Formal Verification of 5GAKA-LCCO protocol supporting Forward Secrecy: Based on enhanced BAN Logic

Gunwoo Kim, Yongho Ko, and Ilsun You*
Kookmin University, Seoul, 02707, Republic of Korea
{gguakim22, koyh0911, isyou}@kookmin.ac.kr

Abstract

As 5G technology becomes more advanced and innovative, various vulnerabilities are being discovered. Furthermore, as technology develops further, not only in 5G but also in Beyond 5G (B5G) and 6G, strong security is required, and research is underway to satisfy this. In particular, standardization is underway to reuse the credentials generated in 5G basic authentication at the application layer, and in order to support strong security for this standard, forward secrecy (FS) for the key must be satisfied. Therefore, 5G primary authentication protocols supporting FS have been proposed. Among the proposed protocols, 5GAKA-LCCO has the advantage of protecting against replay attacks due to timestamp utilization and supporting overhead reduction by reducing the number of round trips. Therefore, since it was judged to be valuable to closely verify the security of 5GAKA-LCCO, we performed formal verification. accordingly, we verify through BAN logic whether the 5GAKA-LCCO protocol truly satisfies the security properties. However, since BAN logic does not have rules to verify FS properties, we proposed new notations and rules for FS verification. Based on the enhanced BAN Logic, we verified the protocol and found that this protocol is not secure. 5GAKA-LCCO still does not support FS properties, and various vulnerabilities such as Denial of Service (DoS) attacks and synchronization problems exist.

Keywords: 5G Network, 5G Primary Authentication, Forward Secrecy, BAN Logic

1 Introduction

Fifth-generation mobile communications (5G) connects the digital world and the real world in various fields based on the characteristics of Enhanced Mobile BroadBand (EMBB), Massive Machine-Type Communications (MMTC), and Ultra-Reliable and Low-Latency Communications (URLLC) [1]. In line with the industry and digital transformation paradigm of the 4th Industrial Revolution era, such as artificial intelligence, big data, and the Internet of Things, the development of industry through 5G technology has brought about many changes and innovations [2]. In addition, mobile communication technology is rapidly evolving as global companies such as Samsung Electronics, Ericsson, Nokia, and Orange are accelerating research to take the lead in not only 5G technology but also Beyond 5G (B5G) and 6G technology [3, 4, 5, 6, 7, 8]. However, as technology deepens and innovates, many new security threats and attacks are emerging, but current security standards have limitations in responding to these new threats [9, 10, 11, 12, 13, 14, 15].

Accordingly, stronger security is required in next-generation mobile communication technologies such as B5G and 6G, and much research is being conducted to meet security requirements [16, 17, 18]. For example, various vulnerabilities were discovered in the 5G primary authentication method, and as various attack scenarios were announced [19], it became necessary

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No. 52
*Corresponding author: Department of Financial Information Security, Kookmin University, Seoul, 02707, Republic of Korea, Tel: +82-02-910-5127

to strengthen the security of primary authentication [20, 21]. In addition, in next-generation communications, that is, B5G/6G, standardization is underway to reuse credentials generated during primary authentication for applications, so higher security strength support is needed for primary authentication (e.g., Authentication and Key Management for Applications (AKMA)) [22]. furthermore, in B5G/6G, as standardization is underway to reuse credentials generated during primary authentication in the application layer, higher security strength support is required for primary authentication, and Forward Secrecy (FS) support for keys is essential to support high-security strength. Therefore, various studies have been conducted to support FS and support higher security strength [23, 24, 20, 21, 25]. In fact, many studies have been conducted in the direction of recycling Elliptic Curve Integrated Encryption Scheme (ECIES) shared keys.

[23] achieved strong security strength by reusing the symmetric key exchanged through ECIES to encrypt the challenge value. [24] attempted to support FS by reusing the symmetric key exchanged through ECIES when creating the Master Session Key, and [20] attempted to support FS by deriving a new key using the long-term key k and the Home Network's private key and use this key to support FS. [21] attempted to support key strengthening using $RAND_{SN}$ and T_{SN}. Among them, [21] has an innovative look unlike existing standards, uses timestamps to respond to replay attacks, and has less computational and communication overheads than existing standards. Therefore, in this study, we will verify the security of the 5GAKA-LCCO protocol that supports improved security and discuss its security properties. To verify security, we verified using the BAN Logic among the formal verification [26]. However, since the BAN Logic that led the field of formal verification does not have the ability to verify FS properties, we added new notations and rules to enable verification in our BAN Logic. We thoroughly verified the protocol using the rules we proposed and described the vulnerabilities of the protocol as a result of the verification. The main contributions of this paper are summarized as follows:

- An enhanced BAN Logic was proposed by adding new notations and rules to verify FS properties.
- A thorough formal verification was performed on the proposed protocol based on enhanced BAN Logic.
- Vulnerabilities in the protocol were discovered through formal verification, and based on this, five vulnerabilities were described in detail.

The rest of the paper is organized as follows. Section 2 performs an analysis of the 5GAKA-LCCO protocol that satisfies FS properties, and Section 3 adds new notations and rules that can verify whether FS properties are satisfied in BAN Logic, and formal verification of the protocol is thoroughly performed based on the proposed enhanced BAN Logic. In Section 4, we perform vulnerability analysis of the protocol through detailed descriptions of vulnerabilities discovered through formal verification. Finally, Section 5 provides the conclusion.

2 Overview of the 5GAKA-LCCO Protocol

2.1 Notations

Table 1 shows abbreviations and meaning to be used throughout this paper [27].

Table 1: Abbreviations and Meanings

Abbreviations	meaning
UE	User Equipment
SN	Serving Network
HN	Home Network
SUPI	SUbscriber Permanent Identifier
SUCI	SUbscriber Concealed Identifier
r	An ephemeral private key of the UE for Diffie–Hellman exchange
R	An ephemeral public key of the UE for Diffie–Hellman exchange
PK_{HN}	An ephemeral public key of the HN for Diffie–Hellman exchange
K	A long-term key between the UE and the HN
K_{AUSF}, K_{SEAF}	An master session key / An anchor key
$RAND$	HN's challenge message
$RAND_{SN}$	SN's challenge message
ID_{SN}	Unique identifier of SN
T_{HN}, T_{SN}	the current time of the HN, a timestamp generated by the SN
EK	An encryption key
ICB	An initial counter block
MK	A MAC key
MAC_{UE}	A MAC of the UE
AMF	The authentication management field
$AUTN$	An authentication token of the HN

2.2 5GAKA-LCCO Protocol

[21] is a 5G primary authentication protocol proposed to improve the high computational overhead of 5G-IPAKA and support improved security such as SUCI replay attack and FS support. Compared to 5G-AKA, the existing standard 5G authentication protocol, this protocol has the advantage of low computation and communication overheads because the round trip is significantly lightweight. Additionally, we responded to linkability attacks by deleting the `Sync_Failure` process and added freshness through timestamps. In addition, security for the master session key was improved because $RAND_{SN}$ and T_{SN} were reflected when deriving the session key. Figure 1 is the 5GAKA-LCCO protocol, and the detailed steps are as follows.

