User-to-User Mutual Authentication and Key Agreement Scheme for LTE Cellular System

Mohammed Ramadan[1], Fagen Li[1], ChunXiang Xu[1], Abdeldime Mohamed[2], Hisham Abdalla[1], Ahmed Abdalla[1]

(Corresponding author: Mohammed Ramadan)

School of Computer Science and Engineering, University of Electronic Science and Technology of China[1]
2006 Xiyuan Avenue, Gaoxin West Zone, Chengdu 611731, P.R. China
School of Information Science and Engineering, Southeast University, Nanjing 210096, P.R. China[2]
(Email: nopatia@gmail.com)

(Received July 6, 2015; revised and accepted Aug. 12 & Sept. 29, 2015)

Abstract

Long Term Evolution LTE is the first technology that provides exclusively packet-switched data and modifies the security architecture of the 2G and 3G systems. The LTE security architecture offers confidentiality, access control, a kind of obscurity and mutual authentication. However, numerous types of attacks can be encountered during the mutual authentication process which is a challenge-response based technique. Therefore, a high secure public key algorithm can be implemented to improve the network security services. As the network operator is often considered as not being a highly trusted party and can thus face threats, the communications ends are the only secure parties to provide such security features. This paper proposes a secure mutual authentication and key agreement scheme for LTE cellular system with user-to-user security. The network side in this scheme operates as a proxy and non-trusted party to provide the security architecture with more flexibility and reliability. This is achieved by using designated verifier proxy signature and key agreement protocol based bilinear pairing with some changes in both security algorithms and LTE security architecture within the LTE standardization. Our security and performance analysis demonstrated that the proposed scheme is more secure compared to the basic authentication and key agreements schemes.

Keywords: 4G security, LTE-AKA, LTE proxy signature, mobile communication security

1 Introduction

LTE also referred to as 4G communication system is the next generation of mobile communication system that is being developed by 3GPP for secure and fast communication for 4G mobile communication standards. LTE has high efficiency, and good communication specifications [26]. It provides high communications features, such as bandwidth, data rate and switching techniques. The LTE architecture provides more secure communication than 2G and 3G mobile communication systems by providing mutual authentication between the User Equipment (UE) and Mobility Management Entity (MME). Authentication and Key Agreement protocol for Evolved Packet System EPS-AKA is a technique which executes authentication and session key distribution in LTE security architecture and it is a challenge-response based mechanism that employs symmetric cryptography. The fundamental EPS/LTE architecture is founded on UMTS-AKA and it provides secure network access. When a subscriber attempts to access WLAN, the International Mobile Subscriber Identity (IMSI) is sent through a Network Access Identifier (NAI) to the Access Point (AP). Although the basic EPS-AKA has some advantages, such as larger authentication keys, stronger hash function (SHA-1), support for mutual authentication, support for signaling message data integrity, support for signaling information encryption, support for user data encryption and protection, it has many vulnerabilities as elaborated in [31].

1.1 Motivation

The basic AKA protocol is a challenge-response protocol which it has many vulnerabilities. The primary objectives of this paper is to find a solution to the basic EPS-AKA problems such as false base station attack, IMSI catcher, and to achieve a strong security scheme which can provide user-to-user mutual authentication and key agreement security. By solving these problems, the users gain more trust in their network due to the network operator working only as a proxy. Moreover, the network operator can help the users to implement their security features, and it is considered to be a protected party.

The proposed scheme is based on designated verifier

proxy signature (DVPS) which is a special type of proxy signature in which the designated verifier (UE) alone can check the validity of the proxy (MME) signatures. Our proposed scheme consists of five main algorithms, setup and key generation, signature generation by the users UE's, signature verification and proxy signature generation by the network MME, proxy signature verification by the designated verifiers (users UE's), and session key generation by the users UE's. The original signer (User A) delegates its signing power to the proxy signer (Network operator) to generate proxy signatures for the designated verifier (User B) whereas in the last algorithm, User B checks the validity of the proxy signatures by using its own secret key. Furthermore, in our proposed scheme we made some changes to make DVPS more compatible with the LTE security architecture and to provide user-to-user mutual authentication and key agreement protocol. Designated verifier signature and proxy signature offers many kinds of security levels as proposed in the literature in the field of DVS [15, 17, 24, 30, 33, 36].

The rest of the paper is organized as follows: Section 2 introduces the basic EPS-AKA protocol; Section 3 presents briefly the basic EPS-AKA Vulnerabilities and some threats which are the motivations for this paper; Section 4 discusses the preliminaries of our proposed scheme and we introduce the basic principles of bilinear pairing and designated verifier signature; Section 5 presents our proposed system model and we firstly introduce some assumptions and definitions then present the phases of our proposed scheme; in Sections 6 and 7 we evaluate our proposed scheme by analyzing the security and the performance efficiency respectively; Finally Section 8 concludes this work.

2 The Basic EPS-AKA Protocol

The basic EPS-AKA scheme is a challenge-response based protocol and is quite similar to the UMTS-AKA version [6], except for the key set identifier (eKSI) in the challenge, and for separation indicator process when the user equipment (UE) verifies that the separation bit is set for E-UTRAN access. However, the main purpose of EPS-AKA protocol is the authentication of the user and the establishment of a new local master key KASME between the MME and the UE. EPS-AKA is also used for verification of the freshness of the authentication vector and authentication of its origin (the users home network) by the USIM. KASME is used in subsequent procedures for deriving further keys for the protection of the user plane, Radio Resource Control signalling, and Non-Access Stratum signaling [29].

The EPS-AKA procedure is as follows:

1) Generate EPS authentication vectors (AVs) in the HSS upon request from the MME, and distribute them to the MME. Hence, the MME needs to identify the UE before requesting authentication vectors from the HSS.
2) Mutual authentication and establishing a new shared key between the serving network and the UE.
3) Authentication data distribution between serving networks.

