Received August 24, 2019, accepted September 12, 2019, date of publication September 17, 2019, date of current version October 4, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2941913*

# An Authentication Protocol in LTE-WLAN Heterogeneous Converged Network Based on Certificateless Signcryption Scheme With Identity Privacy Protection

**LILING CAO, YUQING LIU, AND SHOUQI CAO**
Department of Engineering Science and Technology, Shanghai Ocean University, Shanghai 201306, China

Corresponding author: Shouqi Cao (sqcao@shou.edu.cn)

This work was supported in part by the Doctoral Scientific Research Foundation of Shanghai Ocean University under Grant A2-0203-00-100361, in part by the 2017 ''innovative action plan'' of Science and Technology Commission of Shanghai Municipality under Grant 17050502000, and in part by the 2017 cooperative project on Industry-Academy-Research of Shanghai Lingang Administrative Committee (Key technology research and demonstration line construction of advanced laser intelligent manufacturing equipment).

**ABSTRACT** Aiming at to avoid the security drawbacks of the authentication protocol in Long Term Evolution-Wireless Local Area Network (LTE-WLAN) heterogeneous converged network proposed by the 3rd Generation Partnership Project (3GPP), an improved protocol based on hybrid cryptosystem is proposed to achieve access authentication for WLAN user equipment(UE) with identity privacy protection. The security analysis shows that by using certificateless signcryption(CLSC) scheme without pairing calculation based on Elliptic Curve Cryptography (ECC), hash chain and identity index mechanism, the proposed authentication protocol provides the following ten kinds of security properties: anonymous protection for International Mobile Subscriber Identity (IMSI), update on shared keys, protection for master session key(MSK), resistance to impersonation attack, replay attack, man-in-the-middle attack, redirect attack and Denial of Service (DoS) attack, mutual authentication between communication entities, and without framework modification from the original protocol. The performance analysis shows that the approximate calculation time of all the communication entities is 79 *ms* in total and that of UE is 266 *us*. Thus, our proposed protocol is superior to some other related improved protocols in terms of security and efficiency.

**INDEX TERMS** Authentication, LTE-WLAN, certificateless signcryption, identity privacy protection.

## I. INTRODUCTION

Heterogeneous converged network has become the development trend of future communication system, providing users with diversified services. Authentication in such network, which provides identity authentication for communication entities, has always been a research hotspot and attracted extensive attentions. EAP-AKA/EAP-AKA' (Extensible Authentication Protocol-Authentication and Key Agreement/ Improved Extensible Authentication Protocol-Authentication and Key Agreement) is the authentication protocol in LTE-WLAN heterogeneous converged network proposed by 3GPP, which adopts symmetric cryptography to realize the authentication of users, meeting most security requirements of wireless networks, and successfully protecting communication entities from attacks.

The LTE network, which is mainly composed of UE (User Equipment), E-UTRAN (Evolved UMTS Terrestrial Radio Access Network), EPC (Evolved Packet Core), and non-3GPP Access Network, adopts loose coupling way [1] to converge WLAN and other non-3GPP networks [2], as shown in Figure 1 [3]. When non-3GPP user device such as WLAN-UE connects to EPC, AAA(Authentication, Authorization, Accounting) server implements mutual authentication with UE on behalf of EPC, where HSS (Home Subscriber Server) is a central database storing user authentication information.

In LTE-WLAN converged network, when WLAN-UE is connected to HPLMN (Home Public Land Mobile Network), AAA obtains authentication information from HSS and

The associate editor coordinating the review of this manuscript and approving it for publication was Congduan Li.

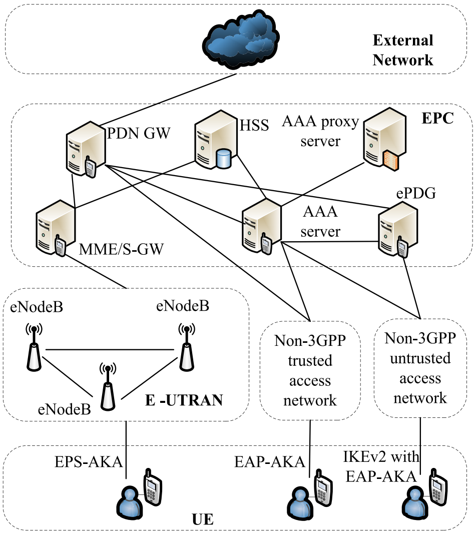

**FIGURE 1.** LTE network architecture [3].

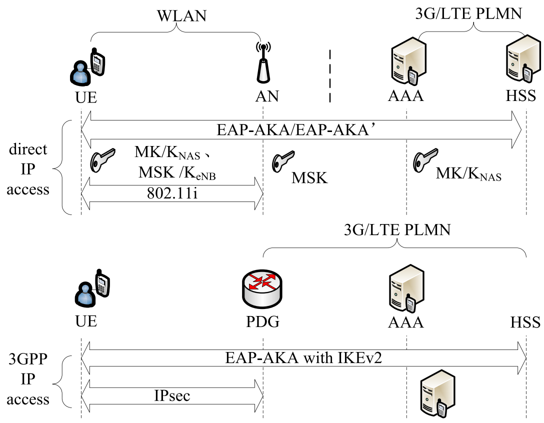

**FIGURE 2.** Two types of IP access for LTE-WLAN converged network [4].

realizes authentication and key negotiation with WLAN-UE through WLAN network. When being authenticated successfully, users can choose two types of IP access: WLAN 3GPP IP access (referred to as 3GPP access) and WLAN direct IP access (referred to as WLAN access). The former is connected to IP network through PDN GW(Packet Data Network Gateway) of HPLMN; The latter directly accesses the IP network through WLAN AN(Access Network), as shown in Figure 2 [4]. When WLAN-UE is roaming in VPLMN (Visited Land Mobile Network), AAA proxy in the visited network will forward the messages from AAA in the home network to WLAN-UE, so as to realize the authentication and key negotiation between AAA and WLAN-UE. If the authentication successes, users can still choose two types of IP access above.

EAP-AKA/EAP-AKA' authentication protocol is used in both types of IP access. Four types of authentication protocols are defined in TS33.234 standard [5], i)authentication for WLAN access, ii) reauthentication for WLAN access, iii) authentication for 3GPP access and iv) reauthentication for 3GPP access. Detailed description about EAP-AKA/EAP-AKA' can be referred to RFC5448 [6]. Then, only authentication for WLAN access is studied in this paper.

Although EAP-AKA/EAP-AKA' authentication protocol has realized the authentication between UE and HSS, meeting basic security requirements, researchers [4], [7]–[9] have pointed out that this protocol has many security drawbacks, mainly as follows:

(i) Mutual authentication between HSS and UE has been realized in EAP-AKA protocol, while mutual authentication between AAA and HSS, between AAA and WLAN AN has not been realized.

(ii) MSK, the communication key between WLAN-UE and WLAN AN, is sent from AAA to WLAN AN in plaintext. Therefore, attackers can easily obtain MSK to disguise as a legal WLAN AN to communicate with WLAN-UE. Literature [4] points out that AAA can sends protected MSK to WLAN AN, but gives no specific scheme. Since there is no shared key between WLAN AN and AAA, MSK protection cannot be realized based on symmetric encryption system.

Besides, The authentication vector and $SN_{ID}$ transmitted between HSS and AAA are all transmitted in plaintext, which may be eavesdropped or intercepted.

(iii) As the unique identity of the user in registration process, IMSI is stored in the UICC(Universal Integrated Circuit Card) card in the device owned by the user. Therefore, user identity information IMSI may be obtained through replicating the UICC card. During the user authentication for the initial access to network, IMSI is transmitted to HSS in plaintext through multiple AAAs, and malicious AAAs can leak IMSI to attackers. Therefore, EAP-AKA/EAP-AKA' protocol contains privacy protection vulnerability for IMSI.

(iv) The EAP-AKA authentication protocol lacks the mechanism to update the shared key between WLAN-UE and HSS, while security only depends on the single pre-shared key $K$. The leakage of the pre-shared key will cause the whole system to crash, and make the session keys between WLAN-UE and WLAN AN, WLAN-UE and AAA produced in the authentication process have no forward security.

(v) Literature [4] describes in detail that in the EAP-AKA protocol, attackers can launch re-direction attack to lure legal users to access to other WLAN networks with higher billing or lower security level, mainly due to the lack of WLAN AN authentication in the EAP-AKA authentication process.