1. Unlike 5G-AKA, the authentication process begins by transmitting $RAND_{SN}$ and T_{SN} generated from the SN to the UE.

2. The UE that receives $RAND_{SN}$ and T_{SN} creates an ephemeral private-public key pair *(r, R)* to use in the SUCI setting. After that, using $RAND_{SN}$ and T_{SN}, Create a key block containing $EK \parallel ICB \parallel MK \parallel K_{AUSF}$. Compute MAC_{UE} and configure SUCI using the generated values. At this time, the UE does not perform verification of the timestamp.

3. The UE transmits SUPI encrypted with EK and SUCI containing UE's public key R to the SN.

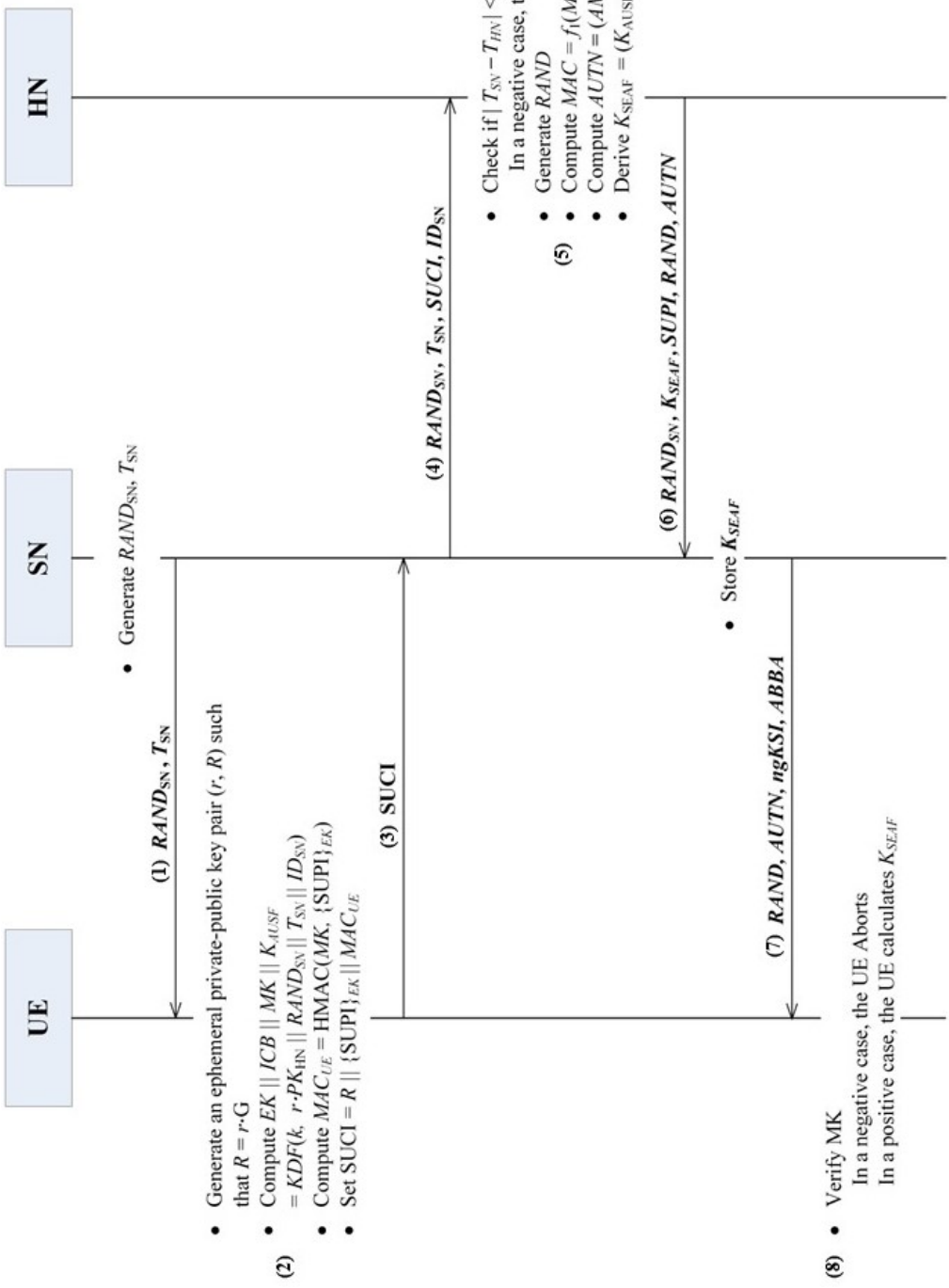

Figure 1: 5GAKA-LCCO Protocol

4. The SN that receives the message from the UE transmits $RAND_{SN}$, T_{SN}, and ID_{SN} in addition to SUCI to the HN.

5. The HN, which receives the message from SN, verifies T_{SN}. If T_{SN} verification fails, it is aborted, and if successful, SUCI is decrypted. Through SUCI decryption, the HN authenticates the UE. HN generates $RAND$, a challenge message, and computes MAC and $AUTN$. Additionally, K_{SEAF}, the anchor key, is Derived through K_{AUSF}.

6. The HN transmits $RAND_{SN}$, SUPI, and the generated K_{SEAF}, $RAND$, and $AUTN$ to SN.

7. The SN stores K_{SEAF} received from HN and transmits $RAND$, $AUTN$, $ngKSI$, and $ABBA$ to UE.

8. The UE verifies the $AUTN$ based on the MK. When successful, derive K_{SEAF} from the existing K_{AUSF}, save it, and use it for later setup. In case of failure, the UE aborts.

   This protocol uses challenge values and timestamps to generate SUCI and uses them for authentication to reduce round trips and make it lightweight. Despite these efforts, this protocol does not fully support FS properties, and various other vulnerabilities exist. Therefore, we thoroughly analyze the protocol by performing formal verification based on the proposed BAN Logic.

3 Formal Verification based on enhanced BAN Logic

3.1 Forward Secrecy

As times advance, cyber-attacks are becoming more sophisticated and common. Therefore, in today's digital environment, support for perfect forward secrecy in security protocols is becoming more and more essential [28]. For example, even for the TLS v1.3 protocol, support for perfect forward secrecy is considered an important design goal [29]. FS refers to the case where the past session key is not leaked when the long-term key is leaked, and a protocol that supports this property is said to have FS [30, 31]. To satisfy FS, ephemeral Diffie–Hellman (DH) key exchange or Elliptic-curve Diffie–Hellman (ECDH) key exchange encryption methods are mainly used [30]. Additionally, to support FS, the private key must not be kept in persistent storage [32]. In addition to TLS, support for perfect forward secrecy is becoming an essential element in mobile communications [33], and as various attack scenarios are being announced in 5G, security strengthening has become necessary. Since strong security technology is required not only in 5G but also in B5G and 6G, FS support is selected as a key aspect. In addition, as the standardization of reusing credentials generated during primary authentication in applications is progressing, the importance of FS support to satisfy this is becoming more and more highlighted.

3.2 BAN Logic

To trust a security protocol, a safety analysis of the protocol is required. Therefore, formal verification is used to verify the safety of security protocols. Among the formal verification methods, the method of systematizing and verifying the logical derivation relationships between propositions is called Modal Logic.

