in response to an *identifier request* message (as explained in Section II-D).

TABLE I: Description of 5G-AKA parameters

Parameter	Content/Description
R	Random Challenge
AK	Anonymity Key
CK	Confidentiality Key
IK	Integrity Key
RES	Response
MAC	Message Authentication Code
$CONC$	Concealed Sequence Number
$AUTN$	Authentication Token
$AUTS$	Resynchronization Token
$XRES$	Expected Response
$HRES/HXRES$	Hash of $RES/XRES$
K_{AUSF}	Intermediate Key
K_{SEAF}	Anchor Key

Figure 4 shows the 5G-AKA and its associated failure mechanisms. Table I details the various acronyms used in Figure 4. In Figure 4, R is a uniformly chosen 128-bit random number, functions f_1,..., f_5, $f_1{}^*$ and $f_5{}^*$ are symmetric key algorithms. f_1, f_2 and $f_1{}^*$ act as message authentication functions, and f_3, f_4, f_5 and $f_5{}^*$ are used as key derivation functions. Key derivation is performed using the Key Derivation Function (KDF) specified in 3GPP TS 33.220 [12]. A successful 5G-AKA culminates in the derivation of the anchor key K_{SEAF} by both SN and UE, from which further keys for subsequent communication are derived. The two cases of authentication failure for the 5G-AKA are as follows:

1) **MAC_Failure:** As the first step in authentication confirmation, the UE checks whether the received MAC value is correct or not. In case of a failure [Case ¬(i) in Figure 4], the UE replies with a $MAC\_Failure$ message back to the SN.
2) **Sync_Failure:** After MAC verification, the UE checks the freshness of the sequence number SQN_{UE} received

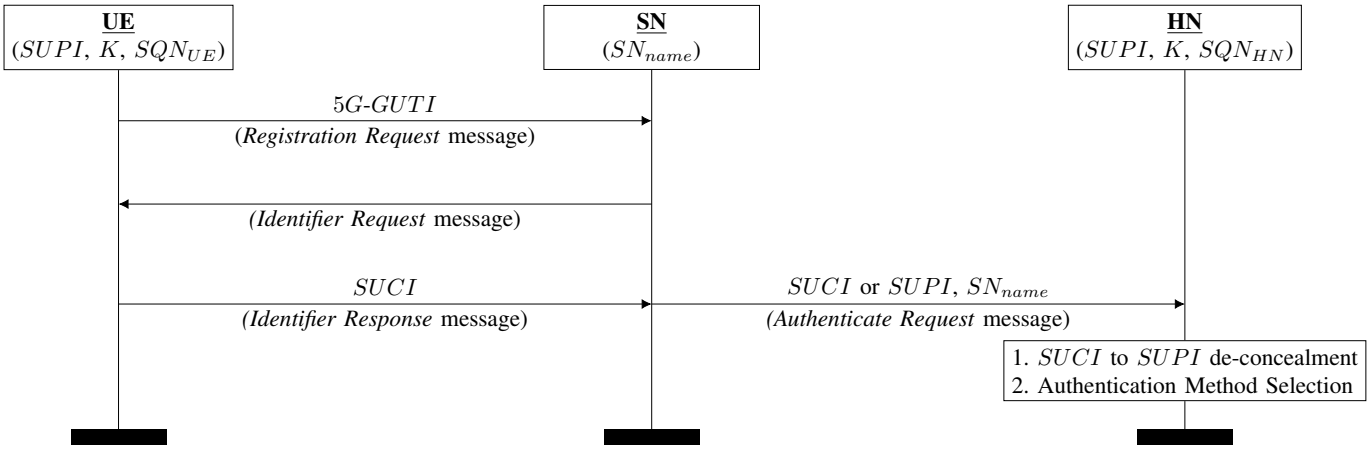


Fig. 3: Initiation of Authentication Procedure.

in the authentication challenge. In case of this failure [Case (i) and ¬(ii) Figure 4], it responds with a *Sync_Failure* message along with a re-sync token $AUTS$. Note that in Figure 4, the sequence number freshness check is denoted by $XSQN_{HN} > SQN_{UE} - \triangle$. What this actually means is that there is some "window" of size $\triangle$, within which sequence numbers smaller than the current sequence number of UE will be accepted given they previously had not been received by the UE. This mechanism is there to handle out-of-order delivery of challenge messages from HN to UE.

During the execution of 5G-AKA, it is crucial that SQN is protected from an eavesdropper during the exchange of messages between the UE and SN as its exposure may lead to the compromise of the identity and location of a subscriber. We will see in Section V-B how SQN leakage can manifest into privacy vulnerabilities.

F. Lawful Interception

Note from Figure 4 that at the culmination of a successful 5G-AKA, the HN provides the SUPI of the UE to the SN. This is required essentially for two main purposes; accurate billing and Lawful Interception (LI) requirements. The law enforcement agencies of almost all countries require that their local service providers should have the capability to locate and track any particular mobile user once required by law. The SUPI is later also used as an input to the key derivation functions between UE and SN. This ensures that the SUPI value provisioned by the HN is the one claimed by the UE, otherwise the communication breaks down.

G. Paging Messages

When a UE does not have any ongoing data transmissions, it enters an *idle* state in order to preserve energy. If delivery of a network service like a call or SMS needs to be delivered to the UE, the network probes the *idle* UE by sending a "paging" message and the UE responds correspondingly. The paging procedure works because even when in the *idle* state, the UE keeps on monitoring for the paging message at certain device-specific time intervals. The device is able to preserve battery because, at other times, it switches off its receiver. The idle UE decodes these broadcast probes and if it detects its identity in these messages, it randomly acquires an available radio channel and asks the concerned base station for "connection setup" for exchange of further signalling messages.

III. The Past - Inherited Challenges

The first and foremost task for 5G Release 15 was to address the privacy vulnerabilities that existed in the previous generations. Hence, before we discuss the improvements offered by Release 15, we take a look at the vulnerabilities that already existed in the early generations that affect subscription privacy on the radio channel. Table II provides a summary of the attacks on subscription privacy in earlier generations.

A. IMSI-catching

As mentioned in Section II-B, for obvious privacy reasons, GUTI is utilized for subscription identification purposes over the wireless interface before the establishment of a secure channel. However, there are certain situations where authentication through the use of these temporary identifiers is not possible. For example, when a user registers with a network for the first time and is not yet assigned a temporary identifier. Another case is when the network is unable to resolve the IMSI from the presented GUTI. An active man-in-the-middle adversary can intentionally simulate this scenario to force an unsuspecting user to reveal its long-term identity. These attacks are known as "IMSI-catching" attacks [18] and persist in mobile networks, including LTE [14], [11]. IMSI-catching attacks have threatened all generations of mobile telephony for decades [19]. In IMSI-catching, through the use of *identifier request* messages (Section II-D) the attacker obtains the identities of everybody around in an attack area. The attacker needs no previous assumption of who might be there, and needs no previous information about the victim. It is thus a powerful attack, which breaches the subscription privacy

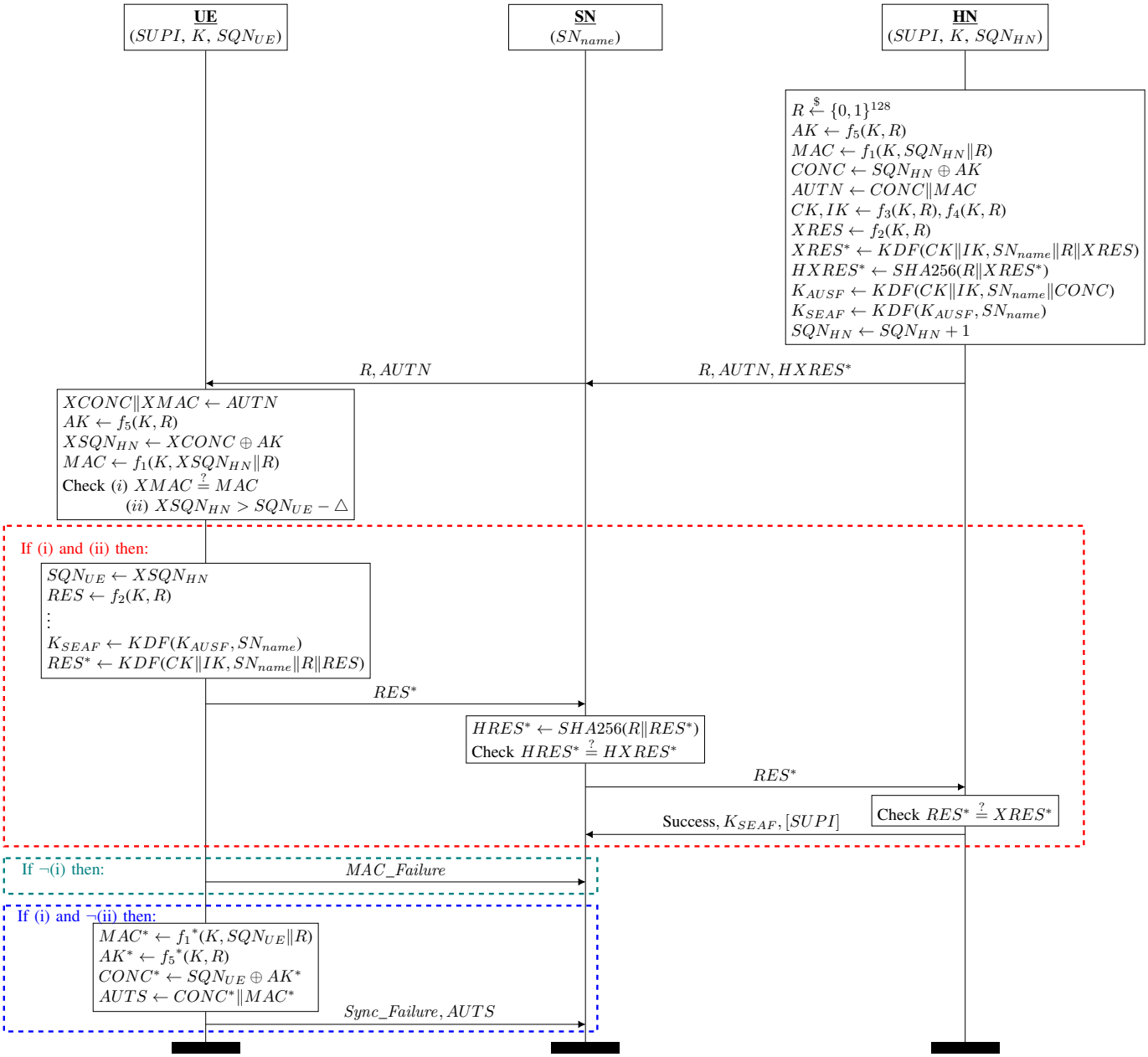


Fig. 4: The 5G-AKA protocol and its associated failure mechanisms.

completely. IMSI-catching is well documented as a *Key Issue* (Appendix A) in 3GPP TR 33.899 (sub-clause 5.7.3.2) [6].

