# Anonymous Delegation-based Authenticated Key Agreement Protocol for Global Mobility Networks with Communication Privacy

Zuowen Tan[1,2]

[1] School of Information Technology, Jiangxi University of Finance and Economics, China
[2] Key Laboratory of Information Security, School of Mathematics and Information Science, Guangzhou University, China
tanzyw@163.com

## Abstract

Global mobility networks are designed to accommodate service from local network service provider along with user's movement. We present a new delegation-based authentication protocol using the Elliptic curve cryptosystems. We give the formal security analysis using the Burrows-Abadi-Needham (BAN) logic along with random oracle models. We perform the formal security verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool to demonstrate that the presented scheme is secure. In addition, better trade-off among security and functionality features, and communication and computation costs makes our scheme suitable and applicable in the global mobility networks as compared to other existing related delegation-based authentication schemes.

**Keywords:** Authenticated key agreement, BAN logic, Provable security, Random oracle model

## 1 Introduction

In the global mobility networks, mobile users can connect local network service provider along with user's movement. The authentication protocol for the mobility networks involves three entities, a mobile user (MU), a visited location register (VLR) and a home location register (HLR). When MU roams into VLR, the roaming mechanism ensures that MU gets access to the local network after VLR validates the legality of MU with help of HLR. Due to openness of global mobility networks, eavesdropping becomes much easier than in wired communication networks. The roaming mechanism should accomplish authentication function and achieve anonymity of mobile users. Authentication can avoid illegal access from malicious intruders. For example, GSM [1] adopts the symmetric encryption/decryption algorithm A5 to achieve user authentication. However, it cannot still provide mobile users with privacy protection [2-3]. Furthermore, MU cannot authenticate VLR in GSM [4]. User's privacy is an imperative issue in global mobility networks. In cellular networks, GSM and 3GPP roaming protocols provide a certain degree of anonymity by using some temporary identity called TMSI (Temporary Mobile Subscriber Identity) rather than the real identity IMSI (International Mobile Subscriber Identity). The basic requirement of mutual authentication between the VLR and MU cannot reveal the real identity of the mobile user. This is the basic privacy protection, anonymity. The other aspect of privacy protection is unlinkability of mobile users. Untraceability is essential in global mobility networks. An authentication protocol should hide user's movements from any eavesdroppers and other foreign servers (except the VLR). Different sessions of the same user within one foreign domain can be easily linked by the VLR. Hereafter, we call the property as weak un-traceability. The concept "weak" means that the HLR and VLR may link two different sessions to a same MU.

To the best of my knowledge, the existing security model of authentication schemes for global mobility networks does not include the following security property. After MU and VLR have established a session key, there communication message encrypted with the session key cannot be compromised by any other entities even including the HLR, which is called communication confidentiality. In the literature, HLR is always modeled as a trusty entity. In essence, although the HLR is not malicious, it may be curious. For example, an operator at the end of HLR attempts to find out service content with which a VLR provides a certain registered user. If the session key is acquired by the HLR, the privacy of the MU and the VLR cannot be well protected. It is essential in roaming services to ensure the privacy of the MU and the VLR. In our security model, we call it communication confidentiality. Unfortunately, the previous authentication protocols for the global mobility networks in the literature have never mentioned the property, communication confidentiality between the MU/ VLR and the HLR.

This motivates us to design a new authenticated key agreement protocol for global mobility network which is equipped with both authentication functionality and

*Corresponding Author: Zuowen Tan; E-mail: tanzyw@163.com

DOI: 10.3966/160792642019012001006

strong security properties such as communication confidentiality, privacy preservation, and resistance against known key attacks.

In this paper, we propose a novel delegation-based authenticated key agreement (DBAKA) scheme. Analysis of BAN-logic demonstrates that the proposed authentication protocol achieves mutual authentication between/among the participants and it allows MU to establish session keys with VLR.

The remainder of this paper is organized as follows. Section 2 briefly discusses the related authentication schemes for roaming networks. In Section 3, we present a novel DBAKA protocol. The formal security analysis under the random oracle model is given in Section 4. Section 5 makes comparison of our scheme with related existing DBAKA schemes in term of security, computation cost and communication cost. Finally, Section 6 concludes the paper.

## 2 Related Work

In order to remove the weaknesses of the authentication protocols based on private key cryptosystem, public key system based authentication protocols have been proposed to provide the MU with the privacy protection [5-6]. However, due to the resource limitations of the mobile devices, MU cannot support too complicated encryption or decryption operations. The other issue that the public key cryptosystem based authentication protocols bring about is that the public key certificate of MU compromises real identity of MU.

Recent years have witnessed the efforts on anonymous authentication for wireless communications [7-14]. For example, one approach is that HLR and VLR preshare a roaming key. Thus, during the authentication phase, HLR is offline. Mun et al. proposed an anonymous authentication scheme for roaming service [15]. However, Zhao et al. [14] found that Mun et al.'s protocol cannot withstand replay attacks, man-in-the-middle attacks, and inside attacks. Furthermore, the authentication protocols for roaming network [15-17] require that the HLR is online during the whole authentication phase.

In 2005, Lee and Yeh introduced the concept delegation to authentication protocols [4]. The delegation method is based on the proxy signature which is generated by the proxy signer after the original signer has delegated his signature authority to the proxy signer [18]. In contrast with online authentication, offline authentication is executed by VLR alone without HLR. Unfortunately, in 2008, Tang and Wu [19] pointed out that Lee and Yeh's DBAKA protocol [4] cannot withstand the VLR impersonation attack and the redirect attack. In 2009, Lee et al. [20] also indicated that the Lee and Yeh's scheme [4] fails to achieve the non-repudiation. The VLR can forge authentication message during off-line authentication phase. The Lee and Yeh's scheme is vulnerable to masquerade user attacks. Lu and Zhou [21-22] showed that Tang and Wu's protocol [19] is vulnerable to the replication attack. In 2010, Youn and Lim [23] demonstrated that Lee et al.'s protocol [20] cannot achieve weak untraceability. Moreover, Lee et al.'s protocol [20] cannot provide forward secrecy [24-25]. Lee et al. [24] found that neither of Lee-Yeh's [4] and Lee et al.'s protocols [20] achieve weak untraceability [26]. Wang and Lin showed [27] that Youn and Lim's enhanced DBAKA protocol [23] suffers from Denial of Service (DoS) attack. Wang et al. [28] also showed that Youn and Lim's enhanced DBAKA protocol [23] cannot provide weak untraceability. Recently, Gope et al. [25] pointed that the improved protocol [24] suffers from DoS attack. Furthermore, it cannot provide perfect forward secrecy, or untraceability. In 2013, Ou and Hwang proposed a double delegation based authentication and key agreement protocol [29]. In their DBAKA protocol, MU and VLR obtain the proxy signature from HLR. This method facilitates the operation. Furthermore, even online authentication only requires MS and VLR to be online at the same time. Recently, Tsai et al. [30] presented an efficient DBAKA protocol by using ECC. In 2014, Kim et al. demonstrated [31] that Tsai et al.'s protocol suffers from known session key attacks. They also presented an improved version [31]. Hwang and You [32] adopt the embedded concurrent signcryption scheme to propose a DBAKA protocol. However, these schemes are vulnerable to known key session attacks. Furthermore, they fail to provide communication confidentiality.

## 3 The Proposed DBAKA Protocol

The section presents an improved DBAKA protocol. The various phases related to the proposed DBAKA protocol are given in subsequent sections. The notations used in the proposed protocol are summarized in Table 1.

**Table 1.** The notations

| Notation | Description |
|---|---|
| $p, q$ | two large primes |
| $G$ | a cyclic group over the elliptic curve |
| $Q$ | a point of large prime order $q$ in $G$ |
| $En(sk, m)$ | symmetric encryption with key $sk$ on message $m$ |
| $De(sk, c)$ | symmetric decryption with key $sk$ on cipher text $c$ |
| $ID_V/ID_H$ | the identity of VLR/the identity of HLR |
| $h_1()$ | cryptographic hash function: $\{0,1\}^* \to Z_q^*$ |
| $h_i()$ | cryptographic hash function: $\{0,1\}^* \to \{0,1\}^{l_i}$, $i$=2,..6 |
| $h_7$ () | cryptographic hash function: $\{0,1\}^* \to \{0,1\}^k$ |

## 3.1 Setup Phase

The system parameter includes a finite field $F_p$ over a large prime $p$ with the length larger than 160 bit, a cyclic group $G$ over the elliptic curve $E_p(a,b)$: $y^2 \equiv x^3 + ax + b$ (mod $p$), where $a,b \in F_p$ and $4a^3 + 27b^2 \neq 0$ (mod $p$). $Q$ is a point of large prime order $q$ in the elliptic curve group $G$. The functions, $h_i : \{0,1\}^* \to \{0,1\}^{l_i}$, $i$ = 1, 2, …, 6, $h_7 : \{0,1\}^* \to \{0,1\}^k$, are secure cryptographic hash functions, where $k$ is a security parameter.

In the system, HLR with identity $\mathrm{ID_H}$ and VLR with identity $\mathrm{ID_V}$ have their own public/secret key. Let $x_H / Y_H$ and $x_V / Y_V$ denote HLR'*s* and VLR'*s* private/public key pair, respectively, where $Y_V = x_V Q$, $x_H, x_V \in Z_q^*$. All the participants can obtain the HLRs' and VLRs' public keys and check the validity of their PKI certificates. The system public parameters are {*G*, *p, q, Q, h<sub></sub>*}

## 3.2 Registration Phase

MU issues registration request to HLR. Then HLR applies Schnorr signature scheme [33] over ECC to generate a proxy key. Without loss of generality, we assume that all the communications during registration phase are performed through a secure channel. The registration is also described in Figure 1.

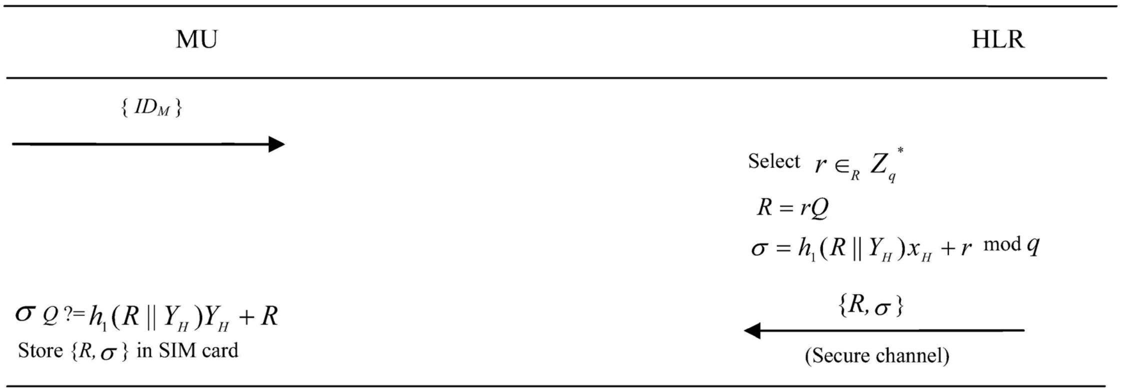

MU
HLR
$\{ ID_M \}$
Select $r \in_R Z_q^*$
$R = rQ$
$\sigma = h_1(R \| Y_H)x_H + r \bmod q$
$\{R, \sigma\}$
(Secure channel)
$\sigma Q ?= h_1(R \| Y_H)Y_H + R$
Store $\{R, \sigma\}$ in SIM card

**Figure 1.** Registration Phase

- **Step 1.** MU issues his identity $ID_M$ to HLR.
- **Step 2.** HLR randomly chooses a number $r \in Z_q^*$ and computes a proxy key pair $(R, \sigma)$

$$R = rQ \text{ , } \sigma = h_1(R \| Y_H)x_H + r \bmod q. \qquad \textbf{(1)}$$

Next, HLR sends ($R$, $\sigma$) to MU. HLR stores ($ID_M$, $R$) in a list. Note that HLR is not required to store $\sigma$ in its database.

