Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **1**, January **2014**

Design and Analysis of Chameleon Hashing Based Handover Authentication Scheme for Wireless Networks

Chin-Chen Chang[1,2,3], Ya-Chieh Huang[1], and Hao-Chuan Tsai[3]

[1]Department of Information Engineering and Computer Science
Feng Chia University
Taichung, Taiwan, 40724, R.O.C.

[2]Department of Computer Science and Information Engineering
Asia University
Taichung, Taiwan, 413, R.O.C.

[3]Department of Computer Science and Information Engineering
National Chung Cheng University
Chiayi, Taiwan, 621, R.O.C.

e-mail: ccc@cs.ccu.edu.tw; M9705952@fcu.edu.tw; tsaihc@cs.ccu.edu.tw

Received December, 2012; revised October, 2013

Abstract. *An increasing number of mobile users are allowed and promoted universal access over the wireless networks. Roughly speaking, an authentication mechanism is needed between mobile users and access points, also, an authenticated key is highly desirable to support secure communications in wireless networks. In addition, the anonymous property is an important security requirement, such as the information of customer behavior, which is needed to achieve. Recent researches have focused on these issues and have provided definitions and some constructions. Especially, Choi and Jung proposed an efficient handover authentication scheme which enjoys both computation efficiency and communication efficiency as compared well-known handover authentication schemes recently. Unfortunately, we still find out that Choi and Jung's scheme is vulnerable to a man-in-the-middle attack. To make handover authentication scheme more impeccable, therefore, we propose an enhanced version to provide the better security and the computation efficiency.*
Keywords: handover, mobile authentication, key agreement, scalable, wireless networks

1. **Introduction.** Message authentication is highly considered in network environments. It provides the receiver that the message was sent by a specified sender and the message was not altered en route. To provide this property, a session key should be established among entities to encrypt and be used to authenticate messages. In the same vein, it is very important to provide a secure and efficient authentication strategy in the wireless networks, such as WLAN, WiMAX, and 3GPP [1, 2], since they are prone to suffer attacks. In addition, user mobility is highly desirable to the development of computer networks and the telecommunication systems, especially in wireless networks. In one scenario, a mobile node (MN) initially subscribed to the current attachment point (AP) can travel to

other AP with different operations and access services. In general, compared with wired nodes AP, the MN is powerless to execute a lot of complicated operations. Therefore, reducing energy consumption and authentication delay for the persistent connectivity of mobility is essential.

For all these purposes, many researches [5, 6, 9, 13, 14, 15, 16] have been proposed to solve the problems of handover authentication. Roughly, two types of handover authentication schemes can be categorized. The first type is AAA-based schemes [13, 14]. The AAA-based schemes have the better security strength and good latency performance owing to pre-authentication. This is because these schemes have assumed that an AAA server has robust security features. However, the cost complexity of the overall system is increased sharply due to the fact that establishment of trust relationship and authentication traffic among infrastructure nodes. Also, the problems, such as connection loss and the single point failure of the AAA server, are raised. The second one is called the security-context-transfer (SCT) schemes [5, 15, 16]. Different from the AAA-based schemes, SCT-based schemes do not need to authenticate between an AAA server and an AP. The SCT-based schemes, nevertheless, still assumes to establish the high cost trusted relationship among APs.

In spite of the above categories, a related research adopting the ID-based cryptosystem has been proposed [4, 7, 10]. Similar to the traditional MAC address mechanism, the proposed scheme only uses the identities of the involved entities to perform the handover authentication between an MN and an AP. The ID-based handover authentication scheme has the advantages in terms of fast authentication process. Without communicating to the AAA server, the ID-based handover authentication scheme also has the simple architecture, i.e., it does not need to establish any trust relationship among infrastructure nodes. Unfortunately, the ID-based handover authentication scheme suffers from the key escrow problem [6]. Compared to the AAA-based and SCT-based schemes, the complexity of the overall system can lead the heavy burden to the involved entities. This is mainly due to the fact that the high complexity operations, such as the pairing operations, are required. In addition, the ID-based handover authentication scheme does not provide a robust key exchange; hence, it is unsuitable for the wireless network environments, especially for those MNs who are resource-constrained.

