Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **6**, November **2016**

A Universal Authentication Scheme with Anonymity for Heterogeneous Wireless Networks

Chin-Chen Chang

Department of Information Engineering and Computer Science
Feng Chia University
100 Wenhwa Road, Taichung 40724, Taiwan, R.O.C.
ccc@cs.ccu.edu.tw

Wan-Ting Tseng and Hao-Chuan Tsai

Department of Computer Science and Information Engineering
National Chung Cheng University
168 Sec 1, University Road, Chiayi 621, Taiwan, R.O.C.
miot1177@gmail.com; tsaihc@cs.ccu.edu.tw

Received December, 2015; revised September, 2016

Abstract. *With the increased demand in ubiquitous wireless access, we merge different but complementary wireless access craftsmanship to compose global wireless heterogeneous network, such as GSM and 3GPP, to provide mobile users the advantage of roaming services without geographical limitation. Hence, it has a great challenge to provide authentication in such a distributed heterogeneous network. Typically, a roaming scenario involves three entities, a mobile user (MS), a visited network (VN), and a home network (HN). In this paper, we proposed a new version with novel architecture, includes a universal authentication scheme with both computation efficiency and communication efficiency. The security of the proposed scheme is based on the elliptic curve cryptography. Despite elliptic curve cryptography involves more complicated operations; for the practical inspect, the proposed scheme is still suitable for the implementation. In addition, we provide a self-verified mobile authentication scheme, and then utilize random oracle to prove the proposed scheme is secure.*
Keywords: Mobile authentication, Anonymous, Key agreement, BLS, Wireless networks, Random oracle

1. **Introduction.** Wireless network technologies have grown significantly in the last decade. Especially, Wireless Local Area Networks (WLAN) [27] and Wireless Personal Area Networks (WPAN) [8] provide the advantage of high transmission rate on Internet access. In addition, user mobility is a highly desirable feature in the development of computer networks and telecommunication systems because it needs to meet current requirements of the applications. To achieve this goal, this cellular network, such as GSM [27] and 3GPP [31], provides mobile users the advantage of roaming services without geographical limitations. With such a network environment, mobile users who subscribed initially to their home networks can travel to other networks with different operations and still be able to access services. Also, it is also desirable to integrate seamless connectivity between the high bandwidth WLAN network and the cellular network for universal roaming. To do so, the different service providers must authenticate the mobile users who subscribed originally to their own home networks. However, it is a great challenge

to provide authentication in such a distributed, heterogeneous network, since no trusted authentication server exists for both the mobile users and the visited networks. Previously proposed schemes [7], [25] only supported unilateral authentication, e,g., authentication of mobile users by a visited network. Such an incomplete authentication creates the potential problem of a deposit attack [30]. Hence, for security purposes, mutual authentication should be provided to the involved entities. Typically, a roaming scenario involves three entities, a mobile user (MS), a visited network (VN), and a home network (HN). Initially, a mobile user who wants to subscribe to other networks must register with the specific home network. Next, when a mobile user travels to a visited network, the conventional way to perform user authentication is for the visited network to verify the legitimacy of the mobile user with the home network, which serves as the guarantor. In addition, to preserve privacy, it is highly desirable for mobile users to have anonymity with respect to adversaries as well as the visited networks. The visited network is allowed to ensure the legitimacy, but not the identity, of the mobile user. Hence, the design of a secure roaming scheme should ensure the anonymity of the user.

In the past decade, many research projects (e.g. [3], [6], [9], [15], [28], [30], [33], [34], [35]) have been proposed to achieve these requirements. Recently, Yang et al.s [29] proposed a novel set of solutions to achieve secure roaming. Their solutions only require that the mobile user and the visited network be involved in each authentication round, eliminating the need for any interaction with the home network. Their solutions, which are based on the elliptic curve cryptosystem [10], simultaneously are robust and preserve the anonymity of mobile users. However, the computation overhead of Yang et al.s scheme is excessive since it uses the complicated group key signature operations. In addition, their scheme does not achieve the essential requirement eliminating traceability. Shrestha et al. [22] proposed a Kerberos based [12] inter-domain roaming authentication scheme that is different from Yang et al.s scheme. To reduce the heavy burden of the mobile users, Shrestha et al.s scheme utilizes the pre-shared secret keys to authenticate the involved entities and to establish session keys. In addition, the visited network generates a certificate ticket, named Token, for the mobile user to reduce the computation costs and the communication rounds. Compared with similar, existing schemes [21], [23], Shrestha et al.s scheme has the advantages of both computation efficiency and communication efficiency. Unfortunately, according to our observation, some weaknesses still exist in Shrestha et al.s scheme, including the key management problem, the token storage problem, and the failure to provide complete anonymity for mobile users. To eliminate these weaknesses, we proposed a new version with a novel architecture. Our contributions include a universal authentication scheme that is efficient with respect to both computations and communications. The security of the proposed scheme is based on the elliptic curve cryptography [10], which involves more complicated operations than symmetric cryptosystems. However, from the practical aspect, the proposed scheme is still suitable for the implementation, since, in actuality, a fast scalar point multiplication algorithm [17] is used in the elliptic curve cryptography. More importantly, elliptic curve cryptosystems can be implemented with significantly fewer parameters, leading to significant performance advantages, for the same level of security per best currently known algorithms, such as RSA [19], and ElGamal [5]. The proposed scheme has the following attractive properties:

(1). Mutual authentication can be achieved between a mobile user and a visited network. More precisely, the home network is not involved in each protocol execution.