- **Step 3.** Upon receiving the pair ($R$, $\sigma$), MU validates it by checking whether the following equation holds:

$$\sigma Q = h_1(R \| Y_H)Y_H + R \text{ .} \qquad \textbf{(2)}$$

Then the key pair $(R, \sigma)$ is kept in MU's SIM card.

## 3.3 Online Authentication Phase

MU and VLR cooperatively establish an authenticated key with help of HLR. The online authentication phase is also described in Figure 2.

- **Step 1.** MU→ VLR: {($C_1$, $C_2$), ($C_3$, $C_4$), $ID_H$, $s$, $R_2$}

Before MU wants to launch an online authentication, MU sets the total number $n$ of offline authentication. MU selects two random numbers, $n_0$, $n_1$, and computes the hash chain: $N_n = h_2(n_0)$, $N_{n-1} = h_2(N_n)$, …, $N_1 = h_2(N_2)$, $N_0 = h_2(N_1)$. Then these hash values ($N_0$, $N_1$,…, $N_n$) are kept in the SIM card. Next MU selects a random number $r_1 \in Z_q^*$ and computes

$$R_1 = r_1 Q, c_0 = h_3(\sigma \| R \| R_1) \oplus N_0 \text{ .} \qquad \textbf{(3)}$$

MU executes the hashed ElGamal encryption with HLR's and VLR's public key, respectively. MU first selects a random number $d_1, d_2 \in Z_q^*$ and computes

$$C_1 = d_1 Q, C_2 = (\sigma \| n_1 \| c_0 \| ID_V \| R_1) \oplus h_4(d_1 Y_H) \text{ ,} \qquad \textbf{(4)}$$

$$C_3 = d_2 Q, C_4 = (h_2(n_1) \| R) \oplus h_4(d_2 Y_V) \text{ .} \qquad \textbf{(5)}$$

Finally, MU generates a Schnorr signature on message which will be sent to VLR. MU first selects a random number $r_2 \in Z_q^*$, and calculates

$$R_2 = r_2 Q, s = r_2 + \sigma h_1(R_2 \| C_1 \| C_2 \| h_2(n_1) \| ID_V \| ID_H) \text{ .}$$

MU transmits the message {($C_1$, $C_2$), ($C_3$, $C_4$), $ID_H$, $s$, $R_2$} to VLR.

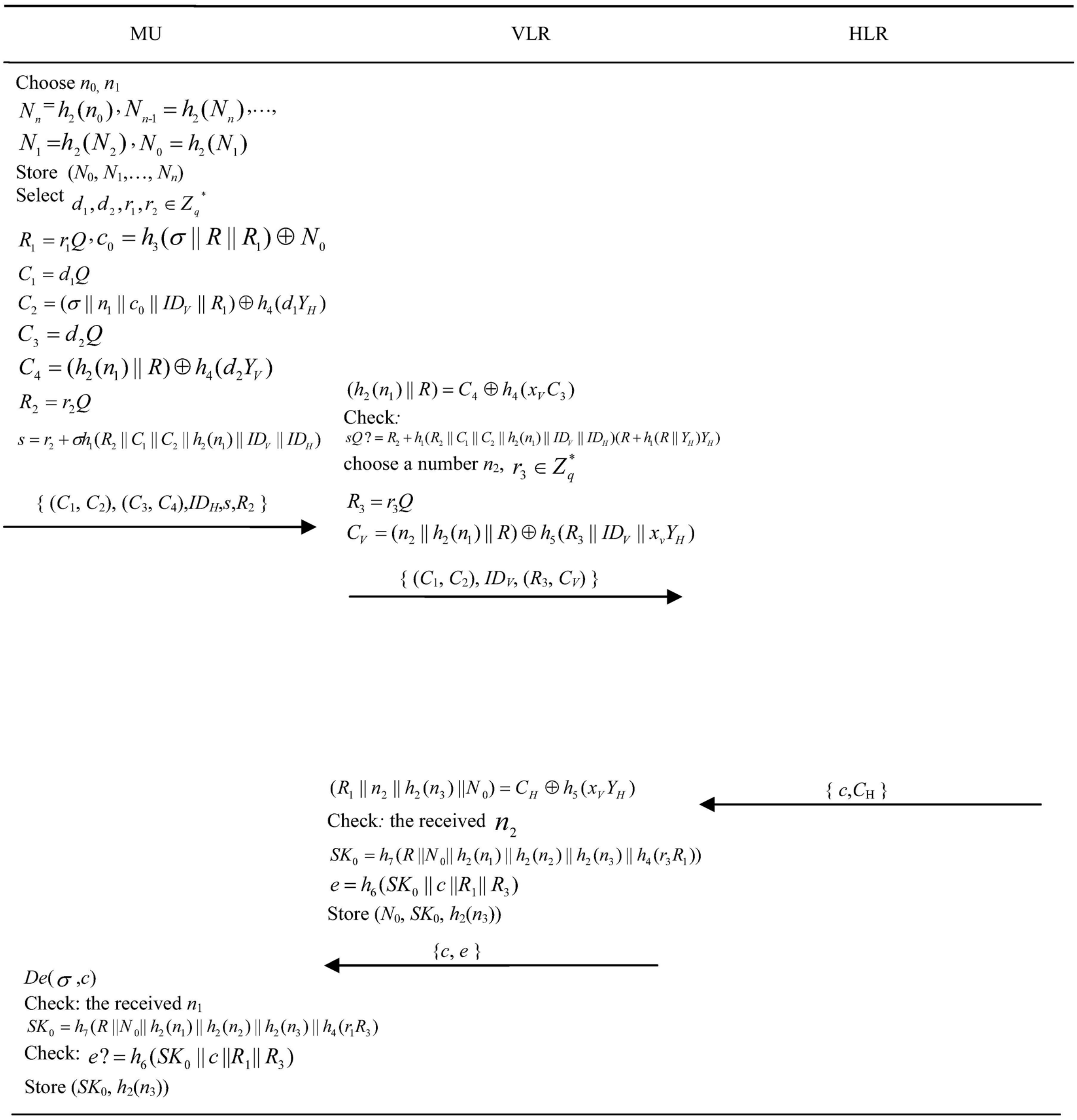

MU
VLR
HLR
Choose $n_{0,}$ $n_1$
$N_n = h_2(n_0)$, $N_{n\text{-}1} = h_2(N_n),\cdots,$
$N_1 = h_2(N_2)$, $N_0 = h_2(N_1)$
Store $(N_0, N_1,\ldots, N_n)$
Select $d_1, d_2, r_1, r_2 \in Z_q^*$
$R_1 = r_1Q$, $c_0 = h_3(\sigma \| R \| R_1) \oplus N_0$
$C_1 = d_1Q$
$C_2 = (\sigma \| n_1 \| c_0 \| ID_V \| R_1) \oplus h_4(d_1Y_H)$
$C_3 = d_2Q$
$C_4 = (h_2(n_1) \| R) \oplus h_4(d_2Y_V)$
$R_2 = r_2Q$
$s = r_2 + \sigma h_1(R_2 \| C_1 \| C_2 \| h_2(n_1) \| ID_V \| ID_H)$
$\{ (C_1, C_2), (C_3, C_4), ID_H, s, R_2 \}$
$(h_2(n_1) \| R) = C_4 \oplus h_4(x_VC_3)$
Check:
$sQ ?= R_2 + h_1(R_2 \| C_1 \| C_2 \| h_2(n_1) \| ID_V \| ID_H)(R + h_1(R \| Y_H)Y_H)$
choose a number $n_2$, $r_3 \in Z_q^*$
$R_3 = r_3Q$
$C_V = (n_2 \| h_2(n_1) \| R) \oplus h_5(R_3 \| ID_V \| x_vY_H)$
$\{ (C_1, C_2), ID_V, (R_3, C_V) \}$
$\{ c, C_{\mathrm{H}} \}$
$(R_1 \| n_2 \| h_2(n_3) \| N_0) = C_H \oplus h_5(x_VY_H)$
Check: the received $n_2$
$SK_0 = h_7(R \| N_0 \| h_2(n_1) \| h_2(n_2) \| h_2(n_3) \| h_4(r_3R_1))$
$e = h_6(SK_0 \| c \| R_1 \| R_3)$
Store $(N_0, SK_0, h_2(n_3))$
$\{c, e\}$
$De(\sigma, c)$
Check: the received $n_1$
$SK_0 = h_7(R \| N_0 \| h_2(n_1) \| h_2(n_2) \| h_2(n_3) \| h_4(r_1R_3)$
Check: $e ?= h_6(SK_0 \| c \| R_1 \| R_3)$
Store $(SK_0, h_2(n_3))$

**Figure 2.** Online authentication and key agreement phase

- **Step 2.** VLR→HLR: $\{(C_1, C_2), ID_V, (R_3, C_V)\}$

Upon receiving the message from MU, VLR decrypts ($C_3$, $C_4$) with $h_4(x_vC_3)$ and obtains $h_2(n_1)$, $R$. Then VLR checks whether the equation holds:

$$sQ = R_2 + h_1(R_2 \| C_1 \| C_2 \| h_2(n_1) \| ID_V \| ID_H)$$
$$(R + h_1(R \| Y_H)Y_H).$$

If the equation holds, VLR randomly chooses a number $n_2$, $r_3 \in Z_q^*$, and computes

$$R_3 = r_3Q, C_V = (n_2 \| h_2(n_1) \| R) \oplus h_5(R_3 \| ID_V \| x_vY_H). \quad \mathbf{(6)}$$

Finally, VLR sends $\{(C_1, C_2), ID_V, (R_3, C_V)\}$ to HLR.