Recently, Choi and Jung proposed an efficient handover authentication scheme. They adopted the credential mechanism based on Chameleon Hashing [12], which is a variant of the blind signature. A credential value will be signed by the AAA server with a chameleon hash value to be used to future mutual authentication. Also, it provides an ephemeral authenticated Diffie-Hellman key exchange [8] to protect the later communications. The authors claimed that their scheme has the advantage in terms of delay time and energy consumption. Unfortunately, according to our investigation, a weakness, a man-in-the-middle attack, is still found in Choi and Jung's scheme. To eliminate the weakness, we therefore propose a new version.

The rest of this paper is organized as follows. Section 2 demonstrates the weakness of Choi and Jung's scheme. And in Section 3, we propose the enhanced scheme with a novel architecture. Next, the security properties are given in Section 4 Finally, we make some conclusions in Section 5

2. **Overview of Chameleon Hashing Based Handover Authentication Scheme.**

More recently, Choi and Jung [6] proposed the first efficient handover authentication using credentials based on chameleon hashing. The main idea of their proposed scheme is that, between the visited access point (AP) and the mobile user (MN), the credential generated by using the collision resistant hash function is used to generate an authenticated

ephemeral Diffie-Hellman key exchange [8] for both involved entities. Compared to the traditional AAA-based schemes, Choi and Jung's scheme achieves the simple authentication architecture and also provides the robust key exchange. Unfortunately, we found out that Choi and Jung's scheme suffers from a simple attack, a man-in-the-middle attack. Under such an attack scenario, a malicious mobile user can fool both the legitimate mobile user and the visited access point into establishing two different individual session keys with her without being detected. In addition, the privacy of mobile users is not well-protected. For saving the capacity of the paper, in this section, we only demonstrate the weakness that is found in Choi and Jung's scheme rather than describe the full steps in Choi and Jung's scheme The following notations are used throughout this section

PK_{AAA}/SK_{AAA} :public/private key pair of the traditional RSA of the AAA server

$T_{Exp,}T_{Curr}$:expiration and current time

$\alpha(i)_x$:a random element of a mobile node x, $\alpha(i)_x$ is also a secret key for finding collision and Diffie-Hellman secret key

$r(i)_x$:a hash value in the form of $h(g^{\alpha(i)_x}(\mathrm{mod}p)||T_{Curr})$ for a mobile node x

$m(i)_x$:a random element which satisfies the equation

$m(0)_x + \alpha(0)_x r(0)_x = m(i)_x + \alpha(i)_x r(i)_x$, where $m(0)_x$ is a random element

$m(0)_x \in Z_q^*$ for the prime order q

$y(i)_x$:public key $y(i)_x = g^{\alpha(i)_x}(\mathrm{mod}p)$ of a mobile node x

$CH_y(m,r)$:the chameleon hash function $CH_y(m,r) = g^m y^r(\mathrm{mod}p)$

Choi and Jung's scheme consists of two phases, the initialization phase and the handover authentication phase. In the initialization phase, the *MN* performs an initial full authentication with an AAA server during a bootstrapping procedure and receives a credential C from the AAA server. Also, the AAA server provides the credential C to *AP*s after every expiration time of the credential. After completing the initialization phase, once the *MN* moves into the service range of a new *AP*, the *MN* needs to perform a handover authentication phase with a new *AP*. We assume that the *MN* has completed the initial full authentication phase with the AAA server and then obtains the credential.

$$\begin{aligned} C(0)_{MN} &= Sign_{SK_{AAA}}(CH_{y(0)_{MN}}(m(0)_{MN}, r(0)_{MN})||T_{Exp}) \\ &= Sign_{SK_{AAA}}(g^{m(0)_{MN}} g^{\alpha(0)_{MN} r(0)_{MN}}||T_{Exp}). \end{aligned}$$

Note that the *MN* keeps the parameters $\alpha(0)_{MN}, m(0)_{MN}$ and $r(0)_{MN}$ as his secret keys. Next, the attack scenario on the handover authentication phase is described as follows.