The MME invokes the procedure by requesting EPS authentication vectors from the HSS. The authentication information request shall include the IMSI, the serving network identity 'SN id' of the requesting MME, and an indication that the authentication information is requested for EPS. The SN id is required for the computation of KASME in the HSS. Then the MME invokes the authentication request procedure by selecting the next unused EPS authentication vector from the ordered array of EPS authentication vectors in the MME database (if there is more than one). If the MME has no EPS AV it requests one from the HSS. The MME then sends the random challenge RAND and the authentication token for network authentication AUTN from the selected EPS authentication vector to the mobile equipment, which forwards it to the USIM. The MME also generates a key set identifier eKSI and includes it in the Authentication Request. For the verification process and when the USIM receive RAND and AUTN, then the USIM first computes the anonymity key $AK = f5_K(RAND)$ and retrieves the sequence number $SQN = (SQN \bigoplus AK) \bigoplus AK$, where K is the permanent pre-shared secret key between USIM and AuC, and then the USIM computes $XMAC = f1K(SQN \parallel RAND \parallel AMF)$ and verifies that it equals the MAC included in AUTN. For the authentication response process and upon receipt of the Authentication Response message the MME checks whether the received RES matches the expected response XRES from the selected authentication vector. If it does then the authentication of the user has been successful [10]. Figure 1 illustrates the handshaking procedures of the basic EPS-AKA protocol.

3 Vulnerabilities of the Basic EPS-AKA

For network access security, 2G mobile systems such as GSM and CDMA were designed to be protected against external attacks. However, these designs have led to numerous interception attacks [27, 35]. In 3G network, a mobile station is connected to a visited network by means of a radio link to a particular base station (Node B). Multiple base stations of the network are connected to a Radio Network Controller (RNC) and multiple RNCs are controlled by a GPRS2 Support Node (GSN) in the packet-switched case or a Mobile Switching Center (MSC) in the circuit-switched case. The Visitor Location Register (VLR) and the serving GSN keep track of all mobile stations that are currently connected to the network. Every subscriber can be identified by its International Mobile Subscriber Identity (IMSI). In order to protect against profiling attacks, this permanent identifier is sent over the air interface as infrequently as possible. Instead, locally valid

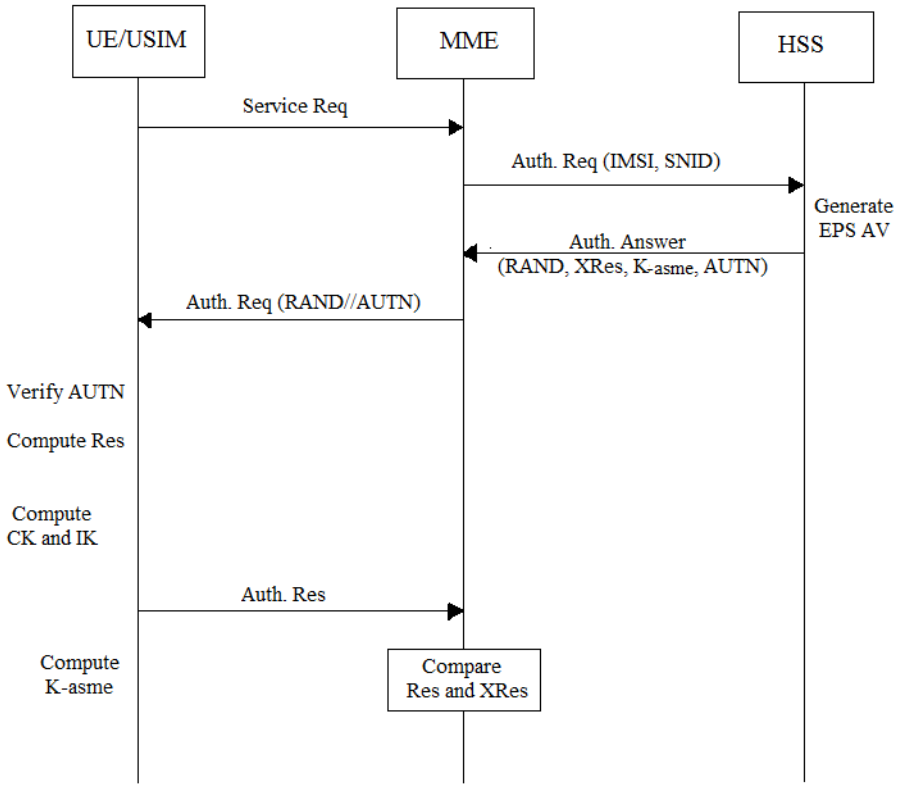

Figure 1: The basic EPS-AKA scheme

Temporary Mobile Subscriber Identity (TMSI) is used to identify a subscriber whenever possible. Every UMTS subscriber has a dedicated home network with which he shares a long term secret key Ki. The Home Location Register (HLR) keeps track of the current location of all subscribers of the home network. Mutual authentication between a mobile station and a visited network is carried out with the support of the current Serving GSN (SGSN) or the MSC/VLR respectively. UMTS supports encryption of the radio interface as well as integrity protection of the signaling messages. For a detailed description we refer to [1, 2].

Wireless cellular networks were originally designed to provide ubiquitous access for communication. Although the 2G network was designed with some security aspects in mind, GSM just featured cryptographic algorithms to guarantee privacy and authentication. The GSM security architecture, proposed two decades ago, is nowadays known to be insufficient given current computational power. UMTS-based 3G networks enhanced the system by implementing stronger encryption and a two-way authentication scheme. Both encryption and authentication are further enhanced in LTE. However, with the current threat landscape and the increasing sophistication of attacks, such security architecture is not enough to guarantee the availability of mobility networks.

The Authentication and Key Agreement protocol in EPS has a known vulnerability that can be exploited to breach the privacy of the user's identity and even his location [3, 4, 5]. However, many works tried to solve this problem by proposing alternative protocols [25]. The vulnerability, (i.e. sending the International Mobile Subscriber Identity in plaintext when no temporary identifier is valid) which was inherited from UMTS, can be used for tracking the user and/or detecting the user's presence. One of the latest proposed alternative protocols noted as Security Enhanced Authentication and Key Agreement (SE-AKA) was Cryptanalyzed in [1] and it was found vulnerable to brute force and intelligent brute force attacks when no padding is used.

There are several other types of attacks that could be threats to the LTE mobile network such as malware spreading, phishing, and DoS/DDoS attacks. DoS/DDoS is classified, based on the traffic load maliciously generated, into low and high traffics for DoS and DDoS respectively. We note that a special class of attack is defined for the case of the attacker being already within the network perimeter and not requiring a charge of malicious traffic. This is the case of an insider attack. Furthermore, some attacks have a local scope, disrupting service at the RAN level and blocking service for a single cell or sector. And other types of attacks can have a much wider scope, and are capable of disrupting a large portion of the mobility network. Local attack is a radio jamming and saturation of the wireless interface and such attacks can be launched from a single device or radio transmitter [20]. However,

the proposed scheme is secure against such attacks and particularly against the common attack, false base station and IMSI catcher attack.

