Computers, Materials & Continua
DOI:10.32604/cmc.2022.017338
Article

Tech Science Press

Preserving Privacy of User Identity Based on Pseudonym Variable in 5G

Mamoon M. Saeed[1], Mohammad Kamrul Hasan[2,*], Rosilah Hassan[2], Rania Mokhtar[3], Rashid A. Saeed[3,4], Elsadig Saeid[1] and Manoj Gupta[5]

[1]Electrical Engineering Department, Faculty of Engineering, Alzaiem Alazahri University, Khartoum, Sudan
[2]Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan, Malaysia (UKM), 43600, Bangi, Malaysia
[3]Department of Computer Engineering, College of Computers and Information Technology, Taif University, PO Box 11099, Taif, 21944, Saudi Arabia
[4]Department of Electronics Engineering, College of Engineering, Sudan University of Science and Technology, Khartoum, Sudan
[5]Department of Electronics and Communication Engineering, JECRC University, Jaipur, India
* Corresponding Author: Mohammad Kamrul Hasan. Email: mkhasan@ukm.edu.my

Received: 27 January 2021; Accepted: 19 May 2021

Abstract: The fifth generation (5G) system is the forthcoming generation of the mobile communication system. It has numerous additional features and offers an extensively high data rate, more capacity, and low latency. However, these features and applications have many problems and issues in terms of security, which has become a great challenge in the telecommunication industry. This paper aimed to propose a solution to preserve the user identity privacy in the 5G system that can identify permanent identity by using Variable Mobile Subscriber Identity, which randomly changes and does not use the permanent identity between the user equipment and home network. Through this mechanism, the user identity privacy would be secured and hidden. Moreover, it improves the synchronization between mobile users and home networks. Additionally, its compliance with the Authentication and Key Agreement (AKA) structure was adopted in the previous generations. It can be deployed efficiently in the preceding generations because the current architecture imposes minimal modifications on the network parties without changes in the authentication vector's message size. Moreover, the addition of any hardware to the AKA carries minor adjustments on the network parties. In this paper, the ProVerif is used to verify the proposed scheme.

Keywords: 5G; privacy and security; user identity; IMSI; authentication and key agreement (AKA)

1 Introduction

Mobile communication is important to the lives of people to accomplish daily routines; therefore, this field has been given much attention by researchers. The use of mobile communication has become widespread in business, medicine, and Internet of Things (IoT) as well as in all aspects of life [1]. IoT has potential applications in device-to-device (D2D) communications, industries, medicines, machines, and vehicles, which need extensively high data rates and data interchange. It is well known that big data and cloud computing are crucial aspects of the forthcoming fifth generation (5G) network, under which an enormous number of services run. At the same time, security and privacy become more critical for most applications [2]. The threat vector for 5G can across/accelerate with the wide spectrum of 5G services and applications and its vital role to serve society for social and economic growth as well as public safety. 5G will become a higher connected service network (SN) than the previous network generations, leading to an increased exposure to threats and attacks [3]. For criminals driven by various motives, such as cyber warfare, state-sponsored political motives, adversaries, organized crime cartels, and espionage, there is a greater chance that 5G will be a crucial target. Mastering and learning the current challenges and threats to fourth generation (4G) networks are among the best approaches to prepare for security challenges in 5G. It will inherit most of the security threats in 4G (Long-Term Evolution (LTE) and LTE Advanced) networks, as previously mentioned, due to the core IP-based nature of 5G. 3GPP ensures the user's security and privacy to allow the companies and customers to exchange information securely. Compared with previous generations, the authentication will change to mutual authentication between user equipment (UE), home network (HN), and SN rather than between UE and HN only without the SN involvement as in the second generation [4].

The Authentication and Key Agreement (AKA) protocol uses the international mobile subscriber identity (IMSI) to identify the UE in the network and accomplish the authentication process; simultaneously, the permanent identity, namely, IMSI, sends through clear text [5]. However, 3GPP uses Globally Unique Temporary Identifier (GUTI) and Cell Radio Network Temporary Identifier (C-RNTI) as well as Temporary Mobile Subscriber Identity (TMSI) for a particular mobile subscriber at diverse stages for various facilities in the 4G system architecture [6].

In this paper, authentication in the 5G system is analyzed. The paper assumes the basic architecture of the 5G system in the same way as the 4G system. In Section 2, the security and privacy of the 5G system are discussed. In Sections 3, 4, and 5, the related works, user identity privacy issues, and AKA procedure are presented, respectively. In Sections 6 and 7, the proposed solution and Enhanced Authentication and Key Agreement (EAKA) are presented and verified. In Section 8, the user identity's proposed preservation privacy based on the pseudonym variable in 5G is analyzed. Finally, Section 9 concludes the paper with remarks and recommendations.

1.1 Mobile Security and Privacy

Security and privacy in mobile communication are vital issues in which many updates and developments are centralized on the authentication and enhancement of the AKA protocol [7]. The authentication process in 4G is implemented between three parties: Home Subscriber Server (HSS), Mobility Management Entity (MME), and UE with Universal Subscriber Identity Module (USIM) and Mobile Equipment (ME), as presented in Fig. 1. The UE sends a message to the SN consisting of the IMSI (in plain text). The MME sends a message consisting of the IMSI to the HSS in the authentication vector (AV).

As presented in Fig. 1, the HSS responds to the AV request by generating Random Changeable Challenge (RAND) with 128 Ciphering Key (CK), Integrity Key (IK), and Anonymity Key (AK), and the Expected Responses (XRES) are computed over RAND challenges. AK and Authentication Management Field (AMF) keys are slightly longer than the calculated Sequence Number (SQN). Then, by using the SQN, RAND, and AMF, the Message Authentication Code (MAC) is computed by using the Network Authentication Function (f1). Subsequently, f2, f3, f4, and f5 were produced by XORing the Authentication Token (AUTN), which contains the SQN with the MAC. Finally, the AV, which consists of CK, IK, XRES, AUTN, and RAND, is created by the HSS. The AV is sent to the MME, which then forwards the AUTN and RAND upon an authentication request to the UE and saves the XRES [8].