When the *MN* moves into the new *AP* (AP_n), he first chooses a random element $\alpha(1)_{MN}$ as his Diffie-Hellman secret key and then computes $r(1)_{MN}$ and $m(1)_{MN}$, respectively, where $r(1)_{MN} = h(g^{\alpha(1)_{MN}}(\mathrm{mod}p)||T_{Curr})$ and $m(1)_{MN}$ is generated by solving for $m(i)_x$ in the equation $m(0)_x + \alpha(0)_x r(0)_x = m(i)_x + \alpha(i)_x r(i)_x$, i.e., $m(1)_{MN} = m(0)_{MN} + \alpha(0)_{MN} r(0)_{MN} - \alpha(1)_{MN} r(1)_{MN}$. Next, the *MN* sends the computed results $g^{\alpha(1)_{MN}}(\mathrm{mod}p)$ and $m(1)_{MN}$ along with his credential $C(0)_{MN}$ and the timestamps T_{Curr}, T_{Exp} to AP_n. Without loss of generality, assume that there exists a malicious mobile user MN_f who is also a legitimate user. She can generate a random element $\alpha(1)_{MN_f}$ and compute the corresponding $r(1)_{MN_f} = h(g^{\alpha(1)_{MN_f}}(\mathrm{mod}p)||T_{Curr})$ and $m(1)_{MN_f} = m(0)_{MN_f} + \alpha(0)_{MN_f} r(0)_{MN_f} - \alpha(1)_{MN_f} r(1)_{MN_f}$. Simultaneously, she replaces the original messages generated by the *MN* with $\{g^{\alpha(1)_{MN_f}}, m(1)_{MN_f}, C(0)_{MN_f}, T_{Curr,}T_{Exp}\}$ and then sends the modified messages to the AP_n. After receiving these messages, AP_n computes $CH_{y(1)_{MN_f}}(m(1)_{MN_f}, r(1)_{MN_f})$ and verifies the credential $C(0)_{MN_f}$ using the public key of the AAA server. It is worth noting that the malicious user can be verified successfully because of the verification.

$$Verify_{PK_{AAA}}(C(0)_{MN_f}) = (CH_{y(1)_{MN_f}}(m(1)_{MN_f}, r(1)_{MN_f})||T_{Exp}) \\ = (g^{\alpha(1)_{MN_f}} g^{m(1)_{MN_f} r(1)_{MNf}}||T_{Exp}).$$

Since it has been fooled into authenticating the MN successfully, the AP_n chooses a random element $\alpha(1)_{AP_n}$ and computes the ephemeral Pairwise Master Key $PMK_{MN_f AP_n} = (g^{\alpha(1)_{MN_f}})^{\alpha(1)_{AP_n}} \bmod p$ that is used to protect user data in the later communications over the insecure networks. Eventually, AP_n generates the corresponding $r(1)_{AP_n}$ and $m(1)_{AP_n}$, and then, sends $\{g^{\alpha(1)_{AP_n}}, m(1)_{AP_n}, C(0)_{AP_n}, T_{Curr}, T_{Exp}, h(PMK, g^{\alpha(1)_{AP_n}})\}$ to the malicious user MN_f. After receiving these messages, the MN_f can compute the $PMK_{MN_f AP_n} = (g^{\alpha(1)_{AP_n}})^{\alpha(1)_{MN_f}} \bmod p$ and response $h(PMK, g^{\alpha(1)_{MN_f}})$ to confirm the PMK agreement with the AP_n. In the same vein, the MN_f sends $\{g^{\alpha(1)_{MN_f}}, m(1)_{MN_f}, C(0)_{MN_f}, T_{Curr,} T_{Exp}\}$ to the victim MN and also computes another $PMK_{MN_f MN} = (g^{\alpha(1)_{MN}})^{\alpha(1)_{MN_f}} \bmod p$. Then, the victim MN will be fooled into authenticating the MN_f successfully because of the verification

$$Verify_{PK_{AAA}}(C(0)_{MN_f}) = (CH_{y(1)_{MN_f}}(m(1)_{MN_f}, r(1)_{MN_f})||T_{Exp}) \\ = (g^{\alpha(1)_{MN_f}} g^{m(1)_{MN_f} r(1)_{MNf}}||T_{Exp}).$$

Simultaneously, the MN will establish another pairwise master key $PMK_{MN_f MN} = (g^{\alpha(1)_{MN_f}})^{\alpha(1)_{MN}} \bmod p$ with the malicious user MN_f. We can observe that the malicious user MN_f can establish two individual keys $PMK_{MN_f MN}$ and $PMK_{MN_f AP_n}$ with the corresponding entities MN and AP_n, respectively. The attack scenario can be summarized in Fig. 1.