4 Preliminaries

Our scheme relies on designated verifier proxy signature DVPS and key agreement protocol based bilinear pairing. We will briefly introduce the basic principles and some properties related to these techniques.

4.1 Bilinear Pairing

Let G_1 be a group of the order of a large prime number q and G_2 be a multiplicative subgroup of a finite field $\mathbb{F}$ of the same order and P be a generator of G_1. A map $e : G_1 \times G_1 \longrightarrow G_2$ is called a bilinear map if it has the following properties [21]:

Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ where $P, Q \in G_1$ and $a, b \in Z_q^*$;

Non-degeneracy: $P, Q \in G_1$, such that $e(P, Q) \neq 1$;

Computability: $P, Q \in G_1$ there is an efficient algorithm to compute $e(P, Q)$.

4.2 DVS

There exist three participants in the system, namely Alice, Bob and Cindy, who act as the original signer, the proxy signer and the receiver (or the designated verifier), respectively. We denote (xi, P_i) as a pair of private key and public key for user i, where $i \in \{A, B, C\}$ indicating Alice, Bob, and Cindy, respectively. A designated verifier proxy signature scheme (DVPS) consists of following algorithms [13]:

Parameters Generation: It takes as input the system security parameter l and outputs the system parameters.

Key Generation: It takes as input the security parameter l and outputs the key set: (xi, P_i) for $i = A, B, C$.

Proxy Key Generation: A deterministic algorithm that takes as input the original signer's secret key, the proxy signer's secret key, the identity of the proxy signer and the warrant m_w to generate the proxy key. That is Proxy Key Gen (x_A, x_B, ID_B, m_w), where X_A and X_B are the secret keys of the original signer and the proxy signer respectively and ID_B is the identity of the proxy signer.

Sign: A deterministic algorithm that takes as input the proxy key, the designated verifier's public key and a message m to generate a signature (σ), where proxy key is generated by the above Proxy Key Generation algorithm.

Verify: A deterministic algorithm that accepts a message m, a signature (σ), the original signer's public key, the proxy signer's public key, the proxy signer's identity and the receiver's secret key and then returns Valid if the signature is correct, and otherwise outputs invalid.

5 Proposed System Model

The proposed design provides user-to-user mutual authentication and key agreement technique for LTE cellular system which we termed as LTE-AKA. The basic LTE-AKA scheme does not provide end-to-end security and it has many vulnerabilities as shown in Section 3. We seek to address these vulnerabilities in our proposed scheme with more flexibility and security than the basic EPS-AKA scheme. We achieve this by using the system parameters in our model and distribute them between the entities during the communication modes. For example the system parameters will be distributed in advance and stored in both USIM card and HSS/AuC and for the security parameters and public keys will be distributed in the synchronization mode.

5.1 System Model Assumptions

The following assumptions are made with regard to our proposed scheme:

1) Assume user A and user B belongs to the same serving network and here we used the serving network identity SNID.

2) Using the home network identity HNID in case user A and B are not using the same serving network.

3) The identifier IMEI is assumed to be the message to be signed.

4) The identifiers IMSI, GUTI, SNID are assumed to be the identities to be hashed.

5) The pre-shared key (K) is used as a secret value during the session key phase.

5.2 Definitions of System Model Key Terms

5.2.1 Definitions

The major parties are the Home Network which is signified by (HSS), and the Visited/Serving Network which is signified by (MME). However, the subsequent definitions and terms are vital for our proposed scheme [23].

Home Service Server (HSS): The fundamental subscriber database at the home network (HPLMN). It is the definitive database of mobile subscriber information for a wireless carrier's network. It is also the real-time list that links phones, phone numbers, user accounts and service plan information.

Mobility Management Entity (MME): The MME is situated in the visited network (VPLMN). It is the network termination for the challenge-response part of the EPS-AKA protocol. It is also the host for the Access Security Management Entity (ASME), which is responsible of access security.

User Equipment (UE): The user/subscriber equipment is made up of the mobile equipment (ME) and the subscriber module (UICC/USIM).

Base station or eNodeB (eNB): The radio access point in LTE. It belongs to the visited network (VPLMN).

Serving Network Identity (SNID): SNID refers to the network accessed by the user and it is made up of PLMN ID (MCC+MNC). However, it classifies the specific serving network to UE's while in their roaming mode.

Authentication Center (AuC): It is a security database and it recommends any security information management; which (SIM) card is trying a network connection when a phone has a live network signal, and it provides security to ensure that third parties are incapable of exploiting network subscriber services.

International Mobile Station Equipment Identity (IMEI): It is a type of serial number that solely recognizes the mobile equipment internationally. The IMEI is allocated by the equipment manufacturer and registered by the network operator.

International Mobile Subscriber Identity (IMSI): IMSI is a permanent identity. Each registered user is solely recognized by its (IMSI) which is saved in the subscriber identity module (USIM).

Globally Unique Temporary UE Identity (GUTI): GUTI is a temporary identity that is transferred between UE and the network. It is arbitrarily allotted by the MME to every mobile in the region, when it is switched on. It consists of two major components:

1) GUMMEI which identifies the MME that assigned the GUTI.
2) M-TMSI which identifies the UE within the MME that assigned the GUTI.

5.2.2 Notations and Terms

Table 1 illustrates the notations used in the proposed LTE-AKA scheme.

Table 1: The notations and terms of the proposed scheme

Notations	Description
Subscript A	User A
Subscript B	User B
Subscript A/B	User A and user B
UE	User equipment
K	Pre-shared key
X	User's secret key
A	Public key for UE_A
B	Public key for UE_B
H/SNID	Home/Serving network identity
SK	Session key
Req	Authentication request
Res	Authentication response
XRes	Expected authentication response

5.3 The Proposed LTE-AKA Scheme

The proposed scheme is based on designated verifier signature and pairing based key agreement protocol to provide AKA scheme for the LTE cellular communication system [13, 21]. As we presented in Section 3, the basic EPS-AKA scheme is challenge-response algorithm which has many security weaknesses such as false base station attack and IMSI catcher attack (See Section 6). However, our proposed scheme solves such weaknesses with the same bandwidth consumption and handshaking process. And it only needs two handshaking processes for both authentication and key agreement processes. However, the network operator entities MME and HSS/AuC in our proposed scheme are only as a proxy signer and it is responsible for the system parameters and then assigns the GUTI for the visited network and for the users who belong to this location area. Hence, the session key will be changeable according to the current location. It will be computable only for the communication ends of the UE. Therefore, we assume two cases for our proposed scheme according to the security based mobility mode. Figure 2 illustrates the handshaking process for both cases.