B. (Raw) IMSI-probing

In its discussions, 3GPP distinguishes between "IMSI-catching" and "IMSI-probing". IMSI-probing is where an attacker already knows the subscription identity, e.g., an IMSI or an MSISDN plus some associated information, and wants to find out whether the subscriber with this identity is present in a given area. This is a far less powerful attack than IMSI-catching. There are many possible ways to carry out such an attack, e.g., send a bunch of (if possible silent [20]) SMSs or other "activity triggers" to that MSISDN and see whether there is a corresponding flurry of signalling in the cell you are testing. Preventing all sorts of IMSI-probing attacks would be difficult and would involve a lot of overhead, e.g., dummy signalling to conceal when the real signalling happens. Consequently, it was not thought worthwhile to address this attack by 3GPP.

C. Unauthenticated IMEI Request

In GSM and UMTS systems, it was possible for an attacker to request the subscriber for its IMEI via an unauthenticated *identity request* message [13], [15], [17]. However, from LTE onwards, such provisions were removed and now the network can only request the user for its IMEI after establishment of

TABLE II: Summary of privacy attacks in the previous generations

Attack		Type			Attacker Capabilities					Generation			Section
		Identity Disclosure	Location Leak	User Traceability	Radio Passive	Radio Active	IMSI	MSISDN	TMSI / GUTI	2G	3G	4G	
IMSI-catching	[11], [13], [14], [15], [16], [17], [18], [19]	●	●	●	●	●	○	○	○	●	●	●	III-A
(Raw) IMSI-probing	[20]	○	●	●	●	◐	○	●	○	●	●	●	III-B
Unauthenticated IMEI Request	[13], [15], [17]	●	●	●	●	●	○	○	○	●	●	◐	III-C
GUTI Persistence	[21], [22]	○	●	●	●	○	◐	◐	○	●	●	●	III-D
GUTI-MSISDN Mapping	[22], [23], [24], [25]	○	●	●	○	◐	○	●	○	●	●	●	III-E
C-RNTI based Tracking	[26]	○	●	◐	●	◐	○	●	○	●	●	●	III-F
GUTI Reallocation Replay Attack	[21], [27]	○	○	●	●	●	○	○	○	●	●	●	III-G
Localization through Measurement Reports	[22], [28]	○	●	●	●	●	?	●	●	○	○	●	III-H
IMSI-paging Attack	[29], [22], [21], [30]	○	●	●	●	●	◐	◐	○	●	●	●	III-I
ToRPEDO Attack	[31]	◐	●	●	●	◐	○	●	○	●	●	●	III-J
AKA Protocol Linkability Attack (LFM)	[21], [29], [32]	○	○	●	●	●	○	○	○	○	●	●	III-K

Legend: ● = yes, applicable ◐ = partially/limited/optional ○ = no, not applicable ? = property unknown

a secure channel between them [33]. However, under certain special circumstance, e.g., when the UE has no IMSI or no valid GUTI during *emergency attach*, the IMEI is sent before a security context is activated. This is to restrain the misuse of ME for placing invalid emergency calls [34].

D. GUTI Persistence

Temporary subscriber identifiers like GUTI are used as a privacy measure to mitigate subscription identification and tracking by eavesdroppers on the radio link, making it harder to track the location or activity of a particular subscriber. In an LTE system, the updating of GUTI is recommended on the following occasions:

- When the SN gets changed or during a new *Attach* procedure;
- During a Tracking Area (TA) update;
- When the SN issues "GUTI reallocation command".

The major problem with the mechanism of GUTI allocation in the current LTE system is that it is up to the SN policy configuration when (if at all) to reallocate the GUTI. It is also possible for the SN to keep (re)allocating the same old GUTI to the UE. The UE neither takes part in the generation of the GUTI nor verifies the freshness of the newly allocated GUTI. This opens up possibilities for either poor implementations or poor configuration that keeps the GUTI unchanged for a long time. The evidence of these poor practices has been found in real mobile network operators [22], [21] where the operators tend not to frequently update the GUTI on these occasions. The reason ascribed to such practices is to avoid the signalling storms [35] within the networks. In LTE networks, acquiring or tracking the temporary subscription identifiers has been one of the most important attack strategies in compromising subscription privacy [22]. GUTI persistence has been identified as a *Key Issue* in 3GPP TR 33.899 (sub-clause 5.7.3.1) [6].

E. Mapping between GUTI and MSISDN

These attacks are somewhat related to the IMSI-probing ones but are more fine-grained. In these attacks, the attacker starts with similar assumptions about knowing one of the subscription long-term identities and the aim is to locate and then further trace that subscriber. The attack uses the usual techniques of either initiating phone calls [23] or sending silent SMSs [24] to the target MSISDN. This results in triggering of their paging procedures, which ultimately lead to a mapping between the known identity (usually MSISDN) and the GUTI [25]. This enables an attacker to track a particular subscriber for a long duration due to infrequent updation of GUTI in LTE (details in Section III-D). Note that in these attacks paging messages are sought by the attackers instead of looking out for a generic signalling flurry.

F. C-RNTI based Tracking

The Cell Random Network Temporary Identifier (C-RNTI) is a physical layer 16-bit identifier unique within a given cell and is assigned to each device during the "Random Access Procedure" (see Section III-I for details). Passive analysis of real LTE traffic has revealed that the C-RNTI is included in the header (in unencrypted form) of every single packet [26]. This leads to linking of the radio traffic (both user and control plane) by a passive adversary. Further mapping to a user's GUTI or MSISDN is trivial and can be undertaken via the use of silent text messages. Through tracking of the C-RNTI value, an attacker can easily determine how long a given user stays at a given location.

Further analysis of captured LTE traffic has revealed that during mobility handover events these physical layer identifiers can be linked together. This leads to traceability of users when they move from cell to cell. This was because the captured handover triggering messages were sent in the clear. According

to the response of the standardization bodies, these messages are not suppose to be in the clear.

G. GUTI Reallocation Replay Attack

As explained in Section II-B, subscribers communicate with the networks using GUTIs as their identifiers for privacy purposes. To avoid traceability of subscribers based upon GUTI, it is imperative that these temporary identifiers are updated frequently. To update the GUTI, the mobile networks use a process called "GUTI Reallocation Procedure" (sub-clause 5.4.1 of TS 24.301 [36]). Figure 5 depicts this procedure as defined for an LTE system in [36]. In this figure, $oGUTI$ depicts the old GUTI and $nGUTI$ is the new GUTI, while CK is the "confidentiality key". The procedure is as follows:

- The UE identifies itself to the network on a dedicated channel via its currently allocated temporary identifier $oGUTI$.
- The network identifies the UE and establishes the means of ciphering for subsequent communication.
- Thereafter, a new GUTI ($nGUTI$) is sent to the UE in a message encrypted with CK via a $GUTI\_Reallocation\_Command$. If required, this message may also contain the identity of the current location area ($nLAI$).
- Upon receipt of the GUTI reallocation command, the GUTI replies via the $GUTI\_Reallocation\_Complete$ message to acknowledge receipt of the new GUTI.

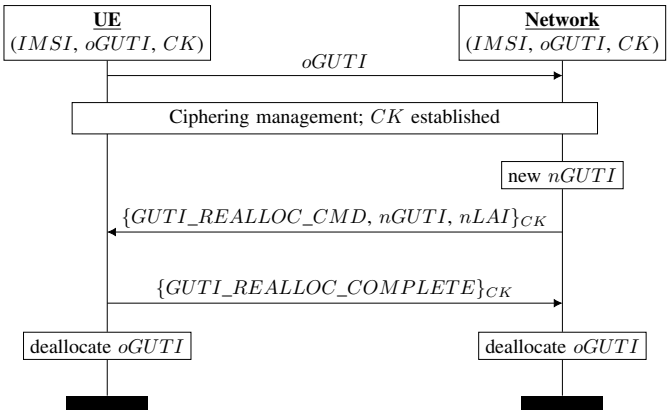


Fig. 5: GUTI Reallocation Procedure.

If the network does not receive the expected acknowledgment from the UE, it maintains both $oGUTI$ and $nGUTI$ for the concerned IMSI. The standard defines two methods for the means of ciphering, i.e., for the establishment of the confidentiality key CK: (1) either a new key is established via the authentication procedure; or (2) a previously established ciphering key is restored via the security mode setup procedure. The option of using the restored keys allows a linkability attack on the GUTI reallocation procedure [21], [27]. As the $GUTI\_Reallocation\_Command$ does not contain a replay protection mechanism, an adversary is able to exploit this weakness. The adversary first captures a GUTI reallocation command. Later, when the UE has already updated its GUTI but not yet the ciphering key CK, the attacker replays the captured reallocation command. The victim UE has no way to detect this replay attack. It successfully decrypts this reallocation command and replies via a $GUTI\_Reallocation\_Complete$ message. This allows the adversary to distinguish the target UE from any other, as other UEs will not be able to decrypt the reallocation command and hence will not reply with the completion message, even though in the meantime the target UE was assigned with an updated GUTI. This results in the adversary being able to track the target user with minimal effort.

H. RRC Protocol Vulnerabilities / Misimplementations

The Radio Resource Control (RRC) protocol is used to set up and manage the radio connectivity between the UE and SN. The major functions of the RRC protocol include connection establishment and release functions, broadcast of system information, radio bearer establishment, reconfiguration and release, RRC connection mobility procedures, paging notification and release, etc. Within the protocol stack, it exists at the network (IP) layer. The RRC protocol is specified in 3GPP TS 25.331 [37] for UMTS and in 3GPP TS 36.331 [38] for LTE. In LTE, when the UE selects a cell in RRC *idle mode*, it does not validate whether the base station is authentic or fake. As a result, the UE may clamp on to a rogue base station. So far, the mobile telephony systems have focused on providing secure communication in the RRC *connected state* and security aspects in RRC *idle state* have not been considered. This vulnerability of UE to false base station attacks during the RRC *idle state* has been acknowledged as a *Key Issue* in TR 33.899 (sub-clause 5.4.3.1) [6].

The LTE RRC protocol also contains a "network information broadcast" function in which GUTIs associated with the SNs are broadcasted over the air [22]. These broadcasts are neither encrypted nor authenticated, hence can be decoded easily by an adversary. Since these broadcasts are location specific, techniques described in [23] can be exploited to reveal presence of subscribers in that specific area (a type of IMSI-probing attack, as explained in Section III-B). Another type of RRC message which contains subscriber-specific sensitive information is the "UE measurement report". In particular, two types of UE measurement reports have been exploited in the literature [22] to compromise location of subscribers:

- **Measurement Report:** *Measurement report* is a necessary part of the handover procedure of LTE networks. The SN sends a "measurement configuration" message to the UE indicating what type of measurement is to be performed. In response, the UE compiles and sends the appropriate *measurement report*. The earlier LTE specifications (Version 12.5.0 of TS 36.331 and earlier) allowed transmission of these RRC messages before establishment of a security context between the UE and SN. This has been exploited to compromise the location of subscribers by decoding of the location information contained within these messages [22], [28]. However, later the specification was updated to allow *measurement report* transmission

only after establishment of the security context between UE and SN. Although the attack descriptions in [22] mention "mapping between GUTI and IMSI via semi-passive attacks", it is unclear whether knowledge of the victim's IMSI contributes towards these attacks - hence the *property unknown* label (?) in Table II.