In addition, Choi and Jung's scheme does not provide well-protection to the identity of mobile users, i.e., lack of anonymity. Integrating the relevant privacy information about mobile users into wireless networks is a crucial issue. In the past decade, many researchers pointed out that some behaviors, such as the information of the customer behavior and track of the user are the personal privacy. It is desirable to protect the identity of the mobile user from eavesdroppers as well as the uninvolved APs. That is, the identity of the user has either to be encrypted or be replaced by a temporal identity. According to such an observation, we have found that Choi and Jung's scheme has a personal privacy problem which means that the anonymity is not well provided. In Choi and Jung's scheme, the identity is transmitted in the plaintext over the public channel. All instances, including eavesdroppers, can know the real identity of the mobile user who communicates with the specific APs.

3. **The Proposed Handover Authentication Scheme.**

3.1. **Design Goals.**

To enable the efficient handover authentication for both the mobile user and the access point, our scheme design will achieve the following security and performance guarantees: 1) Validity: to allow the involved entities to accept the same session key in the absence of an active adversary; 2) Explicit authentication: as we have discussed, the weakness of Chameleon hashing based scheme is that only the implicit authentication is ensured, and this can lead a malicious mobile user impersonates either the access point or another mobile user to fool into the specific mobile user. Hence, our scheme will provide explicit authentication of all communicating entities; 3) Session key indistinguishability: there exists no probabilistic polynomial-time adversary to distinguish

