The Security of the 5G AKA Protocol: A Review

Shiting Long
shiting.long@ut.ee
Supervisor: Vitaly Skachek

December 20, 2019

Abstract

The 5G technology promises to largely enhance the speed, coverage and reliability of the wireless network. However, the security of 5G should be highlighted as well because 5G serves as a united platform that supports significantly more end devices than the previous generations, which leads to a remarkably high level of uncertainty in malicious behaviour prevention. This review aims at outlining the Authentication and Key Arrangement (AKA) protocol in 5G and analyzing its vulnerabilities. We present a comprehensive description of the 5G AKA protocol and summarize the discovered vulnerabilities in this protocol with corresponding countermeasures.

1 Introduction

While the ICT industry is walking into another decade, the fifth generation cellular network technology (5G) has been drawing a global scale of attention and enthusiasm. The generation in the terminology is defined by the speed of data transmission and the change of speed between generations may lead to tremendous market change. 1G stimulated the evolution of mobile phones, 2G digitalized the phone calls and enabled text messages, 3G empowered mobile phones as platforms of multimedia, and 4G provided high-speed internet access in cities. However, the annual visual network index released by Cisco [1] shows that the demand for more mobile-connected devices and faster connection speed has been growing rapidly. Such demand might not be simply satisfied by an incremental approach based on 4G. Thus, it motivates people to wonder what could be expected in the next generation.

The major 5G technologies include ultra-densification, mmWave (millimeter wave), and massive multiple-input multiple-output (MIMO) [2]. Ultra-densification means that the network distributed over land areas are a lot smaller than before, which efficiently increases the network capacity. Since terrestrial wireless communication systems usually require a certain slim range of microwave frequencies, such spectral band is saturated. On the contrary, mmWave spectrum lies idle and thus 5G can utilize it. Shortening the wavelength implies shortening the antennas, which makes it possible for devices to carry more antennas. The MIMO technology is therefore in need to control the signals processed by a massive amount of antennas.

With the development of 5G, new standards of performance regarding connectivity, throughput, latency are naturally required, but the capability to ensure security and privacy of the users should be addressed as well [3]. Security guarantees for user and device identities, network interfaces, platforms, etc., are all included in the scope of 5G security. This paper mainly discusses the security of mutual authentication and key arrangement in 5G, namely the 5G Authentication and Key Arrangement (AKA) protocol, which is provided by the 3rd Generation Partnership Project (3GPP) group.

The most important security mechanisms relating to communications are mutually authenticating the parties participating in the communication and establishing a secure channel to protect the ongoing communication. In 5G communications, we can simplify the parties in the communication as subscribers and their service providers. The 5G AKA protocol should be able to provide such security mechanisms under an adversarial environment.

Reviews of 5G security have traditionally focused on the architectural vulnerabilities in the 5G system [4, 5]. However, the protocol level of the 5G system requires considerations as well because it provides intrinsic security assumptions for the system. Researchers have analysed and shown different vulnerabilities in the 5G AKA protocol [6–8], but have not reviewed the protocol from the point of view of a reader unfamiliar with the protocol. In this report, we illustrate the 5G AKA protocol and summarize its discovered vulnerabilities to offer a basic understanding of the protocol to the general readers.

The outline of this paper is organized as follows. We present the specifications of the 5G AKA protocol in Section 2. The vulnerabilities and the corresponding countermeasures of the protocol are introduced in Section 3. We draw a conclusion in Section 4.

2 The 5G AKA Protocol

This and the following section are based on the research of D. Basin et al. [6]. Hence, the 5G AKA protocol in the specification `3GPP TS 33.501` [9] is analysed in this paper in accordance with [6].

2.1 Entities in the Cellular Network Architecture

The three main entities in the cellular network architecture (See Figure 1) are User Equipment (UE), Home Network (HN) and Serving Network (SN). UEs are the devices containing Universal Subscriber Identity Module (USIM), including mobile phones and IoT devices, which serve as subscribers. HNs are the carriers of the subscribers containing databases of their UEs. SNs are the entities that UEs may connect to and they provide services to the authenticated UEs.