BAN Logic, one of the representative techniques of Modal Logic, was very popular in the early days and led the field of formalized security analysis because its structure is simple and

intuitive, and the verification results are highly reliable [26]. However, BAN Logic does not have the ability to verify whether FS properties are satisfied, so it has the disadvantage of not being able to completely verify the security properties of recently proposed FS support protocols. In modern times, as FS support has been emphasized in the latest protocols such as TLS v1.3, 5G authentication protocol, etc., supporting FS in security protocols is moving towards becoming essential. Therefore, it is necessary to verify whether the security protocol satisfies the FS properties.

Therefore, we have added new notations and rules that can verify that FS properties are satisfied in order to complement these shortcomings of BAN Logic and accurately analyze the latest security protocols. Through our proposed enhanced BAN Logic, more security properties can be verified, and based on the proposed notations and rules, we verified 5GAKA-LCCO, a 5G authentication protocol that supports FS.

3.3 Enhanced BAN Logic

BAN Logic is verified through Idealization, Assumption, Goals, and Derivation processes. In the Idealization process, only encrypted messages between communication participants are expressed, and in the Assumption process, preconditions are defined so that they can be applied to BAN logic. In the Goals process, the security goals required by the protocol are set. The existing notations and rules used in the above process and the notations and rules we proposed are shown in Table 2 and Table 3.

We proposed three notations, and the details of the notations we proposed are as follows.

- $P \, \epsilon \, K$ indicates that the private key K is an ephemeral key and P removes K from itself.
- $P \overset{K}{\longleftrightarrow} Q \propto KEM\,(K_1, K_2, \cdots, K_n)$ indicates that the secret key K is agreed between P and Q through $(K_1, K_2, \cdots, K_n)$
- $\pi\left(P \overset{K}{\longleftrightarrow} Q\right)$ indicates that the secret key K satisfies the Forward Secrecy.

We added the following two Rules to verify whether the protocol's FS properties are supported, and the details are as follows.

- **KEM Rule**

  1. P believes P's public key g^X
  2. P believes that Q sent P's public key g^X. At this time, Q's public key g^Y is derived from P's Private key X and Q's public key g^Y

  – If these two beliefs are satisfied, a new belief can be derived:
  P believes that the shared secret key between P and Q is derived from P's Private key X and Q's public key g^Y.

The difference between DH rules and KEM rules is that in the case of DH rules, you can only check that the key has been exchanged, but in the case of KEM rules, you can check through which key the key was exchanged.

The Forward Secrecy (FS) rule means that all participants deriving the shared secret key K satisfies the FS security properties for K. A detailed description of the FS rule is as follows.

Table 2: Notations of BAN logic

Notation	Meaning
$P \mid\equiv X$	P believes the message X
$P \triangleleft X$	P receives the message X
$P \mid\sim X$	P previously sent the message X
$P \Rightarrow X$	P has authority over X
$\#(X)$	The message X is fresh
$\langle X \rangle_K$	X is combined with a secret K
$\{X\}_K$	X is encrypted with a key K
$P \overset{K}{\longleftrightarrow} Q$	K is a secret key shared between P and Q
$\overset{K}{\longmapsto} P$	K is the public key of P
$P \overset{K}{\Leftrightarrow} Q$	K is a shared secret between P and Q
$P \in K$	K is a ephemeral private key, and P removes K from itself
$P \overset{K}{\longleftrightarrow} Q \propto KEM\,(K_1, K_2, \cdots, K_n)$	K is a secret key, and agreed between P and Q through $K_1, K_2, \cdots, K_n$
$\pi\left(P \overset{K}{\longleftrightarrow} Q\right)$	K is a secret key, and satisfies Forward Secrecy

- **Forward Secrecy Rule**

  1. P believes that K (shared secret key $P \overset{g^{XY}}{\longleftrightarrow} Q$) is derived from P's private key X and Q's public key g^Y
  2. P believes that Q removes the private key Y corresponding to the public key g^Y
  3. P believes that P removes P's private key X

  – If these three beliefs are satisfied, a new weak belief can be derived:
  P weak believes that the secret shared key g^{XY} between P and Q satisfies Forward Secrecy.

  1. Q believes that K(shared secret key $Q \overset{g^{XY}}{\longleftrightarrow} P$) is derived from P's private key X and Q's public key g^X
  2. Q believes that P removes the private key X corresponding to the public key g^X
  3. Q believes that Q removes Q's private key Y

  – If these three beliefs are satisfied, a new weak belief can be derived:
  Q weak believes that the secret shared key g^{XY} between Q and P satisfies Forward Secrecy.

- P weak believes that the secret shared key g^{XY} between P and Q satisfies FS.
- Q weak believes that the secret shared key g^{XY} between Q and P satisfies FS.

  – If these weak beliefs are satisfied, a new belief can be derived:
  all participants believe that satisfies the FS for the shared secret key g^{XY}

The FS rule is supported only when the FS attribute for the secret shared key created between P and Q is satisfied on both P and Q, and if only one participant is satisfied, the FS attribute is not supported.

3.4 Formal Verification of the 5GAKA-LCCO Protocol using enhanced BAN Logic

The results verified through BAN logic in this paper are as follows. First, The idealization form of the Initiation Phase of the protocol is shown below:

$$SN \rightarrow HN\text{: } \left\{RAND_{SN}, T_{SN}, ID_{SN}, \overset{X}{\longmapsto} UE, \text{ESUPI}, \langle \text{ESUPI}, UE \overset{MK}{\Leftrightarrow} HN\rangle_{MK}\right\}_{K_{SN,HN}} \tag{I1}$$

$$\text{where ESUPI} = \left\{\text{SUPI}, \overset{X}{\longmapsto} UE, UE \,\epsilon\, X, UE \overset{K_{AUSF}}{\longleftrightarrow} HN, UE \overset{EK}{\longleftrightarrow} HN\right\}_{EK}$$

$$HN \rightarrow SN\text{: } \left\{RAND_{SN}, UE \overset{K_{SEAF}}{\longleftrightarrow} SN, \text{SUPI}, RAND, AUTN\right\}_{K_{SN,HN}} \tag{I2}$$

$$\text{where AUTN} = \left(AMF, \langle AMF, RAND, UE \overset{MK}{\Leftrightarrow} HN\rangle_{MK}\right)$$

$$SN \rightarrow UE\text{: } \langle AMF, RAND, UE \overset{K_{AUSF}}{\longleftrightarrow} HN, UE \overset{MK}{\Leftrightarrow} HN\rangle \tag{I3}$$

We have set the following 11 security goals.