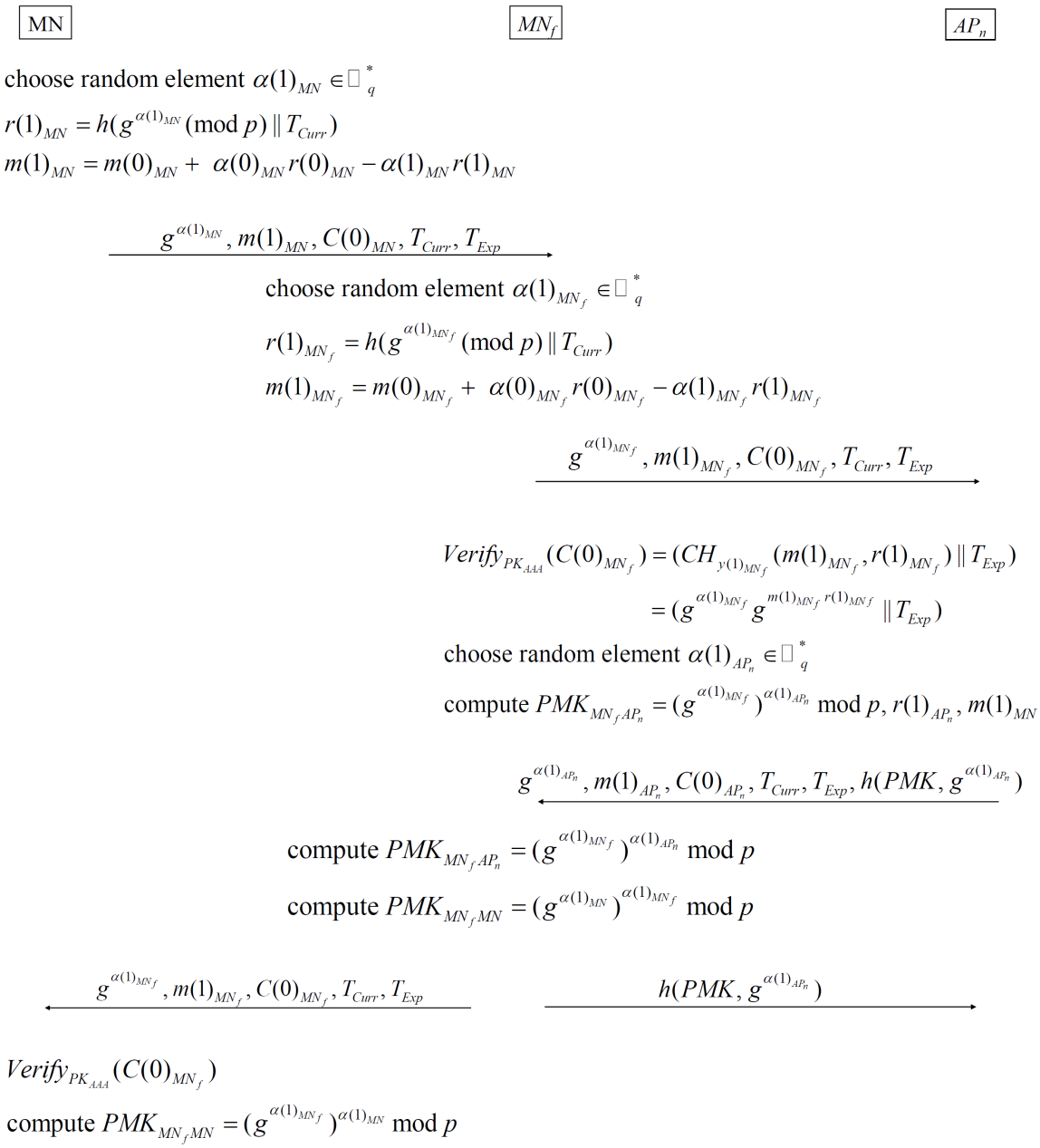

FIGURE 1. A man-in-the-middle attack in the handover authentication phase

keys between the real session key and a random string; 4) Lightweight: to allow communicating entities to perform handover authentication with minimum communication and computation overhead.

3.2. **Notations and Preliminaries.** Before demonstrating the proposed scheme, the system has to initialize the security parameters as follows. Firstly, the system chooses a finite field F_p over a large odd prime number p, and then, defines an elliptic curve equation $E_p(a,b) : y^2 = x^3 + ax + b \ (\mathrm{mod}\, p)$ with the prime order q over F_p, for the chosen $a, b \in F_p$ which satisfy the equation $4a^3 + 27b^2 \neq 0 \ (\mathrm{mod}\, p)$ [11]. Finally, the system chooses a base point P with the prime order q over $E_p(a,b)$ and publishes $E_p(a,b)$ and P. Note that $H(\cdot) : \{0,1\}^* \to \{0,1\}^l$ is a cryptographic one-way hash function

Let κ be a system security parameter. All systems can be categorized into three entities, AAA server is the trusted and the unique entity, mobile user entity is the set $MN(\kappa) = \{MN_1, MN_2, ..., MN_{Q_u(\pi)}\}$, and access point entity is the set $AP(\kappa) = \{AP_1, AP_2, ..., AP_{Q_i(\pi)}\}$, respectively, where Q_u and Q_i are two polynomials and each element in the sets are the corresponding identities. Except for the mobile users, we assume that all entities are associated with the elliptic curve cryptographic public key pairs.

3.3. **The Concrete Scheme.** We now describe the proposed scheme which consists of two phases, the initial authentication phase and the handover authentication phase, respectively, as follows.

A. Initial authentication phase

Initially, the mobile user *MN* chooses two random elements $a(0)_{MN}, x(0)_{MN} \in Z_q^*$, and then computes the corresponding $\alpha(0)_{MN} = H(a(0)_{MN}P||H(ID_{MN})||T_{Curr})$. Next, he computes $\theta = x(0)_{MN}P + \alpha(0)_{MN}a(0)_{MN}P$, i.e., $\theta = CH_{y(0)_{MN}}(x(0)_{MN}, \alpha(0)_{MN})$ and sends the computed result along with $H(ID_{MN})$ to the AAA server securely. Then, the AAA server verifies the transcripts and computes the corresponding credential

$$\begin{aligned} C(0)_{MN} &= Sign_{SK_{AAA}}(CH_{y(0)_{MN}}(x(0)_{MN}, \alpha(0)_{MN})||T_{Exp}||H^2(ID_{MN})) \\ &= Sign_{SK_{AAA}}(x(0)_{MN}P + \alpha(0)_{MN}a(0)_{MN}P||T_{Exp}||H^2(ID_{MN})), \end{aligned}$$

and returns it along with the expiration time T_{Exp} to the *MN* securely. Eventually, the *MN* keeps $\{a(0)_{MN}, x(0)_{MN}\}$ as his master secret keys. It is worth noting that, in this phase, the communication between the *MN* and the AAA server can apply the secure mechanisms, such as EAP-AKA or EAP-TLS, to ensure the confidentiality and the integrity for both involved entities. Although these secure mechanisms may lead the extra overhead of *MN* than the usual communication channel, for overall aspect, it would not burden the *MN* because the *MN* needs to perform this phase only one time.