- **Step 3.** HLR →VLR: $\{ c, C_{\mathrm{H}} \}$

After HLR receives message from VLR, HLR computes

$$(n_2 \| h_2(n_1) \| R) = C_V \oplus h_5(R_3 \| ID_V \| x_vY_H), \quad \mathbf{(7)}$$

$$(\sigma \| n_1 \| c_0 \| ID_V \| R_1) = C_2 \oplus h_4(x_HC_1). \quad \mathbf{(8)}$$

And HLR checks the validity of ($\sigma$, $R$) through (2). If (2) holds, HLR has authenticated MU. Then HLR checks whether the received $h_2(n_1)$ is equal with $h_2(n_1)$, and the decrypted $ID_V$ is the same as the received identity. If they both are valid, HLR chooses a random number $n_3$ and computes

$$N_0 = h_3(\sigma \| R \| R_1) \oplus c_0, \quad \mathbf{(9)}$$

$$c = En(\sigma, n_1 \| h_2(n_2) \| n_3 \| R_3), \quad \mathbf{(10)}$$

$$C_H = (R_1 \| n_2 \| h_2(n_3) \| N_0) \oplus h_5(x_HY_V). \quad \mathbf{(11)}$$

Finally, HLR sends $\{c, C_H\}$ back to VLR.

- **Step 4.** VLR→MU: $\{c, e\}$

VLR decrypts $C_{\mathrm{H}}$ and obtains $\{R_1, n_2, h_2(n_3), N_0\}$. Next VLR checks whether the received $n_2$ is right. If it is invalid, VLR refuses the login request from MU. Otherwise, VLR computes

$$SK_0 = h_7(R \| N_0 \| h_2(n_1) \| h_2(n_2) \| h_2(n_3) \| h_4(r_3 R_1)), \quad \textbf{(12)}$$

$$e = h_6(SK_0 \| c \| R_1 \| R_3). \quad \textbf{(13)}$$

Finally, VLR stores $\{R, N_0, SK_0, h_2(n_3)\}$ and responds MU with $\{c, e\}$.

- **Step 5.** MU executes the decryption algorithm $De(\sigma, c)$ and obtains $\{n_1, h_2(n_2), n_3, R_3\}$. MU checks whether the received $n_1$ is right. If it is invalid, MU refuses the response from VLR. Otherwise, MU computes $SK_0 = h_7(R \| N_0 \| h_2(n_1) \| h_2(n_2) \| h_2(n_3) \| h_4(r_1 R_3))$ and checks whether the equation holds: $e = h_6(SK_0 \| c \| R_1 \| R_3)$. If it holds, MU stores ($SK_0$, $h_2(n_3)$) in the SIM card.

## 3.4 Offline Authentication Phase

MU and VLR cooperatively perform offline authentication which would not need the intervention of HLR during the authentication phase. Figure 3 illustrates the offline authentication process. We describe it as follows.

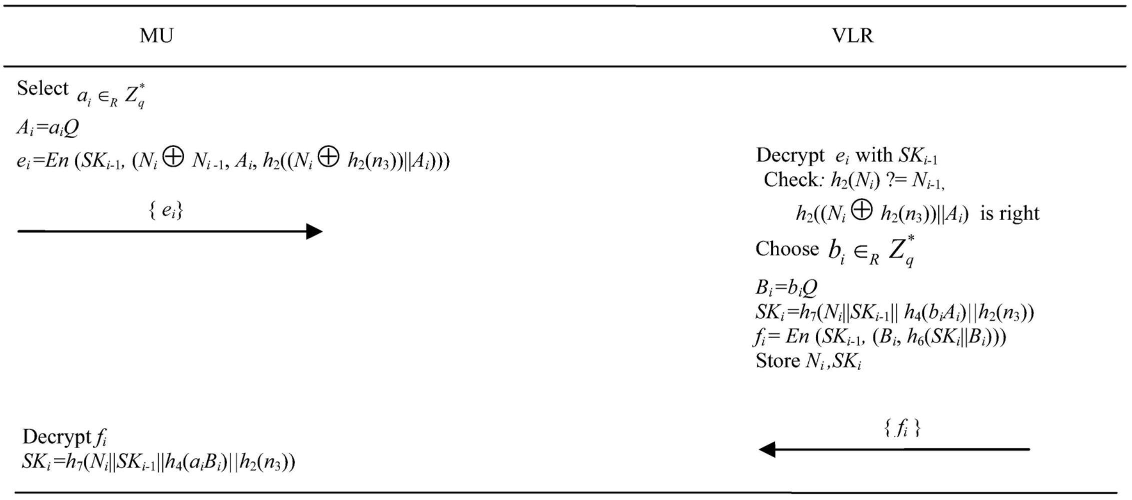

MU
VLR
Select $a_i \in_R Z_q^*$
$A_i = a_i Q$
$e_i = En(SK_{i-1}, (N_i \oplus N_{i-1}, A_i, h_2((N_i \oplus h_2(n_3)) \| A_i)))$
$\{e_i\}$
Decrypt $e_i$ with $SK_{i-1}$
Check: $h_2(N_i)$ ?= $N_{i-1}$,
$h_2((N_i \oplus h_2(n_3)) \| A_i)$ is right
Choose $b_i \in_R Z_q^*$
$B_i = b_i Q$
$SK_i = h_7(N_i \| SK_{i-1} \| h_4(b_i A_i) \| h_2(n_3))$
$f_i = En(SK_{i-1}, (B_i, h_6(SK_i \| B_i)))$
Store $N_i, SK_i$
$\{f_i\}$
Decrypt $f_i$
$SK_i = h_7(N_i \| SK_{i-1} \| h_4(a_i B_i) \| h_2(n_3))$

**Figure 3.** Offline authentication and key agreement phase

- **Step 1.** MU→ VLR: $\{e_i\}$

When MU attempts to launch the $i$-th ($i = 1, 2, \ldots, n$) offline authentication, MU first picks ($N_i$, $SK_{i-1}$, $h_2(n_3)$) in the SIM card. Then MU selects a random number $a_i \in_R Z_q^*$ and computes $A_i = a_i Q$, $e_i = En(SK_{i-1}, (N_i \oplus N_{i-1}, A_i, h_2((N_i \oplus h_2(n_3)) \| A_i))$ )and transmits $e_i$ to VLR.

- **Step 2.** VLR→MU: $\{f_i\}$

VLR decrypts $e_i$ with last authenticated session key $SK_{i-1}$ and obtains $N_i$ by using the stored $N_{i-1}$. Then VLR checks whether hash value of $N_i$ is $N_{i-1}$ and the third part of plaintext is equal to $h_2((N_i \oplus h_2(n_3)) \| A_i)$. If either is not equal, VLR refuses the authentication request. Otherwise, VLR selects a random number $b_i \in_R Z_q^*$ and calculates

$$B_i = b_i Q,\ SK_i = h_7(R \| N_i \| SK_{i-1} \| h_4(b_i A_i) \| h_2(n_3)), \quad \textbf{(14)}$$

$$f_i = En(SK_{i-1}, (B_i, h_6(SK_i \| B_i))). \quad \textbf{(15)}$$

VLR stores the hash values $N_i$ and the key $SK_i$, and removes $\{SK_{i-1}, N_{i-1}\}$. Finally VLR transmits $f_i$ to MU.

- **Step 3.** After MU receives the response from VLR, MU decrypts $f_i$ with the key $SK_{i-1}$ and obtains $B_i$. Then MU computes $SK_i = h_7(N_i \| SK_{i-1} \| h_4(a_i B_i) \| h_2(n_3))$. MU checks whether $h_6(SK_i \| B_i)$ is right. If so, MU stores the session key $SK_i$.

MU can perform offline authentications $n$ times. Then MU launches another online authentication to VLR with the intervention of HLR.

## 3.5 Revocation Phase

When MU's mobile device is stolen/lost or MU's service subscription expires, the HLR suspends MU's service or revokes the MU and all VLRs will not provide MU with the roaming service any longer. In order to attain the aim, HLR searches for $R$ corresponding to the MU who will be suspended or revoked. Then HLR periodically releases $R$ on a bulletin.

When VLR is required to access by a new mobile user MU the first time, VLR decrypts $C_4$ and checks if one part of a proxy key pair, $R$, is in the suspended service list. If $R$ is in the revocation list, VLR refuses MU.

Each time HLR needs to revoke a certain MU, HLR removes the MU's account only by simply putting the key $R$ in the revocation list with keeping his/her identity unchanged and unpublished. Hence MU can use his/her old identity to apply for a new proxy key pair in the next registration with HLR. Meanwhile, the approach helps to provide user anonymity.

# 4 Security Analysis

In the following, we prove the security of the proposed protocol through the random oracle model, the BAN logic [34] and the AVISPA tool [35-36], respectively.

## 4.1 Formal Security Analysis in Random Oracle Model

Let $G$ be an elliptic curve group over finite field $F_p$ and $Q$ is a point of large prime order $q$ in $G$.

**Definition 1.** Given ($Q$, $aQ$, $bQ$) in $G$ where unknown $a,b \in Z_q^*$, what is the value $abQ$? It is referred to as **Elliptic curve Diffie-Hellman problem (ECDHP)**.

The success probability of a probabilistic polynomial time Turing machine $\Delta$ in solving ECDHPs in $G$ is defined as:

$$Succ_G^{CDH}(\Delta) = Pr[\Delta(aQ,bQ) = abQ : a,b \in_R Z_q^*].$$

**Definition 2. The elliptic curve Diffie-Hellman (ECDH assumption)** is the assumption that ECDHPs are hard. In other words, for any probabilistic Turing machine $\Delta$, $Succ_G^{CDH}(\Delta)$ is negligible.

We will adopt the security model proposed by Abdalla et al. [37] (hereafter called as AFP security model) which is appropriate for three-party authenticated key agreement scenario. The participants, a mobile user, a visited location register and a semi-trusted home location register, are denoted by U, V, and S, respectively. The *i*th instance of U is denoted by $U^i$. The *j*th instance of V is denoted by $V^j$ and the *k*th instance of S is denoted by $S^k$. For the semantic security, the AFP security model is defined by a game which consists of two phases. In the first phase, an adversary $A$ is allowed to adaptively issue *Send*, *Reveal* and *Test* queries. In the second phase, the adversary $A$ executes a single *Test* query with chosen bit $b$ directed to a fresh instance and the query outputs a guess bit $b'$ for $b$. If $b' = b$, then the adversary $A$ wins the game.

**Definition 3.** Let *Succ*($A$) be the event that the adversary $A$ wins the above game, i.e., $A$ is successful in breaking the semantic security of the DBAKA protocol. The advantage of the adversary $A$ in breaking the **semantic security** of our protocol by guessing the correct bit $b'$ is defined by

$$Adv_G^{DBAKA}(A) = |\,2Pr(Succ(A)) - 1\,| = |\,2Pr[b' = b] - 1\,|.$$

A DBAKA protocol is said to be semantically secure in AFP security model if the advantage of any probabilistic polynomial time-bounded adversary $A$ is negligible.