Case 1: The two subscribers belong to the same visiting network, i.e. same MME and in this case the MME request the system parameters from the home network (HSS) which are computed by the AuC in advance. However, the same SNID will be used for the AKA protocol.

Case 2: Here we assume the two subscribers wishing to connect each other are on different visited networks i.e. different MME's (roaming mode) and the LTE-AKA will be achieved separately and some parameters exchange via home network HSS and some system parameters will be exchanged via the secured link between MME's. In this case the home network identity PLMN ID will be used for the AKA protocol.

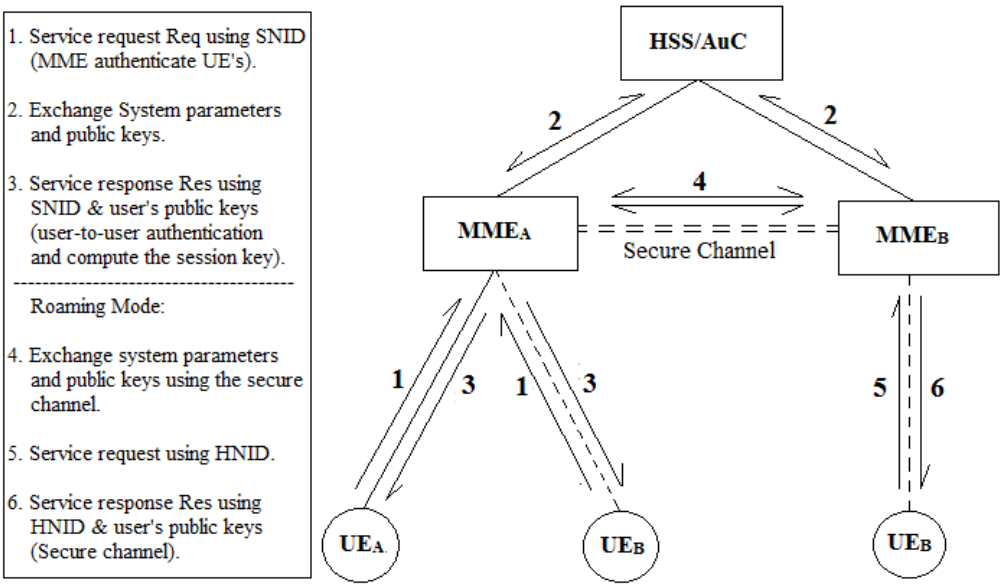

Figure 2: The proposed LTE-AKA handshaking process

The main objective of our scheme is to provide user-to-user AKA security scheme by let the MME's works as a proxy and use the user's identifier IMEI's as a message and the subscriber's GUTI or use the specific IMSI as identifiers with the network identifier SNID, and later for the session key. The AuC uses the same parameters to verify the UE, and then sends another signature which we called RES to the UE, then when the UE received the RES's it will compute the changeable session key depending on the current GUTI identifiers which is allocated in advance by MME. The UE's is continuously listening to the broadcast messages from MME through the base station (eNB) to determine the tracking area by using the parameter Tracking Area Identity (TAI). The ME is comparing the TAI which is received with that stored in the USIM and if not equal, UE requests a new TAI. This case occurs when the mobile is switched on or when the specific UE moved from one location area to another. Hence, the system parameters and keys will be distributed in the paging/synchronization processes before the call setup process. The proposed LTE-AKA scheme consists of the following four phases.

Phase 1: Setup and Key Generation.

Setup: This phase calculates the system parameters in the synchronization mode, when the UE connecting to the base station (eNB) which is in the idle, i.e. NAS security context. This phase works as follows:

1) UEA want to get access to the network services and connect to UEB, so we have four entities such as: UEA, UEB, visited network MME, and the home network HSS.
2) The setup algorithm will be done by the HSS/AuC, and it takes as input the system security parameter, and outputs the system parameters $\{G_1, G_2, P, q, e, H_1, H_2\}$, where

G_1**:** Cyclic additive group of order q;

G_2**:** Multiplicative group of order q;

P**:** Generator of G_1;

e**:** Bilinear map $e : G_1 \times G_1 \longrightarrow G_2$;

H_1**:** One way hash function: $\{0,1\}^* \longrightarrow G_1$;

H_2**:** One way hash function: $\{0,1\}^* \longrightarrow Z_q^*$.

Key Generation: This algorithm will be achieved by the users, and it computes the public/private keys, and we assume there are two users A and B which are willing to contact each other, this algorithm works as follows:

For UE_A**:**
Pick a secret key $xA \in Z_q^*$ and calculate the corresponding public key

$$A = x_A P.$$

Then using its own public key and identifications $(IMSI_A/GUTI_A)$ calculates:

$$\begin{aligned} Q_A &= H_1(IMSI_A \parallel GUTI_A, A) \\ D_A &= x_A Q_A, A. \end{aligned}$$

For UE_B**:**
Pick a secret key $xB \in Z_q^*$ and calculate the corresponding public key

$$B = x_B P.$$

Then using its own public key and identifications ($IMSI_B/GUTI_B$) calculates:

$$\begin{aligned} Q_B &= H_1(IMSI_B \parallel GUTI_B, B) \\ D_B &= x_B Q_B, B. \end{aligned}$$

For MME:

Pick a secret key $x_N \in Z_P^*$ and calculate the corresponding public key

$$N = x_N P.$$

Then using the public key and home / serving network identification (H / SNID) calculates:

$$Q_N = H_1(H/SNID, N).$$

These keys $\{D_A, D_B, N, Q_N\}$ will be distributed between entities in the synchronization mode and it will be used in the further phases. However, when the mobile user ME enter the specific serving network, and start to send location update messages including its own public key, and it can get the parameters for the specific serving network.

Phase 2: MME authenticate the users UE_A and UE_B

When the user A wants to get access to user B, Then it will start to compute the following parameters and send them to MME:

For UE_A:

Using MME's parameters N and Q_N, and its own secret key compute the corresponding request Req_A and send it to MME as follows:

$$Req_A = x_A Q_N.$$

For UE_B:

User B uses its own secret key and the network parameters as follows to compute Req_B and send it to MME as follows:

$$Req_B = x_B Q_N.$$

For MME:

When MME receives the service requests Req_A, Req_B it will start to authenticate UE_A and UE_B using the system parameters and the user's public keys as follows.