$$UE \mid\equiv HN \mid\equiv ID_{SN} \tag{G1}$$

$$HN \mid\equiv UE \mid\equiv ID_{SN} \tag{G2}$$

$$HN \mid\equiv UE \mid\equiv \text{SUPI} \tag{G3}$$

$$HN \mid\equiv UE \overset{K_{AUSF}}{\longleftrightarrow} HN \tag{G4}$$

$$HN \mid\equiv UE \mid\equiv UE \overset{K_{AUSF}}{\longleftrightarrow} HN \tag{G5}$$

$$UE \mid\equiv UE \overset{K_{AUSF}}{\longleftrightarrow} HN \tag{G6}$$

$$UE \mid\equiv HN \mid\equiv UE \overset{K_{AUSF}}{\longleftrightarrow} HN \tag{G7}$$

$$UE \mid\equiv UE \overset{K_{SEAF}}{\longleftrightarrow} HN \tag{G8}$$

$$SN \mid\equiv UE \overset{K_{SEAF}}{\longleftrightarrow} HN \tag{G9}$$

$$HN^{\,w} \mid\equiv\ \pi\left(UE \overset{K_{XY}}{\longleftrightarrow} HN\right) \tag{G10}$$

$$UE^{\,w} \mid\equiv\ \pi\left(UE \overset{K_{XY}}{\longleftrightarrow} HN\right) \tag{G11}$$

The important point here is that if (G1) and (G2) are not present, the UE can create a SUCI by receiving the forged ID_{SN} presented by the attacker. Afterwards, the SUCI can be delivered

Table 3: Rules of BAN logic

Rule	Formula
Message Meaning Rule (MM)	$\frac{P \mid\equiv P \overset{K}{\longleftrightarrow} Q, \quad P \triangleleft \{X\}_K}{P \mid\equiv Q \mid\sim X} \qquad \frac{P \mid\equiv P \overset{K}{\Leftrightarrow} Q, \quad P \triangleleft \langle X \rangle_K}{P \mid\equiv Q \mid\sim X}$
	$\frac{P \mid\equiv \overset{K}{\longmapsto} Q, \quad P \triangleleft \{X\}_{Q^{-1}}}{P \mid\equiv Q \mid\sim X}$
Nonce Verification Rule (NV)	$\frac{P \mid\equiv \#(X), \quad P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$
Jurisdiction Rule (JR)	$\frac{P \mid\equiv Q \Rightarrow X, \quad P \mid\equiv Q \mid\sim X}{P \mid\equiv X}$
Diffie-Hellman Rule (DH)	$\frac{P \mid\equiv Q \mid\sim \overset{g^Y}{\longmapsto} Q, \quad P \mid\equiv \overset{g^X}{\longmapsto} P}{P \mid\equiv P \overset{g^{XY}}{\longleftrightarrow} Q}$ $\frac{P \mid\equiv Q \mid\sim \overset{g^Y}{\longmapsto} Q, \quad P \mid\equiv \overset{g^X}{\longmapsto} P}{P \mid\equiv P \overset{g^{XY}}{\Leftrightarrow} Q}$
Freshness Rule (FR)	$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y)}$
Decomposition Rule (DR)	$\frac{P \triangleleft (X, Y)}{P \triangleleft X} \qquad \frac{P \mid\equiv X, \quad P \mid\equiv Y}{P \mid\equiv (X, Y)}$
Belief Conjunction Rule (BC)	$\frac{P \mid\equiv Q \mid\equiv (X,Y)}{P \mid\equiv Q \mid\equiv X} \qquad \frac{P \mid\equiv Q \mid\sim (X,Y)}{P \mid\equiv Q \mid\sim X}$
Hash Rule (HR)	$\frac{P \mid\equiv Q \mid\sim H(X), \quad P \triangleleft X}{P \mid\equiv Q \mid\sim X}$
KEM Rule (KEM)	$\frac{P \mid\equiv \overset{g^X}{\longmapsto} P, \quad P \mid\equiv Q \mid\sim \overset{g^Y}{\longmapsto} Q \propto KEM\left(X, \overset{g^Y}{\longmapsto} Q\right)}{P \mid\equiv Q \mid\sim X}$
Forwoard Secrecy (FS) Rule	$\frac{P \mid\equiv P \overset{g^{XY}}{\longleftrightarrow} Q \propto KEM\left(X, \overset{g^Y}{\longmapsto} Q\right), \quad P \mid\equiv Q \mid\equiv Q \in Y, \quad P \mid\equiv P \in X}{P^w \mid\equiv \pi\left(P \overset{g^{XY}}{\longleftrightarrow} Q\right)}$ $\frac{Q \mid\equiv Q \overset{g^{XY}}{\longleftrightarrow} P \propto KEM\left(Y, \overset{g^X}{\longmapsto} P\right), \quad Q \mid\equiv P \mid\equiv P \in X, \quad Q \mid\equiv Q \in Y}{Q^w \mid\equiv \pi\left(Q \overset{g^{XY}}{\longleftrightarrow} P\right)}$ $\frac{P^w \mid\equiv \pi\left(P \overset{g^{XY}}{\longleftrightarrow} Q\right), \quad Q^w \mid\equiv \pi\left(Q \overset{g^{XY}}{\longleftrightarrow} P\right)}{P \mid\equiv \pi\left(P \overset{g^{XY}}{\longleftrightarrow} Q\right), \quad Q \mid\equiv \pi\left(Q \overset{g^{XY}}{\longleftrightarrow} P\right)}$

to a malicious or normal SN, and the SN can access the HN through this SUCI to perform session hijacking. Additionally, for this protocol to be safe, the following three conditions must be satisfied in order.

1. First, HN must know the UE's SUPI, k and SQN
2. The UE must verify the HN by checking the HN's MAC.
   ($MAC = KDF(k, RAND \parallel AMF \parallel SQN)$)
3. If the MAC is valid, the UE calculates RES^* and has it verified by the HN.
   ($RES^* = KDF(CK \parallel IK, ID_{SN}, RAND, RES)$)

In other words, only when (G1) is guaranteed can the UE calculate and present SUCI. Since HN can be authenticated only when (G2) is guaranteed, satisfying (G1) and (G2) is a very important security goal.

We added the following assumptions for verification.

$$HN \mid\equiv UE \overset{K_{SN,HN}}{\longleftrightarrow} HN \tag{A1}$$

$$HN \mid\equiv \#(T_{SN}) \tag{A2}$$

$$HN \mid\equiv \overset{Y}{\longmapsto} HN \tag{A3}$$

$$SN \mid\equiv SN \overset{K_{SN,HN}}{\longleftrightarrow} HN \tag{A4}$$

$$SN \mid\equiv \#(RAND_{SN}) \tag{A5}$$

$$SN \mid\equiv HN \Rightarrow UE \overset{K_{SEAF}}{\longleftrightarrow} SN \tag{A6}$$

$$UE \mid\equiv \overset{X}{\longmapsto} UE \tag{A7}$$

$$UE \mid\equiv HN \mid\sim \overset{Y}{\longmapsto} HN \tag{A8}$$

$$UE \triangleleft (RAND_{SN}, T_{SN}, ID_{SN}) \tag{A9}$$

$$UE \mid\equiv UE \overset{K}{\longleftrightarrow} HN \tag{A10}$$

$$UE \mid\equiv \#(\overset{X}{\longmapsto} UE) \tag{A11}$$

We also performed verification by adding unjustified assumptions (H1) and (H2). Because there is a problem with the protocol, it is impossible to verify the protocol without these two assumptions. Adding assumptions (H1) and (H2) means that the protocol is not secure.