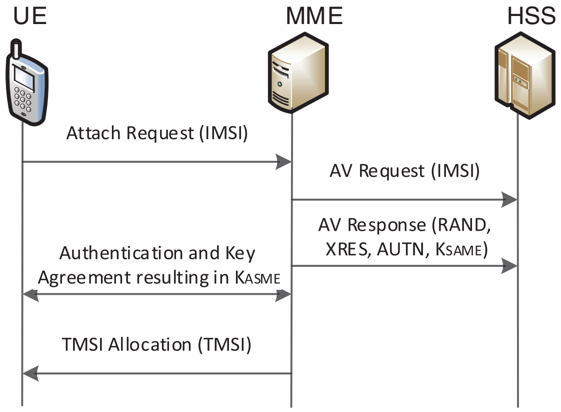

UE
MME
HSS
Attach Request (IMSI)
AV Request (IMSI)
AV Response (RAND, XRES, AUTN, KSAME)
Authentication and Key Agreement resulting in KASME
TMSI Allocation (TMSI)

Figure 1: Authentication and key agreement (AKA) in 4G

For 5G applications, i.e., healthcare, financial, and other IoT network, the authentication would ensure a high degree of security and privacy. Numerous researchers are interested in and focused on 5G security and privacy to enhance identity privacy and hide permanent IMSI. There are many proposals and researches for user identity privacy. Some studies assumed the new architecture with Network Functions Virtualization (NFV) and Software-Defined Networking (SDN) for 5G networks, as presented in Tab. 1.

Conversely, some researchers have assumed the same architecture of 4G for 5G networks with new proposals for enhanced user identity privacy. Two groups are working on security architecture and AKA proposal in 5G using the standard guideline [9]. Low computation complexity and communication overhead have been achieved due to the consideration of similar security architecture for the previous generations; the proposal can also fit easily in the preceding generations and the current architecture. Furthermore, it imposes minimal modifications to the network parties. However, a new security architecture and the AKA mechanism are also being considered for 5G with the NFV and SDN, as presented in Tab. 1. However, a significant drawback of this proposal is that devices using NFV are required to adjust the most network entities that require costly hardware to be replaced, which may be more expensive and require high computation complexity and communication overhead [10].

2 Related Works

Extensive research has studied the uses of the SN shared group keys, private key, or public-key SN while hiding the permanent identity. In [11], a procedure was developed based on identity-based encryption to challenge this type of encryption. However, the method is called privacy enhanced fast mutual authentication (PEFMA) used to encrypt the IMSI. In this procedure, the SN has public keys, and the UE does not need to join the HN. The permanent identity of UE is hidden once it is encrypted using the public key of the SN. The PEFMA can run without communicating with the HN, as the SN and UE have the public keys.

Table 1: Potential security solutions for targeted threats

Security solutions	Primary focus	Privacy	Cloud	SDN	NFV	Link
DoS, DDoS detection	Security of centralized control points	√		√	√	
Configuration verification	Flow rule verification in SDN switches			√		
Access control	Control access to SDN and core network elements		√	√	√	
Traffic isolation	Ensures isolation for VNFs and virtual slices			√		
Link security	Provide security to control channels			√		√
Identity verification	User identity verification for roaming and cloud services	√				
Identity security	Ensure identity security of users	√				
Location security	Ensure security of user location	√				
IMSI security	Secure the subscriber identity through encryption	√				
Mobile terminal security	Anti-malware technologies to secure mobile terminals	√				
Integrity verification	Security of data and storage systems in clouds		√			
HX-DoS mitigation	Security for cloud web services		√			
Service access control	Service-based access control security for clouds		√			

In [12], the Mobility Support System (MSS) is offered as a primary key to keep the permanent identity of the user in a 5G system secured with a slight effect on the communication standards. Contrarily, two crypto libraries, namely, Nettle and Open SSL, are used to implement the 5G communication standard in four Android-based schemes. The developed method for Android execution is evaluated; such an execution involves the unequal method of Elliptic Curve Integrated Encryption Scheme (ECIES). Furthermore, the effect of the applied estimation of encrypting the IMSI in 5G networks is induced by using ECIES without the MAC [13].

In [14], the structures of 3GPP AKA are presented to offer faultless onward privacy for the session key. The USIM card and mobile device interfaces do not influence the new design and, consequently, permit re-use of the present prepared USIM. However, motionless extortions continue to the sitting K'ASME key. The paper proposes to bind the belongings of a secret key K by considering a sensibly slight effect on the legacy of 3GPP constructions.

Another study investigated the IMSI encryption in which the IMSI–NC and CC data have defined and publicized the hidden identifier [15]. However, the routing requests for validation data between HN and visited network as well as the request for other IMSI data to be publicized within the HN are discussed here.

A proposal on Quantum Key GRID based the Authentication and Key Agreement in 5G (QKG-AKA) for dynamic security association, which has also been deployed in 4G [16,17]. Another study proposed the efficient and lightweight secure SEL-AKA algorithm for the 5G scheme. The suggested mechanism is designed regardless of the use of the global public-key infrastructure. These encryption solutions offer user anonymity by employing numerous methods for encrypting the identity via private-key or public-key cryptography. However, the additional calculation and complication may result in increased bandwidth and calculation period and may need new parameters.

Researchers have used pseudonyms to hide the permanent identity in 5G; for instance, [18] proposed a novel scheme for defending the permanent identity by regenerating a pseudonym in the intermediate of the HN and the UE. The pseudonym is locally initiated at the HN and UE, leading to a poor performance by the available USIMs. Two main stages are suggested in this work. First is fast attachment by the UE when the SN or HN does not join any pseudonym. In this situation, the UE allocates a TMSI by the SN and a pseudonym P by the HN. At the second stage, the UE is enforced to detect itself using P, whereas the UE TMSI is no longer at risk within the SN, and a new pseudonym will be used to support the unlinkability.

In [19,20], a new version of the 5G AKA protocol is suggested, in which random numbers replace the sequence numbers since the existing 5G (USMs) can accomplish randomized asymmetric encryption processes; thus, the utilization of random numbers for AKA protocol is conceivable. Furthermore, the suggested solution offers two extra security topographies, i.e., forward security and post-compromise security, which do not exist in the present 5G AKA procedure. Then, the performance is evaluated (both the communication efficiency and computation) by the suggested AKA protocol, and its results are compared with those of the presented 5G AKA procedure.

These methods attempt to develop pseudonym in 5G systems. However, the techniques have various drawbacks: the administration of pseudonyms requires superfluous handling exertion and memory cost. The distribution of pseudonyms to all UE from the system requires an extra bandwidth. Finally, numerous studies suggested new architectures and formats in 5G networks. For example, in [20], a general idea was provided for the security contests in SDN, NFV, and clouds as well as customer solitude contests. Moreover, the authors recommended that shared activities and trust imitations must occur among numerous parts in the procedure, such as network operator, service provider, application designer, user, and manufacturer, on information using and storing to preserve the user privacy in 5G networks.

In [21], the user privacy issues in LTE and WiMAX have been addressed at the MAC and physical layers. The privacy improvement in 5G was indicated by the production of a flexible 5G system architecture that authorizes the generation of trust replicas. Reference [22] proposed two key agreement protocols and the Privacy-Preserving Authentication (PPAKA-IBS and PPAKA-HAMC) to ensure protected and unknown communications in the D2D group.