- **Radio Link Failure (RLF) Reports:** *RLF reports* are used to troubleshoot signal coverage issues. These reports contain serving and neighboring base stations' identifiers along with their corresponding power measurements, which can be used as inputs to trilateration techniques such as [39] to determine an accurate position of the UE. The LTE standard (Appendix A.6 of [38]) does not allow transmission of *RLF reports* before establishment of a security context between the UE and SN. However, practical investigations [22] of real-world mobile networks has found that LTE phones (baseband processor to be more specific) do transmit these reports without a security context, leading to location leaks of the subscribers. This shows that the related guidelines within the standard are vague and ambiguous (described in an appendix located at the end of a 900+ page document), which leads to incorrect implementation by multiple manufacturers.

I. IMSI-based Paging

Figure 6 outlines the paging procedure in LTE. The Mobility Management Entity (MME) (a part of the SN's core network) is responsible for initiating paging and authentication of the mobile device, while eNodeB is the LTE base station (part of SN's access network). At the commencement of the paging, the MME starts a timer (T3413) and expects a response from the UE before the expiration of this timer. UEs in RRC Idle mode use Discontinuous Reception (DRX) also known as the *paging cycle* to reduce power consumption. This DRX cycle determines how frequently the UE checks for paging messages. The default DRX cycle is broadcast by the SN via the System Information Block (SIB). The Paging Occasion (PO) for a UE (i.e., when it wakes up to check for paging messages) is given by three numbers: the *paging cycle* $T \in \{32, 64, 128, 256\}$; the Paging Frame Index (PFI), which is an integer between 0 and $T - 1$; and a *subframe index* s where, $0 \leq s \leq 9$. The UE decodes the RRC paging messages and if it finds its identifier within this message then it initiates the acquirement of an available radio channel through the "Random Access Procedure". Thereafter, the UE requests the eNodeB via the "RRC Connection Request" to configure radio resources for signalling exchange. After completion of this RRC connection setup, the UE send a "Service Request" message and enters the *connected* state.

In LTE paging, two types of identities could be used to alert idle UEs about incoming data: temporary identifier GUTI or permanent identifier IMSI. Usually, it is the GUTI which is utilized as an identifier within the paging messages. However, in situations where the SN loses its context with the UE due to a crash or restart, the provision is there to send the IMSI as the UE identifier. Using the IMSI as the UE identifier while

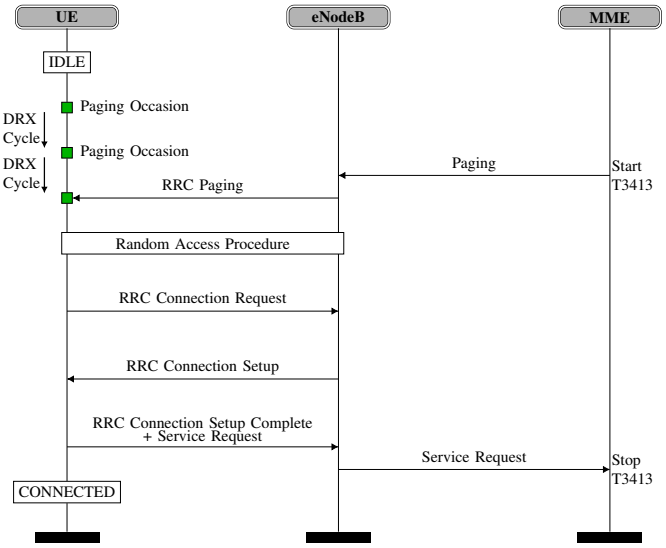


Fig. 6: The LTE paging mechanism.

sending paging messages has been reported as a privacy threat to users [22], [29], [30], [21].

A passive adversary can just observe the radio communication in an interested location and come to know which subscribers are located in that particular area. Since during the paging procedure a security context is not yet established between the UE and SN, an active adversary can set up a false base station in an area of interest (airports, hospitals, etc.). It can then start sending out IMSI-based paging requests to the subscribers and, based upon the responses, will come to know which IMSIs are present in that particular area. The LTE subscribers reply to IMSI-based paging triggers via their GUTIs. Hence, this leads to a correlation between the IMSIs and GUTIs. This, combined with the initiation of paging mechanism via placing phone calls to the MSISDN (Section III-E), allows an attacker to further correlate its IMSI and GUTI with the MSISDN. Thus active/passive listeners, fake SNs, etc. can track down subscribers with reasonable accuracy to a specific geographic area, which has serious privacy implications. IMSI-based paging has been identified as a *Key Issue* in 3GPP TR 33.899 (sub-clause 5.7.3.10) [6].

J. ToRPEDO Attack

In LTE paging, the POs are determined by the UE's IMSI. This mechanism has been exploited to verify the presence (or absence) of a target in a specific location via an attack called ToRPEDO (TRacking via Paging mEssage DistributiOn) [31]. This attack leverages the fact that the PO for a specific UE is always fixed as it is based upon its IMSI. Hence, through triggering successive paging procedures, the attacker is ultimately able to determine the presence or absence of a target UE with high confidence.

Moreover, in the ToRPEDO process, the attacker learns the last 7 bits of the UE's IMSI. We now briefly outline this leakage process. In LTE, the last 10 bits of the subcriber's IMSI are used for calculating the PO of a device. In this

calculation, however, the IMSI is considered to be a 14/15-digit decimal number instead of a TBCD encoded number. Without loss of generality, if we consider $T = 128$, then successfully calculating the victim's PO will leak the last 7 bits of the victim's IMSI.

K. Linkability of AKA Failure Messages

All generations of mobile telephony suffer from a location attack known as the *Linkability of (AKA) Failure Messages* (LFM) attack [32], [29], [21]. The LFM attack exploits the fact that in an AKA protocol (see Section II-E), in the event of an erroneous authentication challenge, the reason for the authentication failure is exposed to the attacker, i.e., either $MAC\_Failure$ or $Sync\_Failure$. This allows an attacker to link two different AKA sessions to identify a target user. The LFM attack is simple to execute in practice. The attacker first observes an AKA session of the target user and records the authentication challenge $(R, AUTN)$. Later, when the attacker wants to check whether another AKA session belongs to the same user or not, he replays the recorded authentication challenge and observes the type of failure message received. In the case of $MAC\_Failure$ it is some other user, while in the case of $Sync\_Failure$ it is the same user. Note that in an LFM attack no further computations are required and the results are precise. Hence this is a devastating attack (albeit under additional assumptions about the attacker's capabilities) which compromises subscription location and, as an extension, allows user-traceability.

IV. The Present - Privacy Improvements by 3GPP Release 15

Release 15 comes with several new security features that significantly improve subscription privacy on the radio interface [40], [41]. Table III provides a summary of the effect of these new features upon the vulnerabilities from previous generations.

A. Concealment of SUPI

Keeping in view the severity of the threats posed by SUPI exposure via IMSI-catching attacks (Section III-A), 3GPP decided to address this problem in 5G Release 15 (sub-clause 5.2.5 of TS 33.501) [3]. In the event of identification failure via a 5G-GUTI, unlike earlier generations, 5G security specifications do not allow plaintext transmissions of the SUPI over the radio interface. Instead, a public-key based privacy-preserving identifier containing the concealed SUPI is transmitted. The public-key scheme chosen by 3GPP for this purpose is the *Elliptic Curve Integrated Encryption Scheme* (ECIES) [45]. The concealed identifier is called the SUCI. The UE generates the SUCI with the public key pk of the HN using an ECIES-based protection scheme. We now provide an overview of the ECIES-based protection scheme as described in TS 33.501 (Annex C.3) [3].

ECIES is a hybrid encryption scheme that combines Elliptic Curve Cryptography (ECC) [46] with symmetric cryptography; it is a semantically secure probabilistic encryption scheme ensuring that successive encryptions of the same plaintext with the same public key result in different ciphertexts with very high probability. The use of ECIES for concealment of the SUPI adheres to the Standards for Efficient Cryptography Group (SECG) specifications [47], [48]. To compute a fresh SUCI, the UE generates a fresh ECC ephemeral public/private key pair utilizing the HN public key pk. This public key is securely provisioned to the UE during the USIM registration. Processing on the UE side is undertaken according to the encryption operation illustrated in Figure 7a. The final output of this protection scheme is the concatenation of the ECC ephemeral public key, the ciphertext value, the MAC tag value, and any other parameters, if applicable. The HN uses the received ECC ephemeral public key and its private key (corresponding to public key pk) to deconceal the received SUCI. Processing on the HN side is illustrated in Figure 7b. TS 33.501 includes two ECIES profiles, both for approximately 128-bit security level. Both profiles use AES-128 in CTR mode for confidentiality and HMAC-SHA-256 for authenticity in the symmetric cryptography part, and use either Curve25519 or secp256r1 elliptic curves for the public-key cryptography part.

Only the MSIN part of the SUPI is concealed by this protection scheme, while the home network identifier (MCC/MNC) is transmitted in plaintext as it is required for routing in roaming use cases. The data fields constituting the SUCI are:

- **Protection Scheme Identifier:** This field represents the specified protection scheme.
- **Home Network Public Key Identifier:** This represents the public key pk provisioned by the HN.
- **Home Network Identifier:** This contains the MCC and MNC part of the SUPI.
- **Protection Scheme Output:** This represents the output of the public-key based protection scheme.

As the pk comes pre-configured on the USIM, a public-key infrastructure is not needed. Also, the subscription identification is achieved in just one pass of communication, which helps in reducing the connection set-up time. Further, this scheme is oblivious to desynchronization [49] of identifiers between the UE and HN and requires simple key management, both of which lead to significant reduction in connection failures. However, there still remain aspects which require further improvement. We discuss these issues in further detail in Section V-D.

B. Strict Refreshment of GUTI

In 5G Release 15 (sub-clause 6.12.3 of TS 33.501), it is mandatory to refresh the 5G-GUTI on the following occasions:

- **Initial Registration:** If the SN receives a *Registration Request* message of type "initial registration" or "mobility registration update" from a UE, it should send a new 5G-GUTI to the UE in the registration procedure.
- **Mobility Registration Update:** If the SN receives a *Registration Request* message of type "mobility registration update" from a UE, it should send a new 5G-GUTI to the UE in the registration procedure.