(vi) EAP-AKA/EAP-AKA' protocol cannot resist replay attack and man-in-the-middle attack. When intercepting the legal connection request from the user, an attacker sends the connection request once again through the replay attack. When obtaining authentication vector from AAA or HSS, the attacker forwards the authentication vector to the legal user for challenge. When the legal user sends response message for the challenge to AAA, the attacker intercepts it and forwards it to AAA. Then, the attacker will be authenticated as a legitimate user by AAA and successfully implement replay attack and man-in-the-middle attack.

(vii) EAP-AKA/EAP-AKA' protocol is vulnerable to DoS attack. Once an attacker obtains IMSI, the attacker can launch DoS attacks against AAA and HSS by disguising as a legitimate user.

Therefore, many researchers [4], [10]–[15] have devoted to improving the security of the authentication protocol in LTE-WLAN heterogeneous converged network. However, all these improved protocols still have drawbacks. Thus, our work contributes to constructing an authentication protocol called IEAP-AKA in LTE-WLAN network based on hybrid cryptosystem and certificateless signcryption to achieve access authentication for WLAN-UE with identity privacy protection. The proposed authentication protocol has shown a considerable amount of good performance as compared to some recent related ones.

This paper is organized as followed: Section II summaries and analyzes the recent related improved protocols based on EAP-AKA/EAP-AKA'. Section III introduces our improved authentication protocol in detail. Section IV describes the security and performance analysis of the proposed protocol and Section V gives the conclusion of the work.

## II. INTRODUCTION AND ANALYSIS OF RECENT SCHEMES

### A. INTRODUCTION AND ANALYSIS OF THE SCHEME PROPOSED BY IMEN ELBOUABIDI et al.

Tseng [10] proposed a unified authentication scheme for 3G-WLAN converged network using hybrid cryptography, in which the public key cryptography based on elliptic curve Diffie-Hellman algorithm and symmetric cryptography were adopted. Elbouabidi *et al.* [11] fully affirmed the design idea of realizing authentication in unified form in converged network based on hybrid cryptography, and proposed authentication schemes for WLAN access and reauthentication for WLAN access, which improved the security performance and reduced the access latency. However, in the scheme proposed by Imen Elbouabidi et al., AAA server can obtain secret key $K$ shared by UE and HSS, then malicious AAA can disguise legal UE to send access request to HSS. In addition, the protocol does not provide identity privacy protection with practicability.

### B. INTRODUCTION AND ANALYSIS OF THE SCHEME PROPOSED BY FU

Fu [4] proposed an authentication protocol for WLAN access in LTE-WLAN network based on proxy signature mechanism and elliptic curve cryptography(ECC). In the scheme proposed by Fu, the UE sends proxy signature information to WLAN AN, then WLAN AN verifies the legitimacy of the UE by performing the process that is similar to EAP-AKA protocol on the basis of the validation of the signature information. The scheme can solve the problem of identity leakage and avoid attacks from mendacious access points, but there are still defects shown as follows, (i) the proxy signature algorithm UE adopts is based on ECC, which is not suitable for UE with limited resources. (ii) to prevent the attacker from tracking UE according to the public key in proxy signature, the proxy signature mechanism of UE is weakened. In the scheme, a subset of users randomly share the proxy signature keys, which can avoid only partial DOS attacks. The legal user UE$'$ who shares proxy signature keys with the legal user UE can impersonate UE to implement denial-of-service (DoS) attacks to AAA. (iii) some assumptions in the scheme are not in line with the actual application. For instance, it has been assumed that a secure connection and shared keys have been established between AAA and WLAN AN, and between AAA and HSS. (iv) there is no key update mechanism, so that the scheme cannot support forward security.

### C. INTRODUCTION AND ANALYSIS OF THE SCHEME PROPOSED BY WU et al.

Wu and Liaw [12] put forward authentication schemes for WLAN access and reauthentication for WLAN access mainly based on the techniques such as hash-based message authentication code, digital signature and hash chain, which can resist replay attack, guessing attack, masquerade attack, and etc. However, anonymity of the users is realized by using public key cryptosystems, which is impractical for UE with limited resources. In addition, the specific cryptographic scheme in the public key cryptography system has not been indicated in the scheme. And there is no shared key update mechanism between UE and HSS. Besides, the framework of the scheme proposed by Wu et al. has been modified too much from EAP-AKA protocol, which requires large-scale upgrading in existing infrastructure.

### D. INTRODUCTION AND ANALYSIS OF THE SCHEME PROPOSED BY ZHANG et al.

In the scheme proposed by Zhang *et al.* [13], MSK was encrypted by the session key shared between UE and WLAN AN to solve the security problem that MSK was transmitted in plaintext. However, with the increase in quantity and mobility for UE, it will be complicated to manage and update the shared session keys between UE and WLAN AN. Dong and Wang [9] has improved the scheme in [13] by adopting public key cryptosystem, but also has many problems: (i) UE sends $RAND_{UE}$, $IMSI$ encrypted by initial shared secret key $K$ to AAA, but AAA cannot decrypt the ciphertext to get $RAND_{UE}$,$IMSI$ without the knowledge of which $K$ belonging to the specific user should be used to decrypt the ciphertext. (ii) The scheme proposed by Zhang et al. has been modified too much from EAP-AKA protocol, which also requires large-scale upgrading in existing infrastructure.

### E. INTRODUCTION AND ANALYSIS OF THE SCHEME PROPOSED BY BASSOLI R et al.

Bassoli *et al.* [14] realized the authentication between UE and AAA based on public key cryptosystem without the adoption of authentication vectors that used in original EAP-AKA protocol. Therefore, the scheme proposed by Bassoli R et al. has also been modified too much from EAP-AKA protocol. Besides, in the protocol proposed by Bassoli R et al., *IMSI* is encrypted by the same public key from AAA to achieve identity anonymity protection in every round of authentication process without dynamic identity updating mechanism, which provides the traceability of the user. In addition, AAA server can obtain shared secret key $K$ between UE and HSS, then malicious AAA can disguise legal UE to send access request to HSS.

### F. INTRODUCTION AND ANALYSIS OF THE SCHEME PROPOSED BY EL IDRISSI Y E H et al.

El Idrissi *et al.* [15] proposed an improved scheme based on Elliptic curve cryptography, in which the shared session key between UE and HSS was generated by key exchange algorithm ECDH(Elliptic Curve Diffie-Hellman) and updated in every round of authentication process. Although the improved scheme provides forward security and mutual authentication between communication entities, the assumptions in the scheme are not in line with the actual application. In their scheme, AAA and HSS have established secure connection without any authentication process, so do AAA and WLAN AN. In addition, the scheme provides security features without identity anonymity protection. As AAA transmits *IMSI* to HSS in plaintext.

## III. IMPROVED SCHEME IEAP-AKA

In this section, a security enhanced authentication scheme in LTE-WLAN heterogeneous converged network based on certificateless signcryption scheme with identity privacy protection is proposed to achieve high security without drawbacks in original EAP-AKA protocol.

### A. INTRODUCTION OF CLSC SCHEME

Signcryption is a cryptographic primitive that provides authentication (signing) and confidentiality (encrypting) simultaneously at a lower computational cost and communication overhead. Then, CLSC is a signcryption scheme based on elliptic curve cryptosystem (ECC) without time-consuming pairing operation. Notions used in CLSC are listed in Table 1. CLSC scheme, which consists of seven polynomial time algorithms, can be summarized in Table 2 according to the following expression.

$$\{outputs\} \xleftarrow{\text{algorithm executive}} \text{algorithm}(inputs)$$

For example, $\{pk_i\} \xleftarrow{\text{user } i} \text{PUK}(ID_i, x_i, system\ params)$ means that user$i$ executes PUK algorithm to generate public key $pk_i$ by taking $ID_i$, $x_i$, *system params* as inputs.

Then, in our previous research [16],we proposed a CLSC scheme which is provably secure against indistinguishability under adaptive chosen-ciphertext attack (IND-CCA2) and existential unforgeability under adaptive chosen-message attack (EUF-CMA) resting on Gap Diffie-Hellman (GDH) assumption and discrete logarithm problem in the random oracle model. Furthermore, the proposed scheme resists the ephemeral secret leakage (ESL) attack, public key replacement (PKR) attack, malicious but passive KGC (MPK) attack, and presents efficient computational overhead compared with the existing related CLSC schemes. Therefore, in this paper, our scheme implement authentication based on our CLSC to improve the security.