MME check $e(Req_A, P) = e(Q_N, A)$ for UE_A, if not equal abort the request. If equal, then using Req_A and B compute Res_B response and send it to UE_B:

$$Res_B = H_2(IMEI_B, e(Req_A, x_N Q_N, B)).$$

Then For UE_B MME check $e(Req_B, P) = e(Q_N, B)$, if not equal abort the request. If equal, then by the same way compute Res_A and send it to UE_A:

$$Res_A = H_2(IMEI_A, e(Req_B, x_N Q_N, A)).$$

Phase 3: User-to-User authentication.

As the subscriber authentication and network operator processes are bedeviled with security problems as outlined in Section 6, we proposed scheme that can achieve user-to-user authentication and the MME act as a proxy, and $UE_{A/B}$ as a designated verifiers. The algorithm for achieving this purpose as follows:

For UE_A:

When receive Res_A from MME then compute $XRes_A$:

$$XRes_A = H_2(IMEI_A, e(Req_A, B + N)).$$

And check and validate the equality $Res_A = XRes_A$ holds, if not outputs invalid and abort access.

For UE_B:

When receive Res_B from MME then compute $XRes_B$:

$$XRes_B = H_2(IMEI_B, e(Req_B, A + N)).$$

And check the equality $Res_B = XRes_B$ holds, if not outputs invalid and abort access. Figure 3 illustrates this phase at the UE/USIM side when the users authenticate each other.

Correctness:

This correctness for UE_A and it is the same process for UE_B: When the UE_A receives the

$$Res_A = H_2(IMEI_A, e(Req_B, x_N Q_N, A)).$$

It starts to compute:

$$XRes_A = H_2(IMEI_A, e(Req_A, B + N)).$$

Where,

$$\begin{aligned} A &= x_A P \\ Req_B &= x_B Q_N. \end{aligned}$$

Then,

$$Res_A = H_2(IMEI_A, e(x_B Q_N, x_N Q_N, x_A P)).$$

From the bilinear properties we get:

$$\begin{aligned} Res_A &= H_2(IMEI_A, e(x_A P, x_B Q_N) \\ &\quad \cdot e(x_A P, x_N Q_N)) \\ &= H_2(IMEI_A, e(x_A Q_N, x_B P) \\ &\quad \cdot e(x_A Q_N, x_N P)) \\ &= H_2(IMEI_A, e(Req_A, B) \\ &\quad \cdot e(Req_A, N)) \end{aligned}$$

Then,

$$\begin{aligned} Res_A &= H_2(IMEI_A, e(Req_A, B + N)) \\ &= XRes_A. \end{aligned}$$

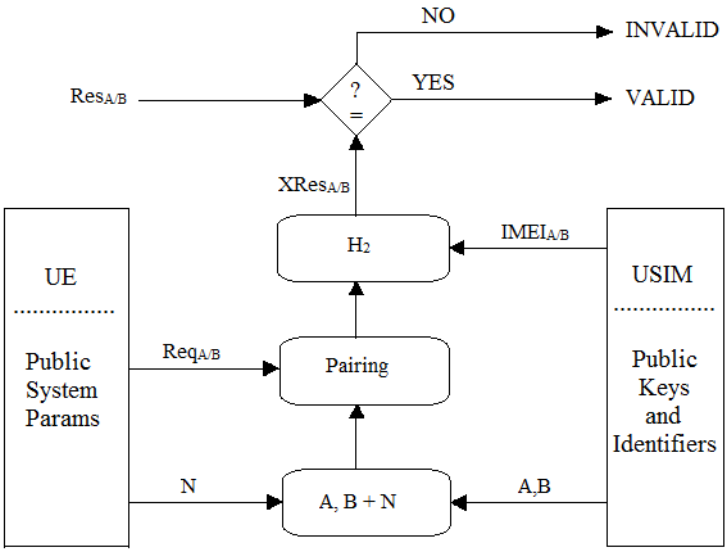

Figure 3: User-to-User authentication

Phase 4: Establish a shared secret key between UE_A and UE_B.

In our proposed scheme we assume that the network operator is not highly trusted, and the UE can only share a secret key. The proposed scheme can provide User-to-User security as well as mutual authentication between the two entities. Users A and B used the pre-shared key K which is distributed in advance and store in SIM card and AuC, this key comes from the standard security architecture in the LTE system, and the parameters $Q_{A/B}$ and $D_{A/B}$ which is distributed in advance during the setup and key generation phase, and this value depends on the identifiers (temporary or permanent) which in turn depends on the current location for the specific mobile station, i.e. the current serving network MME. Then users $UE_{A/B}$ can compute the session key as follows:

For UE_A:

Using the pre-shared key (K) the user UE_A can calculate the following parameters which are distributed during the Setup and key generation phase.

$$\begin{aligned} Q_A &= H_1(IMSI_A/GUTI_A, A) \\ D_B &= x_B Q_B, B. \\ T_A &= KQ_A. \end{aligned}$$

Then compute the shared secret session key

$$SK_A = e(T_A, D_B + x_A Q_B).$$

For UE_B:

By the same way UE_B calculate the following parameters:

$$\begin{aligned} Q_B &= H_1(IMSI_B/GUTI_B, B) \\ D_A &= x_A Q_A, A \\ T_B &= KQ_B. \end{aligned}$$

Then compute the shared secret session key:

$$SK_B = e(T_B, D_A + x_B Q_A).$$

UE_A and UE_B will compute the same shared secret key:

$$\begin{aligned} SK &= SK_A \\ &= SK_B \\ &= e(Q_A, Q_B)^{K(XA+XB)} x_A x_B P. \end{aligned}$$

6 Security Analysis of the Proposed Scheme

This section provides the security analysis of the proposed scheme. The proposed LTE-AKA scheme is more secure than the regular EPS-AKA which has a plethora of flaws as discussed in Section 3. The security analysis for LTE security architecture develops from UE's until the core network HSS/AuC. As the most common security features for mobile communication are discretion (location and data), authentication, access security, and imitation, the LTE security mechanisms should be able to attain these security features. Moreover, all these security features derived from the access level because the access level is the first line of defense against attacks. That means, the proposed LTE-AKA scheme offers a strong user-to-user mutual authentication and key agreement mechanism compared to that of [34]. The security necessities and analysis are as follows.