In [23], in a new structure designed for 5G network security, the scrutiny of independence management and flexible validation of AKA are addressed. The AKA in the 4G network is proven by the symmetric-key, whereas the 5G network needs validation between the UE and SN and other third parties, such as service suppliers. The hybrid and flexible validation of UE could be performed practically using three diverse methods: validation by the service supplier and SN, validation by the service supplier only, and validation by the SN only. Conversely, in [24], 5G is declared to be accepting novel-based multiparty ecologies, in which many performers can cooperate in the overhaul source. According to the authors 5G intensively relies on software replicas, such as slicing and SDN. It is also suggested that the precursors of the 5G system need to go through the regularity of the systems while confirming the users' privacy. The authors in [25] conducted a similar study as [26]; however, they conducted correlational research and presented SDN into the 5G network to support operative validation handover (HO) and fortification of privacy. In [27], an approach based on a trusted third party worked like a disseminated network between the service supplier and the customer. In [28], the complete official archetypal of a procedure from the AKA group is provided. Moreover, missing security objects are identified, and exact requests are removed from the 3GPP principles describing 5G.

In [29], 4G-RAM is proposed to discourse the current subjects of the 4G network and consider it as an excellent communication and information technology network that suits the increasing 5G demands and acute PS schemes. However, the verification and re-authentication processes of 4G-RAM indicated that integrity and confidentiality are sheltered with the dynamic LTE K. Therefore, it overwhelmed the critical privacy susceptibilities of the LTE network, such as the user tracking based on redirection, IMSI, AV de-synchronization, denial-of-service attacks, and man-in-the-middle attack prevention. 4G-RAM is used to minimize access dormancy by suggesting PEPS-AKA and 4G + FRP that contain slight verification signaling related to other new solutions.

Most of the methods aimed to provide mutual entity authentication in 5G networks and suggested a novel verification procedure, with complete communal verification between the SN and UE. Moreover, these methods modified the AKA protocol, message elements, SN, and UE, as well as new extra components, such as NVF and SDN. This is a significant drawback because using those methods is essential to the adjustment of the bodily level network, which could lead the hardware to be replaced; however, this may be more expensive than the conventional AKA protocol.

As discussed above, research on the critical topic of privacy in 5G networks has been conducted. Thus, their comparison is presented in Tab. 2. A snapshot of the related works is also shown.

Table 2: Protocol comparison

Papers	Methods of IMSI hiding	Communication overhead	Auth. message size	Computation complexity
[22,26]	Encryption	High	No change	High
[13,14]	pseudonyms	Low	Change	Medium
[16,17]	SDN, NVF, and change AKA	High	Change	High

Table 3: Results of the automatic verification of the fixed procedures

Properties	Identification	AKA	EAKA
Security IMSI	√	x	√
CK, IK	NA	√	√
Confidential	NA	√	√
Information authentication	NA	√	√
Integrity	NA	√	√

Note: √ proved to hold **x** Attack found **NA** Not Applicable.

3 User Identity Privacy Issues

User identity privacy is the main issue in mobile communication security, whereas the IMSI exposure is the main issue in user identity privacy. The IMSI is used in the network to identify the UE; therefore, assailants may capture it. Such a vulnerability is usually noted as IMSI catching [30]. For that, the 3GPP allocates several diverse short-term identities, such as C-RNTI, GUTI, and M-TMSI, to a mobile user for different networking services within the mobile network. To improve the confidentiality of the UE identity, the mobile user, instead of using the permanent one (IMSI), can use these temporary identities to identify itself to start a new service request from the network [31,32]. Although this procedure is employed to enhance user identity privacy, the user's permanent identity stays exposed to IMSI catchers. There are some circumstances where the UE uses the IMSI (in clear text) to identify itself; following are some cases for such scenarios:

(a) The SN might not get well the GUTI of the UE.
(b) UE starts the first attachment.
(c) UE performs the HO between MMEs, and the new MME could not get the GUTI of the UE from the previous MME.
(d) MME could not recover the permanent identity of the UE.

In the 5G system, user identity privacy must be improved to keep an extra privacy level and to achieve safe interchanging of information with mutual authentication. In the 5G system, a robust identity administration mechanism is requested to defend the user's identity from unauthorized access of users. The 5G network will be dealing with the environment by different bearings and comprise several investors.

4 AKA Protocol

To provide both the established and shared IK and cipher key CK and to achieve mutual authentication between the HN and UE, the AKA process is applied for the physical channel of E-UTRAN. The details of the AKA protocol are discussed in a previous report [14].

The Evolved Packet System–Authentication and Key Agreement (EPS-AKA) process involves two sub-processes. The first sub-process is directed toward the AKA whereas the second to the distribution of validation data from the HN to the MME. The first sub-algorithm is executed by the MME while receiving the authentication data response from the HSS. Contrarily, the second sub-process is executed by the MME while receiving the attached request from the UE.

The HSS and UE share a permanent top-secret key K. Two SQNs, i.e., SQN_{UE} and SQN_{HE}, are also preserved by the UE HSS to enhance the network's authentication. SQN_{UE} is the uppermost sequence number acknowledged by the USIM, whereas SQN_{HE} is a counter for each UE equipment that is utilized to generate the AVs in the HSS. The EPS-AKA provides a set of MAC functions {f1, f2} and key generation functions {f3, f4, f5}. K, as presented in Fig. 2, organizes the functions.