$$HN \mid\equiv UE \mid\sim \overset{X}{\longmapsto} UE \tag{H1}$$

$$HN \mid\equiv UE \overset{K}{\longleftrightarrow} HN \tag{H2}$$

from (I1), we derive

$$HN \triangleleft \left\{ RAND_{SN}, T_{SN}, ID_{SN}, \overset{X}{\longmapsto} UE, \text{ESUPI}, \langle \text{ESUPI}, UE \overset{MK}{\Leftrightarrow} HN \rangle_{MK} \right\}_{K_{SN,HN}}$$

by (I1) (D1a)

$$HN \mid\equiv SN \mid\equiv \left(RAND_{SN}, T_{SN}, ID_{SN}, \overset{X}{\longmapsto} UE, \text{ESUPI}, \langle \text{ESUPI}, UE \overset{MK}{\Leftrightarrow} HN \rangle_{MK} \right)$$

by (D1a), (A1), MM, (A2), FR, NV (D1b)

$HN \mid\equiv SN \mid\equiv \overset{X}{\longmapsto} UE$ by (D1b), BC (D1c)

Here, despite (A3), it is not possible to prove that $K_{XY} = x \cdot y \cdot G$ is securely derived according to the Diffie-Hellman Rule through the belief (D1c). That is why HN does not have UE's belief on $\overset{X}{\longmapsto} UE$.
To proceed, (H1) is added, which is applied to the Diffie-Hellman Rule along with (A3) to derive the important belief (D1d).

$HN \mid\equiv UE \overset{K_{XY}}{\longleftrightarrow} HN$ by (H1), (A3), DH (D1d)

$HN \mid\equiv SN \mid\equiv (RAND_{SN}, T_{SN}, ID_{SN})$ by (D1b), BC (D1e)

To generate a key block through the formula (1), in addition to $RAND_{SN}, T_{SN}, ID_{SN}$, and K_{XY}, the long-term secret key K between UE and HN must be obtained. Without UE's SUPI, HN cannot retrieve K from the secret key set. But, it can recover SUPI only if it possesses knowledge of EK, and EK is derived from a key block that is generated when K is provided as input. The catch here is that K can only be acquired with SUPI, creating an apparent paradox. Even though this analysis cannot advance any more, it proceeds to examine the remainder of the protocol through the inclusion of (H2).

With (D1d), (D1e), (A4), and (H2), we can intuitively obtain the following beliefs on the keys, EK, MK, and K_{AUSF} through the formula (1).

$$HN \mid\equiv UE \overset{EK}{\longleftrightarrow} HN \quad \text{(D1f)}$$

$$HN \mid\equiv \#(UE \overset{EK}{\longleftrightarrow} HN) \quad \text{(D1g)}$$

$$HN \mid\equiv UE \overset{K_{AUSF}}{\longleftrightarrow} HN \quad \text{(D1h)}$$

$$HN \mid\equiv UE \overset{MK}{\Leftrightarrow} HN \quad \text{(D1i)}$$

$$HN \mid\equiv \#(UE \overset{MK}{\Leftrightarrow} HN) \quad \text{(D1j)}$$

$HN \triangleleft \text{ESUPI}$ by (D1b) (D1k)

$$HN \mid\equiv SN \mid\equiv \left(\text{SUPI}, \overset{X}{\longmapsto} UE, UE \in x, UE \overset{K_{AUSF}}{\longleftrightarrow} HN, UE \overset{EK}{\longleftrightarrow} HN \right)$$

by (D1k), (D1f), MM, (D1g), FR, NV (D1l)

$HN \mid\equiv UE \mid\equiv UE \overset{EK}{\longleftrightarrow} HN$ by (D1l), BC (D1m)

$HN \mid\equiv UE \mid\equiv UE \overset{K_{AUSF}}{\longleftrightarrow} HN$ by (D1l), BC (D1n)

$HN \mid\equiv UE \mid\equiv UE \,\epsilon\, x$ by (D1l), BC (D1o)

$HN \mid\equiv UE \mid\equiv \overset{X}{\longmapsto} UE$ by (D1l), BC (D1p)

$HN \mid\equiv UE \mid\equiv \text{SUPI}$ by (D1l), BC (D1q)

$HN \mid\equiv UE \mid\equiv \left(\text{ESUPI}, UE \overset{MK}{\Leftrightarrow} HN\right)$ by (D1b), BC, (D1i), MM, (D1j), FR, NV (D1r)

$HN \mid\equiv UE \mid\equiv UE \overset{MK}{\Leftrightarrow} HN$ by (D1r), BC (D1s)

$HN \mid\equiv UE \mid\equiv UE \overset{K_{XY}}{\longleftrightarrow} HN \propto KEM\,(X, y)$ by (D1d) (D1t)

Here, note that HN cannot achieve the goal (G10) $HN \overset{w}{\mid\equiv} \pi\left(UE \overset{K_{XY}}{\longleftrightarrow} HN\right)$ due to the lack of the belief HN believes $HN \,\epsilon\, y$. It indicates that this protocol does not satisfy forward secrecy.
Without (H1), HN is still vulnerable to resource exhaustion attacks because an attacker can replay an old SUCI to cause a victim to uselessly compute the ECDH key agreement, an expensive computation. Moreover, (H2) indicates that this protocol should be corrected to allow HN to first recover SUPI without K.

From (I2), we derive

$SN \triangleleft \left\{RAND_{SN}, UE \overset{K_{SEAF}}{\longleftrightarrow} SN, \text{SUPI}, RAND, AUTN\right\}_{K_{SN,HN}}$ by (I2) (D2a)

$SN \mid\equiv HN \mid\equiv \left(RAND_{SN}, UE \overset{K_{SEAF}}{\longleftrightarrow} SN, \text{SUPI}, RAND, AUTN\right)$
by (D2a), (A4), MM, (A5), FR, NV (D2b)

$SN \mid\equiv HN \mid\equiv \text{SUPI}$ by (D2b), BC (D2c)

$SN \mid\equiv UE \overset{K_{SEAF}}{\longleftrightarrow} SN$ by (D2b), BC, (A6), JR (D2d)

From (I3), we derive

$UE \triangleleft \left\langle AMF, RAND, UE \overset{K_{AUSF}}{\longleftrightarrow} HN, UE \overset{MK}{\Leftrightarrow} HN\right\rangle_{MK}$ by (I3) (D3a)

$UE \mid\equiv UE \overset{K_{XY}}{\longleftrightarrow} HN$ by (A7), (A8), DH (D3b)

Note that in the first place UE is informed of the values, $RAND_{SN}, T_{SN}, ID_{SN}$, which is defined as an assumption (A9). Therefore, based on the formula (1), we can intuitively get the following beliefs on the keys, MK and K_{AUSF} with (A9), (A10), (D3b).

$$UE \mid\equiv UE \overset{MK}{\Leftrightarrow} HN \tag{D3c}$$

$$UE \mid\equiv \#(UE \overset{MK}{\Leftrightarrow} HN) \quad \text{by (A11)} \tag{D3d}$$

$$UE \mid\equiv UE \overset{K_{AUSF}}{\longleftrightarrow} HN \quad \text{by (A11)} \tag{D3e}$$

$$UE \mid\equiv UE \overset{K_{SEAF}}{\longleftrightarrow} HN \quad \text{by (A11)} \tag{D3f}$$

Now, with the new beliefs (D3c), and (D3d), we advance (D3a) more.

$$UE \mid\equiv HN \mid\equiv \left(AMF, RAND, UE \overset{K_{AUSF}}{\longleftrightarrow} HN, UE \overset{MK}{\Leftrightarrow} HN\right)$$
by (D3a), (D3c), MM, (D3d), FR, NV (D3g)

$$UE \mid\equiv HN \mid\equiv UE \overset{K_{AUSF}}{\longleftrightarrow} HN \quad \text{by (D3g), BC} \tag{D3h}$$

$$UE \mid\equiv UE \overset{K_{XY}}{\longleftrightarrow} HN \propto KEM\,(x, Y) \quad \text{by (D3b)} \tag{D3i}$$

Here, note that UE cannot achieve the goal (G11) $UE \overset{w}{} \mid\equiv \pi \left(UE \overset{K_{XY}}{\longleftrightarrow} HN\right)$ due to the lack of the belief UE believes HN believes $HN \ \epsilon \ y$. It indicates that this protocol does not satisfy forward secrecy.