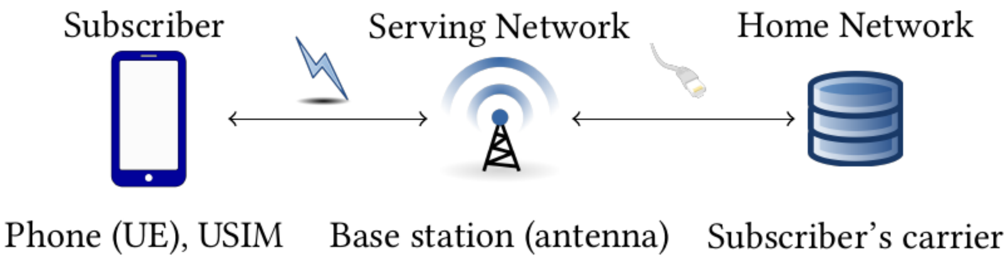


Figure 1: **The Communications among the Three Entities.** The UE communicates with the SN via a wireless network (insecure) and the SN communicates with the HN via a wired network (secure). [6]

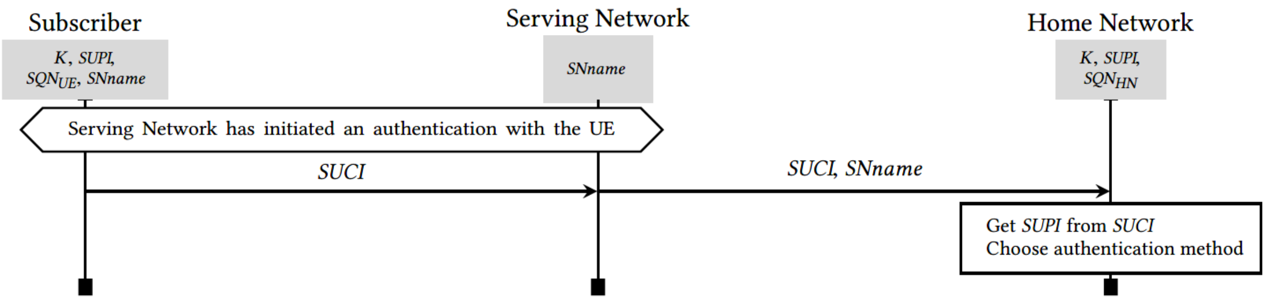


Figure 2: **The Initial Procedure of the 5G AKA Protocol [6].**

2.2 Protocol Specifications

2.2.1 Security Primitives

(i) Each UE in the 5G system has a 5G Subscription Permanent Identifier ($SUPI$), which serves as an authenticated id for the UE [10]. Note that the $SUPI$ contains the address of the HN, denoted as $idHN$ in [6].

(ii) A server name ($SNname$), which concatenates a service code and the SN id, is used in the derivation of the key seed for establishing the secure channel between the UE and the SN [9].

(iii) A long-term secret symmetric key K is shared between a UE and its corresponding HN.

(iv) A public key of an HN ($pkHN$).

(v) A counter (SQN) stored in both the UE (SQN_{UE}) and its HN (SQN_{HN}).

2.2.2 Initiation Procedure

Before an actual authentication process happens (when a SN is triggered by a UE, see Figure 2), the UE needs to compute a Subscription Concealed Identifier ($SUCI$), where $SUCI = \langle aenc(\langle SUPI, R_s \rangle, pkHN), idHN \rangle$. Here $aenc$ denotes asymmetric encryption and R_s denotes some random nonce. The UE sends the $SUCI$ to the SN, then the SN sends $SUCI$ and $SNname$ to the HN that the UE specified in the $SUCI$. Finally, the HN can choose an authentication method to authenticate the UE.

2.2.3 Authentication Procedure

The authentication procedure mainly consists of two phases: a challenge-response and an optional re-synchronization procedure [6]. The former does the regular authentication procedure and the latter