(2). A session key assisted is available only to mobile communication users and the visited network, and such a session key would not be revealed to either the uninvolved servers or adversaries.

(3). In this new method, only the service providers need to adopt the public-key cryptosystem. This property can provide the well scalability of the mobile users.
(4). The risk of compromising the pre-shared secret that is stored by the service provider is reduced; avoiding the need for the service provider to maintain these stored secrets makes the service provider scaleable when it must manage a large number of mobile users.
(5). Mobile users information is private, and, compared with the previous schemes, computation efficiency and communication round efficiencies can be ensured for both communication entities.

The rest of this paper is organized as follows. We briefly review Shrestha et al.s scheme and describe their weaknesses in Section 2. The propose scheme is demonstrated in Section 3. Then, the security analysis and the performance analysis are described in Section 4 and Section 5, respectively. Finally, we give conclusions in Section 6.

2. **Drawbacks on Kerberos Based Mobile Authentication.** To provide better reliability and simpler architecture, Shrestha et al. [22] recently proposed a Kerberos-based authentication mechanism for wireless heterogeneous networks. Different from the previously proposed schemes, the shared secret keys, which are utilized to ensure communication security, have to be distributed among involved entities. More importantly, when a mobile user roams to a visited network, an extra certificate ticket Token has been exploited to reduce the communication burden without communicating to the home network. Shrestha et al.s scheme has the attractive advantage in terms of computational efficiency and round efficiency. However, according to our observation, some potential weaknesses, such as key management problem and token storage problem are not well processed in Shrestha et al.s scheme. Before describing the weaknesses that exist in Shrestha et al.s scheme, we first briefly review their scheme.

Step 1: When a mobile user MS roams to a visited network VN, MS sends his identity ID_{MS} and the address of the home network HN to VN. And then, VN re-transmits the authentication request to the corresponding HN.

Step 2: After receiving the messages from VN, HN firstly verifies the validity of MS identity. In addition, HN generates a session key SK and utilizes the pre-secret key , which is a pre-shared secret key between MS and HN, to encrypt the generated result with the visited network identity VNID and a ticket TKT, where TKT $= E_{K_V}\{\ ID_{MS} \parallel \text{SK} \parallel niAddr \parallel Lifetime\ \}$ and K_V is a pre-shared secret key between HN and VN, respectively. Subsequently, HN returns these encrypted results to VN.

Step 3: VN then forwards the encrypted result $E_{K_m}\{\ ID_{MS} \parallel \text{SK} \parallel niAddr \parallel Lifetime\ \}$ to MS. After receiving the encrypted result, MS utilizes the pre-shared secret key K_m to retrieve the session key SK, VNID, the ticket TKT, and the Lifetime. Simultaneously, MS generates a random nonce N_1 to compute an authenticator $Auth = E_{SK}\{\ ID_{MS} \parallel \text{SK} \parallel niAddr \parallel N_1\ \}$, which is encrypted by the session key SK. And then, MS sends the encrypted authenticator along with the retrieved TKT to VN.

Step 4: After receiving the messages from MS, VN decrypts the previously received TKT to obtain the session key SK. VN utilizes SK to decrypt the authenticator $Auth$ and then retrieves the identity of MS and the network interface address $niAddr$ to verify MS; if it holds, VN authenticates MS successfully and also generates a $Token$, which is used to future authenticate by other visited networks. Eventually, VN sends the $Token$ along with $E_{SK}\{N_1 + 1\}$ to MS.

Step 5: Finally, MS decrypts $E_{SK}\{N_1 + 1\}$ and verifies the retrieved nonce. If it holds, MS authenticates VN successfully and stores $Token$ in the local side.

We now describe the existed weaknesses in Shrestha et al.s scheme.

A.Key Management Problem

In Shrestha et al. scheme, each mobile user is associated with a shared secret key which is shared with his home network. The main use of these secret keys is used to achieve mutual authentication between mobile users and their home network. By applying the Kerberos cryptosystem without a centralized ticket server, all networks, including the visited networks and the home networks, have to pre-share extra secret keys with each other. However, the number of shared secret key that the networks need to protect will be increased linearly. i.e., $C_2^{N_1}(=N_1(N_1\text{-}1)/2)+N_2$ where N_1 is the number of the networks and N_2 is the number of secret keys that are shared between the mobile users and their home networks. Due to the fact that a number of networks exist and a million mobile users may register to the specific network, it could lead a heavy burden for this specific network. This is a great challenge for this network to maintain these pre-shared secret keys securely. In addition, the symmetric key based scheme, such as Kerberos based, may be vulnerable to the potential weaknesses, denial-of-service attacks and deposit attacks [30]. Hence, according to our observation, a key management problem is existed in Shrestha et al.s scheme.