- When (G1) is achieved, the UE can calculate and present SUCI, and the HN can be authenticated only when (G2) is achieved. Additionally, the fact that (G1) and (G2) are not satisfied means that a session hijacking attack by a malicious SN is achievable. However, since this protocol cannot derive (G1) and (G2), this protocol is vulnerable to session hijacking attacks.
- Since we cannot achieve (D1d), we added the assumption (H1). However, the assumption (H1) is an unjustified assumption, and using (H1) means that the protocol is not secure. Additionally, without (H1), HN is not safe against DoS attacks because an attacker can replay SUCI.
- For HN to find the shared secret key K matching the received SUCI, we added the assumption (H2). However, (H2) is an unjustified assumption, which means that this protocol is not safe.
- Failure to achieve (G10) and (G11) means that FS is not supported. However, this protocol cannot achieve (G10) because there is no belief: *HN* believes that *HN* removed y, and it cannot achieve (G11) because there is no belief: *UE* believes that *HN* believes that *HN* removed y. Therefore, it means that FS is not satisfied.

4 Security Analysis

We verified the 5GAKA-LCCO protocol through enhanced BAN Logic. The verification results showed that it was not safe, and this chapter describes in detail the possible attacks that occurred through the verification.

1. Session hijacking attack by malicious SN
   Figure 2, 3 shows a session hijacking attack by a malicious SN on 5GAKA-LCCO and 5G-AKA. In 5G-AKA, the 5G standard primary authentication protocol, the protocol does not end in a one-round trip, but the UE transmits the *RES* value to the SN. The *RES* value is used as a challenge, and this value is verified by the SN and HN to authenticate the UE. After verifying the *RES*, the HN shares the anchor key K_{SEAF}, so it can respond to session hijacking attacks by malicious SN. However, 5GAKA-LCCO does not have this process and cannot respond to session hijacking attacks because it immediately shares the anchor key. Also, in this protocol, the UE and HN do not trust ID_{SN}. Therefore, when an attacker sends a message to a UE seeking session hijacking to collude with a malicious SN, SUCI is returned, and this SUCI is received by the malicious SN. Afterward, the malicious SN performs authentication by transmitting the received SUCI to the HN, and thus the SN receives K_{SEAF} from the HN. This attack is a problem that occurs because there is no process to verify the UE's challenge value, *RES*.

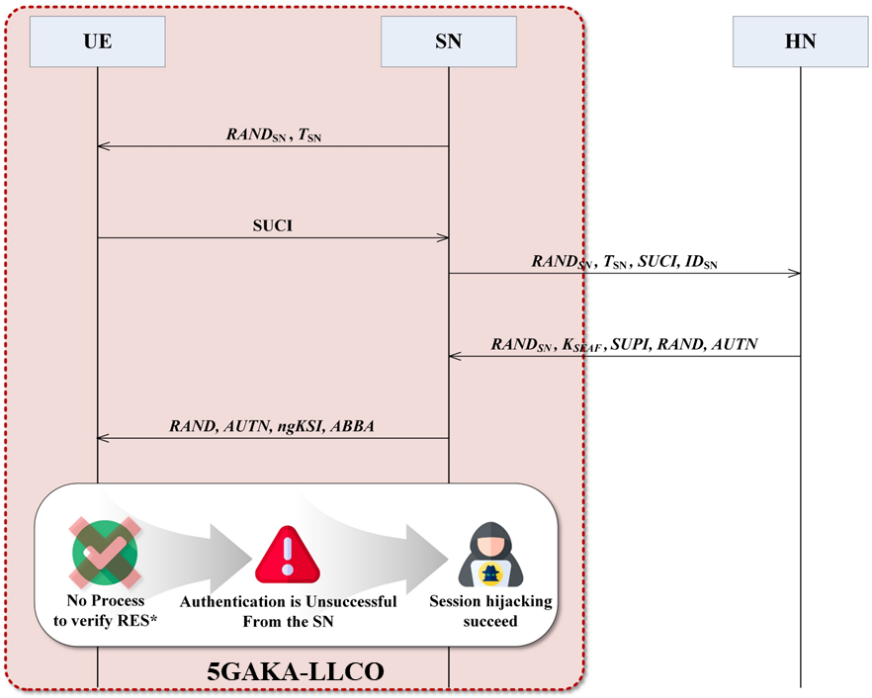

Figure 2: Session hijacking attack (5GAKA-LCCO)

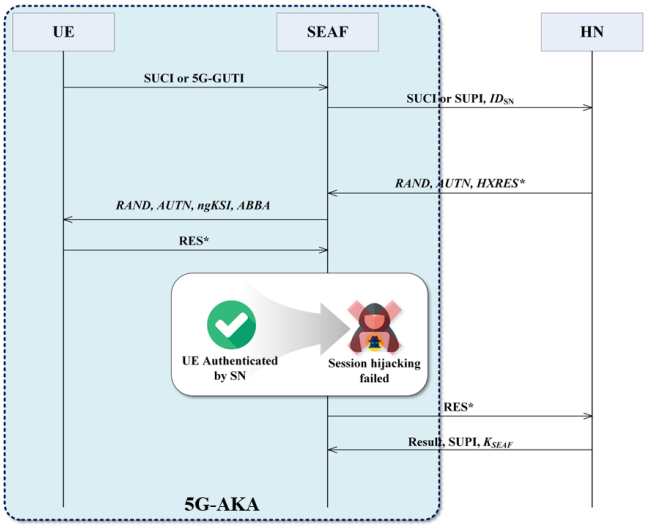

Figure 3: Session hijacking attack (5G-AKA)

2. Denial-of-Service (DoS) attack for HN
   Figure 4 is a possible DoS attack in 5GAKA-LCCO.This attack can also occur in 5G-AKA and EAP-AKA′ and occurs because HN does not trust the UE's public key. In a situation where no trust is established between the UE and the HN, a resource starvation attack is allowed in order for the HN to know the UE's SUPI. This attack is designed to be allowed in the 5G primary authentication protocol, so it is an attack that does not require a strict response.