TABLE III: Effect of 5G privacy enhancements upon existing attacks

5G Privacy Enhancing Features	Existing Attacks from Previous Generations									3GPP Reference	Section
	IMSI-catching	(Raw) IMSI-probing	GUTI Persistence	GUTI-MSISDN Mapping	GUTI Reallocation Replay	Localization via UE Reports	IMSI-paging	ToRPEDO Attack	LFM Attack		
SUPI Concealment	●	○	○	○	○	○	○	○	○	Sub-clause 5.2.5 of TS 33.501 [3]	IV-A
Strict GUTI Refreshment	○	○	●	●	○	○	○	◐	○	Sub-clause 6.12.3 of TS 33.501 [3]	IV-B
False Base Station Detection Framework	◐	○	○	○	◐	●	◐	○	◐	Annex E of TS 33.501 [3]	IV-C
De-coupling of SUPI from Paging	○	○	○	○	○	○	●	○	○	Sub-clause 9.3.3.18 of TS 38.413 [42]	IV-D
GUTI-based Paging Occasion	○	○	○	○	○	○	○	●	○	Sub-clause 7.1 of TS 38.304 [43]	IV-E
Secure Radio Redirections	◐	○	○	○	◐	◐	◐	○	○	TS 38.331 [44]	IV-F

Legend: ● = resolves, applicable ◐ = partial/limited effect ○ = does not resolve, not applicable

- **Periodic Registration Update:** If the SN receives a *Registration Request* message of type "periodic registration update" from a UE, it should send a new 5G-GUTI to the UE in the registration procedure.
- **Network Triggered Service Request:** Upon receiving a *Service Request* message sent by the UE in response to a paging message, the SN sends a new 5G-GUTI to the UE.

These mandatory update features makes identifying or tracing subscribers, based on 5G-GUTI, impractical. Further, it is left to network operator's implementation to re-assign 5G-GUTI more frequently, for example after a *Service Request* message from the UE not triggered by the network.

C. False Base Station Detection Framework

As evident from the description of vulnerabilities in Section III, most attacks on previous generations leverage false base stations before the UE can go into an authenticated state. To counter such vulnerabilities, a general framework for detecting false base stations has been described in 5G Release 15 (Annex E of [3]). This network-based detection framework uses radio condition information (measurement reports of Section III-H)) received from the devices which could be used to make it significantly harder for false base stations to remain stealthy. The received-signal strength and location information in measurement reports can be used to detect a false base station which tries to attract the UEs by transmitting signal with higher power than that of the genuine base stations. These reports can also be used to detect a false base station which replays the original network broadcast information without any modification. To detect a false base station which replays modified broadcast information to prevent victim UEs from switching back and forth between itself and the genuine base stations (e.g., by modifying neighboring cells, cell reselection criteria, registration timers, etc. to avoid the so called ping-pong effect), information on broadcast information can be used to detect inconsistency from the deployment information. Further, false base stations using unusual frequencies or cell identifiers can be detected by analyzing the respective information in the received measurements reports. Networks and devices can utilise other additional security and privacy features which are proprietary to the operators. Effective false base station detection should result in significant privacy improvement. This is because it has already been proven by [50] that in case of uncorrupted mobile network participants, the AKA protocol provides anonymity guarantees to the UE.

D. Decoupling of SUPI from the Paging Mechanism

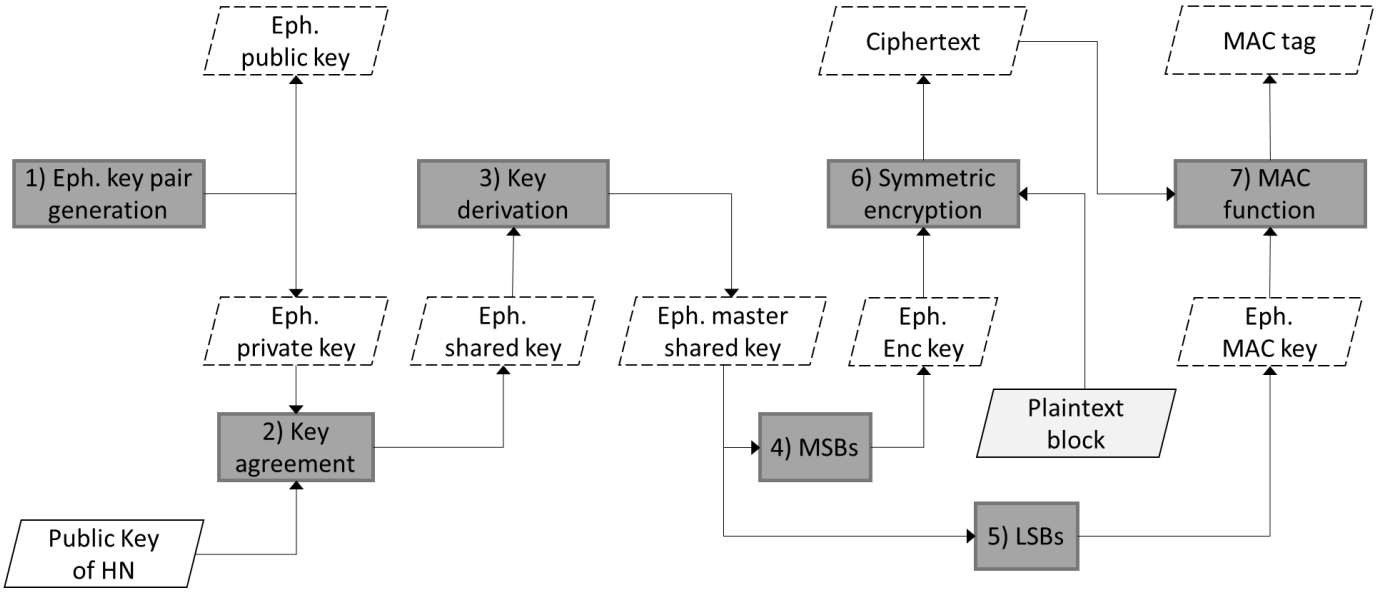
The provision of paging UE based on SUPI has been removed from 5G (sub-clause 9.3.3.18 of TS 38.413) [42]. Moreover, the calculation of the paging frame index and paging occasions is no longer based on SUPI and is instead based on 5G-GUTI. Coupled with the mandatory 5G-GUTI update mechanism (Section IV-B), this makes it impractical for false base stations to use paging messages to identify or trace subscribers.

E. GUTI-based Paging Occasions

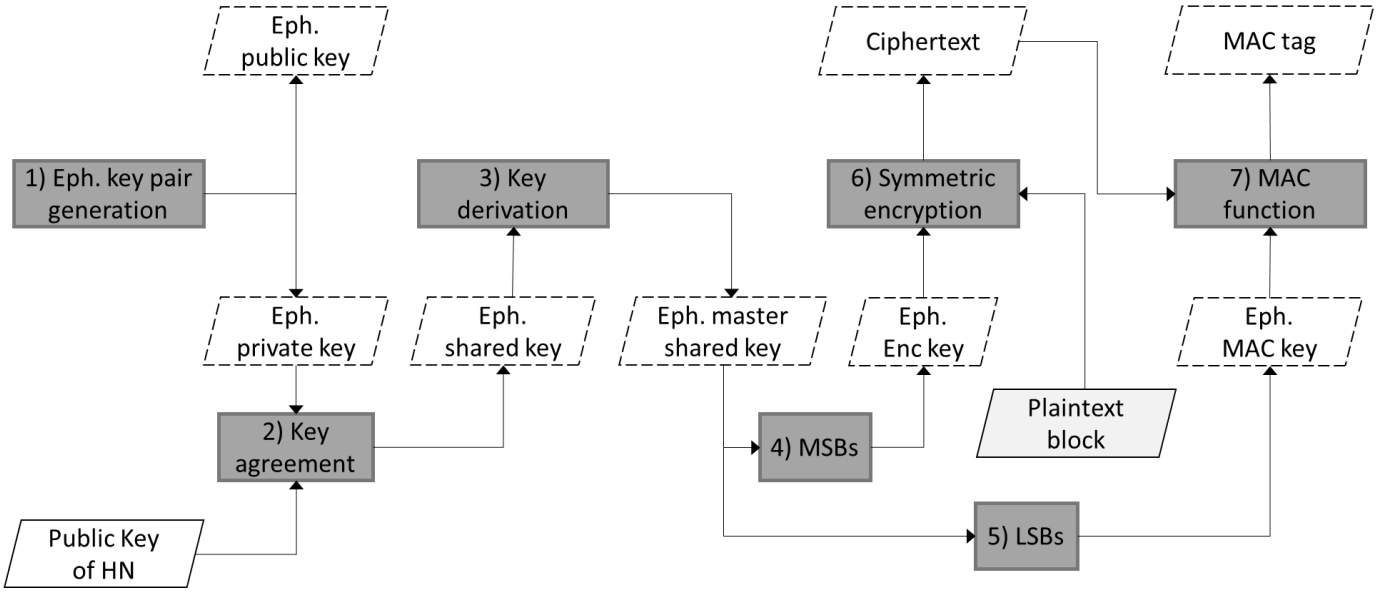
While in LTE, POs were determined based on the device's IMSI; now in 5G they are based on a temporary identifier (called a 5G-S-TMSI) which is a subset of the device's GUTI. The result of this change is that now the ToRPEDO attack (Section III-J) which leveraged fixed POs for a target UE is not able to exploit the permanency in paging timings anymore. This enhancement along with frequent GUTI refreshment (Section IV-B) results in enhanced user privacy.

F. Secure Radio Redirections

It is mandatory in 5G Release 15 (TS 38.331 [44]) to integrity protect RRC messages that redirect devices. This feature mitigates false-base-station-based rogue redirections.



(a) Encryption at the UE side



(b) Decryption at the HN side

Fig. 7: Detail of ECIES-based Protection Scheme as defined in 3GPP TS 33.501 [3].

As a result, the level of difficulty of launching various privacy attacks which rely on rogue redirections increases manifold.

V. The Future - Outstanding Issues, New Attacks & Proposed Measures

The successful deployment of future 5G systems requires resolution of the outstanding subscription privacy issues. In this section, we highlight the subscription privacy vulnerabilities which were not addressed by Release 15. We also discuss recent literature which either suggests improvements or presents new attacks on 5G subscription privacy.

A. Unresolved Vulnerabilities

An examination of Table III reveals that there are three privacy issues from previous generations which were not aptly addressed by Release 15: (Raw) IMSI-probing (Section III-B), C-RNTI-based tracking (Section III-F) and the AKA-protocol-based LFM attack (Section III-K). Regarding (Raw) IMSI-probing, as already discussed in Section III-B,

it is highly unlikely that 3GPP will adopt countermeasures to this particular problem because of the high overhead of the necessary dummy signalling. The only feasible solution to handle the C-RNTI-based privacy breaches is to employ a network-wide PKI [51] since this requires encryption of these pre-authentication identifiers. This is unlikely to be a desirable option for 3GPP due to the high costs associated with deploying and maintaining a PKI.