B. Tokens Management and Improper Session Key Problem

To provide better re-authentication efficiency, initially, a mobile user is assigned a $Token$ to communicate with his home network. Although this approach is simple and efficient, a token is only permitted to be used between two assignable visiting networks. Hence, in order to move among all the visiting networks, the mobile users need the extra costs for storing a lot of tokens. In addition, a session key communicated between a mobile user and a visiting network is generated by the home network rather than negotiated with a visiting network. For personal privacy, it is not allowed the home network to obtain the session key between the mobile user and the visiting network. It is trivial to observe that the home server can also obtain the session key which should be known only between the mobile user and the visiting network. Thus, Shrestha et al.s scheme does not provide good key establishment property.

3. **The Proposed Scheme.** Before demonstrating the security analysis, we first define the security models for authenticated key agreement and depict the security basis on which the security of the proposed scheme relies.

Assume that an adversary A who can interact between the participants via oracle queries. These queries indicate the adversary capabilities in real attacks throughout the networks. The types of the oracle queries which are generalizations of models of Bellare and Rogaway [2] can be available to the adversary are modeled as in the following.

·$Excute(\Pi_U^i, \Pi_S^j)$:This query models passive attacks. That is, the adversary can obtain the messages exchanged during the honest execution of the protocol between a client instance Π_U^i and a server instance Π_S^j. In addition, this query is imperative for the adversary to perform dictionary attacks.

·$Send(\Pi_U^i, m)$:This query models active attacks. The adversary is able to generate the arbitrary message m to send to an instance Π_U^i, and then the instance will return the computed result to the adversary. For example, a query $Send(\Pi_U^i, "start")$ initializes the key exchange protocol, and then adversary receives the initial flow that the initiator sends to the receiver.

·$Reveal(\Pi_U^i)$:This query models that the loss of an ever used session key should not harm other sessions. Note that the adversary can issue this query only if $\mathrm{ACC}(\Pi_U^i)$ is set to true.

·$corrupt(\Pi_U^i)$:This query models the perfect forward secrecy, if the security of a session key between two more participants is preserved even if one of these participants has been compromised. More precisely, the long-lived key of the participant is returned to the

adversary, and the damage caused by losing of the participants long-lived key should be restricted to those sessions where the participant will participate in the future.

$\cdot Test(\Pi_U^i)$:This query models the security of the established session key. That is, it captures the adversarys ability to distinguish real keys from random ones. In order to answer it, a hidden random coin b is flipped by the instance Π_U^i. When the adversary issues a single $Test$ query to Π_U^i, the adversary either obtains the session key if $b = 1$ or a random key of the domain if $b = 0$, i.e., the $Test$ query is allowed only once at any time during the execution of the adversary.

$\cdot Hash(m)$:These are cryptographic hash functions that are viewed as random functions with the appreciate range in the ideal hash model. And, the adversary can issue this query to have the hash result. Note that if m has never been queried before, it then returns a truly random string to the adversary and stores m in the hash table; otherwise, it returns the previously generated result to the adversary.

The goal of the adversary is to try to guess the hidden bit b involved in the $Test$ query by outputting a guess b'. We say that the adversary wins a game of breaking authenticated key exchange, which is abbreviated to $\mathbf{A}KE$, the security if the adversary issues $Test$ queries to a fresh instance Π_U^i and successfully guesses the hidden bit b. The probability that the adversary wins the game is $\Pr[b' = b]$. In addition, the AKE advantage of the adversary is then defined as $Adv_p^{AKE}(E) = 2{\cdot}\Pr[b'{=}b]$-1, where E denotes the adversary. The protocol P is said to be (t,ϵ)-AKE secure if there is no adversary wins the game greater than ϵ with time t.

Bilinear Map and Assumptions

Let G_1, G_2 be two additive groups over points with prime order p and $P{\in}G_1$ be a base point over an elliptic curve. Let $\mathrm{Gen}(1^\kappa)$ be an algorithm generating (p,G_1,G_2,$\hat{e}$,P), where κ is the system security parameter with length of p. A map $\hat{e}$:$G_1{\times}G_1{\rightarrow}G_2$ is a bilinear map if it satisfies the following properties.

Bilinearity : for any $a, b{\in}Z_p^*$ and $P, Q{\in}G_1$, $\hat{e}(aP, bQ){=}\hat{e}(P, abQ){=}\hat{e}(abP, Q){=}\hat{e}(P, Q)^{ab}$. In addition, this can be extended as in the following. For all $P, Q, R{\in}G_1$, $\hat{e}(P{+}R, Q){=}\hat{e}(P, Q)$ $\cdot\hat{e}(R, Q)$ and $\hat{e}(P, R + Q){=}\hat{e}(P, R){\cdot}\hat{e}(P, Q)$.

Non-degeneracy:there exists a point $P{\in}G_1$ and $\hat{e}(P, P){\in}G_2$. In other words, $\hat{e}(P, P)$ is not the identity element in G_2. It is worth noting that $\hat{e}(P, P){\in}$ is a generator of G_2.