**TABLE 1.** Notations used in CLSC.

| Notation | Description |
|---|---|
| $n,q$ | large prime Numbers |
| $Fq$ | finite field |
| $Z_n^*$ | $Z_n^* = [1, n-1]$ |
| $E/Fq$ | the elliptic curve $E$ defined in finite field $Fq$ |
| $G$ | an additive group of points on the elliptic curve $E/Fq$ with order $n$ |
| $P$ | the generator of additive group $G$ |
| $ID_i$ | the identity of communication entity $i$ |
| $H(*)$ | secure collision-free one-way hash functions |
| $(s,P_{pub})$ | master secret key/public key pair owned by the KGC |
| $(x_i,P_i)$ | secret value/public key pair of participant $i$, $P_i$ is calculated from $x_i$ |
| $d_i$ | $d_i$ is the partial private key of participant $i$ |
| $r_i$ | a random number generated by sender $i$ (i.e. ephemeral private key) for signcryption |
| $(sk_i,pk_i)$ | private key/public key pair of participant $i$, where $sk_i$=( $x_i$, $d_i$), $pk_i$=($P_i$) |
| $k$ | security parameter set by keg generator centre(KGC) |
| $m/\sigma$ | message plaintext / ciphertext with $k$ bits |
| $(M)_K$ | encrypt plaintext $M$ by secret key $K$ |
| $Signc_X(M)$ | entity $X$ generates signcryption of message $M$ |

**TABLE 2.** Algorithms of a CLSC scheme.

| Algorithm Name(Abbreviation) | Expression |
|---|---|
| setup(SETUP) | $\{s, system\ params\} \xleftarrow{\text{KGC}} \text{SETUP}(k)$ |
| Extract Partial Private Key (EPRK) | $\{d_i\} \xleftarrow{\text{KGC}} \text{EPRK}(s, ID_i, system\ params)$ |
| Set Secret Value(SV) | $\{x_i\} \xleftarrow{\text{user } i} \text{SV}(ID_i, system\ params)$ |
| Set Private Key(PRK) | $\{sk_i\} \xleftarrow{\text{user } i} \text{PRK}(d_i, x_i)$ |
| Set Public Key(PUK) | $\{pk_i\} \xleftarrow{\text{user } i} \text{PUK}(ID_i, x_i, system\ params)$ |
| Signcrypt (SC) | $\{\sigma\} \xleftarrow{\text{sender } i} \text{SC}(m, ID_i, sk_i, pk_i, ID_j, pk_j, system\ params)$ |
| Unsigncrypt (USC) | $\{m\ or\ \perp\} \xleftarrow{\text{receiver } j} \text{USC}(\sigma, ID_i, pk_i, ID_j, sk_j, pk_j)$ |

### B. INTRODUCTION OF OUR IMPROVED SCHEME IEAP-AKA

IEAP-AKA scheme consists of four phases: system initial phase, registration phase, authorization phase, authentication and key agreement phase.

#### 1) SYSTEM INITIAL PHASE:

In this phase, parameters in the authentication system are generated as follows:

(i) The network operator randomly chooses a prime number $q$ with $k$ bits, determines $\{Fq, E/Fq, G, P\}$ based on ECC.

(ii) The network operator randomly chooses $s_{pd} \in Z_n^*$ as master secret key and calculates the public key $P_{pdpub} = s_{pd}P$.

(iii) The network operator chooses secure collision-resistant one-way hash functions: $H_0(*) : (0, 1)^k \to (0, 1)^k$, $H_1(*) : (0, 1)^k \to (0, 1)^k$, $H_2(*) : (0, 1)^k, Z_n^*, Z_n^* \to Z_n^*$.

(iv) The network operator stores $s_{pd}$ and keeps parameters $\{F_q, E, G, P, P_{pdpub}, H_0, H_1, H_2\}$ in public.

### 2) REGISTRATION PHASE:

A user should follow the following steps when making a registration request to his/her hometown network operator:

(i) The user selects a UICC card from the network operator.

(ii) The network operator determines the IMSI for the UICC card selected by the registered user.

(iii) The user chooses a random number $SRAND$ recorded as $SRAND_0$, inputs registration password $PW_{pd}$, while the operator calculates initial secret key $K$ recorded as $K_0$ shared with the registered user based on $PW_{pd}$ and the fingerprint information $B$ collected by an equipment. Then, the operator calculates $K_{IUHi}(i = 0)$ and initial temporary identity $RMSI_i(i = 0)$ as follows.

$$K_i = \begin{cases} H_0(PW_{pd} \oplus B) & (i = 0) \\ H_0(SRAND_0 || K_0) & (i = 1) \\ H_0\left(SRAND_{(i-1)j} || K_{i-1}\right) & (i > 1, j = 1, \ldots N) \end{cases} \tag{1}$$

$$K_{IUHi} = H_0(K) = H_0(K_i) \tag{2}$$

$$RMSI_i = IMSI \oplus K_{IUHi} \tag{3}$$

The network operator stores $\{RMSI_0, SRAND_0$ in the UICC card and sends it to the registered user UE through secure channel. $\{RMSI_0, SRAND_0$ will be used as authentication information in the authentication and key agreement phase.

Besides, parameters with symbol $*$ listed in Table 3 have been stored in the database HSS of operator for every registered user. And the initial datas are recorded as $IDX_1, K_0, SRAND_0, K_1$.

Where, $IDX_i(i \geq 1)$ is the identity index for corresponding user and function $H128\_64$ () is used to take out the first 64 bits of the function variable.

$$IDX_i = \begin{cases} \text{H128\_64}(SRAND_0 \oplus K_0) \quad (i = 1) \\ IDX_{ij} = H128\_64\left(SRAND_{(i-1)j} \oplus K_{i-1}\right) \\ \qquad (i > 1, j = 1, \ldots N) \end{cases} \tag{4}$$

### 3) AUTHORIZATION PHASE:

In authorization phase, the network operator assigns secure parameters to legitimate AAA and HSS for signcryption in the authentication and key agreement phase. The specific steps are as follows:

(i) HSS randomly selects $x_H \in Z_n^*$, calculates public key $P_H = x_H P$, submits $\{ID_H, P_H\}$ to the network operator for authorization request. The operator randomly selects $t_H \in Z_n^*$, calculates $T_H = t_H P, l_H = H_0(ID_H, T_H, P_H) \in (0, 1)^k, d_H = \left(t_H + s_{pd} l_H\right) modq$, sets $d_H$ as partial private key of HSS, and sends it to HSS through a secure channel. HSS sets $(x_H, d_H)$ as the private key and $PK_H = (P_H, T_H)$ as the public key.

**TABLE 3.** **HSS database in improved scheme.**

| Security parameters | Symbol |
|---|---|
| User equipment* | UE |
| International mobile user identification code* | $IMSI$ |
| identity index（$i = 1$）* | $IDX_1$ |
| | $IDX_{(i+1)1}$ |
| | $IDX_{(i+1)2}$ |
| identity index（$i > 1$） | $IDX_{(i+1)3}$ |
| | … |
| | $IDX_{(i+1)N}$ |
| Initial/current shared secret key* | $K_{i-1}$（$i \geq 1$） |
| Random number（$i = 1$）* | $SRAND_0$ |
| | $SRAND_{i1}$ |
| | $SRAND_{i2}$ |
| Random number（$i > 1$） | $SRAND_{i3}$ |
| | … |
| | $SRAND_{iN}$ |
| Updated shared secret key* | $K_i$（$i \geq 1$） |

(ii) AAA randomly selects $x_A \in Z_n^*$, calculates public key $P_A = x_A P$, submits $\{ID_A, P_A\}$ to the network operator for authorization request. The operator randomly selects $t_A \in Z_n^*$, calculates $T_A = t_A P$, $l_A = H_0(ID_A, T_A, P_A) \in (0, 1)^k$, $d_A = \left(t_A + s_{pd} l_A\right) mod\ q$, sets $d_A$ as partial private key of AAA, and sends it to AAA through a secure channel. AAA sets $(x_A, d_A)$ as the private key and $PK_A = (P_A, T_A)$ as the public key.

(iii) WLAN AN randomly selects $x_W \in Z_n^*$, calculates public key $P_W = x_W P$, submits $\{ID_W, P_W\}$ to the network operator for authorization request. The operator randomly selects $t_W \in Z_n^*$, calculates $T_W = t_W P$, $l_W = H_0(ID_W, T_W, P_W) \in (0, 1)^k$, $d_W = \left(t_W + s_{pd} l_W\right) mod\ q$, sets $d_W$ as partial private key of WLAN AN, and sends it to WLAN AN through a secure channel. WLAN AN sets $(x_W, d_W)$ as the private key and $PK_W = (P_W, T_W)$ as the public key.