**Theorem 1.** Assume that hash functions $h_i()$ (i = 1, 2, … 7) are modeled as random oracles $H_i$. Let A be a probabilistic polynomial time bounded adversary. Suppose in order to break the semantic security of the proposed DBAKA protocol, A makes at most $q_s$ times Send queries, $q_i$ (i = 1, 2, … 7) times hash oracle queries, respectively. Then,

$$Adv_G^{DBAKA}(A) \le \frac{3q_s^{\;2}}{2^{k+1}} + \frac{q_s^{\;2} + q_1^{\;2}}{2(q-1)} + \sum_{i=2}^{6} \frac{q_i^{\;2}}{2^{i_i+1}} + \frac{q_s}{q-1}$$
$$+ \frac{3q_2 + 2q_s}{2^{i_2}} + \frac{2q_3}{2^{i_3}} + \frac{2q_4 + q_s}{2^{i_4}} + \frac{q_5}{2^{i_5}} + q_7 \mathrm{Succ}_G^{CDH}(A)$$

*Proof.* We shall use the approach of sequent games [38] to prove this theorem. We define a sequence of modified attack games $\boldsymbol{G_i}$ (i = 0, 1, 2, 3, 4). Let $Succ_i$ be an event defined as successful guessing of the bit $b$ in *Test* query corresponding to each game $G_i$ by an adversary $A$.

**Game $G_0$:** This starting game and the real protocol in random oracles are assumed to be identical. Hence, $G_0$ is the actual attack game. By definition, we have

$$Adv_G^{DBAKA}(A) = |2\Pr[Succ_0] - 1|. \qquad \textbf{(16)}$$

**Game $G_1$:** This game simulates all oracle queries including *Send*, *Reveal*, *Corrupt*, *Test* and *hash* queries. We give the simulation of the hash oracles $H_i$ (i = 1, 2, …, 7) and *Reveal*, *Corrupt*, *Test* queries in Table 2. We simulate the *Send* queries as in the actual attack game. The simulations maintain two lists for queries: (1) list $L_i$ records the answers to hash oracles $H_i$, (2) list $L_A$ records the answers to answers the queries which are initiated by $A$.

This game is perfectly indistinguishable from the actual attack game. Hence, we have

$$\Pr[Succ_1] = \Pr[Succ_0]. \qquad \textbf{(17)}$$

**Game $G_2$**: In this game, we avoid collisions among the hash queries that the adversary asks $H_i$ (i = 1, 2, …, 6} and random numbers in the transcripts of messages. We take the random value $h$ from $\{0,1\}^{l_i}$ for $H_i$ ($i$=2,..6) and $\{0,1\}^k$ for $H_1$. If this query is directly asked by the adversary, and ($i$,*, $h$) $\in L_i$, we abort the game. Otherwise, $h$ is returned. Since that hash value $h$ is chosen uniformly at random, according to the birthday paradox, the probability of collisions is at most $\frac{q_1^{\;2}}{2(q-1)} + \sum_{i=2}^{6} \frac{q_i^{\;2}}{2^{i_i+1}}$. Further, messages contain random numbers $\{n_1, n_2, n_3\}$ and randomly chosen elements $\{R_1, R_3\}$, and the probability of random numbers/elements collision is at most $\frac{3q_s^{\;2}}{2^{k+1}} + \frac{q_s^{\;2}}{2(q-1)}$.

Games $\mathbf{G_2}$ and $\mathbf{G_1}$ are perfectly indistinguishable unless the above-mentioned collision causes the game abort. Hence, we have

$$|\Pr(Succ_2) - \Pr(Succ_1)| \le \frac{3q_s^{\;2}}{2^{k+1}} + \frac{q_s^{\;2} + q_1^{\;2}}{2(q-1)} + \sum_{i=2}^{6} \frac{q_i^{\;2}}{2^{i_i+1}}. \qquad \textbf{(18)}$$

**Table 2.** Simulation of hash, reveal, test, and corrupt oracle queries

```
Hash simulation query performs as follows:
On a hash query $H_i$ ($i$ = 1, 2, …, 7} oracle about $m$
if a record ($i$, $m$, $h$) exists in list $L_i$ , then
        return hash value $h$.
else Select a string $h \leftarrow_R Z_q^*$ for $i$=1; $h \leftarrow_R \{0,1\}^{l_i}$ , for $i$=2,..6; $h \leftarrow_R \{0,1\}^k$ , for $i$=7;
    if the query is initiated by the adversary $A$, then
        Add the triple in the form of ($i$, $m$, $h$) to $L_A$.
    else Add ($i$, $m$, $h$) into $L_i$.
    end if
end if
```

```
Reveal($U^i$/$V^j$) simulation query performs as follows:
if session key $SK$ is defined for instance $U^i$ or $V^j$, then
    This query returns $SK$ as answer
else return $\perp$ as response.
end if
```

```
Corrupt($U$/$V$) simulation query performs as follows:
On a Corrupt($U$) query, return the proxy key pair ($R$, $\sigma$ ) of participant $U$ as the output of the query;
On a Corrupt($V$) query, return the long-lived key, private key $x_V$ of participant $V$ as the output of the query.
```

```
Test($U^i$/$V^j$) simulation query performs as follows:
By using Reveal($U^i$/$V^j$) query, obtain the output of Reveal query.
if the output is $\perp$, then
    return $\perp$ as the output of Test($U^i$/$V^j$) query
else The oracle flips a unbiased coin $b$.
    if $b$ = 1, then
        return the session key $SK$ as the output of the Test query
    else return a random string from $\{0,1\}^k$ as the output of the Test query.
    end if
end if
```

**Game $G_3$:** This game considers a situation where $A$ obtains the correct message transcript luckily without active participation of hash oracles $H$. The authentication phase of our protocol involves six messages communication $m_i$, ($i$=1,..6) where $m_1, m_2, m_3, m_4, m_5$ and $m_6$ represent {($C_1$, $C_2$), ($C_3$, $C_4$), $ID_H$, $s$, $R_2$ }, {($C_1$, $C_2$), $ID_V$, ($R_3$, $C_V$) }, {$c$, $C_H$ }, {$c$, $e$ }, { $e_i$} and {$f_i$}, respectively. We consider following cases, *Send*(U, $m_1$), *Send*(V, $m_2$), *Send*(S, $m_3$), *Send*(V, $m_4$), *Send*(U, $m_5$), and *Send*(V, $m_6$). In each case, we consider the maximum probability of the hash values falling within the list $L_A$. For example, for *Send*(U, $m_1$) query, the values $h_2(n_1)$, $h_3(\sigma \| R \| R_1)$, $h_1(R_2 \| C_1 \| C_2 \| h_2(n_1) \| ID_V \| ID_H)$, $h_4(d_1 Y_H)$, $h_4(d_2 Y_V)$ must be in $L_A$. For this, the probability is at most $\frac{q_s}{q-1} + \frac{q_2}{2^{i_2}} + \frac{q_3}{2^{i_3}} + \frac{2q_4}{2^{i_4}}$ . Considering all the cases, we have

$$| \Pr(Succ_3) - \Pr(Succ_2) | \leq$$
$$\frac{q_s}{q-1} + \frac{3q_2 + 2q_s}{2^{i_2}} + \frac{2q_3}{2^{i_3}} + \frac{2q_4 + q_s}{2^{i_4}} + \frac{q_5}{2^{i_5}} . \quad \textbf{(19)}$$

**Game $G_4$:** In this game, we replace random oracle $H_7$ with private oracle $H$ and we do not use the $h_4(r_1R_3)$ or $h_4(r_3R_1)$ to compute the session key $SK$. Thus, the session key is completely independent of $H_7$, $h_4(r_1R_3)$ or $h_4(r_3R_1)$. Thus, the session key is determined without querying the hash oracle. Since $H$ is a private oracle, the probability that adversary $A$ correctly guesses the value of $b$ in the game is

$$\Pr(Succ_4) = 1/2. \quad \textbf{(20)}$$

Games $\mathbf{G_3}$ and $\mathbf{G_4}$ are perfectly indistinguishable unless the following event AskH occurs: the adversary $A$ queries hash function $H_7$ on $R \| N_0 \| h_2(n_1) \| h_2(n_2) \| h_2(n_3) \| h_4(r_1R_3)$ or on $R \| N_0 \| h_2(n_1) \| h_2(n_2) \| h_2(n_3) \| h_4(r_3R_1)$ . Hence, we have

$$| \Pr(Succ_4) - \Pr(Succ_3) | \leq \Pr(\text{AskH}) . \quad \textbf{(21)}$$

Now, we estimate the probability $\Pr(\text{AskH})$ . According to the definition of event AskH, the event AskH means that the adversary has queried random oracle $H_7$ on ($R$, $N_0$, $h_2(n_1)$, $h_2(n_2)$, $h_2(n_3)$, CDH($R_1$, $R_3$)). Since we have assumed that the number of records in the list $L_7$ is $q_7$, the probability of extracting the CDH($R_1$, $R_3$) value from list $L_7$ is $1/q_7$. Hence, we get

$$\Pr(\text{AskH}) = q_7 \text{Succ}_G^{CDH}(A) . \quad \textbf{(22)}$$

Using the triangular inequality and (17), (20), we have the following:

|Pr[$Succ_0$] - 1/2|
= | Pr[$Succ_1$]- Pr[$Succ_4$]|
≤| Pr[$Succ_1$]- Pr[$Succ_2$]| + |Pr[$Succ_2$]- Pr[$Succ_3$]| +
| Pr[$Succ_3$]- Pr[$Succ_4$]|. **(23)**

From (16)-(23), we get

$$Adv_G^{DBAKA}(A) \le \frac{3{q_s}^2}{2^{k+1}} + \frac{{q_s}^2 + {q_1}^2}{2(q-1)} + \sum_{i=2}^{6} \frac{{q_i}^2}{2^{i_i+1}} + \frac{q_s}{q-1} + \frac{3q_2 + 2q_s}{2^{i_2}} + \frac{2q_3}{2^{i_3}} + \frac{2q_4 + q_s}{2^{i_4}} + \frac{q_5}{2^{i_5}} + q_7 \mathrm{Succ}_G^{CDH}(A)\cdot$$

Thus, we have completed the proof of the theorem.

## 4.2 Authentication Proof Using BAN-logic

In this section, we will conduct security analysis by using the Burrows-Abadi-Needham Logic (generally called BAN-logic) [34]. The detailed analysis will demonstrate that the proposed DBAKA scheme allows MU to agree on session key with VLR. The well-popular BAN-logic uses a set of postulates to analyze the security of authentication and key agreement protocols [39-40]. The logical formal model analysis method can reason the beliefs of participants in an authentication protocol. The three elementary items of BAN logic are formulas/statements, principals and keys. Let X and Y be symbols for statements, P and Q be symbols for principals, K be a symbol for a cryptographic encryption/decryption key. More details can be found in [34, 39].