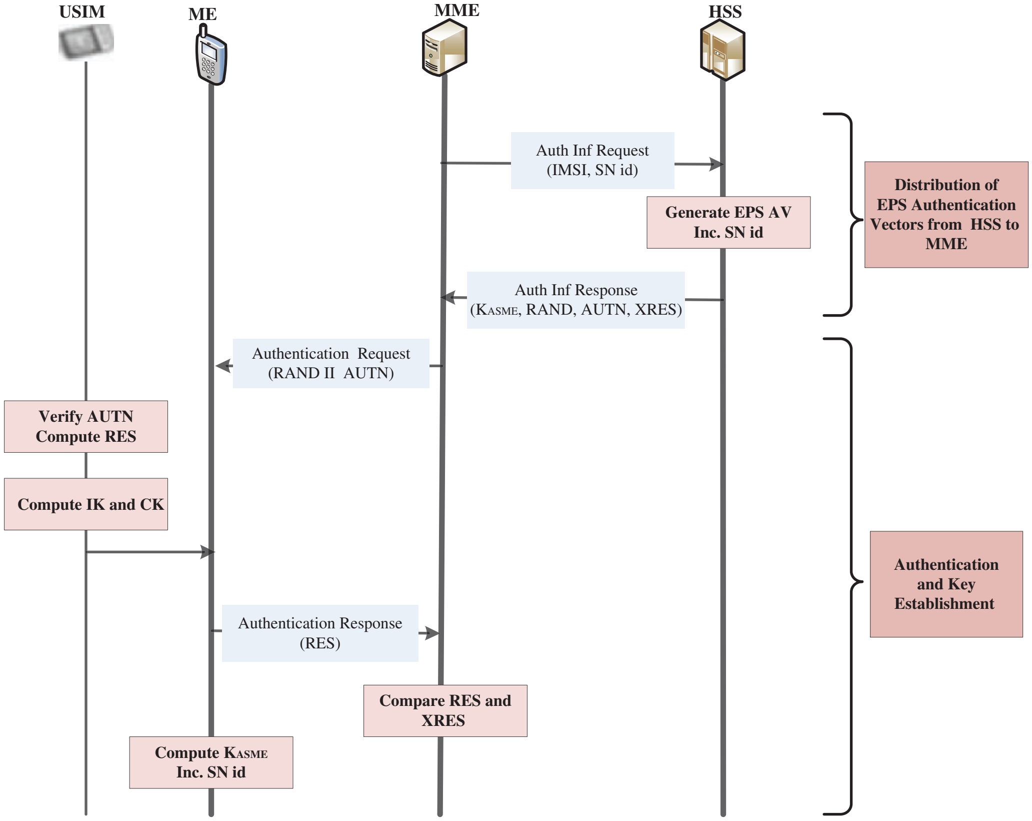


Figure 2: AKA protocol by using the IMSI to identify the UE in the network and accomplish the authentication process authentication and key agreement (AKA)

5 Privacy-Preserving Scheme for the 5G System

To preserve user identity privacy, the permanent identity of the IMSI must be hidden completely by replacing it with the Variable Mobile Subscriber Identity (VMSI); the HSS node can only plan its IMSI for a specific UE. The UE uses the VMSI when it is required to represent its IMSI. In this way, the UE identity privacy is well maintained because the UE and HSS only know the IMSI of the UE, as presented in Fig. 3.

The HSS sends a fresh, unpredictable VMSI called (V_{FRESH}) that is confidential to the UE in the authentication process. To implement this idea, we suggest essential variations in the features and usages of some basic validation boundaries, which are SQN and RAND. In addition, we recommend encryption of the RAND using SQN token as a key, generated randomly at every run for the EAKA protocol, and using the challenge RAND to provide the UE with the sequence number SQN_{HE} and the new VMSI. The RAND challenge is secured, including the token SQN_{HE}, to get the UE sequence number (SQN_{UE}). The UE uses the RAND challenge to get the new SQN_{HE} and the new VMSI (V_{NEW}) through a regular authentication procedure. The UE replaces its VMSI with a new VMSI (V_{NEW}), which would be used the next time the authentication process is carried out. In implementing the proposed solution, the EAKA protocol is introduced. Tab. 3 presents all the acronyms and their descriptions, which are used in the ProVerif code, obtained figures, and algorithms.

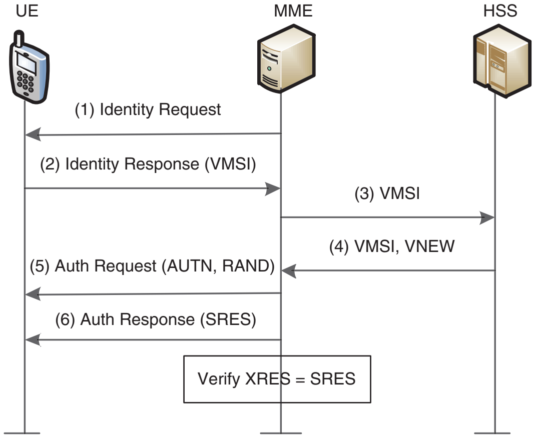


Figure 3: Privacy-preserving scheme for the5G system using EAKA

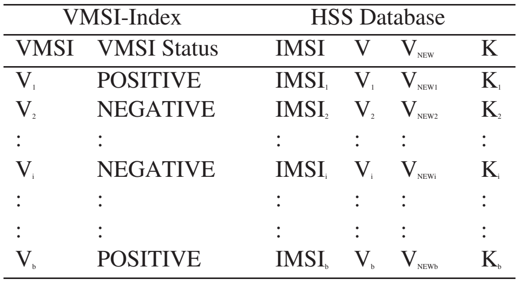
6 Enhaned AKA (EAKA) Protocol

In the beginning, the UE transmits a message containing its VMSI; the message also includes the $VMSI_{FIRST}$ to the SN (MME). Whenever the UE wants to join the network, the MME sends an endorsement data request to the HN (HSS) for the incoming VMSI. The HSS generates a new VMSI and sends it to the MME, and the MME then forwards the VMSI to the UE. The details of the EAKA protocol are discussed in Sections A and B.

A. Enhanced HSS Algorithm

Upon enhancing the HSS algorithm, there are two VMSI values for each UE stored in HSS, namely, V and V_{NEW}. V is employed to support the VMSI currently used by the UE. However, V_{NEW} sends the newly produced VMSI assigned to the UE to be used in the following stages to replace its permanent identity. The HN (HSS) saves the extra values V and V_{NEW} in its database with the secret key K and the IMSI for each UE, as presented in Fig. 4.

This procedure ensures that the HSS can continuously communicate with the current VMSI saved in the UE with the original IMSI saved in the HSS to identify each UE. Likewise, the SN that hosts the MME preserves V and V_{NEW} in its database for every UE within its area of service to be able to identify each user's equipment. There is a permanent memory storage that contains $b = 2^{34}$ unique VMSI entrances named as VMSI-Index and saved in the HSS (see Fig. 3). Every VMSI entrance in the VMSI-Index has a value called VMSI status. A VMSI is previously assigned to several UEs that have a NEGATIVE indicator in its VMSI status, suggesting that other UEs use this VMSI.



VMSI-Index		HSS Database			
VMSI	VMSI Status	IMSI	V	V_{NEW}	K
V_1	POSITIVE	$IMSI_1$	V_1	V_{NEW1}	K_1
V_2	NEGATIVE	$IMSI_2$	V_2	V_{NEW2}	K_2
:	:	:	:	:	:
V_i	NEGATIVE	$IMSI_i$	V_i	V_{NEWi}	K_i
:	:	:	:	:	:
:	:	:	:	:	:
V_b	POSITIVE	$IMSI_b$	V_b	V_{NEWb}	K_b

Figure 4: The VMSI-Index and the HSS's database

A VMSI status with a POSITIVE indicator for a specific VMSI in the VMSI-Index indicates that the VMSI is available and is not used by any UE. Finally, a function ENCODE is specified by an operator and used to encrypt V_{NEW} and SQN_{HE} with the key SQN in the HSS to create the encrypted RAND. To implement the EAKA protocol, there are some changes in the HSS protocol presented in Algorithm 1.