Computable : there exists an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q{\in}G_1$ in polynomial time.

$ComputationBilinearDiffie-HellmanAssumption(CBDH)$.Let $\hat{e}$:$G_1{\times}G_1{\leftarrow}G_2$ be a cryptographic bilinear map as aforementioned. A $(t, \epsilon)-CBDH$ is a probabilistic Turing machine Δ running in time t such that its successful probability $Succ_{P,G_1}^{cbdh}(\Delta)$ is greater than or equal to ϵ:

$$Succ_{P,G_1}^{cbdh}(\Delta) = Pr[\Delta(\hat{e}, P, xP, yP, zP)] = \hat{e}(P, P)^{xyz} \geq \epsilon \tag{1}$$

when given elements xP, yP and zP to compute $\hat{e}(P, P)^{xyz}$, for all $x, y, z{\in}{Z_q}^*$. Let $Succ_{P,G_1}^{cbdh}(t)$ be the upper bound that adversaries have within time t. The $CBDH$ Assumption in G_1 is that $Succ_{P,G_1}^{cbdh}(t){\leq}\epsilon$ for any t/ϵ is not extremely large.

Initially, no trust mutual relationship is established between the mobile user and the visiting network. That means the mobile user cannot trust the visiting network without verifying and vice versa. In addition, we assume that the involved visiting networks are honest and do not perform any malicious manners to the mobile user. In the proposed scheme, it is reasonable to assume that the home network is always trustworthy because we must register it. And in this paper, we assume that each mobile user can obtain all the servers identities, including the home network and the visiting networks, and the

associated public key pairs. Our proposed scheme is based on the concept of Identity Based Cryptography [20].

Let κ be a system security parameter. The entire system can be categorized into two entities, i.e., the mobile user entity set $MS(\kappa)$=$\{MS_1, MS_2, \cdots, MS_{Q_1(\kappa)}\}$ and the server network entity set $SN(\kappa)$=$\{SN_1, SN_2, \cdots, SN_{Q_2(\kappa)}\}$ with large capabilities and powerful computational operations, where Q_1 and Q_2 are two polynomials, and each element in the sets is the corresponding identity. It is worth noting that, to reduce the heavy burden of the mobile users, we assume that the elements of the server entity are associated only with a public key pair of an asymmetric encryption scheme or a signature signing scheme.

The home network SN_H performs the following steps only once: suppose that SN_H has the public key Y_{SN_H}=$x_{SN_H} \cdot P$, where $x_{SN_H} \in Z_P{}^*$ is the private key. To provide anonymity and reversibility for the mobile user MS_a, SN_H generates the unique hidden identity TID_{U_a} by calculating the equation $h(x_{SN_H}, SN_H) = h(MS_a, SN_H) \cdot TID_{U_a} (\mathrm{mod}\ p)$, where $h(\cdot)$ denotes a cryptographic collision-free hash function and behaves like random oracles [2]. After that, SN_H computes Psk_a=$x_{SN_H} \cdot H(TID_{U_a})$, where $H(\cdot)$ is a map-to-point function, as the master delegation key and securely delivers the computed result along with the hidden identity TID_{U_a} to the mobile user MS_a for future roaming authentication. Eventually, SN_H can destroy all of the secret information except for SN_Hs private key. This operation can significantly reduce the storage complexity on the home network side.

When the mobile user MS_a roams to the visiting network SN_{V_i}, the mobile authentication phase is described as follows.

1.MS_a selects a random number $r_a \in Z_p{}^*$ and computes the partial ephemeral Diffie-Hellman key Y_a=$r_a \cdot P$. In addition, MS_a computes Z_a=$Psk_a + r_a \cdot h(Y_a \| ts) \cdot Y_{SN_V}$, where ts is the current timestamp and $Y_{SN_V} = x_{SN_V} \cdot P$ is the public key of the visiting network SN_{V_i}, respectively. Next, MS_a sends the computed results $\{Z_a, Y_a, ts\}$ along with the hidden identity TID_{U_a} to SN_{V_i}.

2.Upon receiving the messages from MS_a, initially, SN_{V_i} checks the validity of the timestamp ts. If the received ts is under the reasonable threshold, SN_{V_i} computes $h(Y_a \| ts)$ and then verifies the equation $\hat{e}(Z_a, P)$=$\hat{e}(H(TID_{U_a}), Y_{SN_H}) \cdot \hat{e}(h(Y_a \| ts)P, Y_a)^{X_{SN_V}}$. This verification is correct since $\hat{e}(Z_a, P)$ =$\hat{e}(Psk_a + r_a \cdot h(Y_a \| ts) \cdot Y_{SN_V}, P)$ =$\hat{e}(x_{SN_H} \cdot H(TID_{U_a}), P) \cdot \hat{e}(r_a \cdot h(Y_a \| ts) \cdot Y_{SN_V}, P)$ =$\hat{e}(H(TID_{U_a}), x_{SN_H} \cdot P) \cdot \hat{e}(r_a \cdot h(Y_a \| ts) \cdot x_{SN_V} \cdot P, P)$ =$\hat{e}(H(TID_{U_a}), Y_{SN_H}) \cdot \hat{e}(h(Y_a \| ts) \cdot P, r_a \cdot x_{SN_V} \cdot P) = \hat{e}(H(TID_{U_a}), Y_{SN_H}) \cdot \hat{e}(h(Y_a) \| ts)P, r_a \cdot P)^{x_{SN_V}}$ =$\hat{e}(H(TID_{U_a}), Y_{SN_H}) \cdot \hat{e}(h(Y_a) \| ts)P, Y_a)^{x_{SN_V}}$.If it holds, SN_{V_i} authenticates MS_a successfully. Next, SN_{V_i} selects a random number $r_v \in Z_p{}^*$, computes $Y_v = r_v \cdot P$ and $K_{VU} = r_v \cdot Y_a = r_v r_P$. To ensure the integrity of the exchange Diffie-Hellman key Y_v, SN_V computes σ=$x_{SN_V} \cdot H(h(K_{VU}))$, which is based on the BLS signature [1], and then sends the computed result along with Y_v to MS_a.