Some primary *BAN*-logic postulates are given below:

- **The message-meaning rule:**

$$\frac{P |\equiv P \xleftrightarrow{K} Q, P \lhd \{X\}_K}{P |\equiv Q |\sim X}, \frac{P |\equiv P \overset{K}{\Leftrightarrow} Q, P \lhd < X >_K}{P |\equiv Q |\sim X})$$

If *P* believes that it shares *K* with *Q* and sees *X* encrypted by *K* (or *X* combined with *K*), then *P* believes that *Q* once said *X*.

- **The nonce-verification rule**:

$$\frac{P |\equiv \#(X), P |\equiv Q |\sim X}{P |\equiv Q |\equiv X}$$

If *P* believes that *X* could have been uttered only recently and *Q* once said *X*, then *P* believes that *Q* believes *X*.

- **The freshness propagation rule**: $\frac{P |\equiv \#(X)}{P |\equiv \#(X,Y)}$

If *P* believes that *X* is fresh, then *P* also believes that (*X*, *Y*) is fresh.

- **The jurisdiction rule**: $\frac{P |\equiv Q |\Rightarrow X, P |\equiv Q |\equiv X}{P |\equiv X}$

If *P* believes that *Q* has an authority the truth over *X*, then *P* trusts *Q* on the truth of *X*.

- **The belief rule**: $\frac{P |\equiv Q |\equiv (X,Y)}{P |\equiv Q |\equiv X}$

If *P* believes that *Q* believes *X* and *Y*, then *P* believes that *Q* believes *X*.

- **The session key rule**: $\frac{P |\equiv \#(SK), P |\equiv Q |\equiv X}{P |\equiv P \xleftrightarrow{SK} X}$

If *P* believes that the session key is fresh and *P* believes that *Q* believes *X* which is the necessary parameter of the session key, then *P* believes that *P* shares the session key *SK* with *Q*. According to the analytic procedures of the BAN logic, the online authentication part of the proposed scheme must satisfy the following goals:

- **Goal (1)**: VLR $|\equiv$ (MU $\xleftrightarrow{SK}$ VLR),
- **Goal (2)**: VLR $|\equiv$ MU $|\equiv$ (MU $\xleftrightarrow{SK}$ VLR),
- **Goal (3)**: MU $|\equiv$ VLR $|\equiv$ (MU $\xleftrightarrow{SK}$ VLR),
- **Goal (4)**: MU $|\equiv$ (MU $\xleftrightarrow{SK}$ VLR).

For space limitation, we only demonstrate that the offline authentication part of the proposed protocol must satisfy the following goals.

- **Goal (5)**: VLR $|\equiv$ (MU $\xleftrightarrow{SK_i}$ VLR),
- **Goal (6)**: VLR $|\equiv$ MU $|\equiv$ (MU $\xleftrightarrow{SK_i}$ VLR),
- **Goal (7)**: MU $|\equiv$ VLR $|\equiv$ (MU $\xleftrightarrow{SK_i}$ VLR),
- **Goal (8)**: MU $|\equiv$ (MU $\xleftrightarrow{SK_i}$ VLR).

First, we analyze the idealized form of the offline authentication part of the proposed protocol as follows.

- Message $M_1$: MU → VLR:

$$\{< N_i >_{N_{i-1}}, A_i, < N_i, A >_{h_2(n_3)}\}_{SK_{i-1}}.$$

- Message $M_2$: VLR → MU:

$$\{B_i, \mathrm{MU} \xleftrightarrow{N_i} \mathrm{VLR}, \mathrm{MU} \overset{h_2(n_3)}{\Leftrightarrow} \mathrm{VLR}, <SK_i>_{MU \xleftrightarrow{b_i A_i} VLR}\}_{MU \xleftrightarrow{SK_{i-1}} VLR}.$$

Next, the assumptions about the initial state of the offline authentication part of the proposed protocol are given below.

- $H_1$: MU $|\equiv \#(A_i, B_i)$,
- $H_2$: VLR $|\equiv \#(A_i, B_i)$,
- $H_3$: MU $|\equiv$ VLR $|\equiv (B_i)$,
- $H_4$: MU $|\equiv$ MU $\xleftrightarrow{SK_{i-1}}$ HLR,
- $H_5$: VLR $|\equiv$ MU $\xleftrightarrow{SK_{i-1}}$ VLR,
- $H_6$: VLR $|\equiv$ MU $\xleftrightarrow{N_{i-1}}$ VLR,
- $H_7$: VLR $|\equiv$ MU $|\equiv (N_i)$,
- $H_8$: VLR $|\equiv$ MU $\xleftrightarrow{b_i A_i}$ VLR,
- $H_9$: MU $|\equiv$ MU $\xleftrightarrow{a_i B_i}$ VLR.

Finally, based on the logical postulates of BAN logic and the assumptions $H_1$-$H_9$, we give the proof of the offline authentication part of the proposed protocol.

From message $M_1$, we obtain

- $S_1$: LR $\lhd \{< N_i >_{N_{i-1}}, A_i, < N_i, A >_{h_2(n_3)}\}_{SK_{i-1}}$.

According to $S_1$, $H_5$, and the message meaning, we have

- $\boldsymbol{S_2}$:$\text{VLR} |\equiv \text{MU} |\sim \{<N_i>_{N_{i-1}}, A_i, <N_i, A>_{h_2(n_3)}\}$.

According to $H_2$ and the freshness propagation rule, we get

- $\boldsymbol{S_3}$: $\text{VLR} |\equiv \#(<N_i>_{N_{i-1}}, A_i, <N_i, A>_{h_2(n_3)})$.

According to $S_2$, $S_3$, and the nonce-verification rule, we have

- $\boldsymbol{S_4}$: $\text{VLR} |\equiv \text{MU} |\equiv (<N_i>_{N_{i-1}}, A_i)$.

According to $S_4$ and the belief rule, we obtain

- $\boldsymbol{S_5}$: $\text{VLR} |\equiv \text{MU} |\equiv (<N_i>_{N_{i-1}})$.
- $\boldsymbol{S_6}$: $\text{VLR} |\equiv \text{MU} |\equiv (A_i)$.

According to $S_5$, $H_6$, and the message meaning rule and the nonce verification rule, we get

- $\boldsymbol{S_7}$: $\text{VLR} |\equiv \text{MU} |\equiv (N_i)$.

According to $S_7$, $H_7$, and the jurisdiction rule, we have

- $\boldsymbol{S_8}$: $\text{VLR} |\equiv (N_i)$.

According to $S_6$, $S_8$, $H_8$, and the nonce-verification rule, we have

- $\boldsymbol{S_9}$: $\text{VLR} |\equiv (\text{MU} \xleftrightarrow{SK_i} \text{VLR})$. (**Goal** (5))

According to $S_9$, $H_2$, and the session key rule, we have

- $\boldsymbol{S_{10}}$:$\text{VLR} |\equiv \text{MU} |\equiv (\text{MU} \xleftrightarrow{SK_i} \text{VLR})$. (**Goal** (6))

From message $M_2$, we get

- $\boldsymbol{S_{11}}$: $\text{MU} \lhd \{B_i, \text{MU} \xleftrightarrow{N_i} \text{VLR}, \text{MU} \overset{h_2(n_3)}{\Leftrightarrow} \text{VLR}, <SK_i>_{MU \xleftrightarrow{b_i A_i} VLR}\}_{MU \xleftrightarrow{SK_{i-1}} VLR}$.

According to $S_{11}$, $H_4$, and the message meaning, we have

- $\boldsymbol{S_{12}}$: $\text{MU} |\equiv \text{VLR} |\sim \{B_i, \text{MU} \xleftrightarrow{N_i} \text{VLR}, \text{MU} \overset{h_2(n_3)}{\Leftrightarrow} \text{VLR}, <SK_i>_{MU \xleftrightarrow{b_i A_i} VLR}\}$.

According to $H_1$ and the freshness propagation rule, we have

- $\boldsymbol{S_{13}}$: $\text{MU} |\equiv \#(B_i, \text{MU} \xleftrightarrow{N_i} \text{VLR}, \text{MU} \overset{h_2(n_3)}{\Leftrightarrow} \text{VLR}, <SK_i>_{MU \xleftrightarrow{b_i A_i} VLR})$.

According to $S_{11}$, $S_{13}$, and the nonce-verification rule, we have

- $\boldsymbol{S_{14}}$: $\text{MU} |\equiv \text{VLR} |\equiv (B_i, \text{MU} \xleftrightarrow{N_i} \text{VLR}, \text{MU} \overset{h_2(n_3)}{\Leftrightarrow} \text{VLR}, <SK_i>_{MU \xleftrightarrow{b_i A_i} VLR})$.

According to $S_{14}$, $H_4$, $H_9$, and the belief rule, we have

- $\boldsymbol{S_{15}}$: $\text{MU} |\equiv \text{VLR} |\equiv (\text{MU} \xleftrightarrow{SK_i} \text{VLR})$. (**Goal** (7))

According to $S_8$, $S_{15}$, $H_3$, and the jurisdiction rule, we have

- $\boldsymbol{S_{16}}$: $\text{MU} |\equiv (\text{MU} \xleftrightarrow{SK_i} \text{VLR})$. (**Goal** (8))

From **Goals** 1-8, it is clear that the MU and the VLR achieve the secure mutual authentication and establish session keys.

## 4.3 Security Verification Using AVISPA

Now, we apply the widely accepted AVISPA [35] tool to simulate our proposed scheme. We give the implementation details of our scheme in high-level protocol specification language (HLPSL) [36]. The simulation results will demonstrate that our scheme is secure against active and passive attacks.

### 4.3.1 HLPSL Specification of Our Scheme

This section briefly summarizes our scheme's roles in HLPSL. The basic roles are user $U_i$, hlregister HLR and vlregister V*j*, which correspond to the participants: mobile user MU, home location register HLR and visited location register VLR, respectively. Besides these roles, we also describe the roles for the session and environment.

In Figure 4, we have depicted the role for $U_i$ in HLPSL. In the registration phase, $U_i$ first sends the registration request securely to the HLR by the *Snd*( ) operation via the secure channel. The type declaration channel (dy) denotes a Dolev-Yao threat model [41] channel under which any adversary can read, modify or delete the message over the public the channel. $U_i$ receives the proxy key pair {SIGM, R} securely from the HLR using the Rcv( ) operation.

In Figure 5, we have finally presented the specifications for the role of goal, environment and session in HLPSL. In the session segment, all the basic roles including Ui, Vj and HLR are instanced with concrete arguments. The environment segment contains the global constant, composition of one or more session, and the intruder knowledge. The six secrecy goals and two authentications are verified.