Firstly, the HSS should confirm that an incoming VMSI is legal and currently not used by several UEs by discovering the received VMSI in the database of the HSS before it decides whether to receive a VMSI-based validation request or not. The request is barred when no attachment is found. The HSS locates the secret key K and the corresponding UE's IMSI when a match is found.

The HSS issues a not-in-use (fresh) VMSI named V_{FRESH} to the assigned UE, and information linked to the UE is updated at the HSS like the sequence number SQN_{HE} and the VMSIs, after the HSS validates that the received VMSI is the latest VMSI transmitted to the UE by checking VMSI $= V_{NEW}$.

The SQN_{HE} is handled at the HSS, which confirms that the previous validation process was successful. Once it receives the V_{NEW} from the UE, the HSS immediately updates the SQN_{HE} (see Algorithm 1).

Algorithm 1: The enhanced HSS and EAKA protocol

```
The enhanced HSS and EAKA protocol
Step 1.  If VMSI is not valid, then drop the request and exit
Step 2.  Else
Step 3.  VMSI = $V_{NEW}$ Then
Step 4.  Update VMSI-Index → $V_{FRESH}$
Step 5.  Update V → VMSI-Index
Step 6.  Update $V_{NEW}$ → V
Step 7.  Update $V_{FRESH}$ → $V_{NEW}$
Step 8.  Update $SQN_{HE}$+ 1→$SQN_{HE}$
Step 9.  $\{0, 1\}^{48}$ → SQN
Step 10. ENC(SQN,(s = ($V_{NEW}$, $SQN_{HE}$))) →RAND
Step 11. f1(K,SQN, AMF,RAND) → MAC
Step 12. f3(K,RAND) → CK
Step 13. f4(K,RAND) → IK
Step 14. f5(K,RAND) →AK
```

(Continued)

```
Step 15. (SQN XOR AK,AMF,MAC)$\rightarrow$ AUTN
Step 16. (AUTN, RAND, XRES, CK, IK) $\rightarrow$ AV
Step 17. End If
Step 18. Go to step (4)
```

The HSS generates AV when it receives the request message as follows:

1. Validate whether the incoming VMSI is now used by any UE or not. If the VMSI is not in use, the HSS rejects the request.
2. If the UE transmits the VMSI (V_{NEW}), the HSS updates the VMSI and other UE's related information at the HSS.
   2.1 From the VMSI-Index HSS selects a fresh VMSI, i.e., V_{FRESH} update VMSI-Index $\rightarrow V_{FRESH}$
   2.2 Store VMSI in V. update V$\rightarrow$ VMSI-Index
   2.3 The V and V_{NEW} are kept within the UE's IMSI at the HSS-database update.update $V_{FRESH} \rightarrow V_{NEW}$
   update $V_{NEW} \rightarrow V$
   2.4 The sequence number SQN_{HE} is updated.
   $SQN_{HE}+ 1\rightarrow SQN_{HE}$
3. A new random key SQN is generated.
   $SQN = (0, 1)^{48}$
4. A challenge RAND is computed by encrypting V_{NEW} and SQN_{HE} using ENCODE with SQN as the input key.
   $RAND = ENCODE\ (SQN, (s = (SQN_{HE}, V_{NEW})))$
5. MAC is computed by function (f1) over RAND, AMF, and SQN.
   $MAC = f1(K, (RAND, AMF, SQN)$
6. The residual authentication parameters are computed: AK, IK, AUTN, XRES, and CK, as presented in Fig. 4.
7. The AV is transmitted to the MME, which must forward RAND and AUTN to the UE.

First, the HSS confirms that an incoming VMSI is valid and now in use by other UE locating the incoming VMSI in the HSS's database (step 1), before it decides whether to accept the VMSI-based authentication demand or not. The request is rejected when no matches are found. Moreover, the HSS locates the secret key K and the corresponding UE's IMSI when a match is found. In step 2, the HSS allocates a fresh (not-in-use) VMSI called V_{FRESH} to the concerned UE and updates information related to the UE in the HSS like the sequence number SQN_{HE} and the VMSIs, after the HSS confirms that the VMSI that arrived is the latest one transmitted to the UE by checking VMSI = V_{NEW} (sub-steps 2.1 through 2.4).

B. The Enhanced UE Algorithm

The algorithm can be enhanced using a unique VMSI value that must be preserved in the UE smart card (USIM). The service provider embeds an individual VMSI value named $VMSI_{FIRST}$ into the USIM before the first connection. The HSS database also stores the $VMSI_{FIRST}$ value in the V_{NEW} for each USIM's IMSI and is set to the NEGATIVE status of the $VMSI_{FIRST}$ entrance in the VMSI-Index. Throughout the first run of the EAKA protocol, the $VMSI_{FIRST}$ is used only once. In other times, the specific function DECODE is used by the service provider to decrypt a RAND at the UE and use the unsystematic key SQN comprised in AUTN to extract the V_{NEW}

and SQN_{HE}. When UE receives AUTN and RAND, it validates the AUTN and calculates the validation reaction message, as presented in Algorithm 2.

Algorithm 2: The enhanced UE and EAKA protocol.

The enhanced UE and EAKA protocol.

```
Step 1.  If step (5) done
Step 2.  $f5(K,RAND) \rightarrow Ak$
Step 3.  $AK$ XOR $AUTN(SQN$ XOR $AK) \rightarrow XSQN$
Step 4.  $f1(K,XSQN,AUTN.AMF,RAND) \rightarrow XMAC$
Step 5.  Verify $XMAC = AUTN.MAC$
Step 6.  $DEC(RAND) \rightarrow s$
Step 7.  $s.SQN_{HE} \rightarrow XSQN$
Step 8.  $s.V_{NEW} \rightarrow XVMSI$
Step 9.  Verify $XSQN = SQN_{UE} + 1$
Step 10. Update $XSQN \rightarrow SQN_{UE}$
Step 11. Update $XVMSI \rightarrow VMSI$
Step 12. $f2(K,RAND) \rightarrow SRES$
Step 13. $f3(K,RAND) \rightarrow CK$
Step 14. $f4(K,RAND) \rightarrow IK$
Step 15. End if
Step 16. Go to step (6)
```

(1) The AK is computed by using the function (f5).
(2) The random key XSQN is extracted.
(3) XMAC is computed over AMF, XSQN, and RAND.
(4) The MAC included in the AUTN is computed using XMAC.
(5) If XMAC equals MAC, RAND is decrypted using DECODE with the input key XSQN to recover $s.SQN_{HE}$ and $s.V_{NEW}$.
(6) The received sequence number is verified as $SQN_{UE} + 1 = s.SQN_{HE}$
(7) The AUTN is verified successfully if SQN_{HE} is in the right range.
(8) The sequence number SQN_{UE} is updated, and the IK, CK, and response RES are computed.
(9) The VMSI updates to $s.V_{NEW}$.
(10) The keys IK and CK are stored in the UE, and the RES is sent back to the MME. The MME compares the XRES, which was received from the HSS with the response (SRES) of the UE. The authentication is successful if $XRES = SRES$.