### 4) AUTHENTICATION AND KEY AGREEMENT PHASEL:

The steps of authentication and key agreement phase are shown in Figure 3 with the details as follows.

(i) WLAN AN and WLAN-UE start establishing a connection and executing mutual authentication.

(ii) WLAN AN requests user identity in Extensible Authentication Protocol over LAN (EAPOL) format.

(iii) When responding to the EAP request/identity for the $i$-th($i \geq 1$) time, WLAN-UE computes $K_{i-1}$, $K_{IUH(i-1)}$ and IMSI according to formula (1,2,5), computes identity index $IDX_i$, temporary identity $HMSI_i$ and shared secret key $K_i$, $RMSI_i$ according to formula (4,6,1,3), stores $K_i$

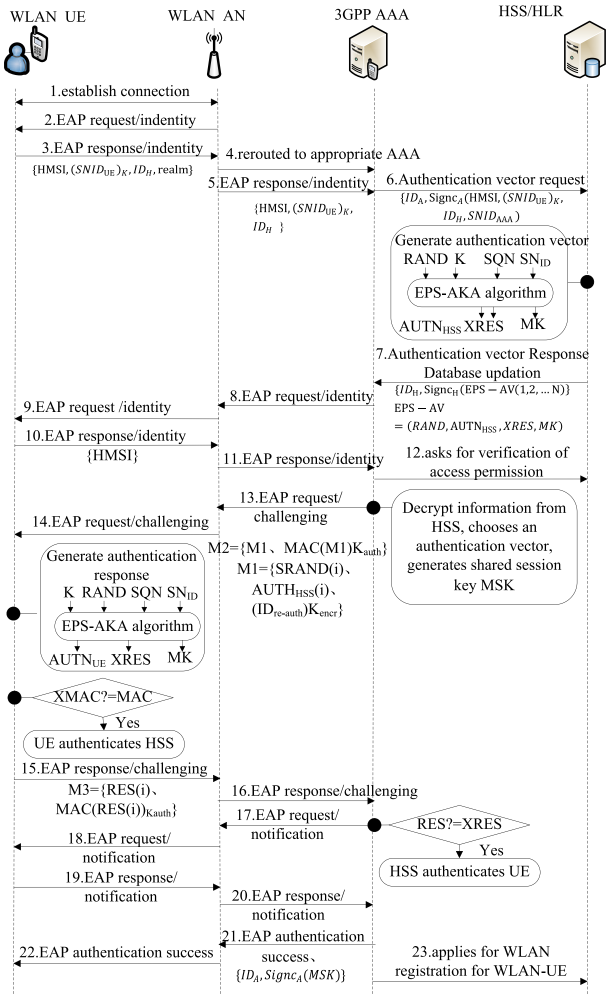
WLAN UE
WLAN AN
3GPP AAA
HSS/HLR
1.establish connection
2.EAP request/indentity
3.EAP response/indentity
{HMSI, $(SNID_{UE})_K$, $ID_H$, realm}
4.rerouted to appropriate AAA
5.EAP response/indentity
{HMSI, $(SNID_{UE})_K$, $ID_H$ }
6.Authentication vector request
{$ID_A$, $Signc_A$(HMSI, $(SNID_{UE})_K$, $ID_H$, $SNID_{AAA}$ )
Generate authentication vector
RAND K SQN $SN_{ID}$
EPS-AKA algorithm
$AUTN_{HSS}$ XRES MK
7.Authentication vector Response
Database updation
{$ID_H$, $Signc_H$(EPS − AV(1,2, ... N)}
EPS − AV = ($RAND$, $AUTN_{HSS}$, $XRES$, $MK$)
8.EAP request/identity
9.EAP request /identity
10.EAP response/identity
{HMSI}
11.EAP response/identity
12.asks for verification of access permission
13.EAP request/ challenging
Decrypt information from HSS, chooses an authentication vector, generates shared session key MSK
14.EAP request/challenging
M2={M1、MAC(M1)$K_{auth}$}
M1={SRAND(i)、$AUTH_{HSS}$(i)、$(ID_{re-auth})K_{encr}$}
Generate authentication response
K RAND SQN $SN_{ID}$
EPS-AKA algorithm
$AUTN_{UE}$ XRES MK
XMAC?=MAC
Yes
UE authenticates HSS
15.EAP response/challenging
M3={RES(i)、MAC(RES(i))$_{Kauth}$}
16.EAP response/challenging
17.EAP request/ notification
RES?=XRES
Yes
HSS authenticates UE
18.EAP request/ notification
19.EAP response/ notification
20.EAP response/ notification
21.EAP authentication success、
{$ID_A$, $Signc_A(MSK)$}
22.EAP authentication success
23.applies for WLAN registration for WLAN-UE

**FIGURE 3. Authentication and key agreement phase in IEAP-AKA authentication protocol.**

and $RMSI_i$.

$$IMSI = RMSI_{i-1} \oplus K_{IUHi-1} \tag{5}$$

$$HMSI_i = \begin{cases} IDX_1 || \mathrm{L}128\_64(SRAND_0 \oplus K_0 \oplus IMSI) \quad (i=1) \\ IDX_i || \mathrm{L}128\_64(SRAND_{(i-1)j} \oplus K_{i-1} \oplus IMSI) \\ \qquad (i > 1, j = 1, \ldots N) \end{cases} \tag{6}$$

where, function $L128\_64$ is used to take out the last 64 bits of the function variable.

Length of security parameters in EAP-AKA and our IEAP-AKA scheme are listed in Table 4 and Table 5.

Then, WLAN-UE sends EAP response/identity message to WLAN AN, which contains HMSI$_i$, $(SNID_{\mathrm{UE}})_{Ki}$, $ID_H$, realm}, and where $SNID_{\mathrm{UE}}$ is the identity of the access network WLAN AN that UE connects and $ID_H$ is the identity of HSS.

(iv) WLAN AN will be rerouted to appropriate AAA based on realm information, perhaps passing through one or more AAA proxy.

**TABLE 4. Length setting of security parameters for EAP-AKA protocol.**

| Security parameters | Length(bit) |
|---|---|
| $K$、$CK$、$IK$、$IMSI$、$RAND$ | 128 |
| $AK$、$AMF$、$SQN$ | 48 |
| $AUTN$ | 160 |
| $SN_{ID}$、$MAC$、$XMAC$、$RES$、$XRES$ | 64 |
| $K_{ASME}$ | 256 |

**TABLE 5. Length setting of security parameters for protocol in this paper.**

| Security parameters | Length(bit) |
|---|---|
| $K_{IUH}$、$HMSI$、$SRAND$ | 128 |
| $IDX$ | 64 |

(v) The WLAN AN forwards the EAP response/identity message to AAA.

(vi) Based on HMSI, AAA searches in its database and checks whether there is an unused authentication vectors available for the user. If an unused authentication vector is not available, AAA requests an authentication vector from HSS. The message includes

$$\{ID_A, Signc_A(HMSI_i, (SNID_{UE})_{Ki}, ID_H, SNID_{AAA})$$

where $SNID_{AAA}$ is the identity of the access network WLAN AN that AAA connects and $ID_A$ is the identity of AAA.

(vii) On receiving the message from AAA, HSS executes the following steps.

HSS accomplishes the identity authentication of AAA by verifying the received signcryption information using the public key $PK_A = (P_A, T_A)$ of AAA that is corresponding to ID$_{\mathrm{A}}$ in the database of HSS and his own secret key $(x_H, d_H)$.