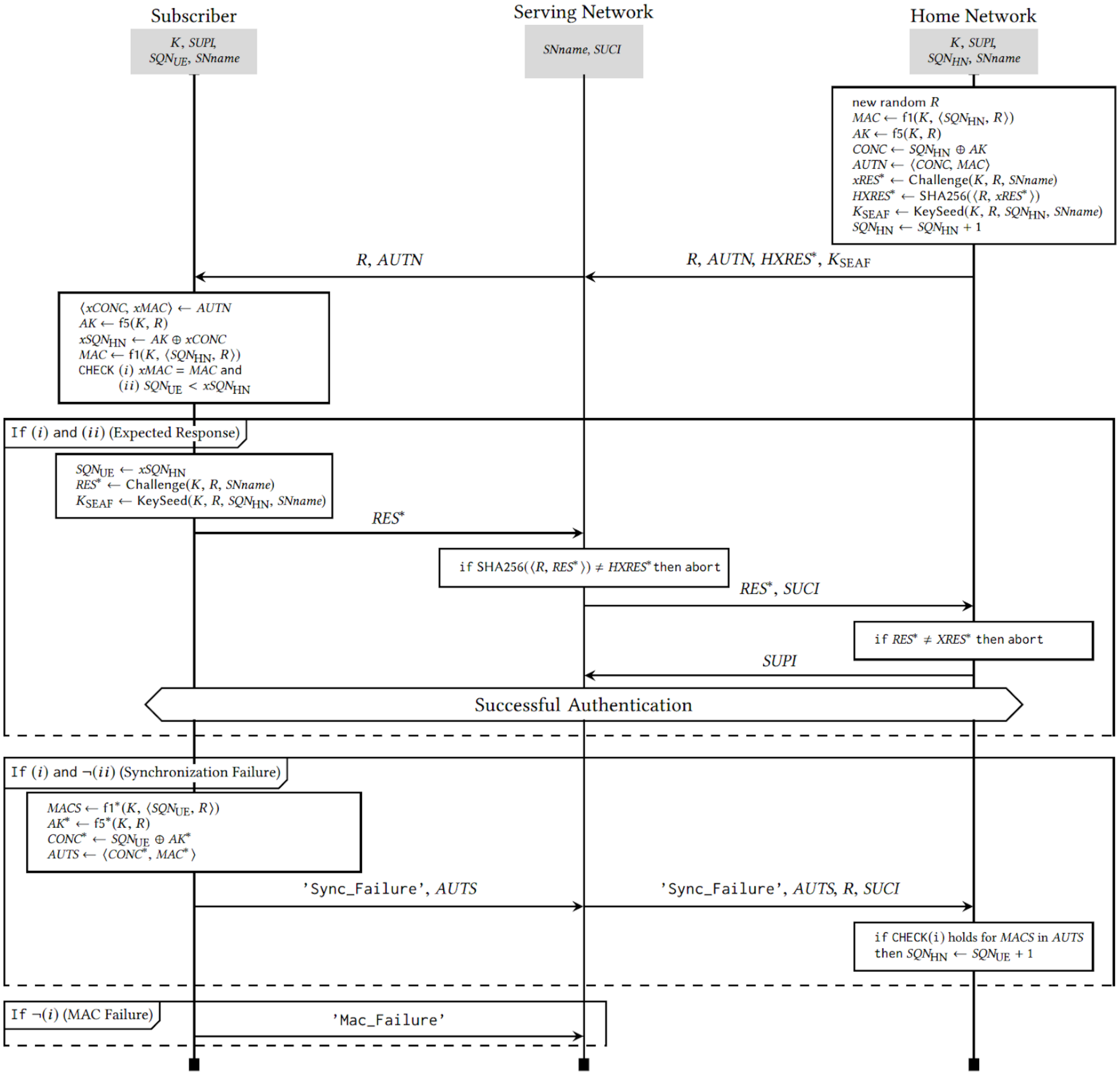

Subscriber
K, $SUPI$, SQN_{UE}, $SName$
Serving Network
$SName$, $SUCI$
Home Network
K, $SUPI$, SQN_{HN}, $SName$
new random R
$MAC \leftarrow$ f1(K, $\langle SQN_{HN}, R\rangle$)
$AK \leftarrow$ f5(K, R)
$CONC \leftarrow SQN_{HN} \oplus AK$
$AUTN \leftarrow \langle CONC, MAC\rangle$
$xRES^* \leftarrow$ Challenge(K, R, $SName$)
$HXRES^* \leftarrow$ SHA256($\langle R, xRES^*\rangle$)
$K_{SEAF} \leftarrow$ KeySeed(K, R, SQN_{HN}, $SName$)
$SQN_{HN} \leftarrow SQN_{HN} + 1$
R, $AUTN$
R, $AUTN$, $HXRES^*$, K_{SEAF}
$\langle xCONC, xMAC\rangle \leftarrow AUTN$
$AK \leftarrow$ f5(K, R)
$xSQN_{HN} \leftarrow AK \oplus xCONC$
$MAC \leftarrow$ f1(K, $\langle SQN_{HN}, R\rangle$)
CHECK (i) $xMAC = MAC$ and
(ii) $SQN_{UE} < xSQN_{HN}$
If (i) and (ii) (Expected Response)
$SQN_{UE} \leftarrow xSQN_{HN}$
$RES^* \leftarrow$ Challenge(K, R, $SName$)
$K_{SEAF} \leftarrow$ KeySeed(K, R, SQN_{HN}, $SName$)
RES^*
if SHA256($\langle R, RES^*\rangle$) $\neq HXRES^*$ then abort
RES^*, $SUCI$
if $RES^* \neq XRES^*$ then abort
$SUPI$
Successful Authentication
If (i) and $\neg$(ii) (Synchronization Failure)
$MACS \leftarrow$ f1*(K, $\langle SQN_{UE}, R\rangle$)
$AK^* \leftarrow$ f5*(K, R)
$CONC^* \leftarrow SQN_{UE} \oplus AK^*$
$AUTS \leftarrow \langle CONC^*, MAC^*\rangle$
'Sync_Failure', $AUTS$
'Sync_Failure', $AUTS$, R, $SUCI$
if CHECK(i) holds for $MACS$ in $AUTS$
then $SQN_{HN} \leftarrow SQN_{UE} + 1$
If $\neg$(i) (MAC Failure)
'Mac_Failure'

Figure 3: **The 5G AKA Protocol Continuing Figure 2.** The functions $f1$, $f1^*$ are message authentication functions, and $f5$, $f5^*$ are key derivation functions. The functions *Challenge*() and *KeySeed*() are complex key derivation functions. Note that the functions described above are all unrelated one-way keyed functions. The UE does two checks which lead to different branches: MAC check and *SQN* check. [6]

prevents out-of-sync problems that might be caused by the *SQN*s in the UE and its HN (See Figure 3).

In the challenge-response phase, the system continues the initiation procedure. The HN then computes the following values:

- A random nonce R (the challenge),
- $AUTN$ (a Message Authentication Code (MAC) which contains SQN_{HN} and R, following by a mask of SQN_{HN}),