The MME sends an authentication to reject the message to the UE if $XRES \neq SRES$, as presented in Algorithm 2.

C. Formal Verification

For the performance measurement and implementation of the cryptographic protocols, the ProVerif tool is used. This tool is not limited to cryptographic primitives; it also supports hash functions, asymmetric and symmetric encryption, digital signature evidence, etc. ProVerif is compatible with the Linux, Mac, and Windows operating systems. It is used to verify the capability properties, declarations, and observational and communication correspondence.

These competencies are essential and valuable to the security and privacy domain. ProVerif studies, examines, and validates privacy possessions. Furthermore, developing possessions such as verifiability, privacy, and traceability could also be deliberated. The proposed protocol is analyzed in terms of the infinite number of sittings and infinite space of messages. Also, ProVerif is proficient in the modernization of attack: wherever the possessions could not be verified, ProVerif attempts to rebuild an operation suggestion that fabricates the wanted controls. Some authors suggested a new architecture, and others proposed a novel verification procedure, with complete communal verification between the SN and UE. Contrarily, others modified the AKA protocol, message elements, SN, and UE, as well as new extra components such as NVF and SDN.

In this paper, the suggested EAKA enforces protected validation and identification and preserves the privacy of the UEs, i.e., unlinkability and user anonymity threats, as presented in Tab. 3, which are applied in the fixed procedure by ProVerif, as shown in the Appendix. The ProVerif code is also given in the Appendix. The proposal's fundamental idea is that an outside observer (enemy) cannot see any differences in the procedure sequence because any two implementations vary only in user identities where the evidence is produced by utilizing the database of messages [32–34].

7 EAKA Solution Benchmarking

In this section, the current solution is compared with some very related works in the literature. The benchmarking starts with methods of the first classification, i.e., methods that adopt public-key cryptography to enhance privacy. This classification comprises the works of [35–37]. Utilization of public-key cryptography to encrypt the IMSI was the core characteristic of the operations of this class.

The core dissimilarity between the EAKA solution and the existing solutions with regard to user identity privacy is a metaphysical one. The existing methods for the UE require the accomplishment of the operation of encryption before the transfer of the IMSI. Then, the HSS decrypts the IMSI, which is encrypted before processing the demand, as presented in Fig. 5. Fig. 6 shows the computation delay, in which the proposed solution achieved lower computation delays compared with the existing ones. Although the UE's privacy can be conserved throughout the attachment process, the public-key cryptography can enhance it. The high processing, data traffic overhead, and complexity as a product of communicating encrypted IMSIs from one MME to another in the authentication procedures and HO are still substantial. The various method proposals must study the UE's processing power to preserve the processing exertions tolerable at the UE. It presents the issue of improving user identity confidentiality for 5G and new concepts using the 3GPP standard that locally manages a randomized address for the UE's WLAN MAC address as a replacement for a generally managed MAC address to alleviate the recognized risk.

In addition, a different version of the 5G AKA procedure is proposed. In this new procedure, the SQNs are swapped with random numbers. The current USIMs are now capable of performing randomized asymmetric encryption operations. The use of random numbers for the 5G AKA protocol is conceivable.

The EAKA solution is better than the existing ones; the existing methods are complicated and have numerous cryptography functions. The UE's WLAN MAC management and a different version of the 5G AKA would require memory cost and extra processing effort. Thus, the amount of processing effort for user elements is enormous as they are re-processed with every authentication process.

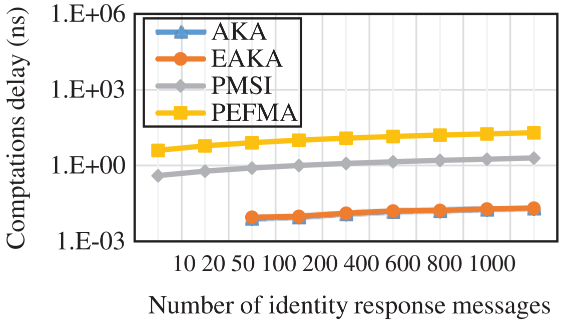


Figure 5: Identification delay comparison among AKA, EAKA, PMSI, and PEFMA

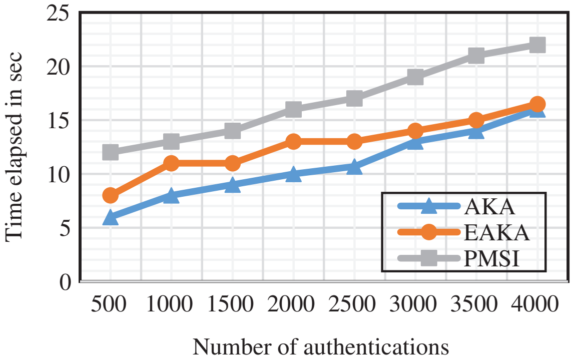


Figure 6: Authentication load at HSS

Additional variance with [19] lies in the management of the SQN. In fact, by reiterating and transmitting PMSI that included multiple false attachment requests to the HN, an adversary can carry out the server HSS to be out of sync. This is because the method proposed in [19] continuously increases the sequence number at the HSS, which would allow an attacker to conduct a denial-of-service (DoS) attack toward the HSS. Conversely, the EAKA solution eliminates this probability as the sequence number is increased at both the HN and UE only on a successful run of the EAKA protocol. Figs. 6 and 7 show the computation overhead on the HSS and UE, comparing the PMSI, AKA, and EAKA. These figures show that the time elapsed in the EAKA is closer to that in the AKA than that in the PMSI, and the time elapsed in the UE is more diminutive than that in the HSS because the overhead in the UE is negligible. Eqs. (1) and (2) are used to calculate the time elapsed:

$$P = P(t_e > t_r) = 1 - P(t_e \leq t_r) \tag{1}$$

$$P(t_e \geq t_r) = \int_{t=0}^{\infty} \int_{t_e=0}^{t} f_e(t_e) f_r(t) dt_e dt \tag{2}$$

When the EAKA is applied in ProVerif, an outside attacker cannot see any differences in the procedure consequence because many implementations vary only in user identities. Moreover, when the number of authentication increases, the IMSI security also increases. Every time the VMSI is randomly changing, the choices become difficult for the attacker, the same as AKA, because the IMSI is kept without any modification. Fig. 8 presents the level of IMSI security in AKA remains constant regardless of the number of authentications. In comparison, the IMSI security level in EAKA is increased because the values of the VMSI randomly change.