3.On receiving $\{Y_v, \sigma\}$, to authenticate the visiting network SN_{V_i}, at first, MS_a computes $h(r_a(Y_v)) = h(r_a r_v P) = h(K_{VU})$ and then verifies the equation $\hat{e}(\sigma, P)$=$\hat{e}(H(h(r_a r_v P)), Y_{SN_V})$. If it holds, MS_a authenticates SN_{V_i} successfully, and then, establishes the session key sk=$h(K_{VU}, TID_{U_a}, SN_V, ts)$ for later communications with SN_{V_i}.

4. **Security Analysis and Discussions.** We analyze the security of the proposed scheme in terms of subscriber validation, key establishment, and anonymity.

Theorem 4.1. *Let us consider the above scheme over a group of prime order p, generated by a base point P. Any adversary A within a time bound t makes at most q_s active sessions and q_e passive eavesdropping with the users, respectively. And A can query at most qh queries. We obtain*

$$Adv_P{}^S(A) \leq 2((q_s{}^2/2p + q_e{}^2/2p^2 + \Delta q_{se}^2) + 2(q_s + q_e) \times q_h{}^2 \times Succ_{P,G_1}^{cbdh}(\tau + t) + (1 + q_s)((1/2p) \times q_h \times Succ_{P,G_1}^{cbdh}(t + 2\tau) + (q_s/p)) \quad (2)$$

where τ denotes the computational time for a multiplication in P with order p.

Proof: We use a sequence of game reduction steps to estimate the tightly upper bound in which the adversary breaks the semantically secure but not violates the authentication. In all games, we use the notation EvS_n to present the involved event in each game. The game starts from game G_0, which presents the real attack game.

Game G_0: This is a real attack in the random oracle model, by the definitions, we have $Adv_P{}^S(A)$=2·Pr[EvS_0]-1.

Game G_1:In this game, we simulate all oracles in a real attack. That means we can simulate all instances as the real entities for the *Send*, *Execute*, and *Corrupt* queries. Additionally, the *Test* query is answered once according to the bit b in each session: if b = 1 (real), then the computed session key during the simulation is returned; otherwise, if $b = 0$ (random), $h'(r_a r_v P, TID_{U_a}, SN_V, ts)$, which is a truly random value, is returned, where h' is a private random oracle. Eventually, it is easy to observe that G_1 is indistinguishable from the real attack G_0. Hence, we have Pr[EvS_1]=Pr[EvS_0].

Game G_2:In this game, we modify G_2 in which some collisions occur in the partial transcripts $\{TID_{U_a}, Z_a, Y_a, ts\}$. Without loss of generality, we assume that the transcripts $\{TID_{U_a}, Y_a, ts\}$ were simulated and generated at random. As a result, according to the birthday paradox, the probability of collisions with the partial transcript is at most $(q_s{}^2/2p + q_e{}^2/2p^2 + \Delta q_{se}^2)$, where Δ and q_{se}^2 denote an upper bound on the guessing probabilities of the servers master key and the number of sessions, respectively; in addition, a similar reason applied to the output of $Hashh$ (a partial message of Z_a) is bounded by $(q_h{}^2/2p^2)$. Consequently, we have |Pr[EvS_2]-Pr[EvS_1]|≤$(q_s{}^2/2p + q_e{}^2/2p^2 + \Delta q_{se}^2)$+$(q_h{}^2/2p^2)$.

Game G_3:In this game, we further deal with the probability of the adversary resorts Execute queries to break the proposed scheme in passive attacks. When the adversary A asks an *Execute* query, we utilize the additional hash oracle h' appeared in the game G_1 to compute the secret message as $h'(r_a r_v P, TID_{U_a}, SN_V, ts)$ instead of the original $Hash$ oracle. It is worth noting that such an additional $Hash$ oracle is inaccessible to A. We can observe that these secret messages computed during such a passive session are independent of $Hash$ and $CBDH - result_{A/B}$.

The games G_3 and G_2 are indistinguishable unless the event $AskH$ occurs.