B. Handover authentication phase

After obtaining the credential from the AAA server, when the *MN* migrates to the new access point (AP_{new}), he has to perform the handover authentication to obtain the service. First, the *MN* chooses a random element $a(1)_{MN} \in Z_q^*$ and computes the corresponding values $\alpha(1)_{MN} = H(a(1)_{MN}P||H(ID_{MN})||T_{Curr})$ and $x(1)_{MN}$, where $x(1)_{MN}$ is computed by solving the Chameleon hashing equation $x(0)_{MN} + a(0)_{MN}\alpha(0)_{MN} = x(1)_{MN} + a(1)_{MN}\alpha(1)_{MN} (\mathrm{mod}\, q)$. Next, he computes $SID = H(ID_{MN}) + a(1)_{MN}\mathrm{A}_{PK_{APnew}}$, where $\mathrm{A}_{PK_{APnew}} = eP$ is the authenticated public key of the AP_{new} and sends the computed results $\{y(1)_{MN} = a(1)_{MN}P, x(1)_{MN} \oplus H(H(ID_{MN})||T_{Curr}), SID, C(0)_{MN}, T_{Curr}, T_{Exp}\}$ to the AP_{new}. After receiving the transcripts, the AP_{new} retrieves the hidden identity of *MN* by using the private key $H(ID_{MN}) = SID - ea(1)_{MN}P$. And then, it computes $H(H(ID_{MN})||T_{Curr})$ to extract $x(1)_{MN}$ from the transcripts. Next, the AP_{new} verifies $Verify_{PK_{AAA}}(C(0)_{MN}) = (CH_{y(1)_{MN}}(x(1)_{MN}, \alpha(1)_{MN})||T_{Exp}||H^2(ID_{MN}))$. If it holds, the AP_{new} authenticates the *MN* successfully. In the same vein, the AP_{new} chooses a random element $b(1)_{AP} \in Z_q^*$ and computes $\beta(1)_{AP} = H(b(1)_{AP}P||H(ID_{MN})||T_{Curr})$, eventually, it sends $\{b(1)_{AP}P, x(1)_{AP} \oplus H(H(ID_{MN})||T_{Curr}), C(0)_{AP}, T_{Curr}, T_{Exp}\}$ to the *MN*. Simultaneously, the AP_{new} can compute the session key $H(a(1)_{MN}b(1)_{AP}P||a(1)_{MN}P||b(1)_{AP}P||H(ID_{MN}))$ to secure the later communications. After receiving the messages from the AP_{new}, the *MN* also applies the same procedure to verify the AP_{new}. If the *MN* authenticates the AP_{new} successfully, he can also compute the same session key.

4. **Security Analysis and Discussions.** Before demonstrating the security, we first depict the security basis on which the proposed scheme relies.

DEFINITION 1. Elliptic Curve Discrete Logarithm Assumption

Let E be an elliptic curve over a finite field F_p with a prime order q, where the operation is denoted multiplicatively. Suppose that G is a base point over $E(F_p)$, a (t,ε)–*ECDL* attacker in $E(F_p)$ is a probabilistic *Turing* machine Δ running in time t such that

$$\mathrm{Succ}_{\mathrm{E}}^{\mathrm{ecdl}}(\Delta) = \Pr_{a,b}[\Delta(aP, bP) = abP] \geq \varepsilon$$

where the probability is taken over the random values a and b. The Elliptic Curve Discrete Logarithm Problem (*ECDLP*) is (t,ε)–intractable if there exists no (t,ε)–attacker in $E(F_p)$. The Elliptic Curve Discrete Logarithm Assumption states that is the case for all polynomial t and any non-negligible ε.

We prove the theorem if no probabilistic polynomial time algorithm solves the elliptic curve discrete logarithm problem with advantage ε, then no polynomial time algorithm wins the chosen ciphertext security game against our proposed scheme with non-negligible advantage

Theorem 1: The proposed scheme is chosen ciphertext secure under the elliptic curve discrete logarithm assumption with the session key indistinguishability property in the random oracle [3]

Proof: We proof by contradiction. Assume that there exists an adversary A who obtains a non-negligible advantage in distinguishing the tested key in the game and constructs an algorithm Λ' solving the elliptic curve discrete logarithm problem. Denote that Λ's advantage in distinguishing the real session key from a random key against the protocol P' is

$$\begin{aligned} Adv_{P'}^{\Lambda'}(\kappa, q_{fake}) = |\Pr[A'(P, aP, bP, Q_b) = b : a, b, r \in_R Z_q; \\ Q_0 = H(abP); Q_1 = H(rP); b \in \{0,1\}] - 1/2|. \end{aligned}$$