According to the decrypted information $HMSI_i$, HSS extracts $IDX_i$ according to formula 6, searches the database in Table 3 , obtains $K_{i-1}$, $SRAND_{i-1}$,and IMSI according to the mapping relation and verifies $HMSI_i$ by checking whether $L128\_64(HMSI_i) = (SRAND_{i-1} \oplus K_{i-1} \oplus IMSI)$ or not. Let $N$ be the number of authentication vectors that HSS generates in one time. HSS obtains updated shared secret key $K_i$, chooses $N$ random numbers recorded as $SRAND_{ij}$ $(j = 1, 2, \ldots N)$, uses EPS-AV generating algorithm list below to generate authentication vectors for authentication in this round, in which $SQN$ is a sequence number produced by the serial number counter owned by HSS, $AMF$ is the authentication management filed of the HSS, which is the domain name of the network to which the user belongs, $MAC$ is the message authentication code, $AUTN$ is the authentication token, Master Key ($MK$) is used to derive the shared keys between UE and AAA and between UE and WLAN AN in the following processes. $f_1$ and $f_2$ are authentication functions, $f_3, f_4, f_5$ and $KDF$ are key derivation functions. In our proposed protocol, $SRAND$, $K_i$ are used to replace $RAND$ and $K$ in original EPS-AKA protocol.

$$XRES = f_{2K}(RAND) \tag{7}$$

$$CK = f_{3K}\,(RAND) \tag{8}$$
$$IK = f_{4K}\,(RAND) \tag{9}$$
$$AK = f_{5K}\,(RAND) \tag{10}$$
$$MK = KDF(CK, IK, SN_{ID}, SQN) \tag{11}$$
$$MAC = f_{1K}\,(SQN||RAND||AMF) \tag{12}$$
$$AUTN_{HSS} = (SQN \oplus AK||AMF||MAC) \tag{13}$$
$$EPS - AV = (RAND, AUTN_{HSS}, XRES, MK) \tag{14}$$

Then, as listed in Table 3, HSS updates identity index with $IDX_{(i+1)j}$ $(j = 1, 2, \ldots N)$ according to formula (4), updates current shared secret key with $K_i$, updates random number with $SRAND_{ij}$ $(j = 1, 2, \ldots N)$ to build the mapping relationship for a new round of entire EAP-AKA authentication.

Then, HSS decrypts $(SNID_{\mathrm{UE}})_{Ki}$ by $K_i$ and verifies whether $SNID_{\mathrm{UE}} = SNID_{AAA}$ or not, so as to accomplishes the identity authentication of WLAN AN to avoid redirection attack. Then, HSS sends signcryption information to AAA containing $\{ID_H, Signc_H(EPS - AV(1, 2, \ldots N)\}$.

(viii) AAA sends EAP-request/identity message to WLAN AN one more time.

(ix) WLAN AN forwards EAP request/identity message to WLAN-UE one more time.

(x) WLAN-UE sends EAP response/identity message containing HMSI$_i$ to WLAN-AN one more time.

(xi) WLAN AN forwards EAP response/identity message to AAA. AAA compares the HMSI$_i$ in successive EAP response/identity message. If they are not the same, AAA asks for authentication vectors from HSS one more time.

(xii) AAA checks whether there is configuration information to access WLAN for WLAN-UE stored in its database. If no configuration information is available, AAA asks for verification of access permission from HSS.

(xiii) AAA decrypts $\{ID_H, Signc_H(EPS - AV(1, 2, \ldots N)\}$ using the public key $PK_H = (P_H, T_H)$ of HSS that is corresponding to $ID_H$ and his own secret key $(x_A, d_A)$ to authenticate HSS, chooses an authentication vector $EPS - AV(j)(j = 1, or\ 2, or\ \ldots\ or\ N)$, generates session key $K_{encr}$ and integrity key $K_{auth}$ from $MK$ for AAA and WLAN-UE and secure communication key $MSK$ for WLAN-UE and WLAN AN, generates $ID_{re-auth}$ for re-authenticaiton and encrypts them using $K_{encr}$. Then, AAA sends challenging request message M2 to WLAN AN, where $MAC\ (M1)_{Kauth}$ is message authentication code calculated using $K_{auth}$, $(ID_{re-auth})_{Kencr}$ is a re-authenticaiton identity encrypted by $K_{encr}$, and $AUTN_{HSS(i)}$ is generated using EPS-AV generating algorithm in original EAP-AKA protocol.

$$M1 = \left\{SRAND_{ij}, AUTN_{HSS(i)}, (ID_{re-auth})_{Kencr}\right\} \quad (j = 1, or\ 2, or\ \ldots or\ N) \tag{15}$$
$$M2 = \{M1, MAC(M1)_{Kauth} \tag{16}$$

(xiv) WLAN AN forwards EAP challenging request message to WLAN-UE.

(xv) WLAN-UE accomplishes the challenging based on the same algorithm in EAP-AKA, computes $MK$ by shared secret key $K_i$ and received $SRAND_{ij}$, extracts $SQN$ from received $AUTN_{HSS(i)}$, computes X$MAC$ and compares it with $MAC$ extracted from $AUTN_{HSS(i)}$. Then WLAN-UE accepts HSS when $XMAC = MAC$, generates session key $K_{encr}$ and integrity key $K_{auth}$ from $MK$, verifies the integrity of message M2, obtains $ID_{re-auth}$ by decryption using $K_{encr}$, and computes $MSK$. Then, WLAN-UE sends challenging reply message M3 to WLAN AN.

$$RES(i) = f_{2Ki}\left(SRAND_{ij}\right) \tag{17}$$
$$M3 = \{RES(i), MAC(RES(i))_{Kauth}\} \tag{18}$$

(xvi) WLAN AN forwards challenging reply message to AAA.

(xvii) After the validation of the integrity of message M3, AAA compares $RES$ and $XRES$. If they are equal, AAA sends notification request message to WLAN AN.

(xviii) WLAN AN forwards notification request message to WLAN-UE.

(xix) WLAN-UE sends notification response message to WLAN AN.

(xx) WLAN AN forwards notification response message to AAA.

(xxi) AAA sends EAP authentication successful message and $\{ID_A, Signc_A(MSK)\}$ to WLAN AN.

(xxii) WLAN AN obtains the $MSK$ by decrypting the signcryption information using the public key $PK_A = (P_A, T_A)$ of AAA that is corresponding to $ID_A$ and his own secret key $(x_W, d_W)$ and forwards authentication successful message to WLAN-UE.

(xxiii) AAA applies for WLAN registration for WLAN-UE from HSS.

## IV. ANALYSIS ON IEAP-AKA SCHEME

### A. SECURITY ANALYSIS

In summarize, our improved IEAP-AKA protocol avoids many defects in the EAP-AKA protocol, which improves the security of 3GPP LTE-WLAN heterogeneous converged network, and provides all security services as that in the original 3GPP LTE-WLAN network, namely mutual authentication between communication entities, security establishment and key negotiation in non-access layer and access layer. Table 6 summarizes the methods we adopt to solve the security defects in original EAP-AKA protocol. And Table 7 summarizes the security features of our protocol and some existing improved protocols. Analysis below shows that our protocol provides the most security features and the highest security level.

#### 1) USER IMPERSONATION ATTACK:

It is practical that the attacker traps the login message of a legal user in step (iii) during the execution of the authentication. In order to respond to the EAP request/identity for the $i$ -th $(i \geq 1)$ time, the attacker has to compute valid $HMSI_i$. As the attacker cannot compute $HMSI_i$ without the

**TABLE 6. Methods adopted to solve the security defects.**

| | security defects in original EAP-AKA protocol | the methods we adopt to solve the security defects |
|---|---|---|
| i | Do not accomplish authentication between AAA and HSS, between AAA and WLAN AN | Accomplishes authentication between AAA and HSS, between AAA and WLAN AN based on certificateless signcryption(CLSC) scheme |
| ii | Vital authentication information are transmitted in plaintext between HSS and AAA, between AAA and WLAN AN(such as $MSK$，$SN_{ID}$，authentication vectors) | Messages are encrypted and transmitted between HSS and AAA, between AAA and WLAN AN based on certificateless signcryption(CLSC) scheme |
| iii | Vulnerability of privacy protection for user identity information IMSI | Identity index is adopted to protect user identity privacy |
| iv | A single initial secret key is shared between UE and HSS which cannot support forward security | Hash chain is adopted to update the shared key, providing forward security |
| v | Redirect attack(mendacious access point attack) | AAA successfully accomplishes the identity authentication of WLAN AN based on CLSC, update mechanism for shared secret key |
| vi | Replay attack, man-in-the-middle attack | Update mechanism for user identity information HMSI |
| vii | DoS attack | Update mechanism for user identity information HMSI |

**TABLE 7. comparison between improved EAP-AKA protocols(in security).**

| Protocol | Our protocol | [4] | [9] | [11] | [12] | [14] | [15] |
|---|---|---|---|---|---|---|---|
| cryptography | Hybrid | Hybrid | Hybrid | Hybrid | Hybrid | public key cryptosystem | public key cryptosystem |
| anonymous protection for IMSI | yes | yes | no | no | yes | yes | yes |
| update on shared key | yes | no | yes | no | no | no | yes |
| Mutual authentication between WLAN AN and AAA | yes | yes | yes | yes | yes | yes | no |
| Mutual authentication between HSS and AAA | yes | no | no | yes | no | no | no |
| Mutual authentication between UE and HSS | yes | yes | yes | yes | yes | no | yes |
| protection for MSK | yes | yes | yes | no | yes | no | no |
| Framework modification from the original protocol | no | yes | no | yes | yes | yes | yes |
| other defects has been found | no | yes | yes | yes | yes | yes | yes |

knowledge of the shared secret key $K_{i-1}$, $IMSI$ and $IDX_i$. Besides, in order to be authenticated by HSS and respond to the EAP response/challenging in step (xv), the attacker has to compute valid $RES$. As the attacker cannot compute the challenging reply message $RES$ without the knowledge of the shared secret key $K_i$. It is clear that the attacker cannot derive shared session keys $K_{encr}$ and $MSK$ without the knowledge of $K_i$ to communicate with AAA and WLAN AN.