- secrecy of sub1: It represents that $r$ is kept secret to HLR only.
- secrecy of sub2: It represents that $\sigma$ (i.e. SIGM) are kept secret to both the user Ui and HLR.
- secrecy of sub3: It represents that $n_0$, $r_1$, $r_2$, $d_1$, $d_2$, (i.e. *N0*', *R*1', *R*2', *D*1', *D*2') are kept secret to Ui only.
- secrecy of sub4: It represents that $r_2$ (i.e. *Rj*') is kept secret to Vj only.
- secrecy of sub5: It represents that $n_3$ (i.e. *N3*') is kept secret among the HLR, Ui and Vj.
- secrecy of sub6: It represents that $SK_0$ (i.e. *SKij*) is kept secret to both Ui and Vj.
- authentication on user-vlregister_r1: Ui generates a random r1. After Vj receives the response from the HLR, Vj authenticates Ui based on R1.
- authentication on vlregister-user_r3: Vj generates a random r3. After Ui receives the message from Vj, Ui authenticates Vj based on the validity of R3.

```
role user (
    Ui, Vj, HLR:   agent,
    Snd, Rcv:      channel(dy),      SKih:      symmetric_key,
    SKij:                            symmetric_key,
    H: hash_func,  AH: hash_func,    BH: hash_func)
    played_by Ui
def=
local State: nat,
    IDh, IDi, IDj, R, SIGM, Ri1, Ri2, Rj3, C1, C2, xj, xh, Q, n0: text, F: hash_func
const user_hlregister_r, user_hlregister_n0, user_hlregister_r1, user_hlregister_n1, user_hlregister_d1, user_vlregister_r, user_vlregister_n0,
    user_vlregister_d2, user_vlregister_r1, user_vlregister_r2, vlregister_ hlregister _ n2, hlregister_user_ r, hlregister_user_ n3,
    vlregister_user_ r3, vlregister_ hlregister _ r3, sub1, sub2, sub3, sub4, sub5, sub6:protocol_id
init State: = 0
transition
1. State = 0 /\ Rcv(start)=|>
State’: = 1 /\ Snd({IDi}_SKih)
2. State = 1 /\ Rcv({F(R’.Q).F(F(H(F(R’.Q).F(xh.Q)).xh).R’)}_SKih) =|>
State’: = 2 /\ secret({R’}, sub1, HLR)/\ secret({SIGM}, sub2, {Ui, HLR})
            /\ R’:=new()/\ N0’:=new()/\R1’:=new() /\ R2’:=new/\()D1’:=new()/\D2’:=new/\ ()n1’:=new()
             /\Snd(F(D1’.P).xor((SIGM.n1’.xor(AH(SIGM.F(R’.Q).F(R1’.Q)), N).IDj.
              F(R1’.Q)), AH(D1’.xh.Q)).F(D2’.Q).xor((AH(n1).F(R’.Q)), AH(D2’.xj.Q)).IDh.
              F(R2’.F(SIGM.H(F(R2’.Q). F(D1’.Q). F(D2’.Q).AH(n1).IDj.IDh))).F(R2’.Q)
 /\ witness(Ui, HLR, user_hlregister_n0, N0’) /\ witness(Ui, HLR, user_hlregister_n1, N1’)/\witness(Ui, Vj, user_vlregister_r, R’)
     /\ witness(Ui, HLR, user_hlregister_r1, R1’) /\ witness(Ui, Vj, user_vlregister_r2, R2’)
          /\ witness(Ui, HLR, user_hlregister_d1, D1’) /\witness(Ui, Vj, user_vlregister_d2, D2’)
     /\ secret({N0’, R1’, R2’, D1’, D2’}, sub3, Ui)
3. State = 2 /\ Rcv(AH(AH(F(R’.Q).AH(N0’).AH(N1’).AH(N2’). AH(N3’).BH(R1’.R3’.Q)).
           xor(SIGM, N1’. AH (N2’). N3’.F(R3’.Q)).F(R1’.Q). F(R2’.Q)).
           xor(SIGM, N1’. AH (N2’). N3’.F(R3’.Q)))=|>
  State’: = 3 /\ AH(AH(F(R’.Q).AH(N0’).AH(N1’).AH(N2’). AH(N3’).BH(R1’.R3’.Q)) /\ secret({R3’ }, sub4, Vj) /\ secret({SKij’}, sub6,
{Ui, Vj}) /\ request(Vj, Ui, vlregister_user_ r3, R3’)/\ request(HLR, Ui, hlregister_user_ n3, N3’)
 end role
```

**Figure 4.** Role specification in HLPS for MU

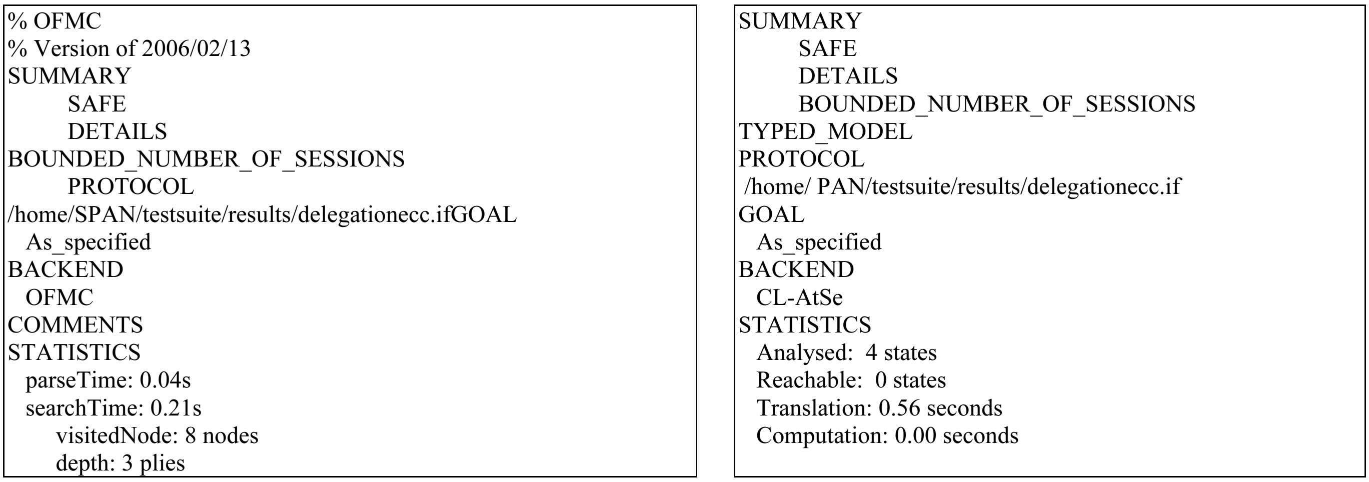
```
role session (
    Ui, Vj, HLR:   agent,
    Snd, Rcv:      channel(dy),      SKih:      symmetric_key,
    SKij:                            symmetric_key,
    H:  hash_func,  AH: hash_func,    BH: hash_func)
def=
  local SI, SJ, RI, RJ: channel(dy)
  composition
      user(Ui, Vj, HLR, SKij, H, AH, BH, SI, RI)
      /\ vlregister (Ui, Vj, HLR, SKij, H, AH, BH, SJ, RJ)/\ hlregister (Ui, Vj, HLR, SKih, H, AH, BH)
end role
role environment()
def=
const ui, vj, hlr: agent,
    skih: symmetric_key,  skjh: symmetric_key, skij: symmetric_key, idh, idi, idj, n0, sigm, ri1, ri2, rj3, d1, d2, xj, xh, q, n0, n1, n2, n3:
text, F: hash_func
const user_hlregister_n0, user_hlregister_r1, user_vlregister_r0, user_vlregister_r1, user_vlregister_r2, hlregister_user_ r, hlregister_user_
    n3, vlregister_user_ r3, vlregister_ hlregister _ n2, vlregister_ user _ n2, vlregister_ hlregister _ r3, hlregister _vlregister_ n3, sub1, sub2,
    sub3, sub4, sub5, sub6: protocol_id
intruder_knowledge={Ui, Vj, HLR, h, ah, bh, q, idh, idj,}
composition
  session(ui, vj, hlr, skij, skih, skjh, h, ah, bh)/\session(i, vj, hlr, skij, skih, skjh, h, ah, bh)
    /\ session(ui, i, hlr, skij, skih, skjh, h, ah, bh)/\session(ui, vj, i, skij, skih, skjh, h, ah, bh)
end role
goal
   secrecy_of sub1, sub2, sub3, sub4, sub5, sub6
   authentication_on user-vlregister_r1
      authentication_on vlregister-user_r3
end goal
environment
```

**Figure 5.** Role specification in HLPSL for the session, goal and environment

### 4.3.2 Analysis of Results

In the section, we specify the simulation results of the proposed DBAKA protocol based on the On-the-fly Model-Checker (OFMC) [42] and Constraint Logic based Attack Searcher (CL-AtSe) backends for the execution test. We use the Security Protocol ANimator for AVISPA [43] to simulate our scheme, for both OFMC and CL-AtSe backends. The back-ends perform a search of a passive intruder to check whether there is the replay attack. For the Dolev-Yao model checking, the back-ends verify whether there is any man-in-the-middle attack possible by the intruder with knowledge of normal sessions between the legitimate agents.

The simulation results using OFMC and CL-AtSe backends have been presented in Figure. 6. It confirms that the proposed DBAKA scheme can resist active attacks such as the replay and man-in-the-middle attacks.



```
% OFMC
% Version of 2006/02/13
SUMMARY
      SAFE
      DETAILS
BOUNDED_NUMBER_OF_SESSIONS
      PROTOCOL
/home/SPAN/testsuite/results/delegationecc.ifGOAL
  As_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.04s
  searchTime: 0.21s
    visitedNode: 8 nodes
    depth: 3 plies
```

```
SUMMARY
      SAFE
      DETAILS
      BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
 /home/ PAN/testsuite/results/delegationecc.if
GOAL
  As_specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed:  4 states
  Reachable:  0 states
  Translation: 0.56 seconds
  Computation: 0.00 seconds
```

**Figure 6.** Analysis of simulation results using OFMC and CL-AtSe backends

## 5 Security and Performance Comparison

Please, leave two blank lines between successive sections as here.

In this section, we will make comparison with the related DBAKA protocols in terms of security and performance.

### 5.1 Security Comparison

In Table 3, we have tabulated an overall security comparison among our scheme and other related DBAKA schemes [4, 21-22, 24, 28-32]. Table 3 shows that the proposed scheme has removed the vulnerability of DBAKA protocols in [29-32], e.g. known key attacks. None of these schemes in [4, 21-22, 24, 28-32] provide communication confidentiality. Furthermore, the existing DBAKA protocols always require that VLR and HLR must share secrets in advance. It is inconvenient for the delegation-based authentication protocols. For each HLR, there are always a great many of VLRs in global mobility networks. In order to provide roaming registered mobile users with access service, each HLR has to share a secret with as many as VLRs, some of which are far geographically from HLR, even in different countries. In addition, since HLR also works as a VLR, HLR (as a VLR) must store shared secrets. Our DBAKA protocol does not require VLR and HLR to share any secret key in advance.