And suppose that there exists an instance MN has accepted the session key of the form $sk = H(a(1)_{MN}b(1)_{AP'}P||a(1)_{MN}P||b(1)_{AP}P||H(ID_{MN}))$ and has the partnership with the specific access point AP'. To clarify the following proof, with lose of the correctness of the proof, we simply transfer the session key computation as $sk = H(a(1)_{MN}b(1)_{AP'}P)$. In addition, A succeeds if she can randomly pick the target instance to ask a *Test* query and to output the correct hidden bit guess. Thus,

$$\Pr[A\ succeed] = \frac{q_{fake}}{q} + (\frac{1}{2}) * \frac{q - q_{fake}}{q} + \eta(\kappa),$$

where q_{fake} and $\eta(\kappa)$ denote the number of the adversaries to fake the target instance and non-negligible probability, respectively. Now, let Q_h be the event that the hash query $H(\cdot)$ has been queried on the transcript $H(a(1)_{MN}b(1)_{AP'}P||a(1)_{MN}P||b(1)_{AP}P||H(ID_{MN}))$ by A, and let Q_{ENC} be the event that A can successfully forge a valid encryption for the MN. After q_{fake} times queries, $\Pr[Q_{ENC}] = q_{fake}/q$, and the adversary A can get the session key with non-negligible probability under such conditions Q_{ENC}. Hence, we can also derive

$$\begin{aligned} \Pr[A\ succeed] = \tfrac{q_{fake}}{q} + \Pr[A\ succeed|Q_h \cap \overline{Q}_{ENC}] * \Pr[Q_h \cap \overline{Q}_{ENC}] \\ + \Pr[A\ succeed|\overline{Q}_h \cap \overline{Q}_{ENC}] * \Pr[\overline{Q}_h \cap \overline{Q}_{ENC}]. \end{aligned}$$

It is trivial $\Pr[A\ succeed|\overline{Q}_h \cap \overline{Q}_{ENC}] = 1/2$ since $H(\cdot)$ is the random oracle and the MN and AP' are fresh instances. Thus, we have

$$\begin{aligned} &\tfrac{q_{fake}}{q} + (\tfrac{1}{2}) * \tfrac{q - q_{fake}}{q} + \eta(\kappa) \leq \tfrac{q_{fake}}{q} + \Pr[A\ succeed|Q_h \cap \overline{Q}_{ENC}] * \Pr[Q_h \cap \overline{Q}_{ENC}] \\ &+ (\tfrac{1}{2}) * (1 - \tfrac{q_{fake}}{q}) \leq \tfrac{q_{fake}}{q} + \Pr[Q_h] + (\tfrac{1}{2}) * \tfrac{q - q_{fake}}{q}. \end{aligned}$$

So far, we can obtain

$$\Pr[Q_h] \geq \eta(\kappa) + \varepsilon.$$

Next, the adversary A can construct an algorithm Λ' to solve the *ECDLP* with the non-negligible probability as follows.

Challenge: given $(X* = aP, Y* = bP)$, where a and b are both random elements over Z_q, compute abP

Given the challenge $(X* = aP, Y* = bP)$, Λ' chooses the private key and then sets all the corresponding public parameters. It also maintains the queried lists L_h, L_{send}, and L_{key}, for the random oracle $H(\cdot)$, the communication transcripts, and the corresponding session keys, respectively. During the experiment, Λ' randomly selects the instances $MN \in \{MN_1, MN_2, ..., MN_{Q_u(\pi)}\}$, $AP \in \{AP_1, AP_2, ..., AP_{Q_i(\pi)}\}$ and then asks the *Test* query after MN (or AP) has accepted the session. In addition, Λ' answers the adversary A's queries as follows.

Hash query: Λ' will answer all $H(\cdot)$ queries at random and record all the inputs and the corresponding outputs in L_h

Send (C_x^i, m) *query*:

(1) If $(C_x = MN$ and $(m = initial))$, the Λ' sets $a_xP = X^*$ and responds with $\{a_xP, x_x \oplus H(H(ID_x)||T_{Curr}), SID, C(0)_x, T_{Curr}, T_{Exp}\}$. It finally records the transcripts and the related component $(*, x_x)$ in its L_{send} list. Note that the corresponding exponent of X^* is unknown.