·$AskH(TIS_{U_a}, Z_a, Y_a, ts, CBDH - result_{A/B})$ has been queried by A to $Hash$ some passive for some passive transcript $\{TID_{U_a}, Z_a, Y_a, ts\}$ with the extra information eP. Thus, we can derive |Pr[EvS_3]-Pr[EvS_2]|≤Pr[$AskH$]. It is also worth noting that, under the CBDH assumption, the partial Bilinear Diffie-Hellman key exchange information from a secret random oracle cannot be available to A. Hence, A cannot distinguish the real session key from the random one with a non-negligible probability from Hash tables. Consequently, we can conclude that Pr[EvS_3]≤$1/2p \times q_h \times Succ_{P,G_1}^{cbdh}(t + 2\tau)$, where τ denotes the computational time for a point multiplication.

Game G_4:In this game, we simulate active attacks via *Send* queries. That is, an adversary A can forward arbitrary messages to the oracle instances simply. Similar to the aforementioned game, for A, $Send(TID_{U_a}$,ID_V,"$start$")-queries can be asked to the visiting network SN_V randomly. If this event happens and the guess for the active session is correct, then we can derive the partial Bilinear Diffie-Hellman information $K' = CBDH_{P,G_1}(Y_a = r_a P, Z_a, r_e{}^* P)$=$r_a r_e{}^* P/CBDH_{P,G_1}(\hat{e}(h(Y_a \| ts)P, Y_a)^{SN_V})$ from the

$Hash$ table. Hence, we can derive that $\Pr[EvS_4] \leq 1/2p \times q_s \times q_h \times Succ^{cbdh}_{P,G_1}(t+2\tau)$.
Game G_5:In this game, the success probability of an adversary who impersonates an entity is concerned. From some transcript $\{TID_{U_a}, Z_a, Y_a, ts\}$, suppose that there exist two $Hash$ queries in $Hash$ tables such that one has $\{TID_{U_a}, Z_a, Y_a, ts\}$, $K_1 = CBDH_{P,G_1}(r_aP, Z_a, r_vP)$ and $\{TID_{U_a}, {Z_a}^*, Y_a, ts\}$ $K_2 = CBDH_{P,G_1}(r_aP, {Z_a}^*, r_eP)$. Let this event denote $CollH$. Assume that the event $CollH$ occurs; if the guess for the $Send(TID_{U_a}, ID_{SN_V},$ "$start$") query was correct, then we can derive the value $CBDH_{P,G_1}(r_aP, {Z_a}^*, r_eP)$ as K_2/K_1. It follows that $\Pr[CollH] \leq 2(q_s+q_e) \times {q_h}^2 \times Succ^{cbdh}_{P,G_1}(t+\tau)$.
textbfGame G_6:Finally, we conclude the probability of event $AskH$, which can be separated into two independent sub-events:
$\cdot AskH$-Server means that an adversary simulates the transcript (Y_a, Z_a) and tries to get the valid response (Y_V, σ).

Since at most one authenticator Z_a can lead to a valid response, as a result, an adversary succeeds in sending a valid transcript is bounded by $(1/p)$. Thus, we can derive that $\Pr[AskH\text{-Server}] \leq (1/p \times q_s)$.
$\cdot AskH$-Passive means that the transcripts between instances of the entities and server have been queried at most $(q_s + q_e)$.

In addition, all possible values in the Hash tables are selected randomly for the answer, which has at most q_h possible answers. Hence, the probability of this sub-event is $\Pr[AskH\text{-Passive}] \leq 2(q_s+q_e) \times q_h Succ^{cbdh}_{P,G_1}(t+\tau)$. Eventually, the probability of the event $AskH$ is bounded by $\Pr[AskH] \leq (1/p \times q_s) + 2(q_s+q_e) \times q_h Succ^{cbdh}_{P,G_1}(t+\tau)$. This concludes the proof of Theorem 1.

5. **Performance Analysis.** The computation overhead and communication overhead for the mobile users, the visited networks, and the home networks are reasonable in the proposed scheme. Due to the limited wireless spectrum supported for communications between mobile users, the limited power constrains, and the limited numbers of visited networks, it is especially important to reduce the computation overhead and communication round. As mentioned earlier, there are only two communication rounds between mobile users and the visited networks rather than communicating with the home network, and this is the minimum number of rounds required to achieve mutual authentication and authenticated key agreement. Table 1 shows the performance comparisons based on the authentication phase, for the proposed scheme and the related schemes. Note that the notations SN_H, SN_V and MS denote home server networks, visited server networks, and mobile users, respectively. In Shrestha et al.s proposed scheme, SN_H pre-generates the number of N pre-share secret keys K_m and K_v that shares with MS and SN_V, respectively. G is the time of session key generation; E/D is the time of encryption / decryption. SN_V pre-generates the number of (N-1) pre-share keys K_r's that share with other SN_V to consist of $Token$. MS executes one encryption operation and two decryption operations. Although pre-generating secret keys provide better efficiency than those asymmetric cryptosystems, it simultaneously causes two problems, maintaining secret key overhead problem and token management problem, respectively. In the proposed scheme, the computation costs for mobile users are quite low. Since, some operations can be precalculated to increase the efficiency, e.g., $r_a \cdot P$. As a result of these improvements, the proposed scheme would not lead a heavy burden for the computation-constrained mobile users.