6.1 Security of the User-to-User Mutual Authentication Scheme

The entity MME has to utilize his secret key x_N to create the signatures and transfer them to the precise users, and UE_A and UE_B cannot create the signature without the knowledge of the MME's secret key, so this feature makes the proposed scheme unforgeable and somehow offers fortification to the network operator side. Furthermore, MME is the lone entity that can verify the legitimacy of the user's signatures; hence no snooping can happen due to the MME's secret key even if the user's secret keys are revealed.

6.2 Security of the Secret Session Key Scheme

The session key attacker can obtain the system parameters and the public keys which are conveyed in public during setup and key generation phase. However, it is difficult for an attacker to work out the session key SK because the attacker does not know the secret keys and the pre-shared key K which are saved securely in both the SIM card and AuC. Furthermore, the attacker can get some information for example one side secret key, but cannot compute the session key. Without knowing all the secret keys x_A, x_B, x_N, which belongs to CDH and it's a hard and difficult problem.

6.3 False Base Station Attack

False base station also referred to as IMSI catcher attack [3, 4, 5], it is a widespread attack in the field of mobile communication security, generally known as man-in-the-middle attack. In this attack, the user's identifiers can put a false base station between the mobile station and base station to act as a real base station. However, our proposed scheme is secure against such attack due to the identifiers protection by using the hash. Therefore, there is no way to try this attack by sending the fake message because the permanent identifier IMEI is used as a message to be signed. Moreover, to compute the SK, the attacker needs to get the secret parameters and they are not known and are not published in public. Furthermore, the proposed scheme provides obscurity to the users somehow by using temporary identifiers (GUTI) instead of (IMSI) when the user is in the roaming mode.

6.4 Known Key Attack and Forward/Backward Secrecy

By obtaining the secret keys of UE_A and UE_B, it still cannot be realistic for the attacker to recover the previous session keys. The reason is that the session key entails the temporary identifiers and the secret keys. Thus, it is impossible to obtain any secret keys or the session key from the public parameters as well as GUTI work as a temporary key for every session. On the other hand, it is also unfeasible to compute the value (x_A, x_B, P) due to the CDH hard problem. The basic EPS-AKA has many flaws as we presented in Section 3, and the most common problem in this context is that the privacy of the user's identities and even their locations by sending the IMSI identifier in clear as we know it as IMSI catcher attack, and many proposed works tried to solve such problems. In general, the proposed scheme is considered to be more secure since it provides user's privacy and access security, achieves user-to-user mutual authentication and key agreement scheme, and the third party (the network side) work as proxy and we consider it as untrusted third party.

6.5 End-to-end Security

Many research works focus on the security between the mobile user and the base station due to the insecure air interface, and it is easy for an attacker to eavesdrop this particular link [8]. However, our proposed scheme provide end-to-end security and only users can compute the session key, and they can authenticate each other as well as the network operator can authenticate the users.

6.6 Replay Attack

The proposed scheme is secure against the replay attack due to the changeable session keys:

$$\begin{aligned} SK &= SK_A = SK_B \\ &= e(Q_A, Q_B)^{K(XA+XB)} x_A x_B P. \end{aligned}$$

The session key derived from the hash value of the temporary identities and the public keys. The temporary identity GUTI is changeable according to the user's location area, and hence when the attacker replays with the previous security parameters, then the request will be rejected because the users UE's will know that this request is invalid.

7 Performance Evaluation

Since 4G cellular systems offer a high specification performance as mentioned in the introduction section, the security feature can be enhanced using the new network utilities as much as a strong security is needed. However, the proposed scheme makes use of these advantages and evaluates the performance of the proposed LTE-AKA protocol.

The performance of our proposed scheme is evaluated using the existing experimental setup of [11, 12] for a variety of cryptographic operations using MIRACLE [32] in PIV 3 GHZ processor with Windows XP operating system and 512 MB memory. From [11, 12] the relative running time for the operations we employed in our proposed model and we define some terms for the running time calculation as follows:

T_p = Pairing operation: 20.01 (ms).

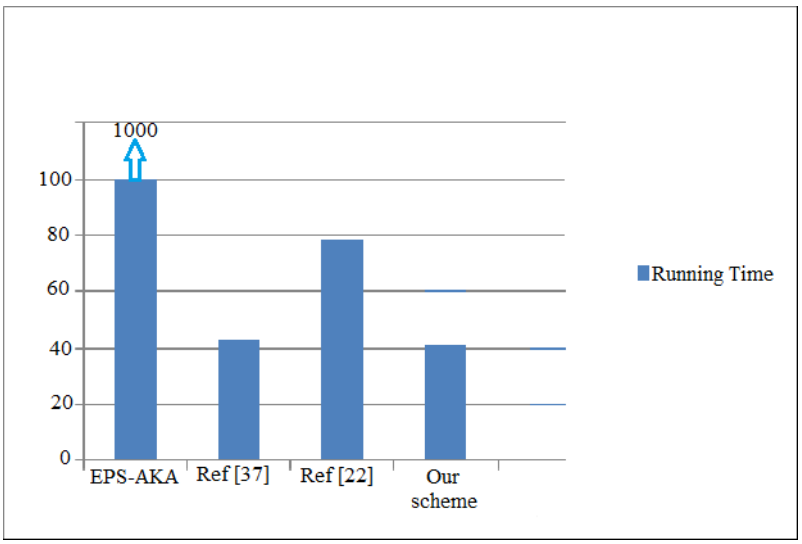

Figure 4: Running time-based efficiency comparison

T_m = Pairing-based scalar multiplication: 6.38 (ms).

T_e = ECC-based scalar multiplication: 0.83 (ms).

T_h = Hash function: 3.04 (ms).

We observe that the implementation of the proposed model required three pairing operations and one exponential operation on the user side and four pairing operations and one exponential operation on the network side, and for the other operations we assumed that the running time is omitted. Table 2 shows the performance efficiency based running time of the proposed model.

According to the computational cost we clearly can note that the total running time in both UE side and MME side is 109.11 (ms). That means, the proposed model scheme is quite reliable to be implemented in the real field of the LTE mobile communication systems comparing with the standard EPS-AKA scheme. Generally, from the above analysis and results it can be noted that the proposed scheme has reasonable computational complexity when it is compared to the basic protocols such as EPS-AKA and Extensible Authentication Protocol (EAP-AKA) which it takes about 1000 ms [28].

In the mobile communication field, computation cost is very important. When a user requests a service to a provider with payment way, the users will care about the transmission and computational cost [16].