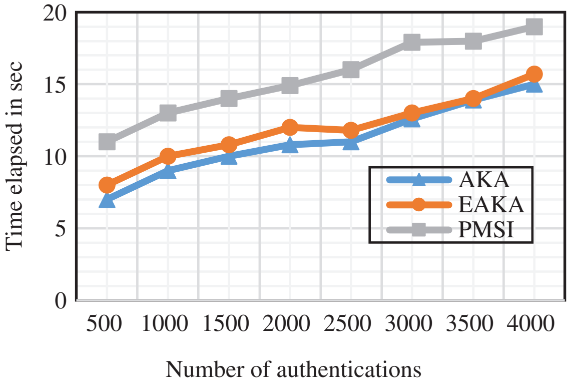


Figure 7: Authentication load at UE

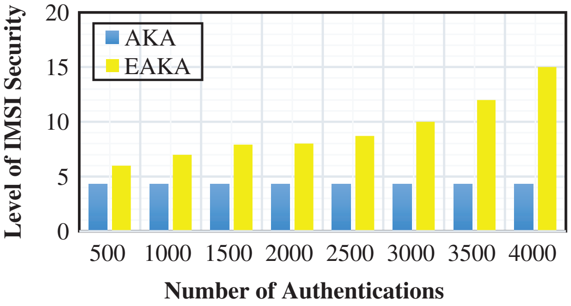


Figure 8: IMSI security comparison between AKA and EAKA

The proposed scheme sets the mainstream of computation overhead in the HN, which requires memory to save the extra values V and V_{NEW} in its database with the secret key K and the IMSI for each UE, as presented in Fig. 4. In comparison to the conventional method using AKA, a negligible computation overhead is placed in the UE. The computation overhead is negligible as the HN's computational power is unlimited (see Fig. 6). As shown in the process of the algorithm in the UE, we also suggest that the overhead of computation in the UE is negligible, as presented in Fig. 7.

8 Conclusion

This paper presented a solution to preserve user identity privacy in the 5G system by enhancing the AKA protocol (EAKA), which proposed a variable pseudonym to identify the user in the 5G network rather than using permanent identity in the previous generations. The EAKA hides the identity of the user completely by using a temporary identity, i.e., VMSI. The temporary identity changes in every attachment, and the permanent IMSI is never used, even in the first attachment. The proposed solution does not add any computation overhead to the UE or the network, except light processing in the HSS. The proposed solution is compared with the AKA and the existing works. It is demonstrated that the EAKA can be used to enhance user privacy in the 5G network without any change in the AKA procedure or architecture. Moreover, it can be implemented in the previous generations to enhance user privacy, as verified by the ProVerif tool.

Funding Statement: The Universiti Kebangsaan Malaysia (UKM) Research Grant Scheme GGPM-2020-028 funded this research.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Thiel and I. Larsen-Ledet, “The role of pseudonymity in mobile e-participation,” in *Proc. ICSS*, Hawaii USA, pp. 2880–2889, 2019.

[2] Q. AliID, N. Ahmad, A. Malik, W. Rehman, A. Din, *et al.*, “ASPA: Advanced strong pseudonym based authentication in intelligent transport system,” *PLOS One*, vol. 14, no. 8, pp. 79114–79128, 2019.

[3] H. Choudhury, “Enhanced anonymity: Customized for roaming and non-roaming IoT-devices in 5gmobile network,”in *Proc. ISEA-ISAP*, Guwahati, India, pp. 55–62, 2020.

[4] I. Gharsallah, S. Smaoui and F. Zarai, “An efficient authentication and key agreement protocol for a group of vehicles devices in 5G cellular networks,”*IET Information Security*, vol. 14, no. 1, pp. 21–29, 2020.

[5] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma *et al.*, “Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9390–9401, 2020.

[6] J. Gomez, D. Carrillo, R. Perez and A. Skarmeta, “Secure authentication and credential establishment in narrowband ioTand 5G,” *Journal, Sensors*, vol. 20, pp. 882, 2020.

[7] J. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano *et al.*, “What will 5g be?,” *IEEE Journal on Selected Area in Communications*, vol. 32, no. 6, pp. 1065–82, 2014.

[8] R. Lu, L. Zhang, J. NI and Y. Fang, “5G Vehicle-to everything services: Gearing up for security and privacy,” in *Proceedings of the IEEE*, vol. 108, no. 2, pp. 373–389, 2020.

[9] L. Jiang, X. Chang, J. Bai, J. Misic, V. Misic *et al.*, “Dependability analysis of 5G-AKAauthentication service from server and user perspectives,”*IEEE Access*, vol. 8, pp. 89562–89574, 2020.

[10] S. Islam, O. Othman, K. Aisha–Hassan, A. Hashim, M. Hasan *et al.*, “Design and evaluation of a multihoming–based mobility management scheme to support inter technology handoff in pnemo,” *Wireless Personal Communications*, vol. 114, no. 2, pp. 1–14, 2020.

[11] H. Kamrul, A. Ismail, S. Islam, W. Hashim, M. Ahmed *et al.*, “A novel hgbbdsa-cti approach for subcarrier allocation in heterogeneous network,” *Telecommunication Systems*, vol. 70, no. 2, pp. 245–262, 2017.

[12] J. Khurpade, D. Rao and P. Sanghavi, “A survey on iot and 5g network,” in *Proc. ICSCET*, Mumbai, India, pp. 1–3, 2018.

[13] P. K. Agyapong, M. Iwamura, D. Staehle, W. Kiess and A. Benjebbour, “Design considerations for a 5g network architecture,” *IEEE Communications Magazine*, vol. 52, no. 11, pp. 65–75, 2014.

[14] 3GPP TS 23.003. “Numbering, addressing and identification,” 2016.

[15] A. Muthana and M. Saeed “Analysis of user identity privacy in lte and proposed solution,” *International Journal of Computer Network and Information Security*, vol. 9, no. 1, pp. 54–63, 2017.

[16] A. Muthana, M. Saeed, A. Ghani and R. Mahmod, “Enhancing privacy of paging procedure in lte,” *International Journal of Engineering and Science Invention*, vol. 7, no. 2, pp. 42–50, 2018.