- $HXRES^*$ (hash of the expected response),
- K_{SEAF} (the key seed for establishing the secure channel between the UE and the SN),

The HN updates its SQN_{HN} and then sends the above values to the SN. The SN sends R and $AUTN$ to UE. The UE needs to compute a response RES^* and send it back to the SN. Here the UE computes K_{SEAF} and updates SQN_{UE} as well. The SN can verify the response by computing the hash given RES^* and compare it with $HXRES^*$. If the two values are equivalent, the SN will send RES^* and $SUCI$ to the HN. Then the HN verifies RES^* again, and a successful authentication is established if RES^* is expected.

The re-synchronization phase is triggered if the UE retrieves an SQN_{HN} that is not equal to the SQN_{UE}. The UE then sends an error message together with an $AUTS$ (a MAC which contains SQN_{UE} and R, following by a mask of SQN_{UE}) message to the SN. The SN needs to send these messages instead of the expected RES^* to the HN. Since the HN can authenticate the UE by $AUTS$ as well, it verifies the UE's identity and updates SQN_{HN} if the UE is authenticated.

3 Vulnerabilities of the 5G AKA Protocol

In this section, we define security requirements for the 5G AKA protocol first and then show the results of a security analysis of the 5G AKA protocol given in [6] as well as a newly discovered threat on 5G AKA protocol [8]. The proposed countermeasures to the vulnerabilities are illustrated in the end.

3.1 Security Requirements

3.1.1 Authentication

Here we use Lowe's taxonomy and its relationship with formal definitions of authenticity (See Appendix C in [6]) to define the authentication requiements in 5G AKA protocol, and we use agents A and B to illustrate two parties in an authentication process.

(i) A UE must obtain non-injective agreement on $SNname$ with its HN after key (K_{SEAF}) confirmation. Note that A has a non-injective agreement with B means that A and B both agree on a set of data when the protocol is completed.

(ii) An SN must obtain weak agreement with a UE that initiated the authentication, and vice versa. Note that A has a weak agreement with B means that A knows that B has run the protocol.