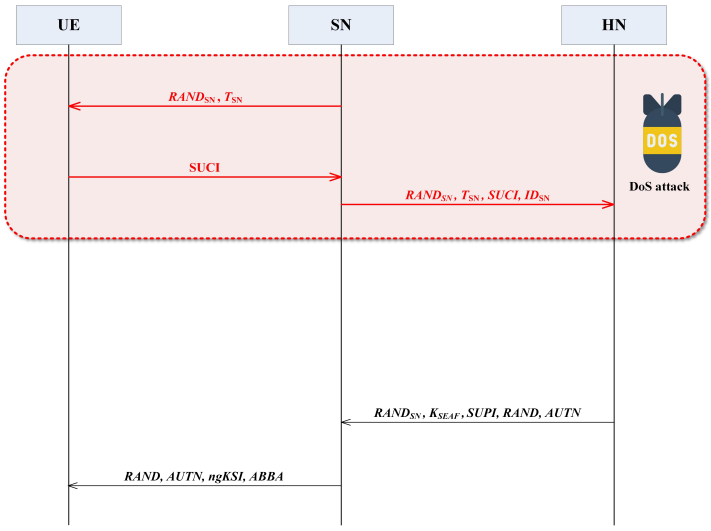

Figure 4: DoS attack for HN

3. Cannot find long term key K corresponding to SUCI
   Figure 5 shows that a problem exists in the protocol itself because K corresponding to SUCI cannot be found in HN. The key block is created using the long-term key K. Additionally, the encryption key, EK, is derived from the generated key block, and SUPI is encrypted with EK. Therefore, HN receives the SUCI value encrypted with EK, but at this time, HN cannot decrypt SUCI. This is because HN needs to know SUPI to obtain k matching it, but it cannot find SUPI because SUPI is encrypted with EK. Therefore, there is a very large error in this protocol which means it cannot proceed any further, and we verified the rest of the protocol through assumptions.

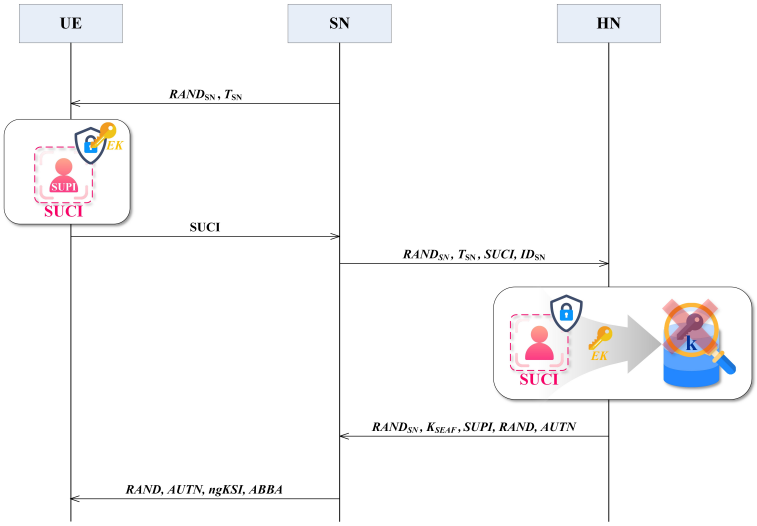

Figure 5: K not found

4. No support FS for session key
   The master session key does not support FS properties, and its description is as in figure 6. To support FS, both (G10) and (G11) must be satisfied. However, this protocol does not ephemerally use HN's public key and does not delete HN's private key on the server side. Therefore, if HN's private key and long-term key are leaked, FS cannot be supported.

5. Time synchronization error between SN and HN
   Time synchronization problems occur due to the use of timestamps, as shown in figure 7. This protocol performed authentication using Timestamp. However, when using timestamps in a mobile communication environment, many problems can occur because time synchronization is required. For example, in situations such as roaming, time synchronization is a huge challenge and can cause many problems. Therefore, due to these issues, the use of timestamps is prohibited in mobile communication environments and is not suitable for the 5G authentication protocol.

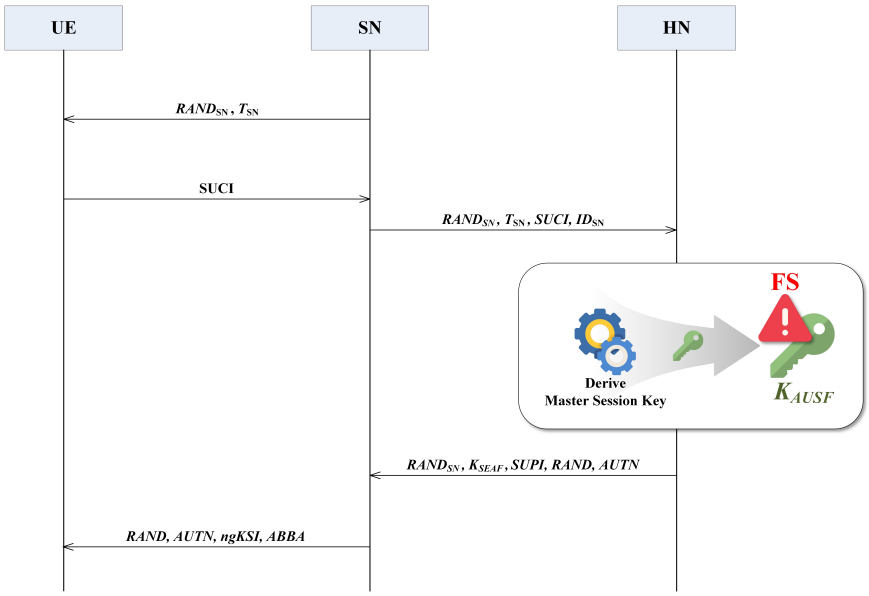

Figure 6: No support FS

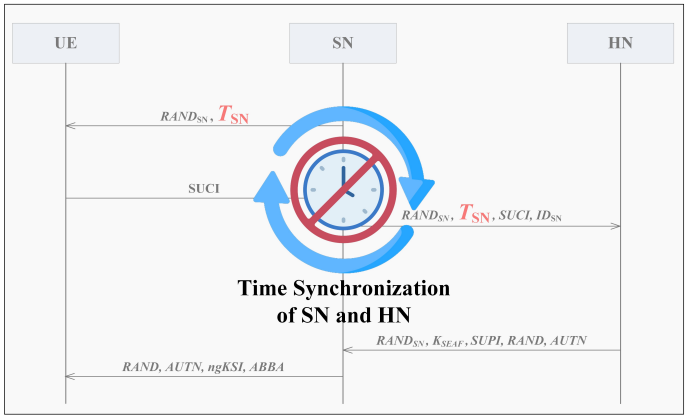

Figure 7: Time synchronization error

5 Conclusion

In this paper, we proposed enhanced notations and rules that can verify FS properties in BAN Logic. Based on the enhanced BAN Logic, we verified that the 5G authentication protocol 5GAKA-LCCO supporting FS is secure. As a result of the verification, we proved that 5GAKA-LCCO is not secure and that this protocol does not support FS properties. In addition to the non-support of FS, four vulnerabilities (Session hijacking, DoS attack, Cannot find K, Time synchronization error) that exist in this protocol are described in detail. In future research, we will improve the discovered vulnerabilities and propose a lightweight 5G authentication protocol that supports FS properties.