Arapinis et al. [29], while highlighting the LFM vulnerability, also proposed a fix to resolve this problem. The proposed fix requires the HNs to have a public/private key pair where each USIM stores the public key of its HN. The AKA failure messages are then encrypted using the network's public key. They verified the privacy properties of their fixes using the automated symbolic analysis tool `ProVerif` [52]. However, their proposed fix has been shown by Fouque et al. [53] to be still suffer from certain privacy weaknesses. Fouque et al. presented their own improved variant of the public-key-based fix for the LFM vulnerability. 3GPP never considered adoption of these proposals, most probably because they are public-key-based and introduce significant overheads. As the UE and HN already share common secrets between them, a more viable way forward is to resolve this issue through the use of symmetric-key techniques. We explore such approaches further in Section V-C.

B. New Attacks on 5G Subscription Privacy

Borgaonkar et al. [54] presented new attacks against all variants of the AKA protocol, including 5G AKA, which breach subscribers' privacy. These attacks exploit a logical vulnerability in the AKA protocol's failure mechanism. This vulnerability stems from the use of XOR within the re-sync token $AUTS$ (see Figure 4), which is a concatenation of two parameters; $CONC^*$ and MAC^*. The parameter $CONC^*$ contains the current sequence number of the UE in a masked form as $SQN_{UE} \oplus AK^*$, where $AK^* = {f_5}^*(K, R)$. Note that during calculation of the masking key AK^*, the value R is extracted from the received authentication challenge (R, $AUTN$). Hence, in case of receiving the same authentication challenge twice at two different times t_1 and t_2, the masked sequence numbers in their corresponding $AUTS$ tokens will be:

$$CONC_1^* = SQN_{UE}^1 \oplus AK_1^*,$$
$$CONC_2^* = SQN_{UE}^2 \oplus AK_2^*,$$

where $AK_1^* = {f_5}^*(K, R)$, $AK_2^* = {f_5}^*(K, R)$, SQN_{UE}^1 is the sequence number of UE at time t_1 and SQN_{UE}^2 is the sequence number at time t_2. Therefore, the adversary can compute:

$$CONC_1^* \oplus CONC_2^* = SQN_{UE}^1 \oplus SQN_{UE}^2.$$

Based upon this logical vulnerability, [54] presented two new attacks against 5G subscription privacy: Activity Monitoring Attack (AMA) and Location Confidentiality Attack (LCA).

In AMA, the aim of the adversary is to learn the n least significant bits of SQN_{UE} at two different time instances, t_1 and t_2. Thereafter, from the difference between the sequence numbers (corresponding to successful authentication sessions), the attacker infers the volume of "activity" (number of calls, SMSs, etc.) a particular user has performed between these two time instances, hence the name Activity Monitoring Attack. To mount AMA, the adversary requires malicious interaction with both UE and HN (via SN). Hence, the compromise of both *identity confidentiality* and *location confidentiality* of the target UE are prerequisites to launch an AMA. Details of a single instance of the attack at a particular time t are now explained. The online phase of the AMA is depicted in Figure 8. During this phase the attacker first fetches $2^{n-1}+1$ successive authentication challenges from the HN for the targeted UE. The attacker then sends a particular $n+1$ of these challenges to the UE, each followed by a replay instance of the initially received authentication challenge $(R_0, AUTN_0)$, and records the corresponding $n+1$ resync tokens, i.e. $AUTS'$ and $AUTS_j$ $(for\ j = 0\ to\ n-1)$. In the offline phase, utilizing the logical vulnerability elaborated earlier, the attacker retrieves the following values from the recorded resync tokens:

$$\delta_i = SQN_{HN}^0 \oplus (SQN_{HN}^0 + 2^i) \text{for } 0 \leq i \leq n-1,$$

where SQN_{HN}^0 is the initial value of the HN's sequence number at the start of the attack. Note that due to receipt of the first authentication challenge $(R_0, AUTN_0)$ from the adversary, the UE will also sync its sequence number to this value at the start of the attack. Further, by feeding these n values into the *SQN inference algorithm* (see Figure 9), the attacker extracts the n least significant bits of SQN_{HN}^0.

In LCA the aim of the attacker is to find out whether some targeted UE is present at a certain location or not. The LCA proceeds as follows:

1) The attacker observes a 5G-AKA session of some targeted user[2] UE_x and extracts the corresponding $CONC_x^*$ value by replaying the observed authentication challenge to UE_x.
2) After some time, if the attacker wishes to check whether another unknown 5G-AKA session belongs to UE_x or not, the attacker again replays the earlier observed challenge from the step above to this unknown user and obtains $CONC_?^*$.
3) Now based upon the value $CONC_x^* \oplus CONC_?^*$, the attacker can infer (with non-negligible probability) whether this new user is UE_x or not. In the case of some other user, this will be a random value, while in the case of UE_x, the attacker will equate $SQN_{UE_x}^{old} \oplus SQN_{UE_x}^{current}$ due to canceling out of the common masking key AK^*. This value (dependent upon the lapsed time) should be small in the case of user UE_x.

Khan and Martin [55] have analyzed these attacks for their effectiveness, practicability and potency against 5G. Their analysis reveals that the AMA is not as effective against 5G as it is against the previous generations (3G/4G). The analysis

[2]Note that it is not necessary for the attacker to know the $SUPI$ of the user to launch this attack.

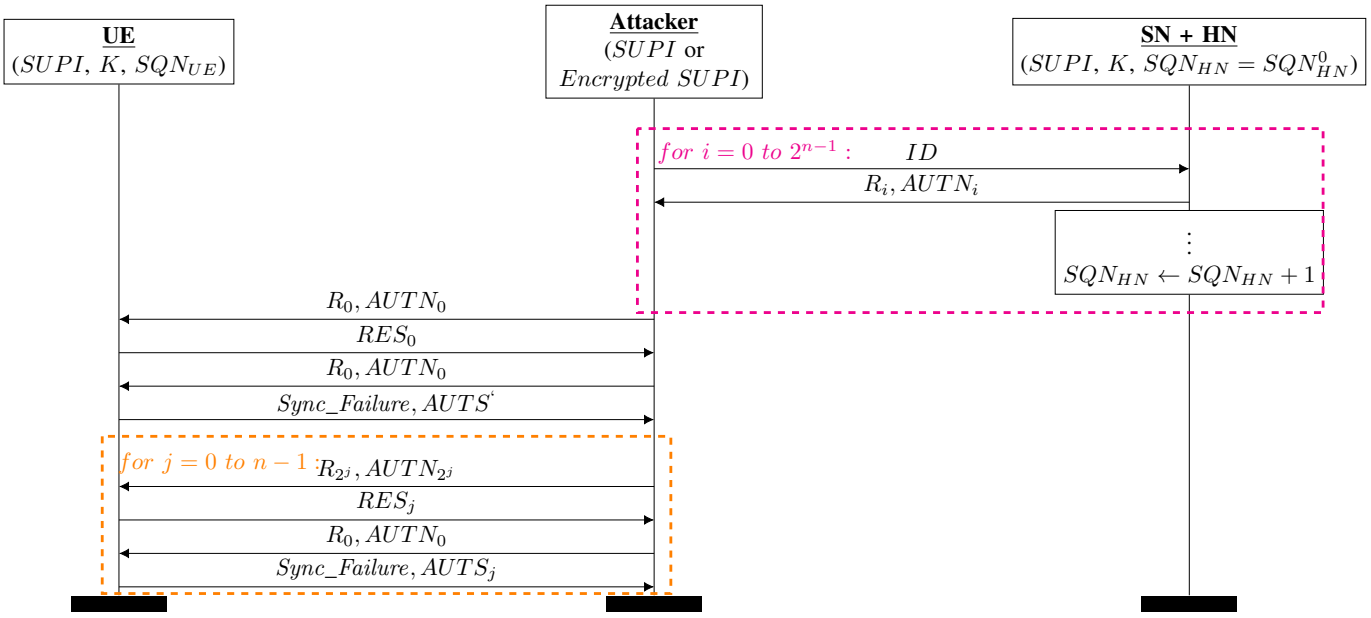


Fig. 8: The online phase of the AMA.

Data: δ_i *for* $0 \leq i \leq n-1$
Result: $X = n$ least significant bits of SQN^0_{HN}
$X \leftarrow [0, 0, \ldots, 0]$ `// init an array of size n`
for $i \leftarrow 0$ **to** $n-1$ **do**
  `// Analyze` δ_i `at bit positions` i, $i+1$
  $(b_1, b_2) \leftarrow (\delta_i[i],\ \delta_i[i+1])$
  if $(b_1, b_2) \Leftrightarrow (1, 0)$ **then**
    `// No remainder propagates when` $SQN^0_{HN} + 2^i$
    $X[i] \leftarrow 0$
  else if $(b_1, b_2) \Leftrightarrow (1, 1)$ **then**
    `// A remainder propagates when` $SQN^0_{HN} + 2^i$
    $X[i] \leftarrow 1$
  else
    `// Not possible`
    Error
  end
end
return (X)

Fig. 9: SQN Inference Algorithm.

also brings to light the fact that the LCA is a direct extension of the existing privacy vulnerability of LFM (Section III-K). They also established that any effective countermeasure (details in Section V-C) introduced to fix the LFM attack will also render these two new attacks ineffective.

C. Fixing LFM, AMA and LCA

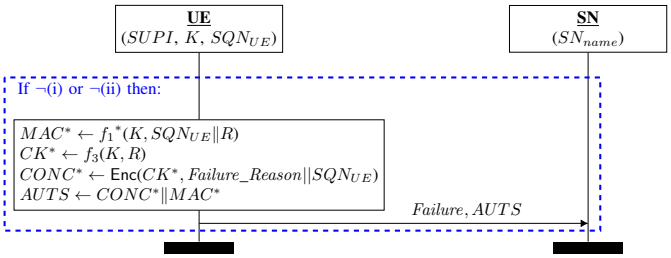
As discussed previously in Section V-A and Section V-B, a symmetric-key-based solution is required which should resolve the three vulnerabilities of LFM, AMA and LCA. We now briefly review some solutions proposed by [54].

1) Symmetrically Encrypting SQN_{UE} (Fix 1): This fix consists of modifying the sequence-number-concealing mechanism. Instead of using XOR to conceal SQN_{UE}, this fix utilizes symmetric encryption. The resulting fix is depicted in Figure 10a. To counter the LFM attack, it suffices to hide the reason for the 5G-AKA protocol failure inside the ciphertext $CONC^*$. The authors of [54] claim that this fix is easy to deploy in the current cellular system as it only requires changes in the baseband module of the UE (i.e. ME) and not USIM. This seems strange as it is the USIM (not the mobile handset) which is directly under the control of the mobile network operator. This solution suffers from a flaw: when an attacker triggers a failure message by injecting the same authentication challenge twice while the SQN_{UE} has not being updated in the UE, then the replied $CONC^*$ will be the same as before, leaking to the attacker that SQN_{UE} is unchanged.