Many research works have been proposed schemes in the field of mobile communication security, particularly in authentication and key agreement protocol such as [7, 9, 14, 18, 19, 22, 37, 38], here we give a reasonable computational cost comparison (UE's side) for our proposed scheme with [22, 37]. This comparison will be calculated based on the operation's computational cost for each reference. Table 3 shows comparison of the computational cost efficiency, Figure 4 illustrates comparisons of the performance efficiency based running time and Table 4 shows comparison of the security-based performance efficiency for our proposed scheme with the basic scheme EPS-AKA and [7, 9, 18].

From the above comparisons we can observe that the proposed scheme can be applied in the practical field of LTE cellular system according to the relatively accepted performance efficiency comparing with the call setup process in LTE cellular system, EAP-AKA, and the previous research works.

8 Conclusion

The LTE cellular system possesses considerable communication flexibility, and the agreement of mobile phone manufacturers is also required. However, the improvement of the deployed public key cryptographic algorithms can be very useful. The LTE security architecture is a mature evolved architecture, with both strengths and weaknesses, and therefore, the PKI infrastructure is more secure and it can be modified as well as the LTE security architecture. In this paper, we proposed a secure LTE-AKA scheme which is based on user-to-user security. The proposed scheme is performed at the end-entities, therefore it is more flexible and there is no need to make any change within the core network. Furthermore, we have analyzed the security and the performance of our scheme and realized that the proposed scheme is more flexible and secure than the basic EPS-AKA scheme which has many weaknesses.

References

[1] 3GPP Technical Specification, 3GPP TS 33.102, V5.3.0, Third Generation Partnership Project; Tech-

Table 2: The performance efficiency Time of the proposed scheme

Entities/Phases	UE Side(ms)	MME Side(ms)
Phase 1	$2T_e + T_h$= 4.7	$T_e + T_h$= 3.87
Phase 2	T_e= 0.83	$2T_p + T_m + T_h$= 49.44
Phase 3	$T_p + T_h$= 23.05	None
Phase 4	$T_p + T_e + T_m$= 27.22	None
Total	55.8	53.31

Table 3: Comparison of computational cost efficiency in (ms)

Computational cost	EPS-AKA	[37]	[22]	Our scheme
UE side	1000	43	78.360	42.695

Table 4: Comparison of security-based efficiency

Security Parameters	**EPS-AKA**	**[7]**	**[9]**	**[18]**	**Our scheme**
Mutual authentication	Y	Y	Y	Y	Y
End-to-end security	N	N	N	N	Y
Privacy preserving	N	Y	N	Y	Y
Replay attack	Y	Y	Y	Y	Y
Forward/Backward secrecy	N	Y	N	Y	Y

nical Specifications Group Services and System Aspects; 3G Security; Security Architecture, Sept.2003.

[2] 3GPP Technical Report, 3GPP TR 31.900, V5.3.0., Third Generation Partnership Project; SIM/USIM Internal and External Interworking Aspects, 2003.

[3] 3rd Generation Partnership Project, 3GPP TR 33.821 V9.0.0 (2009-06), Rationale and Track of Security Decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE), Release 9, June 2009.

[4] 3rd Generation Partnership Project, 3GPP TS 33.401 V11.2.0 (2011-12), 3GPP System Architecture Evolution (SAE); Security Architecture, Release 11, Dec. 2011.

[5] 3rd Generation Partnership Project, 3GPP TS 33.401 V8.8.0 (2011-06), 3GPP System Architecture Evolution (SAE); Security Architecture, Release 8, June 2011.

[6] S. Antipolis, *3GPP, TS 33.102, 3G Security; Security Architecture*, 3rd Generation Partnership Project, Technical Report v3.11.0, 2002.

[7] J. Cao, H. Li, M. D. Ma, Y. Y. Zhang, C. Z. Lai, "A simple and robust handover authentication between HeNB and eNB in LTE networks", *Computer Networks*, vol. 56, no. 8, pp. 2119-2131, 2012.

[8] C. C. Chang, K. L. Chen, M. S. Hwang, "End-to-end security protocol for mobile communications with end-user identification/authentication", *Wireless Personal Communications*, vol. 28, no. 2, pp. 95–106, Jan. 2004.

[9] J. Choi and S. Jung, "A handover authentication using credentials based on chameleon hashing", *IEEE Communication Letters*, vol. 14, no. 1, pp. 54–56, Jan. 2010.

[10] D. Forsberg, G. Horn, W. D. Moeller and V. Niemi, *LTE Security*, John Wiley and Sons, 2010.

[11] D. He and J. Chen, "An efficient certificate-less designated verifier signature scheme", *The International Arab Journal of Information Technology*, vol. 10, no. 4, pp. 389–396, 2013.

[12] D. Hea, J. Chen and R. Zhang, "An efficient identity-based blind signature scheme without bilinear pairings," *Computers & Electrical Engineering*, vol. 37, no. 4, pp. 444–450, July 2011.

[13] X. Huang, Y. Mu, W. Susilo, and F. Zhang, "Short designated verifier proxy signature from pairings", in *Embedded and Ubiquitous Computing (EUC'05)*, LNCS 3823, pp. 835–844, Springer, 2005.

[14] Y. L. Huang, C. Y. Shen, S. W. Shieh, "S-AKA: A provable and secure authentication key agreement protocol for UMTS networks", *IEEE Transactions on Vehicular Technology*, vol. 60, no. 9, pp. 4509-4519, 2011.

[15] M. S. Hwang, C. C. Lee, S. F. Tzeng,"A new proxy signature scheme for a specified group of verifiers", *Information Sciences*, vol. 227, pp. 102–115, Apr. 2013.

[16] M. S. Hwang, C. Y. Liu, "Authenticated encryption schemes: Current status and key issues", *International Journal of Network Security*, vol. 1, no. 2, PP.61–73, Sep. 2005.

[17] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," in *Advances in Cryptology (EUROCRYPT'96)*, LNCS 1070, pp. 143–154, Springer-Verlag, 1996.

[18] Q. Jing, Y. Zhang, A. Fu and X. Liu, "A privacy preserving handover authentication schemes for EAP-based wireless networks", *IEEE Global Telecommunications Conference (GLOBECOM'11)*, pp. 1–6, Dec. 2011.