Furthermore, in the authentication process, other legal communication entities also fail to impersonate as legal WLAN-UE. For legal WLAN AN, who forwards all the messages from WLAN-UE to AAA, cannot accomplish key agreement with AAA without the knowledge of the valid $MK$ to derive $K_{encr}$ to communicate with legal AAA in the following communication. As introduced in section I, AAA server implements mutual authentication with UE, where HSS is a central database storing user authentication information [3]. It means that privileged insider in legal AAA may launch user impersonation attack. And our protocol can resist such insider attack, which will be analyzed as follows. Therefore, our protocol can resist user impersonation attack.

### 2) PRIVILEGED INSIDER ATTACK:

It is practically assumed that the server AAA authenticated by HSS is trusted. But, the communication system may be ruined due to the presence of an insider. So, the server AAA cannot gain control over the secret information of the user. In our protocol, the original password and the fingerprint information transmitted in registration phase are masked. And it is computationally infeasible to extract the password of the user due to the non-invertible property of the one-way hash function. Furthermore, the insider of AAA server cannot compute $HMSI_i$ without the knowledge of the shared secret key $K_{i-1}$, $IMSI$ and $IDX_i$ which are kept secret in HSS. Hence, our protocol can resist privileged insider attack.

### 3) WLAN AN IMPERSONATION ATTACK:

Attacker extracts the parameters from the transmitted message in the $i$-th($i \geq 1$) time authentication in step(v) over the public channel and guesses the parameters $HMSI_i$, $(SNID_{UE})_{Ki}$ and transmits to AAA. However, the computation of $HMSI_i(SNID_{UE})_{Ki}$ relies on the secret parameters $K_{i-1}$, $IMSI$, $IDX_i$ and $K_i$. The attacker cannot guess them in polynomial time. Thus, our protocol can resist WLAN AN impersonation attack.

### 4) AAA IMPERSONATION ATTACK:

To impersonate legal AAA, the attacker has to compute the signcryption message sent to HSS in step (vi) and successfully decrypt the signcryption message sent from HSS to generate $K_{encr}$, $K_{auth}$ and $MSK$ in step (xiii). As the attacker cannot successfully accomplish the tasks above without the knowledge of secret keys $(x_A, d_A)$ owned by legal AAA. Therefore, our protocol can resist AAA impersonation attack.

Furthermore, legal entities also fail to impersonate as legal AAA. For legal WLAN AN, who forwards all the messages from AAA to WLAN-UE, cannot accomplish key agreement with WLAN-UE without the knowledge of the valid $MK$ to derive $K_{encr}$ to communicate with legal UE in the following communication.

### 5) REPLAY ATTACK:

The attacker captures the previous transmitted message to launch the replay attack to make the received entity believe that the transmitted message is from legal entity and fresh. For WLAN-UE, *HMSI* and shared secret key $K_i$ are both updated in every round of authentication, which means that the attacker who replays the previous login message in step (iii) and the response challenging message in step (xv) cannot achieve connection to HSS and be authenticated by HSS. As the previous messages contains invalid *HMSI* and *RES* for a new round of authentication.

According to our previous research [16], each signcrypted message sent by the signcryptioner contains a different randomly chosen number $r_s$ which is used to make message fresh. The receiver rejects the message sent by the attacker due to invalid random number implied in the replay message sent by the attacker. In this way, the attacker fails to impersonate AAA to communicate with HSS and WLAN AN in step (vi) and (xxi) respectively by replay attack. Besides, messages sent by AAA in step (vi) and (xiii) contains the shared secret key $K_i$, derived session key *Kencr* and integrity key *Kauth*, which are updated in every round of authentication, which means that the attacker who replays the previous message in step (vi) and (xiii) cannot successfully communicate with HSS and WLAN AN as legal AAA.

Similarly, the attacker fails to impersonate HSS by replay attack in step (vii) since message sent from HSS to AAA is signcrypted. Legal AAA rejects the message sent by the attacker due to invalid random number implied in the replay message sent by the attacker.

To impersonate legal WLAN AN, the attacker who replays the previous message in step (v) fails to achieve connection to AAA. As in the previous messages, $SNID_{\mathrm{UE}}$ is encrypted by previous shared secret key $K_i$. However, $K_i$ is updated in every round of authentication, then, it is clear that HSS decrypts $(SNID_{\mathrm{UE}})_{Ki}$ by new $K_i$ and verifies that $SNID_{\mathrm{UE}} = SNID_{AAA}$ is not valid in step (vii). Then, the attacker fails to impersonate WLAN AN by replay attack.

Hence, our protocol can resist replay attack.

### 6) MUTUAL AUTHENTICATION:

Based on certificateless public key mechanism and signcryption scheme, our IEAP-AKA scheme accomplishes the authentication between communication entities. During the execution of the protocol, HSS accomplishes the identity authentication of AAA by verifying the received signcryption information sent by AAA in step vii, while AAA authenticates HSS in step (xiii). AAA accomplishes the authentication of WLAN AN in step (vii) by verifying whether $SNID_{\mathrm{UE}} = SNID_{AAA}$ or not, while WLAN AN authenticates AAA in step (xxii) by verifying the received signcryption information sent by AAA. Furthermore, our proposed protocol accomplishes authentication between WLAN-UE and HSS (legal AAA is responsible for HSS to implement the authentication [3]) by verifying whether $XMAC = MAC$, $RES = XRES$ or not respectively in step (xv) and (xvii), which is the same method as that in the original EAP-AKA protocol. Finally, our protocol negotiates session keys when performing the mutual authentication between communication entities, where session key $K_{encr}$ and integrity key $K_{auth}$ are generated for AAA and WLAN-UE and $MSK$ is generated for WLAN-UE and WLAN AN.

### 7) CRUCIAL AUTHENTICATION INFORMATION ENCRYPTED:

Our IEAP-AKA scheme achieves encryption for crucial authentication information based on our secure certificateless signcryption(CLSC) scheme and traditional encryption algorithm. Authentication vectors sent from HSS to AAA are signcrypted by HSS, session key $MSK$ transmitted from AAA to WLAN AN is signcrypted by AAA, and $SN_{ID}$ is encrypted by the shared secret key $K_i$.

### 8) IDENTITY ANONYMITY, UNTRACEABILITY AND DYNAMIC:

In our IEAP-AKA scheme, identity index is proposed to achieve identity anonymity, untraceability and dynamic. Instead of sending IMSI in plaintext in traditional EAP-AKA scheme, HMSI is used in our scheme, which contains identity index, hidden information for IMSI, shared secret key and a random number. On receiving HMSI, HSS verifies the legitimacy of HMSI by searching his database according to the identity index. Besides, HMSI is updated in every round of authentication, which achieves identity untraceability and dynamic simultaneously and avoids attackers sending connection request via replay attack.

### 9) FORWARD SECURITY PROPERTY:

Forward secrecy was first used in [17] in the context of session key exchange protocols. The basic idea is that compromise of long term keys does not compromise past session keys, meaning that past actions are protected in some way against loss of the current key. The same basic idea is described in a different context by M. Bellare and S. K. Miner in 1999 in their digital signature scheme in which the public key is fixed but the secret signing key is updated at regular intervals so as to provide a forward security property: compromise of the current secret key does not enable an adversary to forge signatures pertaining to the past. [18] Generally, in different contexts, as described in [19] forward security means an adversary would not compromise the previous confidential information even if it obtained the current confidential information. Various methods can be used to realize forward security in protocol design. Hash operation which is nonreversible can be used to provide forward security [19], [20]. In our protocol, a simple one-way hash chain technology which contains ( Formula 1) is adopted to update the shared key $K$ between UE and HSS, solving the problem that the security of authentication process only depends on a single initial shared key $K$. In the authentication process for the $i$-th ($i \geq 1$) time, shared key $K_i$ is used to compute the Master Key ($MK$) in step (vii), $MK$ is used to derive session key $K_{encr}$, integrity key $K_{auth}$ for AAA and WLAN-UE and session key $MSK$ for WLAN-UE and WLAN AN in step (xiii). It is clear that even if the attacker obtains the current key $K_i$, $K_{i-1}$ cannot be calculated according to the one-way hash function, so as to ensure the previous confidential information. Therefore, our protocol can provide forward security.