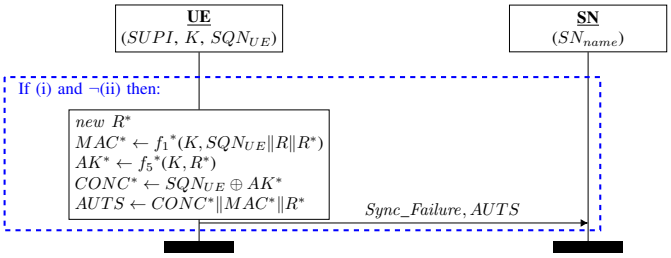
2) Correctly Randomizing $AUTS$ (Fix 2): Another way to fix the AMA and LCA is to generate a new random value (R^*) to conceal SQN_{UE} instead of utilizing the one (R) received in the authentication challenge. This R^* needs to be sent back in the clear to the HN along with $AUTS$ for decryption of SQN_{UE}. Figure 10b depicts this solution. Note that the original R must be used in the calculation of MAC^* to guarantee a fresh response to the received authentication challenge. Otherwise, an attacker will be able to replay an old response back to the HN, forcing it to synchronize its SQN_{HN} to an older value. Also note that this fix does not resolve the LFM attack on its own.

3) Combining Fix 1 and Fix 2 (Fix 3): Both Fix 1 and Fix 2 have limitations of their own. Fix 1 suffers from a

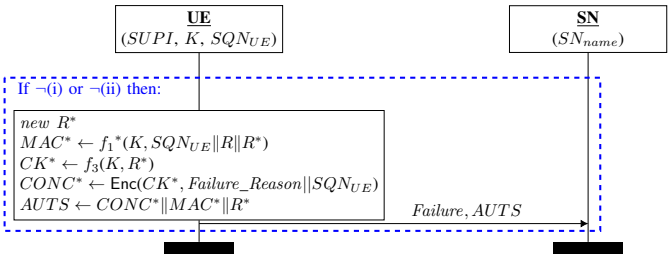
minor flaw, while Fix 2 is not suitable for LFM attack. For a comprehensive solution, which resolves both of these issues, we combine Fix 1 and Fix 2 as suggested in [54]. This combined fix is depicted in Figure 10c and addresses LFM, AMA and LCA without any known flaws / limitations.



(a) Fix 1: Symmetrically encrypting SQN_{UE}.



(b) Fix 2: Correctly randomizing $AUTS$.



(c) Fix 3: Combining Fix_1 and Fix_2.

Fig. 10: Proposed Fixes for 5G-AKA failure messages.

D. Shortcomings of the Current 3GPP SUPI Protection Mechanism

The issues with the current ECIES-based SUPI protection mechanism (IV-A) were communicated to 3GPP by the *European Telecommunications Standards Institute's (ETSI) Security Algorithms Group of Experts (SAGE)* [56] and are detailed as follows:

- **Post-Quantum Vulnerability:** As the ECIES-based scheme employs ECC to provision identity privacy, it relies on the hardness assumption of the Elliptic Curve Discrete Logarithm Problem (ECDLP). A quantum adversary capable of issuing quantum queries to an appropriate quantum computer can easily break this scheme by employing Shor's quantum algorithm [57].
- **Chosen SUPI Attacks:** Any arbitrary third party is able to select a SUPI of its choosing and send the corresponding SUCI to the HN. Thereafter the adversary can look out for various responses from the HN, depending on whether the target user is present in that particular cell area or not. Any noticeable variation in the perceived output would allow the adversary to confirm or deny the presence of the target in that particular cell. There is no mechanism in the ECIES-based scheme to prevent these kinds of attack.
- **Replay Attacks:** The ECIES-based scheme does not have any inherent mechanism to provide freshness guarantees to the HN and is thus susceptible to replay attacks. An adversary can always resend a previously encrypted SUPI to the HN and look out for various responses (such as authentication challenge or a failure message). Based on the received response, a device whose SUPI is unknown to the attacker may be tracked with some confidence [58].
- **Downgrade Attacks:** An active adversary simulating a (false) base station can force the UE to fall back to one of the previous generations (GSM/UMTS/LTE) and can then get hold of the IMSI/SUPI using an *identity request* message. In 3GPP Release 15 [9], the SUPI is derived directly from the IMSI, so these downgrade attacks also compromise the 5G SUPI.
- **Update of HN Public Key:** There could be situations which require the HN to have a robust way of quickly updating its public key to the subscriber UEs. One such scenario could be a malware attack which tries to recover the home network's private key. Such situations enforce the need to have a quick way of updating the corresponding public keys.

E. Quantum-secure and Downgrade-resistant SUPI Protection

As pointed out in Section V-D and by [59], the current ECIES-based SUPI protection solution is vulnerable to quantum cryptanalysis. Until the publication of the 3GPP public-key-based protection mechanism, the technical problem of finding a SUPI protection solution remained open in a purely symmetric-key setting. However, in 2018 Khan et al. [60] addressed all the shortcomings of the ECIES-based mechanism pointed out in Section V-D, except for the downgrade attacks. Interestingly, another paper [61] (at the same event) proposed a protection mechanism for the downgrade attacks against 5G. It seems viable that these two solutions can be combined together to come up with a 5G-SUPI protection mechanism that is both quantum-secure and downgrade-resistant.

F. IBE-based SUPI Protection

Both the current 3GPP SUPI protection mechanism (Section IV-A) and the alternative symmetric key proposal by [60] hide only the MSIN part of the SUPI, while the MCC and MNC parts are sent in the clear over-the-air to the SN for routing of the SUCI to the correct HN. Also, to increase look-up efficiency, mobile network operators divide their subscribers'

database into further sub-domains [62]. Therefore, it is required that the SUCI be delivered to the correct sub-domain within the HN. Typically, this requires between 1 and 3 digits after the MCC/MNC in the MSIN to be sent in the clear as part of the routing information [63]. All this results in a weakening of the privacy protection being offered to the mobile subscriber as a significant part of its identity is now exposed to an attacker. Another limitation of the 3GPP protection mechanism and proposal of [60] is that the SN is entirely dependent upon the HN for revealing the SUCI and the associated LI purposes [64]. Several countermeasures have been proposed in 3GPP meetings for handling of this issue [65], [66], [67], [68], [69]. All of these suggested countermeasures introduce overhead either due to additional signalling messages or due to requirements for new parameters. Moreover, there is nothing stopping the UE and its HN from colluding to provide the SN with a false SUPI.

To counter the mentioned limitations, Khan and Niemi [70] proposed a 5G-SUPI protection scheme based on Identity-based Encryption (IBE). In this scheme, the UE's HN acts as the Private Key Generator (PKG). IBE-based schemes inherently resolve the exposure of the partial MSIN and provide better *Lawful Interception* guarantees as the SN can now work out the SUPI from the SUCI independently of the HN. The proposal by [70] can be argued to be a better alternative to the current 3GPP mechanism, although the associated key-revocation is quite complex. However, compared with [60], it is not quantum secure and the increase in computational and signalling overhead is much higher. Also, it is unclear whether the IBE-based solution can be used in combination with the downgrade protection proposal of [61]. Given these limitations, in the long-term, the solution of [60] might be preferable.

G. Study on Protection against False Base Stations

Another important avenue which still requires further research is that of protection against false-base-station attacks. Although 5G Release 15 provides a false-base-station-detection framework (Section IV-C), its status is informative only. Moreover, the provided framework is generic in nature and focuses only on the detection aspects. Very recently, 3GPP has initiated a comprehensive study [81] which focuses on security enhancements against false base stations for the next 5G Release 16. The aim is to study the potential threats and privacy issues associated with false-base-station scenarios and identify potential solutions for mitigating the risks caused by false base stations. As various attacks against 5G subscription privacy on the radio interface exploit false base stations as the underlying platform, this study will also contribute towards subscription privacy enhancement in Release 16.

VI. Related Work

We believe there does not exist any prior work in the published literature with exclusive focus on 5G subscription privacy. The probable reason for this seems to be that 5G is a very nascent technology within which extensive development and upgrades were undertaken as late as June 2019. Table IV presents a summary of the related literature which has considered security and privacy in 5G or 5G-like networks. Here, we briefly discuss the work carried out in these publications.

Rupprecht et al. [71] categorized and systematized attacks in existing mobile generations (GSM/UMTS/LTE) by their aim, impact and attacker capabilities. They further identified future research directions for 5G networks based on these existing security and privacy issues. The main difference between [71] and our work is that we also consider 5G Release 15, while the privacy analysis of [71] is limited only to the previous generations. Tourani et al. [72] have analyzed security, privacy and access control within the scope of Information-centric Networking (ICN). ICN is a networking paradigm which focuses on content of the traffic rather than its origin - a concept similar [82] to *network slicing* (Appendix B) in 5G. Ahmad et al. [73], [74] analyzed generic security and privacy threats to 5G networks and suggested possible solutions to these threats from the published literature. As both of these works were carried out before the publication of the 5G standard, they are mostly speculative in nature. Khan et al. [75] have presented a survey about security and privacy of 5G. The 5G privacy issues discussed in [75] are again speculative in nature as the manuscript was drafted before the publication of 5G Release 15.

Jover [76] discussed security challenges faced by 5G. The main focus of this work was the integration of a Public Key Infrastructure (PKI) within the current 5G network architecture to resolve outstanding security and privacy issues. Ferrag et al. [77] presented a survey of existing authentication and privacy-preserving schemes for LTE and 5G mobile networks. They provided a classification of threat models in 4G and 5G cellular networks in four categories: attacks against privacy, attacks against integrity, attacks against availability, and attacks against authentication. They also provided a classification of the respective countermeasures into three categories: cryptographic methods, humans factors, and intrusion detection methods. It seems that the work of [77] presumed that all the analysis and contextualization with respect to 4G can be seamlessly applied to 5G. The reason for this is because at the time of publication of [77] (January, 2018) even the Stage-2[3] of 5G Release 15 was not completed (see Figure 1).

Gandotra and Jha [78] presented a survey on various energy-efficient scenarios for green communication in 5G and the related security aspects. For improving the battery lifetime of user terminals, [78] proposed transmitting information through relays and discussed security susceptibilities via these relays and the associated countermeasures. However, [78] did not consider 5G privacy. Rangisetti and Tamma [79] explored the aspects related to migration of mobile network infrastructure in LTE and 5G to Software Defined Networking (SDN) and Network Function Virtualization (NFV). It further elaborated security issues in migration to these new technologies and

[3]"Stage-2" is a stage where logical analysis, devising an abstract architecture of functional elements and the information flows amongst them across reference points between functional entities is carried out.