(iii) An SN must obtain non-injective agreement with its corresponding HN on $SUPI$.

3.1.2 Confidentiality

(i) The key seed K_{SEAF} in a session should be unique, and it should remain confidential even if the attacker obtains other K_{SEAF} used in other sessions.

(ii) The long-term secrets K, $SUPI$ and *skHN* (secret key of HN) should not be compromised.

3.1.3 Privacy

The 5G AKA protocol should provide untraceablity of the UEs under passive attacks, i.e., where the attacker only eavesdrops on the radio link [6]. It implies that the $SUPI$ and SQN of a UE should remain secret, otherwise the identity or the activeness of the UE might be exposed.

3.2 Security Analysis Results

3.2.1 Authentication

The UE's weak agreement with its SN is violated [6]. This is due to the fact that K_{SEAF} and a corresponding $SUPI$ (identifies the UE) that the SN receives are not bonded, because it receives K_{SEAF} prior to $SUPI$. If a pair of SN and HN are running concurrently, the $SUPI$ that SN receives at the end might not correspond to the correct K_{SEAF}. The identities of the UEs are protected, but an attacker can still trick the HN to bill wrong UEs.

An attack against the protocol that exploits the above flaw is thoroughly introduced in [11]. The attacker can eavesdrop the *SUCI* (denote as *SUCI-A* in [11]) from an honest UE, which is an encrypted *SUPI* and contains the address of the corresponding HN. The attacker can then purchase a legitimate USIM that has *SUCI-B* from the same HN and physically extract the secret key K_B. After obtaining the critical primitives, the attacker can initiate two sessions (one for *SUCI-A* and another for *SUCI-B*) with the SN at the same time. As we know, the SN might be confused with the two identities and then link the K_{SEAF} for *SUCI-A* to *SUCI-B*. Since the attacker already learns K_B, he can compute the K_{SEAF} for *SUCI-B* but the SN might treat it as the K_{SEAF} for *SUCI-A*. Therefore, an impersonation attack is completed.

The 5G standard only requires implicit authentication for the UEs, meaning that from a UE's point of view, the authentication of the SN is provided by successfully using its keys. However, the 5G standard does not specify whether the UE should proceed without confirming the key (K_{SEAF}). Therefore, in a scenario that the UE sends sensitive information, an attacker can impersonate the SN because the key may not be needed.

3.2.2 Privacy

The results of [6] show that the 5G AKA protocol is secure with respect to privacy under passive attacks. Although the protocol satisfies the security requirement in Section 3.1.3, it is not safe under active attacks, which are more common in the real world. Similar to the attack introduced in [12], an attacker can track UEs by observing one session and replays the SN's response to another UE, because the answer sent by the UE (MAC failure or Synchronization failure) are distinguishable. The attacker can identify any UE that is not the UE in the observed session because it will return MAC failure, whereas the target UE will return Synchronization failure. This vulnerability is inherited from the 4G AKA protocol as the 5G AKA protocol uses some core functions of its previous version.

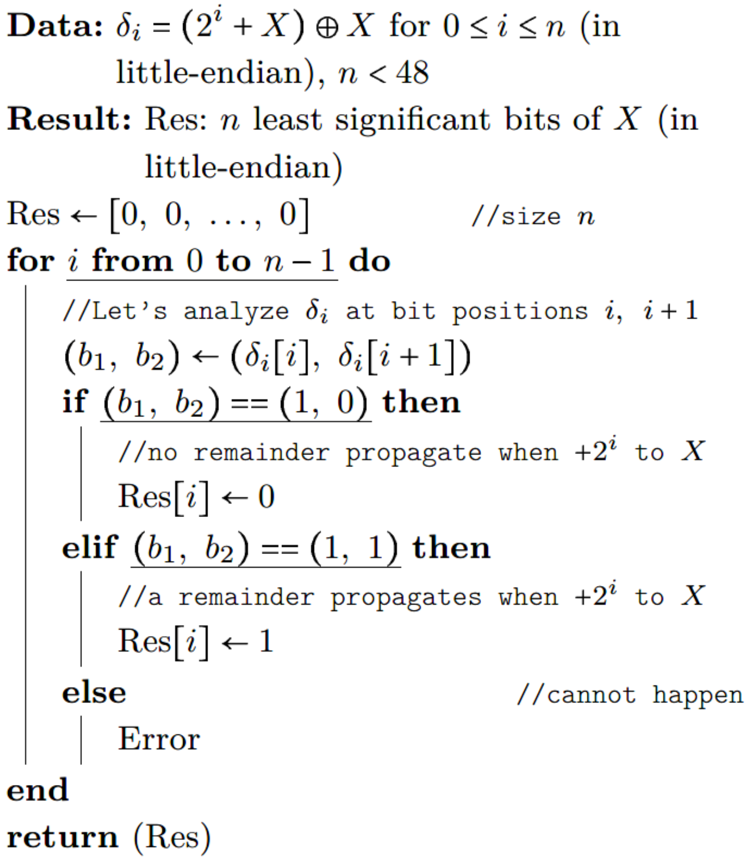
The privacy of the *SQN* is violated due to a logical vulnerability in *AUTS* [8], which is a parameter for the re-synchronization process (see Figure 3). More specifically, given the concealed sequence number $CONC^* = SQN_{UE} \oplus AK^*$ and $AK^* = \mathrm{f5}^*(K,R)$, we know that if the UE is provided challenge $(R,AUTN)$ two times that both leads to synchronization failure, there is $AK_1^* = AK_2^*$. Therefore, we obtain:

$$CONC_1^* \oplus CONC_2^* = (SQN_{UE}^1 \oplus AK_1^*) \oplus (SQN_{UE}^2 \oplus AK_2^*) = SQN_{UE}^1 \oplus SQN_{UE}^2. \tag{1}$$

The attack exploiting this vulnerability is described as follows. Consider an attacker that has fetched $2^n + 1$ consecutive challenges for a targeted UE. The attacker sends the first challenge $(R_0, AUTN_0)$ to the target. At this point the UE should accept this challenge as it passes both MAC and *SQN* check. Then the attacker immediately sends challenge $(R_0, AUTN_0)$ again to the target and gets a synchronization failure, i.e., $CONC_0^* = SQN_{HN}^0 + 1 \oplus AK_0^*$. The attacker needs to inject some $(R_{2^j}, AUTN_{2^j})$ that is accepted by the UE in order to update SQN_{UE} to $SQN_{UE}^0 + 2^j + 1$. Assume the attacker does this step n times. For any $0 \leq j \leq n$, we have:

$$CONC_1^* \oplus CONC_2^* = SQN_{HN}^0 + 1 \oplus SQN_{UE}^0 + 2^j + 1. \tag{2}$$

Therefore, by using an inference algorithm shown in Figure 4, the attacker can learn the n least significant bits of SQN_{HN}. Note that the algorithm runs offline with the data collected by previously



```
Data: $\delta_i = (2^i + X) \oplus X$ for $0 \leq i \leq n$ (in
      little-endian), $n < 48$
Result: Res: $n$ least significant bits of $X$ (in
        little-endian)
Res $\leftarrow [0,\ 0,\ \ldots,\ 0]$                //size $n$
for $i$ from $0$ to $n-1$ do
    //Let's analyze $\delta_i$ at bit positions $i$, $i+1$
    $(b_1,\ b_2) \leftarrow (\delta_i[i],\ \delta_i[i+1])$
    if $(b_1,\ b_2) == (1,\ 0)$ then
        //no remainder propagate when $+2^i$ to $X$
        Res$[i] \leftarrow 0$
    elif $(b_1,\ b_2) == (1,\ 1)$ then
        //a remainder propagates when $+2^i$ to $X$
        Res$[i] \leftarrow 1$
    else                                      //cannot happen
        Error
end
return (Res)
```

Figure 4: **The inference algorithm for calculating the *n* least significant bits of *SQN* [8].**

described active attacks, which makes it more powerful as it runs independently on the established connections.

3.3 Countermeasures

3.3.1 Authentication

There are mainly two suggested fixes for the weak agreement between the SN and the UE [11]. The explicit fix is to bind the identity of the UE, i.e., *SUPI* to the K_{SEAF}, which means adding the *SUCI* in the challenge message that the HN sends to the SN. Since the challenge message contains K_{SEAF} and *SUCI* conceals *SUPI*, the bond between *SUPI* and K_{SEAF} is created. The implicit fix is to bind the sessions within the HN, i.e., the session that the HN initiates an authentication information check after it receives request from the SN with its credential storage. The current protocol confuses one HN session with another HN session which allows the impersonation attack. Hence, a nonce can be introduced in the authentication process of the HN to ensure that it does not mistaken the correct ($SUPI$, K_{SEAF}) tuple.