**Table 3.** Comparison of security features among different schemes

| Scheme | $F_1$ | $F_2$ | $F_3$ | $F_4$ | $F_5$ | $F_6$ | $F_7$ | $F_8$ | $F_9$ | $F_{10}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| Lee-Yeh [4] | No | Yes | Yes | No | No | No | No | No | No | No |
| Lee *et al.* [24] | No | Yes | Yes | No | Yes | Yes | No | No | No | No |
| Lu *et al.* [21] | No | No | Yes | No | Yes | Yes | No | No | No | No |
| Lu-Zhou [22] | Yes | No | Yes | No | Yes | Yes | No | No | No | No |
| Wang *et al.* [28] | Yes | Yes | Yes | No | Yes | Yes | No | No | No | No |
| Ou-Hwang [29] | Yes | Yes | Yes | No | Yes | Yes | No | No | No | No |
| Tsai *et al.* [30] | Yes | Yes | Yes | No | Yes | Yes | No | No | No | No |
| Kim *et al.* [31] | Yes | Yes | Yes | No | Yes | Yes | No | No | No | No |
| Hwang-You [32] | Yes | Yes | Yes | No | Yes | Yes | No | No | No | Yes |
| Ours | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

F1: whether withstands denial-of-service attack or not; F2: whether withstands request replication attack or not; F3: whether withstands impersonation attack or not; F4: whether withstands known-key attack or not; F5: whether provides mutual authentication or not; F6: whether provides non-repudiation or not; F7: whether provides weak un-traceability or not; F8: whether provides communication confidentiality or not; F9: whether provides key confirmation or not; F10: whether requires no secrets pre-sharing or not.

It is observed that our scheme outperforms other recently proposed existing DBAKA schemes as our scheme is secure and supports extra features.

## 5.2 Performance Comparison

Since Ou-Hwang's protocol [29], Tsai et al.'s protocol [30], Hwang et al.'s protocol [31] are more efficient and more secure than other existing DBAKA protocols [4, 21-22, 24, 28, 31], we only compare our scheme with three schemes [29-30, 32] in term of storage cost, computational cost and communication cost.

To measure the message size, we assume that each identity is 32 bits long. The output size of hash function is 160 bits (if we use MD5 hash function) and the block size of symmetric encryption/decryption (for example, AES) is 128 bits. The order $q$ of the generator $Q$ in the elliptic curve group $G$ is a 160-bit prime and $p$ is a 163-bit prime. Such choice of $q$, $p$ delivers a comparable level of security to 1024-bit ElGamal encryption over general field. Since one element of $G$ is a point on the group $E(Fp)$, there are two affine coordinates. By using the point compression method, one can bring two elements of $Fp$ down to one element of $Fp$, i.e., the $y$-coordinate of each point in the group $G$. Therefore, the representation of one point in the group $G$ requires 163 bits.

The comparison result of storage required in SIM card is given in Table 4. Table 4 shows that the proposed DBAKA protocol requires as little storage at MU's device as Tsai et al.'s DBAKA protocol does. Say, n=1000. The MU needs to store about 156.3KB in the SIM card. Note the fact that the current mobile devices, including 4G cellular phones, personal digital assistants (PDAs) and notebook computers, have over a few hundred MB or a few GB of available memory. Hence, the storage of the mobile devices required in our protocol is acceptable. In contrast to our protocol, the DBAKA protocols [29, 32] requires more storage at the MU side.

**Table 4.** Storage required at the MU side

| Size(in bits) | Online authentication | Offline authentication |
|---|---|---|
| Ou-Hwang [29] | 128n+2316 | <128n+1024 |
| Tsai et al. [30] | 128n+579 | <128n+256 |
| Hwang et al. [32] | 128n+2336 | <128n+1280 |
| Our | 128n+579 | <128n+256 |

In the following, we discuss the communication cost. Since the registration is executed only once, we concentrate on the message exchange during the authentication phase. Table 5 shows the comparative study of communication costs among our scheme and other related recently proposed schemes [29-30, 32]. The proposed scheme requires less communication cost as compared to Hwang et al.'s scheme [32] and Ou-Hwang's scheme [29]. Though the proposed scheme requires more communication cost during offline authentication phase, it provides various security and functionality features such as communication confidentiality and key confirmation.

**Table 5.** Communication costs

| | Online authentication | | Offline authentication | |
|---|---|---|---|---|
| | $I_1$ | $I_2$ | $I_1$ | $I_2$ |
| Ou-Hwang [29] | 8960 | 4 | 128 | 1 |
| Tsai et al. [30] | 2662 | 5 | 128 | 1 |
| Hwang et al. [32] | 12160 | 5 | 288 | 2 |
| Our | 5531 | 4 | 1152 | 2 |

$I_1$: total number of bits transmission required during authentication phase; $I_2$: total number of messages transmission required during authentication phase.

We only tabulate the computational costs at MU's side and VLR's side during online/offline authentication phase. We ignore lightweight computations, such as the XOR operations and the addition operation in $Z_q$.

According to [44-46], we summarize and induce the time cost of all operations: $T_s \approx 29t_m$ , $T_h \approx 23t_m$ , $T_M \approx t_h \approx t_m$, $t_{sym} \approx 3t_m$, $T_a \approx 0.12t_m$, $t_e \approx t_{inv} \approx 240t_m$, where $T_s$, $T_a$, $T_h$, $t_{sym}$, $t_h$, $t_m$, $t_e$, $t_{inv}$, and $T_M$ represent the time required to perform one scalar multiplication in $G$, one point addition operation in $G$, one map-to-point hash operation, one symmetric encryption/decryption operation, one hash operation, one modular multiplication in $Z_q$, one exponentiation, one inverse operation and one multiplication in a field, respectively. In Table 6, we have tabulated computation costs of the proposed scheme and the existing related schemes [29-30, 32]. It can be observed that the proposed scheme requires lower computation cost during online authentication phase than that of Ou-Hwang [29]. The proposed scheme has much higher efficiency than Hwang et al. [32]. But the proposed scheme is a little more computationally costly than Tsai et al.'s scheme [30], which in contrary is a result of providing enhanced security with respect to the related DBAKA protocols [30] as shown in Table 3.

**Table 6.** Computation costs

| | | Ou-Hwang [29] | Tsai et al.[30] | Hwang et al.[32] | Our |
|---|---|---|---|---|---|
| $I_1$ | MU | $6t_e+2T_M+3t_m+3t_h \approx 1448\ t_m$ | $1T_h+2T_s+1t_m+1t_{sym}+2t_h \approx 87\ t_m$ | $9t_e+9t_h+2t_m+2T_M+2t_{sym} \approx 2179\ t_m$ | $7T_s+1t_{sym}+11t_h+1t_m \approx 218t_m$ |
| | VLR | $6t_e+2T_M+3t_m+3t_h \approx 1448\ t_m$ | $1T_h+4T_s+2t_{sym}+2t_h+2T_a \approx 147.12\ t_m$ | $6t_e+6t_h+2T_M+2t_{sym} \approx 1454\ t_m$ | $8T_s+7t_h+1T_a \approx 239.12t_m$ |
| | HLR | 0 | $3t_{sym}+1t_h \approx 10\ t_m$ | $7t_e+9t_h+2T_M+3t_{sym}+1t_m+1t_{inv} \approx 1941\ t_m$ | $5T_s+1t_{sym}+7t_h+1T_a \approx 155.12t_m$ |
| $I_2$ | MU | $1t_{sym}+1t_h \approx 4\ t_m$ | $2T_h+1t_{sym} \approx 49\ t_m$ | $4T_h+2t_{sym} \approx 98t_m$ | $2T_s+2t_{sym}+3t_h \approx 67t_m$ |
| | VLR | $1t_{sym}+2t_h \approx 5\ t_m$ | $2T_h+1t_{sym} \approx 49\ t_m$ | $4T_h+2t_{sym} \approx 98t_m$ | $2T_s+2t_{sym}+4t_h \approx 68t_m$ |

$I_1$: computation cost required during authentication phase; $I_2$: computation cost required during authentication phase.

Now we evaluate execution time of each entity. The experiments are conducted on an Intel Pentium4 2600 MHz processor with 1024 MB RAM and on a mobile phone with 1.33 GHZ Processor with 768 MB RAM. As shown in Table 7, the proposed scheme performs better than the protocols in [29-30]. The protocol in [30] has better execution performance than the proposed scheme. However, the scheme in [30] fails to achieve weak un-traceablility, communication confidentially, and not resistant to known key attack. Hence, the computational overhead of the proposed scheme in comparison to Tsai et al.'s DBAKA protocol is worth considering the higher security level and the more functionality properties provided.

**Table 7.** Execution time (in milliseconds)

| | Online authentication | | | Offline authentication | |
|---|---|---|---|---|---|
| | MU | VLR | HLR | MU | VLR |
| [29] | 362.4 | 289.7 | 0 | 0.23 | 1.29 |
| [30] | 21.75 | 29.43 | 2.1 | 2.92 | 12.32 |
| [32] | 544.78 | 290.18 | 388.24 | 5.84 | 24.51 |
| Our | 54.8 | 47.8 | 31.01 | 4.00 | 16.80 |

## 6 Conclusion

In this paper, we have designed a new DBAKA protocol based on elliptic curve cryptosystems. We have applied the random oracle model and the BAN logic for formal security analysis, and also simulated our scheme using the widely-accepted AVISPA tool for the formal security verification. The results show that our scheme is secure from well-known possible attacks. Moreover, the proposed scheme provides security and admired functionality features applicable for global mobile networks. As a consequence, our scheme is efficient and more suitable for practical applications especially for mobile devices as compared to other existing DBAKA schemes.

## Acknowledgements

This work is partially supported by the National Natural Science Foundation of China under Grant No. 61462033, Natural Science Foundation of Jiangxi Province under Grant No. 20161BAB202059, the Science and Technology Project of Provincial Education Department of Jiangxi (GJJ160430), the Open Project Program of Key Laboratory of Guangdong Provincial Key Laboratory of Information Security under Grant No. GDXXAQ2016-10.

## References

[1] M. Rahnema, Overview of the GSM System and Protocol Architecture, *IEEE Communications Magazine*, Vol. 31, No. 4, pp. 92-100, April, 1993.

[2] C.-H. Lee, M.-S. Hwang, W.-P. Yang, Enhanced Privacy and Authentication for the GSM System for Mobile Communications, *Wireless Networks*, Vol. 5, No. 4, pp. 231-243, July, 1999.

[3] M.-S. Hwang, Y.-L. Tang, C.-C. Lee, An Efficient Authentication Protocol for GSM Networks, EUROCOMM 2000, *Information Systems for Enhanced Public Safety and Security*, Munich, Germany, 2000, pp. 326-329.

[4] W.-B. Lee, C.-K. Yeh, A New Delegation-Based Authentication Protocol for Use in Portable Communication Systems, *IEEE Transactions on Wireless Communications*, Vol. 4, No. 1, pp. 57-64, January, 2005.

[5] M. Karuppiah, S. Kumari, X. Li, F. Wu, A. K. Das, M. K. Khan, R. Saravanan, S. Basu, A Dynamic ID-Based Generic Framework for Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks, *Wireless Personal Communications*, Vol. 93, No. 2, pp. 383-407, March, 2017.