TABLE IV: Important recent survey publications related to 5G security and privacy

Reference	Publication Year	Application Area	Main Contribution	Relevance to 5G Subscription Privacy
[71]	2018	2G, 3G, 4G	A survey of existing literature on attacks in previous generations (GSM/UMTS/LTE) of mobile telephony.	Suggests research directions / improvements for 5G subscription privacy.
[72]	2018	ICN	A survey about security, privacy, and access control in information-centric networking.	The privacy attack scenarios discussed are also applicable to 5G networking concepts.
[73], [74]	2017/2018	5G	An overview of 5G security challenges and solutions.	Discusses the privacy challenges in 5G from the user's perspective.
[75]	2019	5G	A survey on the security and privacy of 5G.	Focused on portraying a landscape of futuristic security threats to 5G.
[76]	2019	5G	A survey of remaining security and privacy issues in 5G.	Proposes PKI integration to resolve outstanding issues.
[77]	2018	4G, 5G	A survey of existing authentication and privacy-preserving schemes for 4G and 5G cellular networks.	Discusses privacy attacks on 5G networks and provides recommendations for further research.
[78]	2017	5G	A survey on green communication and the associated security challenges in 5G networks.	Reviews privacy aspects of various 5G enabling technologies like machine-to-machine (M2M) communications, etc.
[79]	2017	SDN	A survey of issues and challenges in designing SDN based 5G networks.	No explicit focus on 5G privacy rather provides SDN based security solutions for 4G and 5G networks.
[80]	2019	5G	A survey on the security of alternative computing paradigms for 5G networks.	Emphasizes the applicability of alternative computing paradigms for enhancement of subscriber privacy.

suggested SDN-based solutions. The work by [79] is focused on the security issues during architecture migration and not on subscription privacy. Choudhry and Sharma [80] surveyed recent computing paradigms as alternative mechanisms for the enhancement of 5G security. This work particularly focuses on the feasibility of catalytic and osmotic computing in 5G networks and not subscription privacy.

VII. Conclusion and Recommendations

Along with the pursuit of a connected future, at least an equivalent – if not greater – focus is required on the security and privacy of these connections. 5G is a platform which will transform everything from education to AI to medicine. But 5G also comes with potentially enormous privacy risks. Due to increasing diversity of devices and emergence of new services, it is necessary for a successful 5G future that these privacy risks be resolved sooner rather than later. As a result of the study undertaken in this paper, several privacy vulnerabilities that remain unresolved in 5G Release 15 are highlighted. This study concludes that new and more rigorous privacy protection mechanisms are required to guarantee robust subscription privacy in 5G. As the next evolutionary step in wireless communication is being taken, 3GPP has the perfect opportunity to embrace a holistic approach to subscribers' privacy. In particular, based upon this study, we suggest that the following avenues should be further explored:

- As 3GPP strive towards a quantum-proof future by supporting 256-bit algorithms [83], it is of utmost importance that the current subscriber identification protection mechanism (being the only public-key-based mechanism in 5G) be replaced with an alternative symmetric proposal, such as that of [60].
- Additionally, it would be desirable that any such proposal be strengthened further against downgrade attacks, such as by integrating the solution of [61].
- For resolution of the AKA protocol linkability and other new privacy attacks on 5G, the fix depicted in Figure 10c could be adopted for 5G-AKA's failure messages.
- Although the attack margin within the *GUTI Reallocation Replay* attack (Section III-G) is already a very narrow one with other new 5G privacy protection measures (such as the false-base-station-detection framework) reducing its efficacy further, it remains desirable to patch it completely.
- Based upon past experience of non-adoption of informative-only parts of published standards, the false-base-station-detection framework of 5G Release 15 should be transformed into a normative one.

References

[1] G. Greenwald, "NSA collecting phone records of millions of Verizon customers daily," https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, Jun 2013, [Online; accessed 23-September-2019].

[2] E. Union, "Regulation (EU) 2016/679 (General Data Protection Regulation)," https://gdpr-info.eu/, May 2016.

[3] 3rd Generation Partnership Project, "Security Architecture and Procedures for 5G Systems (3GPP TS 33.501 Version 15.0.0 Release 15)," Mar 2018.

[4] ——, "3G Security; Security Architecture (3GPP TS 33.102 Version 15.0.0 Release 15)," Jun 2018.

[5] D. A. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A Formal Analysis of 5G Authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, D. Lie, M. Mannan, M. Backes, and X. Wang, Eds. ACM, 2018, pp. 1383–1396.

[6] 3rd Generation Partnership Project, "Study on the security aspects of the next generation system (3GPP TR 33.899 Version 1.3.0 Release 14)," Aug 2017.

[7] N. Husted and S. Myers, "Mobile Location Tracking in Metro Areas: Malnets and Others," in *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010*, E. Al-Shaer, A. D. Keromytis, and V. Shmatikov, Eds. ACM, 2010, pp. 85–96.

[8] M. Jakobsson and S. Wetzel, "Security Weaknesses in Bluetooth," in *Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings*, ser. Lecture Notes in Computer Science, D. Naccache, Ed., vol. 2020. Springer, 2001, pp. 176–191.

[9] 3rd Generation Partnership Project, "System Architecture for the 5G System (3GPP TS 23.501 Version 15.1.0 Release 15)," Mar 2018.

[10] ——, "Mobile Application Part (MAP)Specification (3GPP TS 29.002 Version 15.3.0 Release 15)," Mar 2018.

[11] R. F. Olimid and S. F. Mjølsnes, "On Low-Cost Privacy Exposure Attacks in LTE Mobile Communication," *Proceedings of the Romanian Academy Series A-Mathematics Physics Technical Sciences Information Science*, vol. 18, pp. 361–370, 2017.

[12] 3rd Generation Partnership Project, "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)(3GPP TS 33.220 Version 15.2.0 Release 15)," June 2018.

[13] C. Paget, "Practical Cellphone Spying," *Def Con*, vol. 18, 2010.

[14] S. F. Mjølsnes and R. F. Olimid, "Easy 4G/LTE IMSI Catchers for Non-Programmers," in *Computer Network Security - 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings*, ser. Lecture Notes in Computer Science, J. Rak, J. Bay, I. V. Kotenko, L. J. Popyack, V. A. Skormin, and K. Szczypiorski, Eds., vol. 10446. Springer, 2017, pp. 235–246.

[15] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. R. Weippl, "IMSI-catch me if you can: IMSI-catcher-catchers," in *Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC 2014, New Orleans, LA, USA, December 8-12, 2014*, C. N. P. Jr., A. Hahn, K. R. B. Butler, and M. Sherr, Eds. ACM, 2014, pp. 246–255.

[16] A. Dabrowski, G. Petzl, and E. R. Weippl, "The Messenger Shoots Back: Network Operator Based IMSI Catcher Detection," in *Research in Attacks, Intrusions, and Defenses - 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings*, ser. Lecture Notes in Computer Science, F. Monrose, M. Dacier, G. Blanc, and J. García-Alfaro, Eds., vol. 9854. Springer, 2016, pp. 279–302.

[17] K. Nohl, "Mobile Self-defense," in *31st Chaos Communication Congress 31C3*, 2014.

[18] A. Lilly, "IMSI catchers: hacking mobile communications," *Network Security*, vol. 2017, no. 2, pp. 5–7, 2017.

[19] D. Fox, "Der imsi-catcher," *Datenschutz und Datensicherheit*, vol. 26, no. 4, 2002.

[20] N. J. Croft, "On forensics: A silent SMS attack," in *2012 Information Security for South Africa, Balalaika Hotel, Sandton, Johannesburg, South Africa, August 15-17, 2012*, H. S. Venter, M. Loock, and M. Coetzee, Eds. IEEE, 2012, pp. 1–4.

[21] M. Arapinis, L. I. Mancini, E. Ritter, and M. D. Ryan, "Analysis of Privacy in Mobile Telephony Systems," *Int. J. Inf. Sec.*, vol. 16, no. 5, pp. 491–523, 2017.

[22] A. Shaik, J. Seifert, R. Borgaonkar, N. Asokan, and V. Niemi, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," in *23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016*. The Internet Society, 2016.

[23] D. Kune, J. Koelndorfer, N. Hopper, and Y. Kim, "Location Leaks on the GSM Air Interface," in *19th Annual Network & Distributed System Security Symposium, ISOC-NDSS*, 2012.

[24] K. Nohl and S. Munaut, "Wideband GSM Sniffing," in *27th Chaos Communication Conference*, 2010.

[25] B. Hong, S. Bae, and Y. Kim, "GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier," in *25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018*. The Internet Society, 2018.

[26] R. P. Jover, "LTE security, protocol exploits and location tracking experimentation with low-cost software radio," *CoRR*, vol. abs/1607.05171, 2016.

[27] M. Arapinis, L. I. Mancini, E. Ritter, and M. Ryan, "Privacy through Pseudonymity in Mobile Telephony Systems," in *21st Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014*. The Internet Society, 2014.

[28] D. Forsberg, L. Huang, T. Kashima, and S. Alanärä, "Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface," in *Proceedings of the IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2007, 3-7 September 2007, Athens, Greece*. IEEE, 2007, pp. 1–5.

[29] M. Arapinis, L. I. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar, "New Privacy Issues in Mobile Telephony: Fix and Verification," in *the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012*, T. Yu, G. Danezis, and V. D. Gligor, Eds. ACM, 2012, pp. 205–216.

[30] C. Sørseth, S. X. Zhou, S. F. Mjølsnes, and R. F. Olimid, "Experimental Analysis of Subscribers' Privacy Exposure by LTE Paging," *Wireless Personal Communications*, pp. 1–19, 2018.

[31] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information," in *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society, 2019.

[32] R. Borgaonkar, L. Hirshi, S. Park, A. Shaik, A. Martin, and J.-P. Seifert, "New Adventures in Spying 3G & 4G Users: Locate, Track, Monitor," in *Blackhat, Las Vegas, USA 2017*, July 2017.

[33] 3rd Generation Partnership Project, "3GPP System Architecture Evolution (SAE); Security architecture 3GPP TS 33.401 Version 15.8.0 (Release 15)," June 2019.

[34] ——, "Technical Specification Group Services and System Aspects; International Mobile station Equipment Identities (IMEI) (3GPP TS 22.016 Version 8.0.0 Release 08)," Dec 2008.

[35] O. H. Abdelrahman and E. Gelenbe, "Signalling Storms in 3G Mobile Networks," in *IEEE International Conference on Communications, ICC 2014, Sydney, Australia, June 10-14, 2014*. IEEE, 2014, pp. 1017–1022.

[36] 3rd Generation Partnership Project, "Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 16) (3GPP TS 24.301 Version 16.2.0 Release 16)," Sep 2019.