6 Acknowledgments

- This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2022-00207416, A study on PQC optimization and security protocol migration to neutralize advanced quantum attacks in Beyond 5G-based next-generation IoT computing environments, 100%)

References

[1] P. Persson A. Zaidi S. Magnusson A. Osseiran, S. Parkvall and K. Balachandran. 5g wireless access: an overview. Ericsson Whitepaper, April 2022. https://www.ericsson.com/en/reports-and-papers/white-papers/5g-wireless-access-an-overview [Online; Accessed on September 30, 2023].

[2] P. Likith and M. Sanna. Impact of 5g and digital transformation on storage. Dell Whitepaper, 2021. https://education.dell.com/content/dam/dell-emc/documents/en-us/2021KS_Meer-Impact_of_5G_and_Digital_Transformation_on_Storage.pdf [Online; Accessed on September 30, 2023].

[3] Samsung. [s6gf2022] samsung 6g forum: Live streaming (edit) — samsung. Samsung 6G Forum, June 2022. https://www.youtube.com/watch?v=hjXN_dYXLo8 [Online; Accessed on September 30, 2023].

[4] Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei Gurtov, and Mika Ylianttila. Security for 5g and beyond. *IEEE Communications Surveys & Tutorials*, 21(4):3682–3722, 2019.

[5] Hammad Dutta, Ashutosh and Eman. 5g security challenges and opportunities: A system approach. In *Proc. of the 3rd IEEE 5G World Forum (5GWF'20), Online*, pages 109–114. IEEE, September 2020.

[6] Kadri Kaska, Henrik Beckvard, and Tomáš Minárik. Huawei, 5g and china as a security threat. *NATO Cooperative Cyber Defence Center for Excellence*, 28:1–26, March 2019.

[7] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. 5g security: Analysis of threats and solutions. In *Proc. of the 3rd IEEE Conference on Standards for Communications and Networking (CSCN'17), Helsinki, Finland*, pages 193–199. IEEE, september 2017.

[8] Ravishankar Borgaonkar, Lucca Hirschi, Shinjo Park, and Altaf Shaik. New privacy threat on 3g, 4g, and upcoming 5g aka protocols. Cryptology ePrint Archive, 2018. https://eprint.iacr.org/2018/1175, [Online; Accessed on September 30, 2023].

[9] Roger Piqueras Jover and Vuk Marojevic. Security and protocol exploit analysis of the 5g specifications. *IEEE Access*, 7:24956–24963, February 2019.

[10] Fuwen Liu, Jin Peng, and Min Zuo. Toward a secure access to 5g network. In *Proc. of the 17st IEEE Conference on Trust, Security and Privacy in Computing and Communications (TrustCom '18)/ 12th IEEE Conference On Big Data Science And Engineering (TrustCom/BigDataSE '18) , New York, NY, USA*, pages 1121–1128. IEEE, August 2018.

[11] Syed Rafiul Hussain, Mitziu Echeverria, Imtiaz Karim, Omar Chowdhury, and Elisa Bertino. 5greasoner: A property-directed security and privacy analysis framework for 5g cellular network protocol. In *Proc. of the 26st ACM SIGSAC Conference on Computer and Communications Security (CCS'19), London, United Kingdom*, pages 669–684. ACM Press, November 2019.

[12] Mohamed Amine Ferrag, Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos, and Helge Janicke. Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, 101(1):55–82, January 2018.

[13] Rabia Khan, Pardeep Kumar, Dushantha Nalin K Jayakody, and Madhusanka Liyanage. A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*, 22(1):196–248, August 2019.

[14] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. A formal analysis of 5g authentication. In *Proc. of the 25st ACM SIGSAC Conference on Computer and Communications Security (CCS'18), Toronto, Canada*, pages 1383–1396. ACM Press, October 2018.

[15] Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei Gurtov, and Mika Ylianttila. Security for 5g and beyond. *IEEE Communications Surveys & Tutorials*, 21(4):3682–3722, May 2019.

[16] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. Overview of 5g security challenges and solutions. *IEEE Communications Standards Magazine*, 2(1):36–43, 2018.

[17] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. 5g security: Analysis of threats and solutions. In *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 193–199. IEEE, 2017.

[18] Shunliang Zhang, Yongming Wang, and Weihua Zhou. Towards secure 5g networks: A survey. *Computer Networks*, 162:106871, 2019.

[19] Yuelei Xiao and Shan Gao. Formal verification and analysis of 5g aka protocol using mixed strand space model. *Electronics*, 11(9):1333, April 2022.

[20] Yuelei Xiao and Yang Wu. 5g-ipaka: An improved primary authentication and key agreement protocol for 5g networks. *Information*, 13(3):125, March 2022.

[21] Yuelei Xiao and Shan Gao. 5gaka-lcco: a secure 5g authentication and key agreement protocol with less communication and computation overhead. *Information*, 13(5):257, May 2022.

[22] 3GPP. Authentication and key management for applications (akma) based on 3gpp credentials in the 5g system (5gs) ts 33.535 (release 18). Technical report, The 3rd Generation Partnership Project, June 2023.

[23] Yuchen Wang, Zhenfeng Zhang, and Yongquan Xie. Privacy-preserving and standard-compatible aka protocol for 5g. In *Proc. of the 30th USENIX Security Symposium (USENIX Security '21), Online*, pages 3595–3612. USENIX Association, August 2021.

[24] Geir M Køien. The suci-aka authentication protocol for 5g systems. In *Proc. of the 13st NISK conference on Norwegian Information Security (NISK'20), Online*, Nobember 2020.

[25] J. Arkko, K. Norrman, and J. P. Mattsson. Forward secrecy for the extensible authentication protocol method for authentication and key agreement (eap-aka' fs). IETF Draft draft-ietf-emu-aka-pfs-11 (work-in-progress), July 2023. https://datatracker.ietf.org/doc/draft-ietf-emu-aka-pfs/.

[26] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, February 1990.

[27] 3GPP. Security architecture and procedures for 5g system ts33.501 v18.2.0. Technical report, The 3rd Generation Partnership Project, June 2023.

[28] WebsiteRating. What is perfect forward secrecy? WebsiteRating, May 2023.

[29] T. Jager D. Slamanig C. Striecks D. Derler, K. Gellert. Bloom filter encryption and applications to efficient forward-secret 0-rtt key exchange. *Journal of Cryptology*, 34(13):1–59, March 2021.

[30] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 2018.

[31] Colin Boyd, Anish Mathuria, and Douglas Stebila. *Protocols for authentication and key establishment*. Springer, 2003.

[32] Adam Langley. Protecting data for the long term with forward secrecy. Google, November 2011. https://security.googleblog.com/2011/11/protecting-data-for-long-term-with.

html [Online; Accessed on September 30, 2023].

[33] Ai-fen Sui, Lucas Chi Kwong Hui, Siu-Ming Yiu, KP Chow, Wai Wan Tsang, CF Chong, KH Pun, and HW Chan. An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication. In *Proc. of the 6st IEEE Wireless Communications and Networking Conference (WCNC'05), New Orleans, LA, USA*, pages 2088–2093. IEEE, March 2005.