To estimate the computation efficiency, we summarize the involved operations [11], [16], [17], [32] in Table 2 among the related schemes. We can observe that the total estimated times are 1622.5 ms and 1601.12 ms in Yang et al.s scheme and Shrestha et al.s scheme, respectively. Compared with above researches, the estimated time of the proposed scheme

Table 1. PERFORMANCE COMPARISONS

Metrics	Our Method	Yang et al.	Shrestha et al.
SN_H	-	$2(preG * N)$	$2(preG * N)$+G+2E
SN_V	$4TG_{mul}$+$3TG_{\hat{e}}$	$(preG * N)$+$2TG_{mul}$	$(preG * (N-1))$+$2E + 2D$
MS	$3TG_{mul} + TG_{add}$++$2TG$	$2TG_{mul}$+$2TG_{\hat{e}}$	$E + 2D$

TG_{mul}:The time of executing a scalar multiplication operation of point
TG_{add}:The time of excuting an addition operation of point
$TG_{\hat{e}}$:The time of executing a bilinear map operation

only takes 57.3 ms. Hence, the proposed scheme is more efficient and more suitable for the computation-constrained mobile users than other mechanisms.

Table 2. TIMIES NEEDED BY PRIMITIVE OPERATIONS

Primitive	Time (ms)
Key generation	526.5
Encryption / Verification	0.26
Decryption / Singing	5.08
A scalar multiplication	1.72
An addition operation	0.11
A bilinear map	9.03

Table 3. COMPARISON AMONG RELATED SCHEMES

	Jiang et al.	Yang et al.	Shrestha et al.	Our method
Types	Asymmetric	Asymmetric	Symmetric	Asymmetric
Involved parties	3	2	3	2
Mutual authentication	Yes	Yes	Yes	Yes
User anonymity	Yes	Yes	Yes	Yes
User untraceability	Yes	No	No	Yes
Store preshare key	Partially	Yes	Yes	No
SN_H knows session key	Yes	No	Yes	No
Transmission round	5	3	7	2

In Table 3, we compare the security requirements of our proposed scheme and some related schemes. As Table 3 shows, on key establishment, only the scheme developed by Yang et al. and ours provide session key establishment without acquiring the session key from the home server. This is an important feature for mobile authentication applications with the specific visited networks. Concerning pre-shared secrets, the scheme developed by Jiang et al. does not have to store any pre-shared secret; the home server still must compute the warrants and maintain them for all mobile users. Also, their scheme requires mobile users to publish their public-key to a trusted third party which is more complicated and less efficient than the proposed scheme. Finally, concerning renewal session keys, in Shretha et al.s scheme, the session key which can only be used within the valid time, is generated by the home network or the previous involved visited networks. If the session key has not expired, it is still used for the next session through the re-authentication phase. However, once the valid time has expired, a foreign server must authenticate mobile users by resorting to the home network or the previously involved visited networks once again. Compared with the other schemes, Shrestha et al.s scheme does not fully support renewal session keys.

6. **Conclusions.** In this paper, we propose an ID-based authentication scheme to enhance the communication efficiency in heterogeneous network. The BLS signature is the eventful technique used in our scheme. We analyze the security properties and compare the calculation overhead with Shrestha et al.s scheme. Overall, the proposed scheme is superior to other related schemes concerning security. Moreover, it is suitable for lightweight devices used with wireless heterogeneous network.

REFERENCES

[1] D. Boneh, B. Lynn and H. Shacham, Short Signatures from the Weil Pairing, *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[2] M. Bellare and P. Rogaway, Random Oracles are Practical: a Paradigm for Designing Efficient Protocols, *Proc. of the First ACM Conference on Computer and Communication Security*, NY, USA, pp. 62–73, 1993.

[3] C. C. Chang, C. Y. Lee and Y. C. Chiu, Enhanced Authentication Scheme with Anonymity for Roaming Service in Global Mobility Networks, *Computer Communications*, vol. 32, no. 4, pp. 611–618, 2009.

[4] X. F. Cao, X. W. Zeng, W. D. Kou and L. B. Hu, Identity-based Anonymous Remote Authentication for Value-added Services in Mobile Networks, *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3508–3517, 2009.

[5] T. Elgamal, A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms, *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[6] C. I. Fan, P. H. Ho and R. H. Hsu, Provably Secure Nested One-time Secret Mechanisms for Fast Mutual Authentication and Key Exchange in Mobile Communications, *IEEE/ACM Transactions on Networking*, vol. 18, no. 3, pp. 996–1009, 2010.

[7] K. F. Hwang and C. C. Chang, A Self-encryption Mechanism for Authentication of Roaming and Teleconference Services, *IEEE Transactions on Wireless Communications*, vol. 2, no. 2, pp. 400–407, 2003.