Basin et al. [6] proposed two possible fixes for the key confirmation between the UE and the SN. The first fix binds $AUTN$ to $SNname$ so that the UE authenticates the identity of SN by authenticating HN. The second fix uses an additional key confirmation sent by the SN only. Namely, the SN can send any MACed message with a key derived by K_{SEAF} and prove its knowledge of K_{SEAF} to the UE.

3.3.2 Privacy

In order to hide the identity of a UE, the failure message sent by the SN should be hidden to the attacker. A possible fix is to hide the failure message by the public key of the UE [12]. Therefore, the failure messages are safe under the assumption that the asymmetric encryption is secure.

The simplest fix to ensure the privacy of SQN in [8] is to change the concealling mechanism of $CONC^*$ from XOR to symmetric encryption. More specifically, we have $CONC^* = enc(\langle Failure, SQN_{UE}\rangle, AK^*)$ where $enc()$ denotes symmetric encryption. Note that this change is supported by current USIMs and HNs as they provide symmetric encryption scheme. The secrecy of SQN is then protected by the symmetric encryption.

4 Conclusion

This paper introduces an overview of the 5G technology and raises security concerns related to it. We present a detailed description of the 5G AKA protocol and analyse its security requirements and vulnerabilities. Though most of the specifications are met by the 5G AKA protocol, it is evident that some of its central goals related to security are not fully achieved. Most of the attacks described in this report are computationally easy to accomplish [6,8,12], which implies that the corresponding security properties are violated. In addition, this paper shows that the implicit authentication for the UE might not be sufficient for the 5G AKA protocol, because malicious behaviours might be conducted efficiently given that high-level secrets (e.g. K_{SEAF}) are not required after the authentication process is finished. It is notable that the 5G AKA protocol inherits some of the weaknesses in previous AKA protocols [8, 12]. Regardless of the difficulties in establishing new policies to improve the previous protocols and to ensure that it is compatible with the current protocol, the vulnerabilities discovered before should not be ignored.

It is generally acknowledged that 5G is more powerful than the previous generations of mobile communications. 5G uses high frequencies which enable high-speed communications. However, the mmWaves tranmission of the 5G standard manifests itself in the lower range of connections, thus reducing the coverage area of the base stations (SNs). Therefore, 5G requires more base stations to cover an area than the previous generations. Moreover, 5G is designed as a united platform that supports not only mobile phones but also new devices such as massive IoT. In other words, there are significantly more UEs of different types in 5G. Given above, it is inferred that the challenge of controlling the authentication of a massive amount of parties in 5G is unprecedented. Hence, the security properties regarding the authentication process in 5G should be emphasized. This review expects the vulnerabilities of the current 5G AKA protocol to be resolved in the near future. Moreover, one should always be prepared for new vulnerabilities and it is critical fix them with caution.

References

[1] "Mobile visual networking index (vni) infographic," Feb 2019.

[2] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?," *IEEE Journal on Selected Areas in Communications*, vol. 32, pp. 1065–1082, June 2014.

[3] P. Schneider and G. Horn, "Towards 5G security," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, pp. 1165–1170, Aug 2015.

[4] X. Zhang, A. Kunz, and S. Schröder, "Overview of 5g security in 3gpp," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 181–186, Sep. 2017.

[5] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[6] D. 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*, (New York, NY, USA), pp. 1383–1396.

[7] A. Koutsos, "The 5g-aka authentication protocol privacy," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 464–479.

[8] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, "New privacy threat on 3G, 4G, and upcoming 5G AKA protocols," *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 3, pp. 108 – 127, 2019.

[9] 3GPP, *Security architecture and procedures for 5G system*, 2018. v15.1.0.

[10] 3GPP, *System architecture for the 5G System (5GS)*, 2019. v16.2.0.

[11] M. Dehnel-Wild and C. Cremers, "Security vulnerability in 5G-AKA draft," *Department of Computer Science, University of Oxford, Tech. Rep*, 2018.

[12] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar, "New privacy issues in mobile telephony: Fix and verification," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, (New York, NY, USA), pp. 205–216.