### 10) REDIRECT ATTACK:

In our IEAP-AKA scheme, the identity $SNID_{UE}$ of the access network WLAN AN that UE connects is encrypted by secret key, that is $(SNID_{UE})_K$, while the identity $SNID_{AAA}$ of the access network WLAN AN that AAA connects is signcrypted by the secret key $(x_A, d_A)$ of AAA, that is $Signc_A(SNID_{AAA})$. Therefore, HSS can avoid redirect attacks by checking whether $SNID_{UE} = SNID_{AAA}$ or not. Besides, secret key $K$ is updated in every round of authentication, which avoids attackers sending replay message $(SNID_{UE})_K$ to achieve redirect attack.

### 11) Man-In-The-Middle Attack:

The update mechanism of *HMSI* makes our scheme resist replay attacks. Therefore, if the attacker sends *HMSI* to HSS to request connection through replay attacks, HSS will judge the attacker as an illegal user. Then, the attacker cannot obtain authentication vectors to accomplish man-in-the-middle attacks.

### 12) DoS ATTACK:

In our protocol, the user identity *HMSI* and the shared key are updated in each round of IEAP-AKA authentication, by which the attacker cannot cause DoS attack by replaying *HMSI*. Even if *HMSI* is replayed by attackers, HSS can immediately find the mistake identity information sent by the attackers through the updated identity index *IDX*, thus avoiding DoS attacks which may eat up time and bandwidth to generate and transmit authentication messages. In addition, according to formula (6), parameters *SRAND* and $K$ in *HMSI* are also updated which also effectively avoids DoS attacks.

**TABLE 8.** Calculation time of relevant cryptography operations.

| Symbol | description | calculation time（$us$） |
|---|---|---|
| $T_{HMAC}$ | Calculation time of function HMAC-SHA-256 | 0.55 |
| $T_E$ | Calculation time of symmetric encryption function AES | 130.3 |
| $T_h$ | Calculation time of function SHA1 | 0.4 |
| $T_{AE}$ | The calculation time of the algorithm in asymmetric (public key) cryptosystem | $T_{AE} \approx 100T_E$ |
| $T_{hc}$ | The calculation time of one-way hash chain, which is determined based on the length $l$ of the hash chain | $T_{hc} = lT_h$ |

## B. PERFORMANCE ANALYSIS

Table 8 shows the calculation time [21], [22] of relevant cryptography operations used in the improved schemes mentioned above with the same platform in [23]. As shown in the table, the calculation time of encryption and decryption algorithm in traditional asymmetric (public key) cryptosystem is about 100 times that of in symmetric cryptosystem [4], while the calculation time of the algorithm in public key cryptosystem based on elliptic curve is lower than that of in public key cryptosystem. Since the specific public key cryptography algorithm is not given in improved protocols above, the calculation time of the algorithms in asymmetric (public key) cryptosystem $T_{AE}$ is approximately set to $T_{AE} \approx 100T_E$.

The performance evaluation of authentication protocol is difficult to calculate accurately, which depends on many factors of the actual network, such as bandwidth of the communication channel, topology of the network, calculation capacity and physical location of the mobile devices, and etc. In addition, some improved EAP-AKA protocols above make a lot of framework modifications from the original protocol. Therefore, it is difficult to provide accurate performance analysis of each protocol, and the performance analysis is roughly analyzed and compared, as shown in table 9 with the same platform in [23].

Comparison of the time of UE and the total calculation time is shown in Figure 4 and Figure 5 according to the data in Table 9. Due to the limited resources and bottleneck of power supply in UE, calculation time in each communication entity should be reduced especially for UE, while ensuring the basic security performances.

It can be seen from Figure 4 and Figure 5 that protocols in [9], [11] and our protocol have lower computation cost with little difference. However, according to section II and Table 7, both protocols in [9] and [11] have security vulnerabilities.

**TABLE 9. Comparison between improved EAP-AKA protocols(in Performance).**

| Calculation time （*us*） | UE | WLAN AN | AAA | HSS | total |
|---|---|---|---|---|---|
| Our scheme | $9T_{HMAC}+2T_E$<br>(265.55) | $T_{AE}$<br>(13030) | $3T_{AE}+2T_{HMAC}$<br>$+1T_E$(39221) | $2T_{AE}+6T_{HMAC}+1T_h$<br>$+1T_E$(26584.9) | $6T_{AE}+17T_{HMAC}+1T_h$<br>$+4T_E$(78710.95) |
| [4]<br>$l=2$ | $1T_{AE}+9T_{HMAC}+1T_{hc}$<br>$+3T_E$(13426.65) | $1T_{AE}+1T_{HMAC}$<br>$+2T_E$(13291.15) | $5T_{HMAC}+1T_{hc}$<br>$+4T_E$(524.75) | $5T_{HMAC}+3T_E$<br>(293.65) | $2T_{AE}+20T_{HMAC}+2T_{hc}$<br>$+12T_E$(27636.2) |
| [9] | $7T_{HMAC}+1T_h+2T_E$<br>(264.85) | $3T_{AE}+1T_h$<br>(39090.4) | $3T_{AE}+2T_{HMAC}+2T_h$<br>$+2T_E$(39352.5) | $5T_{HMAC}$<br>(2.75) | $6T_{AE}+14T_{HMAC}+4T_h$<br>$+4T_E$(78710.5) |
| [11] | $9T_{HMAC}+1T_E$<br>(135.25) | $2T_{AE}$<br>(26060) | $2T_{AE}+2T_{HMAC}$<br>(26061.1) | $2T_{AE}+7T_{HMAC}+1T_E$<br>(26194.15) | $6T_{AE}+18T_{HMAC}+2T_E$<br>(78450.5) |
| [12]<br>$l=2$ | $1T_{AE}+4T_{HMAC}+2T_{hc}$<br>$+1T_h+1T_E$(13164.5) | $2T_{AE}+1T_{HMAC}+4T_h$<br>$+1T_E$(26192.45) | $3T_{AE}+3T_{HMAC}+4T_h$<br>$+2T_E$(39353.85) | 0 | $6T_{AE}+8T_{HMAC}+2T_{hc}$<br>$+9T_h+4T_E$(78710.8) |
| [14] | $1T_{AE}+3T_{HMAC}$<br>(13031.65) | $1T_{AE}$<br>(13030) | $6T_{AE}+6T_{HMAC}$<br>(52121.65) | 0 | $6T_{AE}+6T_{HMAC}$<br>(78183.3) |
| [15] | $2T_{AE}+7T_{HMAC}$<br>(26063.85) | $2T_{HMAC}$<br>(1.1) | $1T_{AE}$<br>(13030) | $1T_{AE}+5T_{HMAC}$<br>13032.75 | $4T_{AE}+14T_{HMAC}$<br>(52127.7) |

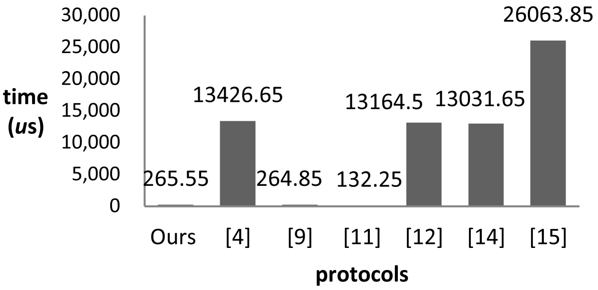

**FIGURE 4.** comparison in calculation time of UE between improved authentication schemes.

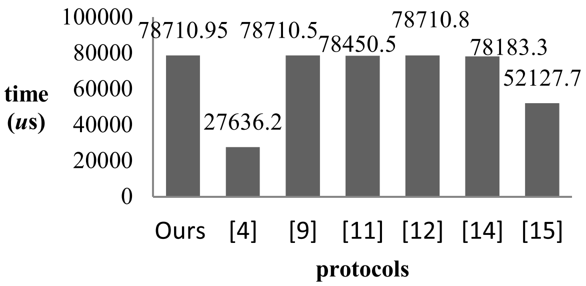

**FIGURE 5.** comparison in total calculation time of all communication entities between improved authentication schemes.

Although authentication parameters such as authentication vectors are generated by AAA, which reduces the calculation burden of HSS and the communication time delay between AAA and HSS in some protocols [12], [14], too many framework modifications are made from the original EAP-AKA protocol.