[8] K. Han, T. Shon and K. Kim, Efficient Mobile Sensor Authentication in Smart Home and WPAN, *IEEE Transactions on Consumer Electronics*, vol. 56, no. 2, pp. 591–596, 2010.

[9] Y. Jiang, C. Lin, X. Shen, and M. Shi, Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks, *IEEE Transactions on Wireless Communications*, vol. 5, no. 9, pp. 2569–2576, 2006.

[10] N. Koblitz, Elliptic Curve Cryptosystems, *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[11] N. Koblitz, A. J. Menezes and S. A. Vanstone, The State of Elliptic Curve Cryptography, *Design, Codes, and Cryptography*, vol. 19, no. 2-3, pp. 173–193, 2000.

[12] J. Kohl and C. Neuman, *The Kerberos Network Authentication Service (V5)*, RFC 1510, IETF, 1993. http://www.ietf.org/rfc/rfc1510.txt

[13] M. Komarova, M. Riguidel, A. Hecker, Fast Re-authentication Protocol for Inter-domain Roaming, *Proc. of IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2007. PIMRC 2007, Athens, pp. 1–5, 2007.

[14] Y. B. Lin and Y. K. Chen, Reducing Authentication Signaling Traffic in Third-generation Mobile Network, *IEEE Transactions on Wireless Communications*, vol. 2, no. 3, pp. 493–501, 2003.

[15] W. B. Lee and 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, 2005.

[16] A. Menezes, P. V. Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[17] S. Moon, Elliptic Curve Scalar Point Multiplication using Radix-4 Booth's Algorithm, *Proc. of IEEE International Symposium on Communications and Information Technology ISCIT*, South Korea, vol. 1, pp. 80–83, 2004.

[18] A. J. Nicholson, M. D. Corner and B. D. Noble, Mobile Device Security using Transient Authentication, *IEEE Transactions on Mobile Computing*, vol. 5, no. 11, pp. 1489–1502, 2006.

[19] R. L. Rivest, A. Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM*, vol. 21, no. 2, 1987.

[20] A. Shamir, Identity-Based Cryptosystems and Signature Scheme, *Lecture Notes in Computer Science*, vol.196, pp. 47–53, 1985.

[21] D. Simon, B. Aboba and R. Hurst, *The EAP-TLS Authentication Protocol*, RFC 5216, IETF, 2008. http://tools.ietf.org/html/rfc5216

[22] A. P. Shrestha, D. Y. Choi, G. R. Kwon, and S. J. Han, Kerberos based Authentication for Inter-domain Roaming in Wireless Heterogeneous Network, *Computers & and Mathematics with Applications*, vol. 60, no. 2, pp. 245–255, 2010.

[23] S. R. Tuladhar, C. E. Caicedo and J. B. D. Joshi, Inter-domain Authentication for Seamless Roaming in Heterogeneous Wireless Networks, *Proc. of IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC '08*, Taichung, pp. 249–255, 2008.

[24] T. Taleb and K. Letaief, A Cooperative Diversity based Handoff Management Scheme, *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1462–1471, 2010.

[25] C. Tang and D. O. Wu, An Efficient Mobile Authentication Scheme for Wireless Networks, *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1408–1416, 2008.

[26] C. Tang and D. O. Wu, Mobile Privacy in Wireless Networks-revisited, *IEEE Transactions on Wireless Communications*, vol. 7, no. 3, pp. 1035–1042, 2008.

[27] S. J. Wang, Anonymous Wireless Authentication on a Portable Cellular Mobile System, *IEEE Transactions on Computers*, vol. 53, no. 10, pp. 1317–1329, 2004.

[28] J. H. Yang and C. C. Chang, An Id-based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on Elliptic Curve Cryptosystem, *Computers & Security*, vol. 28, no. 3–4, pp. 138–143, 2009.

[29] G. Yang, Q. Huang, D. S. Wong, and X. Deng, Universal Authentication Protocols for Anonymous Wireless Communications, *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 168–174, 2010.

[30] G. Yang, D.S. Wong, and X. Deng, Anonymous and Authenticated Key Exchange for Roaming Networks, *IEEE Transactions on Wireless Communications*, vol. 6, no. 9, pp. 3461–3472, 2007.

[31] M. Zhang and Y. Fang, Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol, *IEEE Transactions on Wireless Communications*, vol. 4, no. 2, pp. 734–742, 2005.

[32] Y. C. Zhang, W. Liu, W. J. Lou and Y. G. Fang, Securing Mobile Ad hoc Networks with Certificateless Public Key, *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 386–399, 2006.

[33] J. M. Zhu and J. F. Ma, A New Authentication Scheme with Anonymity for Wireless Environments, *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 231–235, 2004.

[34] Hong-Feng Zhu, Hui-Yan Liu, Yi-Feng Zhang, and Yan Zhang, Three-party Authentication Key Agreement Protocol Based on Chaotic Maps in the Standard Model with Privacy Preserving, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, no. 6, pp. 1077–1087, November 2015.

[35] Hongfeng Zhu and Yan Zhang, Enhanced Graphical Captcha Framework and Applications to Strong Security Authenticated Scheme without Password Table, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, no. 6, pp. 1295–1309, November 2015.