[17] H. Ghafghazi, A. El-Mougy and H. Mouftah, “Enhancing the privacy of lte-based public safety networks,” in *Proc. ICLCNW*, Edmonton, Canada, pp. 753–760, 2014.

[18] F. van den Broek, R. Verdult and J. de Ruiter, “Defeating imsi catchers,” in *Proc. CCS*, New York, NY, USA, pp. 340–351, 2015.

[19] M. Saeed, A. Saeed. and E. Saeid, "Preserving privacy of paging procedure in 5g using identity-division multiplexing," in *First Int. Conf. of Intelligent Computing and Engineering (ICOICE)*, Yemen, pp. 1–6, 2019.

[20] M. K. Hasan, M. Ahmed, A. H. Hashim, A. Razzaque, S. Islam *et al.*, "A novel artificial intelligence based timing synchronization scheme for smart grid applications," *Wireless Personal Communications*, vol. 114, no. 2, pp. 1067–84, 2020.

[21] M. Saeed, R. Saeed and E. Saeid, "Survey of privacy of user identity in 5g: Challenges and proposed solutions," *Saba Journal of Information Technology and Networking*, vol. 7, no. 1, pp. 1–24, 2019.

[22] G. Arfaoui, J. Manuel, S. Vilchez and J. Wary, "Security and resilience in: Current challenges and future directions," in *Proc. Trustcom/BigDataSE/ICESS*, Sydney, NSW, Australia, pp. 1010–1015, 2017.

[23] E. Cobo, J. Nakarmi, M. Näslund and K. Norrman, "Subscription identifier privacy in 5g systems," in *Proc. MoWNeT*, Avignon, France, pp. 1–8, 2017.

[24] J. Arkko, K. Norrman, M. Näslund and B. Sahlin, "Ericsson research, a usim compatible 5g aka protocol with perfect forward secrecy," in *Proc. Trustcom/BigDataSE/ISPA*, Helsinki, Finland, pp. 1205–1209, 2015.

[25] M. Khan, V. Niemi and P. Ginzboorg, "IMSI-Based routing and identity privacy in 5g," in *Proc. OIA*, Jyväskylä, Finland, pp. 338–343, 2018.

[26] M. Hasan, A. Ismail, S. Islam, W. Hashim and B. Pandey, "Dynamic spectrum allocation scheme for heterogeneous network," *Wireless Personal Communications*, vol. 95, no. 2, pp. 299–315, 2017.

[27] S. Vij and A. Jain, "5g: Evolution of a secure mobile technology," in *Proc. OIA, INDIACom*, New Delhi, India, 2016.

[28] R. Mokhtar, S. Khatun, A. Borhanuddin, A. Ramli and R. A. Saeed, "Authentication and user presence monitoring technique for mobile computers using jsr82," in *Proc. BICET*, Bandar Seri Begawan, Brunei, vol. 2, pp. 133–136, 2005.

[29] I. Memon, R. A. Shaikh, M. Hasan, R. Hassan, A. Haq *et al.*, "Protect mobile travelers information in sensitive region based on fuzzy logic in technology," *Security and Communication Networks*, vol. 18, pp. 1–12, 2020.

[30] Z. May, M. Alam, K. Husain and M. Hasan, "An enhanced dynamic transmission opportunity scheme to support varying traffic load over wireless campus networks," *PLOS One*, vol. 15, no. 8, pp. 1–10, 2020.

[31] X. Duan and X. Wang, "Authentication handover and privacy protection in 5ghetnetsusing software-defined networking," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 28–35, 2015.

[32] S. Islam, A. H. Hashim, M. H. Habaebi and M. K. Hasan, "Design and implementation of a multihoming-based scheme to support mobility management in nemo," *Wireless Personal Communications*, vol. 95, no. 2, pp. 457–73, 2017.

[33] S. Islam, M. Hasan and A. Hashim, "A packet delivery cost analysis of a flow-enabled proxy nemo scheme in a distributed mobility anchoring environment," *ElektronikairElektrotechnika*, vol. 26, no. 4, pp. 65–71, 2020.

[34] S. Islam, A. Hashim, M. Habaebi and M. Hasan, "Novel multihoming-based flow mobility scheme for proxy NEMO environment: A numerical approach to analyse handoff performance," *Scienceasia*, vol. 43, no. 1, pp. 27–34, 2017.

[35] M. Khalid, A. Rehman, P. Chaudhary, X. Li, F. Wu *et al.*, "Revised anonymous authentication protocol for adaptive client server infrastructure," *International Journal of Communication Systems*, vol. 33, no. 4, pp. e4253, 2020.

[36] K. Prasad, K. R. Kashyap, K. Sutradhar, T. Kumar and S. Kumar, "Secure authentication scheme with privacy preservation policy on mobile cloud computing environment," *International Journal of Recent Technology and Engineering*, vol. 8, no. 1S4, pp. 374–378, 2019.

[37] B. Blanchet. "Proverif: Cryptographic protocol verifier in the formal model," 2020. [Online] Available: https//www.proverif.ens.fr/, (Accessed on 13/04/2020).

Appendix

```
in(s2 s, (=ID_RESPONSE, vmsi: bitstring));
out(s2 h, vmsi);
in(s2 h, (rand: bitstring, (sqn_ak: bitstring, amf: bitstring, mac: bitstring), xres: bitstring, ck: key, ik: key));
let autn = (sqn_ak, AMF, mac) in
out(s2 s, (AUTH_REQUEST, rand, autn));
in(s2 s, (=AUTH_RESPONSE, =xres)).
let home(id1: bitstring, vmsi1_old: bitstring, vmsi1_new: bitstring, sqn1: bitstring, id2: bitstring, vmsi2_old: bitstring, vmsi2_new: bitstring, sqn2: bitstring) = new ksqn:bitstring;
in(s2 h, vmsi_in: bitstring);
let vmsi_new = switch(vmsi_in, vmsi1_old, vmsi1_new, vmsi2_old, vmsi2_new) in
let k = getKey(switch(vmsi_in, vmsi1_old, id1, vmsi2_old, id2)) in
let sqn = switch(vmsi_in, vmsi1_old, sqn1, vmsi2_old, sqn2) in
let rand = enc((vmsi_new, sqn), tc(ksqn)) in
let mac = f1(k, sqn, AMF, rand) in
let xres = f2(k, rand) in
let ck = f3(k, rand) in
let ik = f4(k, rand) in
let ak = f5(k, rand) in
let autn = (xor_enc(ksqn, ak), AMF, mac) in out(s2 h, (rand, autn, xres, ck, ik)).
```