[19] Q. Jinga, Y. Zhang, X. Liua and A. Fuc, "An efficient handover authentication scheme with location privacy preserving for EAP-based wireless networks", in *IEEE International Conference on Communications (ICC'12)*, pp. 857–862, 2012.

[20] R. P. Jover and P. Giura, "How vulnerabilities in wireless networks can enable advanced persistent threats", *International Journal on Information Technology*, 2013.

[21] B. Kanga, C. Boydb, Ed Dawsonb, "Identity-based strong designated verifier signature schemes: Attacks and new construction", *Computers & Electrical Engineering*, vol. 35, no. 1, Jpp. 49–53, 2009.

[22] Y. Kim, W. Ren, J. Jo, M. Yang, Y. Jiang, J. Zheng, "SFRIC: A secure fast roaming scheme in wireless LAN using ID-based cryptography", in *Proceedings of IEEE International Conference on Communications (ICC'07)*, pp. 1570-1575, June 2007.

[23] G. M. Koien, "Mutual entity authentication for LTE", in *7th International Wireless Communications and Mobile Computing Conference (IWCMC'11)*, pp. 689–694, July 2011.

[24] F. Laguillaumie and D. Vergnaud, "Designated verifiers signature: Anonymity and efficient construction from any bilinear map", in *Fourth Conference on Security in Communication Networks (SCN'04)*, LNCS 3352, pp. 107–121, Springer-Verlag, 2004.

[25] C. Lai, H. Li, R. Lu, X. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks", *Computer Networks*, vol. 57, no. 17, pp. 3492-3510, Dec. 2013.

[26] P. Lescuyer, T. Lucidarme, *Evolved Packet System (EPS): The LTE and SAE Evolution of 3G UMTS*, John Wiley and Sons Ltd, 2012.

[27] W. Millan, P. Gauravaram, "Cryptanalysis of the cellular authentication and voice encryption algorithm", *IEICE Electronics Express*, vol. 1, no. 15, pp. 453–459, 2004.

[28] C. Politis, K. A. Chew and N. Akhtar, "Hybrid multilayer mobility management with AAA context transfer capabilities for all-IP networks", *IEEE Wireless Communications*, vol. 11, no. 4, pp. 76–88, Aug. 2004.

[29] M. Purkhiabani, A. Salahi, "Enhanced authentication and key agreement procedure of next generation 3GPP mobile networks", *International Journal of Information and Electronics Engineering*, vol. 2, no. 1, pp. 69–77, Jan. 2012.

[30] S. Saeednia, S. Kramer, and O. Markovitch, "An efficient strong designated verifier signature scheme", in *The 6th International Conference on Information Security and Cryptology (ICISC'03)*, LNCS 2971, pp. 40–54, Springer-Verlag, 2003.

[31] C. B. Sankaran, "Network access security in next-generation 3GPP systems: A tutorial," *IEEE Communications Magazine*, vol. 47, no. 2, pp. 84–91, 2009.

[32] M. Scott, *MIRACLE – Multiprecision Integer and Rational Arithmetic C/C++ Library*, Shamus Software Ltd, Dublin, Ireland, 2003. (`http://www.shamus.ie`)

[33] W. Susilo, F. Zhang, and Y. Mu."Identity-based strong designated verifier signature schemes", in *Proceedings of the 9th Australasian Conference on Information Security and Privacy (ACISP'04)*, LNCS 3108, pp. 313–324, SpringerVerlag, 2004.

[34] C. E. Vintila, V. V. Patriciu, I. Bica, "Security analysis of LTE access network", in *The Tenth International Conference on Networks (ICN'11)*, pp. 29–34, Jan. 2011.

[35] D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm", in *Advances in Cryptology (CRYPTO'97)*, LNCS 1294, pp. 526–537, Springer, 1997.

[36] H. Xiong, Z. Qin, and Fagen Li, "A certificateless proxy ring signature scheme with provable security", *International Journal of Network Security*, vol. 12, no. 2, pp.92–106, Mar. 2011.

[37] C. Zhang, R. Lu, P. Ho and A. Chen, "A location privacy preserving authentication scheme in vehicular networks", in *IEEE Wireless Communications and Networking Conference (WCNC'08)*, pp. 2543–2548, 2008.

[38] Y. Zhang, X. F. Chen, J. Li, H. Li, "Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks", *Computer Networks*, vol. 75, pp. 192-211, 2014.

Mohammed Ramadan He received his B.S. degree in communications engineering from Karary University in 2007, Khartoum, Sudan, and M.S. degree in computer engineering, information security (GSM security) from University of Electronic Science and Technology of China in 2013, Chengdu, China. He is currently working toward the Ph.D. degree in Information Security, Mobile Communications Security from University of Electronic Science and Technology of China. His current research interests include mobile communications security (LTE security).

Fagen Li received his B.S. degree from Luoyang Institute of Technology, Luoyang, China, in 2001, M.S. degree from Hebei University of Technology, Tianjin, China in 2004 and Ph.D. degree in cryptography from Xidian University, Xi'an, China in 2007. From 2008 to 2009, he was a postdoctoral fellow in Future University Hakodate, Hokkaido, Japan, which is supported by the

Japan Society for the Promotion of Science. He worked as a research fellow in the Institute of Mathematics for Industry, Kyushu University, Fukuoka, Japan, from 2010 to 2012. He is now an associate professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China. His recent research interests include cryptography and network security. He has published more than 70 papers in the international journals and conferences.

ChunXiang Xu is a professor at University of Electronic Science and Technology of China (UESTC). Her research interests include information security, cloud computing security and cryptography. She received her PhD, M.Sc. and B.Sc. degrees at Xidian University, in 2004, 1988 and 1985 respectively, PR China.

Abdeldime Mohamed Salih is a lecture with Karary University, Khartoum-Sudan, now he is a Ph.D. student with Southeast University, School of Information Science and Communication Engineering, Nanjing.

Hisham Abdalla is a doctoral student at University of Electronic Science and Technology of China (UESTC). He received his M.Sc. degree from UESTC and BE degree in computer engineering from Karary University in 2006. His research interests include cloud computing security, cryptography and digital right management.

Ahmed Abdalla He received the B.S. Degree in Electrical Engineering from Karary university in 2005, Khartoum Sudan and the M.S. Degree in M.Sc. in Electronic Engineering, Information and signal processing form University of Electronic Science and Technology of China in 2013, Chengdu, China. He is currently working toward the PhD. Degree Electronic Engineering from University of Electronic Science and Technology of China. His current research interests include radar counter countermeasure and radar signal processing.