[6] M. Prasad, R. Manoharan, DS-AKA-A Novel Secured Authentication Protocol for LTE-A Using Public Key Cryptography, *Journal of Internet Technology*, Vol. 18, No. 4 , pp. 753-763, July, 2017.

[7] C.-H. Chou, K.-Y. Tsai, T.-C. Wu, Robust Remote Mutual Authentication Scheme with Key Agreement, *Journal of Internet Technology*, Vol. 16, No. 7, pp. 1283-1289, December, 2015.

[8] V. Odelu , S. Banerjee , A. K. Das, S. Chattopadhyay, S. Kumari, X. Li, A. Goswami, A Secure Anonymity Preserving Authentication Scheme for Roaming Service in Global Mobility Networks, *Wireless Personal Communications*, Vol. 96, No. 2, pp. 2351-2387, September, 2017, DOI: 10.1007/s11277 -017-4302-4.

[9] P. Gope, T. Hwang, Enhanced Secure Mutual Authentication, and Key Agreement Scheme Preserving User Anonymity in Global Mobile Networks, *Wireless Personal Communications*, Vol. 82, No. 4, pp. 2231-2245, June, 2015.

[10] P. Gope, T. Hwang, An Efficient Mutual Authentication and Key Agreement Scheme Preserving Strong Anonymity of The Mobile User in Global Mobility Networks, *Journal of Network and Computer Applications*, Vol. 62, pp. 1-8, February, 2016.

[11] C.-T. Li, C.-C. Lee, C.-Y. Weng, A Chaotic Maps Based Key Agreement and User Anonymity Protocol without Using Smart Cards and Symmetric Key En/Decryptions, *Journal of Internet Technology*, Vol. 18, No. 5, pp. 975-984, September, 2017.

[12] D. He, J. Bu, S. Chan, C. Chen, M. Yin, Privacy-preserving Universal Authentication Protocol for Wireless Communications, *IEEE Transactions on Wireless Communications*, Vol. 10, No. 2, pp. 431-436, February, 2011.

[13] H. J. Jo, J. H. Paik, D. H. Lee, Efficient Privacy-Preserving Authentication in Wireless Mobile Networks, *IEEE Transactions on Mobile Computing*, Vol. 13, No. 7, pp. 1469-1481, July, 2014.

[14] C.-C. Chang, C.-Y. Sun, S.-C. Chang, Practical Secure and

High Efficient Authentication Scheme in Global Mobility Networks, *Journal of Internet Technology*, Vol. 15, No. 7, pp. 1091-1100, December, 2014.

[15] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, H. H. Choi, Enhanced Secure Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks, *Mathematical and Computer Modelling*, Vol. 55, No. 1-2, pp. 214-222, January, 2012.

[16] V. Odelu, A. K. Das, S. Kumari, X. Huang, M. Wazid, Provably Secure Authenticated Key Agreement Scheme for Distributed Mobile Cloud Computing Services, *Future Generation Computer Systems*, Vol. 68, pp. 74-88, March, 2017.

[17] A. G. Reddy , A. K. Das , E.-J. Yoon, A Secure Anonymous Authentication Protocol for Mobile Services on Elliptic Curve Cryptography, *IEEE Access*, Vol. 4, pp. 4394-4407, July, 2016.

[18] M. Mambo, K. Usuda, E. Okamoto, Proxy Signatures: Delegation of the Power to Sign Messages, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E79-A, No. 9, pp. 1338-1353, September, 1996.

[19] C. Tang, D. O. Wu, An Efficient Mobile Authentication Scheme for Wireless Networks, *IEEE Transactions on Wireless Communications*, Vol. 7, No. 4, pp. 1408-1416, April, 2008.

[20] T.-F. Lee, S.-H. Chang, T. Hwang, S.-K. Chong, Enhanced Delegation-Based Authentication Protocol for PCSs, *IEEE Transactions on Wireless Communications*, Vol. 8, No. 5, pp. 2166-2171, May, 2009.

[21] J. Z. Lu, J. P. Zhou, On the Security of An Efficient Mobile Authentication Scheme for Wireless Networks, *Proceedings of 2010 International Conference on Wireless Communication Networking and Mobile Computing*, Chengdu, China, 2010, pp. 1-3.

[22] J.-Z. Lu, J. Zhou, Preventing Delegation-Based Mobile Authentications from Man-In-The-Middle Attacks, *Computer Standards & Interfaces*, Vol. 34, No. 3, pp. 314-326, March, 2012.

[23] T.-Y. Youn, J. Lim, Improved Delegation-Based Authentication Protocol for Secure Roaming Service with Unlinkability, *IEEE Communications Letters*, Vol. 14, No. 9, pp. 791-793, September, 2010.

[24] C.-C. Lee, R.-X. Chang, T.-Y. Chen, L. A. Chen, An Improved Delegation-Based Authentication Protocol for PCSs, *Information Technology and Control*, Vol. 41, No. 3, pp. 258-267, September, 2012.

[25] P. Gope, T. Hwang, Security Weaknesses on a Delegation-based Authentication Protocol for PCSs, *Information Technology and Control*, Vol. 44, No. 3, pp. 329-333, 2015, DOI:http://dx.doi.org/10.5755/j01.itc.44.3.9777

[26] X. Li, J. Niu, S. Kumari, F. Wu, K.-K. R. Choo, A Robust Biometrics Based Three-Factor Authentication Scheme for Global Mobility Networks in Smart City, *Future Generation Computer Systems*, Vol. 83, pp. 607-618, June, 2018, DOI: https://doi.org/10.1016/j.future.2017.04.012

[27] C. H. Wang, C. Y. Lin, An Efficient Delegation-Based Roaming Payment Protocol Against Denial of Service Attacks, *Proceedings of 2011 International Conference on Electronics, Communications and Control*, Ningbo, China, 2011, pp. 4136-4140.

[28] Y. Wang, Q. Pu, S. Wu, Cryptanalysis and Enhancements of Delegation-Based Authentication Protocol for Secure Roaming Service, *International Journal of Electronic Security and digital Forensics*, Vol. 4, No. 4, pp. 252-260, October, 2012.

[29] H.-H. Ou, M.-S. Hwang, Double Delegation-Based Authentication and Key Agreement Protocol for PCSs, *Wireless Personal Communications: An International Journal*, Vol. 72, No. 1, pp. 437-446, September, 2013.

[30] J.-L. Tsai, N.-W. Lo, T.-C. Wu, Secure Delegation-Based Authentication Protocol for Wireless Roaming Service, *IEEE Communications Letters*, Vol. 16, No. 7, pp. 1100-1102, July, 2012.

[31] M. Kim, N. Park, D. Won, Security Analysis of a Delegation-Based Authentication Protocol for Wireless Roaming Service, in: J. J. Park, S. C. Chen, J. M. Gil, N. Y. Yen (Eds.), *Multimedia and Ubiquitous Engineering*, Lecture Notes in Electrical Engineering, Vol. 308, Springer, 2014, pp. 445-450.

[32] S.-J. Hwang, C.-H. You, A Delegation-Based Unlinkable Authentication Protocol for Portable Communication Systems with Nonrepudiation, in: Y. M. Huang, H. C. Chao, D. J. Deng, J. Park (Eds.), *Advanced Technologies, Embedded and Multimedia for Human-centric Computing*, Lecture Notes in Electrical Engineering, Vol. 260, Springer, 2014, pp 923-932.

[33] C. P. Schnorr, Efficient Signature Generation By Smart Cards, *Journal of Cryptology*, Vol. 4, No. 3, pp. 161-174, January, 1991.

[34] M. Burrows, M. Abadi, R. Needham, A Logic of Authentication, *ACM Transactions on Computer Systems*, Vol. 8, No. 1, pp. 18-36, February, 1990.

[35] AVISPA, Automated Validation of Internet Security Protocols and Applications, http://www.avispa-project.org/.

[36] D. von Oheimb, The High-Level Protocol Specification Language Hlpsl Developed in The EU Project Avispa, *Proceedings of 3rd APPSEM II Workshop on Applied Semantics (APPSEM 2005)*, Frauenchiemsee, Germany, 2005, pp. 1-17.

[37] M. Abdalla, P.-A. Fouque, D. Pointcheval, Password Based Authenticated Key Exchange in The Three-Party Setting, *Proceedings of 8th International Workshop on Theory and Practice in Public Key Cryptography (PKC'05)*, Les Diablerets, Switzerland, 2005, pp. 65-84.

[38] V. Shoup, *Sequences of Games: A Tool gor Taming Complexity in Security Proofs, Cryptology ePrint Archive*, Report 2004/332, November, 2004.

[39] P. Syverson, I. Cervesato, The Logic of Authentication Protocols, Foundations of Security Analysis and Design, in: R. Focardi, R. Gorrieri (Eds.), *Foundations of Security Analysis and Design, Lecture Notes in Computer Science*, Vol. 2171, Springer, 2001, pp. 63-137.

[40] S.-J. Hwang, C.-H. You, A Delegation-Based Unlinkable

Authentication Protocol for Portable Communication Systems with Nonrepudiation, in: Y. M. Huang, H. C. Chao, D. J. Deng, J. Park (eds.), *Advanced Technologies, Embedded and Multimedia for Human-centric Computing, Lecture Notes in Electrical Engineering*, Vol. 260, Springer, 2014, pp 923-932.

[41] D. Dolev, A. Yao, On the Security of Public Key Protocols, *IEEE Transactions on Information Theory*, Vol. 29, No. 2, pp. 198-208, March, 1983.

[42] D. Basin, S. Mödersheim, L. Viganò, OFMC: A Symbolic Model Checker for Security Protocols, *International Journal of Information Security*, Vol. 4, No. 3, pp. 181-208, June, 2005.

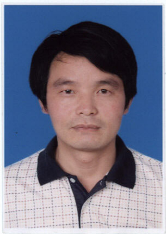
[43] AVISPA, SPAN, the Security Protocol ANimator for AVISPA, http://www.avispa-project.org/.

[44] C.-I. Fan, W.-Z. Sun, V. S.-M. Huang, Provably Secure Randomized Blind Signature Scheme Based on Bilinear Pairing, *Computers and Mathematics with Applications*, Vol. 60, No. 2, pp. 285-293, July, 2010.

[45] N. Koblitz, A. Menezes, S. Vanstone, The State of Elliptic Curve Cryptography, *Design, Codes and Cryptography*, Vol. 19, No. 2-3, pp. 173-193, March, 2000.

[46] Z. W. Tan, An Efficient Identity-Based Tripartite Authenticated Key Agreement Protocol, *Electronic Commerce Research*, Vol. 12, No.4, pp. 505-518, November, 2012.

## Biography



**Zuo-Wen Tan** received the Ph.D. degree in Applied Mathematics from Institute of Systems Science, CAS in 2005. He is currently full professor at Department of Computer Science & Technology, Jiangxi University of Finance & Economics. His research interests include information security and cryptography.