In summarize, the comprehensive security and performance analysis shows that our protocol provides higher security with lower execution time.

### *C. OTHER ANALYSIS*

As mentioned above, our protocol improves the security of EAP-AKA/EAP-AKA' authentication protocol by using some cryptographic techniques. Although our improved protocol provides more security properties without framework modification from the original protocol, the storage capacity and the computation performance of communication entities should be improved to accomplish the authentication process in our protocol. For example, (i) in system initial phase, network operator should store master secret key $S_{pd}$ and calculate the public key $P_{pdpub}$. (ii) in registration phase, HSS should increase the memory requirement to store identity index for anonymous identity protection. (iii) in authorization phase and authentication and key agreement phase, in order to implement certificateless signcryption scheme in our authentication process, communication entities including HSS, AAA and WLAN AN should increase the computation and storage. And UE should calculate $(SNID_{\mathrm{UE}})_{Ki}$ to achieve encryption for crucial authentication information, which may increase the calculation burden of UE.

However, according to the analysis results in TABLE 5 and 9, all the increase of computation and storage is very limited and means nothing for communication entities with abundant resources and sufficient power supply, such as HSS, AAA and WLAN AN. Besides, such increase is also very limited even for UE as computer processing performance continues to increase.

## V. CONCLUSION

Hybrid cryptosystem and cryptographic techniques have been proposed to construct an improved authentication protocol based on EAP-AKA/EAP-AKA' in LTE-WLAN heterogeneous converge network launched by 3GPP. These techniques, including certificateless signcryption(CLSC) scheme without pairing calculation based on ECC, hash chain and identity index mechanism, aim to repair the security loopholes that exist in EAP-AKA/EAP-AKA' protocol and the improved schemes discussed above in section II of this paper. Through the informal security analysis, we have shown that the proposed protocol satisfies known security attributes for authentication protocols, including anonymous protection for user identity, update on shared keys, protection for MSK, resistance to impersonation attack, replay attack, man-in-the-middle attack, redirect attack and DoS attack, mutual authentication between communication entities, and without framework modification from the original protocol. Computational efficiency of proposed protocol presents its lightweight attribute especially in user equipment. This makes the protocol more appropriate for portable mobile equipment.

## REFERENCES

[1] A. K. Salkintzis, C. Fors, and R. Pazhyannur, "WLAN-GPRS integration for next-generation mobile data networks," *IEEE Wireless Commun.*, vol. 9, no. 5, pp. 112–124, Oct. 2002.

[2] H. L. Yu, "Implementation of evolution from mobile packet core network to EPC," *Mobile Commun.*, no. 1, pp. 121–125, Feb. 2011.

[3] W. M. Lang, Q. Jiao, D. H. Hu, and J. Z. Liu, "Researches on the system architecture with LTE and non-3GPP access networks," *Designing Techn. Posts Telecommun.*, no. 8, pp. 41–44, Aug. 2010.

[4] J. Q. Fu, "Research on security protocols in 3G-WLAN integrated network," Ph. D dissertation, College Comput. Sci. Technol., Zhe Jiang Univ., Hangzhou, China, 2010.

[5] *Technical Specification Group Services and System Aspects; 3G Security; Wireless Local Area Network (WLAN) Interworking Security*, document TS33.234 V15.0.0, 3GPP, 2018. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/33_series/33.234/

[6] *Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')*, document RFC 5448, IETF, 2009. [Online]. Available: http://www.rfc-editor.org/info/rfc5448

[7] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 283–302, 1st Quart., 2014.

[8] F. B. Degefa, D. Lee, J. Kim, Y. Choi, and D. Won, "Performance and security enhanced authentication and key agreement protocol for SAE/LTE network," *Comput. Netw.*, vol. 94, pp. 145–163, Jan. 2016.

[9] C. Dong and C. Wang, "A new amended authentication protocol in 3G-WLAN interworking," in *Proc. 3rd Int. Conf. Instrum., Meas., Comput., Commun. Control*, Sep. 2013, pp. 1261–1265.

[10] Y.-M. Tseng, "USIM-based EAP-TLS authentication protocol for wireless local area networks," *Comput. Standards Interfaces*, vol. 31, pp. 128–136, Jan. 2009.

[11] I. Elbouabidi, F. Zarai, M. S. Obaidat, and L. Kamoun, "An efficient design and validation technique for secure handover between 3GPP LTE and WLANs systems," *J. Syst. Softw.*, vol. 91, no. 1, pp. 163–173, May 2014.

[12] W.-C. Wu and H.-T. Liaw, "An authentication, authorization, and accounting mechanism for 3G/WLAN networks," *Secur. Commun. Netw.*, vol. 9, pp. 468–480, Apr. 2016.

[13] S. Zhang, G. A. Xu, Z. M. Hu, and Y. X. Yang, "Analysis and amendment of EAP-AKA protocol," *Res. Comput.*, no. 7, pp. 234–236, Jul. 2005.

[14] R. Bassoli, H. Marques, J. Rodriguez, C. Gruet, and R. Tafazolli, "Enhanced authentication for WLAN–EPS interworking systems," *Electron. Lett.*, vol. 51, pp. 1544–1546, Sep. 2015.

[15] Y. El Hajjaji El Idrissi, N. Zahid, and M. Jedra, "Security analysis of 3GPP (LTE)—WLAN interworking and a new local authentication method based on EAP-AKA," in *Proc. 1st Int. Conf. Future Gener. Commun. Technol.*, London, U.K., Dec. 2012, pp. 137–142.

[16] L. Cao and W. Ge, "Analysis of certificateless signcryption schemes and construction of a secure and efficient pairing-free one based on ECC," *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 9, pp. 4527–4547, Sep. 2018.

[17] C. G. Günther, "An identity-based key-exchange protocol," in *Proc. 7th Eur. Workshop Theory Appl. Cryptograph. Techn.*, Houthalen, Belgium, Apr. 1989, pp. 29–37.

[18] M. Bellare and S. K. Miner, "A forward-secure digital signature scheme," in *Proc. 19th Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, Dec. 1999, pp. 431–448.

[19] L. He, X.-M. Lu, S.-H. Jin, and Z.-Y. Cai, "A one-way hash based low-cost authentication protocol with forward security in RFID system," in *Proc. 2nd Int. Asia Conf. Inform. Control, Autom. Robot.*, Y. Wu and J. Liu, Eds., Mar. 2010, pp. 269–272.

[20] S. Bittl, "Efficient construction of infinite length hash chains with perfect forward secrecy using two independent hash functions," in *Proc. 11th Int. Conf. Secur. Cryptogr. (SECRYPT)*, Aug. 2014, pp. 1–8.

[21] F. Wu, L. Xu, S. Kumari, and X. Li, "A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks," *Comput. Elect. Eng.*, vol. 45, pp. 274–285, Jul. 2015.

[22] K. Hamandi, I. Sarji, A. Chehab, I. H. Elhajj, and A. Kayssi, "Privacy enhanced and computationally efficient HSK-AKA LTE scheme," in *Proc. 27th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, L. Barolli, F. Xhafa, M. Takizawa, T. Enokido, and H. H. Hsu, Eds., Mar. 2013, pp. 929–934.

[23] L. Xu and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care," *J. Med. Syst.*, vol. 39, p. 10, Feb. 2015.

**LILING CAO** was born in Hengyang, Hunan, China, in 1982. She received the B.S. degree in electronic information science and technology and the M.S. degree in physics electronics from Central South University, in 2004 and 2007, respectively, and the Ph.D. degree in testing technology and automation from Tongji University, in 2017.

Since 2017, she has been a Senior Engineer with the College of Engineering Science and Technology, Shanghai Ocean University. Her main research interests include network security and authentication protocol.

**YUQING LIU** was born in 1976. She received the B.S. degree in industry automation, in 1999, the M.S. degree in control theory and control engineering, in 2002, and the Ph.D. degree in structural engineering, in 2005, from the Wuhan University of Technology.

She is currently an Associate Professor with the College of Engineering Science and Technology, Shanghai Ocean University. Her main research interests include the marine Internet of Things engineering, fisheries engineering, and automation technology research.

**SHOUQI CAO** was born in 1973. He received the B.S. degree in mechanical manufacturing technology and equipment, the M.S. degree in mechanical manufacturing and automation, and the Postdoctoral degree in control science and engineering from Sichuan University, in 1996, 1999, and 2009, respectively.

He is currently a Professor and a Doctoral Supervisor with the College of Engineering Science and Technology, Shanghai Ocean University. His main research interests include the marine Internet of Things engineering, fisheries engineering, and automation technology research.