[37] ——, "Radio Resource Control (RRC); Protocol specification (3GPP TS 25.331 Version 15.4.0 Release 15)," Sep 2018.

[38] ——, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (3GPP TS 36.331 Version 15.6.0 Release 15)," Jun 2019.

[39] J. J. Caffery and G. L. Stuber, "Overview of radiolocation in CDMA cellular systems," *IEEE Communications Magazine*, vol. 36, no. 4, pp. 38–45, 1998.

[40] A. Kunz and X. Zhang, "New 3GPP Security Features in 5G Phase 1," in *2018 IEEE Conference on Standards for Communications and Networking, CSCN 2018, Paris, France, October 29-31, 2018*. IEEE, 2018, pp. 1–6.

[41] A. R. Prasad, S. Arumugam, B. Sheeba, and A. Zugenmaier, "3GPP 5G Security," *Journal of ICT Standardization*, vol. 6, no. 1, pp. 137–158, 2018.

[42] 3rd Generation Partnership Project, "NG-RAN; NG Application Protocol (NGAP)(3GPP TS 38.413 Version 15.3.0 Release 15)," Mar 2019.

[43] ——, "NR; User Equipment (UE) procedures in Idle mode and RRC Inactive state (3GPP TS 38.304 Version 15.5.0 Release 15)," Sep 2019.

[44] ——, "NR;Radio Resource Control (RRC) protocol specification (3GPP TS 38.331 Version 15.6.0 Release 15)," Jun 2019.

[45] V. Shoup, "A proposal for an ISO standard for public key encryption," *IACR Cryptology ePrint Archive*, vol. 2001, p. 112, 2001.

[46] D. Hankerson and A. Menezes, "Elliptic Curve Cryptography," in *Encyclopedia of Cryptography and Security, 2nd Ed.*, H. C. A. van Tilborg and S. Jajodia, Eds. Springer, 2011, p. 397.

[47] SECG SEC 1, "Recommended Elliptic Curve Cryptography, Version 2.0," http://www.secg.org/sec1-v2.pdf, 2009.

[48] SECG SEC 2, "Recommended Elliptic Curve Domain Parameters, Version 2.0," http://www.secg.org/sec2-v2.pdf, 2010.

[49] M. Khan, K. Järvinen, P. Ginzboorg, and V. Niemi, "On De-synchronization of User Pseudonyms in Mobile Networks," in *Information Systems Security - 13th International Conference, ICISS 2017, Mumbai, India, December 16-20, 2017, Proceedings*, ser. Lecture Notes in Computer Science, R. K. Shyamasundar, V. Singh, and J. Vaidya, Eds., vol. 10717. Springer, 2017, pp. 347–366.

[50] M. Lee, N. P. Smart, B. Warinschi, and G. J. Watson, "Anonymity guarantees of the UMTS/LTE authentication and connection protocol," *Int. J. Inf. Sec.*, vol. 13, no. 6, pp. 513–527, 2014.
[51] R. P. Jover and V. Marojevic, "Security and Protocol Exploit Analysis of the 5G Specifications," *IEEE Access*, vol. 7, pp. 24 956–24 963, 2019.
[52] B. Blanchet, "Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif," in *Foundations of Security Analysis and Design VII - FOSAD 2012/2013 Tutorial Lectures*, ser. Lecture Notes in Computer Science, A. Aldini, J. López, and F. Martinelli, Eds., vol. 8604. Springer, 2013, pp. 54–87.
[53] P. Fouque, C. Onete, and B. Richard, "Achieving Better Privacy for the 3GPP AKA Protocol," *PoPETs*, vol. 2016, no. 4, pp. 255–275, 2016.
[54] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, "New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols," *PoPETs*, vol. 2019, no. 3, pp. 108–127, 2019.
[55] H. Khan and K. M. Martin, "On the Efficacy of New Privacy Attacks against 5G AKA," in *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, ICETE 2019 - Volume 2: SECRYPT, Prague, Czech Republic, July 26-28, 2019.*, M. S. Obaidat and P. Samarati, Eds. SciTePress, 2019, pp. 431–438.
[56] ETSI-SAGE, "First response on ECIES for concealing IMSI or SUPI," https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionId=832160, Oct 2017.
[57] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*. IEEE Computer Society, 1994, pp. 124–134.
[58] X. Hu, C. Liu, S. Liu, W. You, Y. Li, and Y. Zhao, "A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security," *IEEE Access*, vol. 7, pp. 125 424–125 441, 2019.
[59] S. F. Mjølsnes and R. F. Olimid, "Private Identification of Subscribers in Mobile Networks: Status and Challenges," *IEEE Communications Magazine*, vol. 57, no. 9, pp. 138–144, 2019.
[60] H. Khan, B. Dowling, and K. M. Martin, "Identity Confidentiality in 5G Mobile Telephony Systems," in *Security Standardisation Research - 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings*, ser. Lecture Notes in Computer Science, C. Cremers and A. Lehmann, Eds., vol. 11322. Springer, 2018, pp. 120–142.
[61] M. Khan, P. Ginzboorg, K. Järvinen, and V. Niemi, "Defeating the Downgrade Attack on Identity Privacy in 5G," in *Security Standardisation Research - 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings*, ser. Lecture Notes in Computer Science, C. Cremers and A. Lehmann, Eds., vol. 11322. Springer, 2018, pp. 95–119.
[62] Vodafone, "Discussion paper on embedded routing information in SUCI," https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_90Bis_SanDiego/docs/S3-180761.zip, Mar 2019.
[63] ——, "pCR to 33.501 - addition of routing information into SUCI," https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis_SanDiego/Docs/S3-180763.zip, Mar 2019.
[64] M. Khan, V. Niemi, and P. Ginzboorg, "IMSI-based Routing and Identity Privacy in 5G," in *Proceedings of the 22nd Conference of Open Innovations Association FRUCT, Jyvaskyla, Finland*, 2018.
[65] CATT, "Solution for SUPI privacy and LI requirement," https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis_SanDiego/Docs/S3-180591.zip, Mar 2019.
[66] KPN, N. DOCOMO, DT, BT, and NEC, "Proposal and Discussion for Privacy and LI Solution," https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis_SanDiego/Docs/S3-180684.zip, Mar 2019.
[67] Nokia, "Discussion on LI conformity by verification hash method," https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis_SanDiego/Docs/S3-180768.zip, Mar 2019.
[68] Nokia, Gemalto, and IDEMIA, "SUCI and LI âĂŞ verification hash integrated in 5G AKA," https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis_SanDiego/Docs/S3-180769.zip, Mar 2019.
[69] Ericsson, Q. Incorporated, Samsung, Huawei, Hisilicon, and Intel, "SUCI and LI - verification hash integrated in 5G AKA," https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis_SanDiego/Docs/S3-180818.zip, Mar 2019.
[70] M. Khan and V. Niemi, "Concealing IMSI in 5G Network Using Identity Based Encryption," in *Network and System Security - 11th International Conference, NSS 2017, Helsinki, Finland, August 21-23, 2017, Proceedings*, ser. Lecture Notes in Computer Science, Z. Yan, R. Molva, W. Mazurczyk, and R. Kantola, Eds., vol. 10394. Springer, 2017, pp. 544–554.
[71] D. Rupprecht, A. Dabrowski, T. Holz, E. R. Weippl, and C. Pöpper, "On security research towards future mobile network generations," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 3, pp. 2518–2542, 2018.
[72] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, Privacy, and Access Control in Information-Centric Networking: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 1, pp. 566–600, 2018.
[73] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. V. Gurtov, "5G security: Analysis of threats and solutions," in *IEEE Conference on Standards for Communications and Networking, CSCN 2017, Helsinki, Finland, September 18-20, 2017*. IEEE, 2017, pp. 193–199.
[74] ——, "Overview of 5G Security Challenges and Solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.
[75] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions," *IEEE Communications Surveys & Tutorials*, 2019.
[76] R. P. Jover, "The current state of affairs in 5G security and the main remaining security challenges," *CoRR*, vol. abs/1904.08394, 2019.
[77] M. A. Ferrag, L. A. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Network and Computer Applications*, vol. 101, pp. 55–82, 2018.
[78] P. Gandotra and R. K. Jha, "A survey on green communication and security challenges in 5G wireless communication networks," *J. Network and Computer Applications*, vol. 96, pp. 39–61, 2017.
[79] A. K. Rangisetti and B. R. Tamma, "Software Defined Wireless Networks: A Survey of Issues and Solutions," *Wireless Personal Communications*, vol. 97, no. 4, pp. 6019–6053, 2017.
[80] G. Choudhary and V. Sharma, "A Survey on the Security and the Evolution of Osmotic and Catalytic Computing for 5G Networks," *CoRR*, vol. abs/1909.08844, 2019.
[81] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Study on 5G Security Enhancement against False Base Stations Version 0.6.0 (Release 16)," Aug 2019.
[82] R. Ravindran, A. Chakraborti, S. O. Amin, A. Azgin, and G. Wang, "5G-ICN: Delivering ICN Services over 5G Using Network Slicing," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 101–107, 2017.
[83] 3rd Generation Partnership Project, "Study on the support of 256-bit algorithms for 5G (3GPP TR 33.841 Version 16.1.0 Release 16)," Mar 2019.
[84] C. Cremers and A. Lehmann, Eds., *Security Standardisation Research - 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings*, ser. Lecture Notes in Computer Science, vol. 11322. Springer, 2018.

APPENDIX A
3GPP "KEY ISSUES"

Key Issue is the terminology used in 3GPP studies for a potential security or privacy problem related to the topic. It usually contains a description of the problem, associated threats, and corresponding requirements to mitigate the threats. *Key Issues* by themselves do not mean that problems are substantial, neither do they mean that the threats are feasible. Similarly, the requirements proposed for each *Key Issue* do not imply that they apply to any technical specification. What *Key Issues* provide is an opportunity for interested 3GPP members to investigate and further explore a particular security or privacy aspect.

APPENDIX B
NETWORK SLICING IN 5G

Network slicing is a form of virtual network architecture using the same principles behind Software Defined Networking

(SDN) and Network Functions Virtualisation (NFV) in fixed networks. SDN and NFV deliver greater network flexibility by allowing traditional network architectures to be partitioned into virtual elements that can be linked through software. Network slicing allows multiple virtual networks to be created on top of a common shared physical infrastructure. The virtual networks are then customized to meet the specific needs of applications, services, devices, customers or operators.

In the case of 5G, a single physical network is sliced into multiple virtual networks that can support different Radio Access Networks (RANs), or different service types running across a single RAN. Network slicing plays a critical role in 5G networks because of the multitude of use cases and new services that 5G supports. These new use cases and services place different requirements on the network in terms of functionality, and their performance requirements vary enormously. Network slicing maximises the flexibility of 5G networks, optimizing both the utilization of the infrastructure and the allocation of resources, which enables greater energy and cost efficiencies compared to earlier mobile networks.