(2) If $(C_x \in \{MN_1, MN_2, ..., MN_{Q_u(\pi)}\}$ and m has the form of $\{a_xP, x_x \oplus H(H(ID_x)||T_{Curr}), SID, C(0)_x, T_{Curr}, T_{Exp}\})$, Λ' sets $b_yP = Y^*$, the corresponding x_y and randomly chooses sk^*, and then lets $sk^* = H(\text{target})$, where target denotes the target session key which is still unknown. It finally records the transcripts and the related component $(*, x_y)$ in its L_{send} list. Note that the corresponding exponent of Y^* is unknown. Also, it records $(*, sk^*||X^*||Y^*||SID)$ in its L_h list.

(3) If $(C_x \in \{MN_1, MN_2, ..., MN_{Q_u(\pi)}\}$ and m has the form of $Initial||C_y$ for $C_y \in \{AP_1, AP_2, ..., AP_{Q_i(\pi)}\}$ and $C_x \neq C_y)$, Λ' randomly selects a_x and computes $X^* = a_xP$. Next, it responds with $\{SID, X^*, x_x \oplus H(H(ID_{C_x})||T_{Curr}), C(0)_x, T_{Curr}, T_{Exp}\}$. It finally records the transcripts and the random component (a_x, x_x) in its L_{send} list.

(4) If $(C_x \in \{MN_1, MN_2, ..., MN_{Q_u(\pi)}\}$ and m has the form of $\{Y^*, x_y \oplus H(H(ID_{C_x})||T_{Exp}||T_{Curr}), C(0)_y, T_{Curr}, T_{Exp}\})$, Λ' randomly chooses a_x and computes $X^* = a_xP$, and $sk = H((Y^*)^{a_x}||X^*||Y^*||H(ID_{C_x}))$. In addition, it responds with $\{X^*, Y^*, x_y \oplus H(H(ID_{C_x})||T_{Exp}||T_{Curr}), C(0)_y, T_{Curr}, T_{Exp}, x_x \oplus H(H(ID_{C_x})||T_{Curr}), C(0)_x\})$ and finally records the transcripts and the random component (a_x, x_x) in its L_{send} list, and records $(SID||C_x||C_y||X^*||Y^*||(Y^*)^{a_x}, sk)$ in its L_{key} list.

(5) If $(C_x \in \{MN_1, MN_2, ..., MN_{Q_u(\pi)}\}$ and $C_y \in \{AP_1, AP_2, ..., AP_{Q_i(\pi)}\}$ and m has the form of $\{Y^*, x_y \oplus H(H(ID_{C_x})||T_{Exp}||T_{Curr}), C(0)_y, T_{Curr}, T_{Exp}\})$, Λ' will consult its L_{send} list to find a matched query. If it holds, Λ' will use the value (a_x, x_x) in the matched entry to compute sk; otherwise, it responds with errors.

After receiving the adversary A's guess, Λ' will answer A for searching its L_h list which the entry has the input of the form $(SID||C_x||C_y||X^*||Y^*||(Y^*)^{a_x}, sk^*)$ for some sk^*, outputs sk^* as the elliptic curve Diffie-Hellman key. Two cases can be resulted for the above experiment:

Case 1: the adversary A does not query the result that MN (or AP) has accepted the session, then Λ' aborts.

Case 2: A does make her queries in this way, then MN will accept the session and hold the key formed $H((Y^*)^{a_x} = a_xb_yP||X^*||Y^*||H(ID_{MN}))$, although Λ' knows

nothing about $a_x b_y P$, so it cannot compute this key.

If Case 2 really happens, then Λ' searches for its L_h list for the entry that has the input of the form $(SID||C_x||C_y||X^*||Y^*||(Y^*)^{a_x}, sk^*)$, outputs sk^* as the elliptic curve Diffie-Hellman key and certainly wins its experiment. Hence, the probability that Λ' outputs the correct value $a_x b_y P$ is

$$\Pr[Q_h]/Q_u^2(\pi) \cdot Q_i^2(\pi) \geq \eta(\kappa)/Q_u^2(\pi) \cdot Q_i^2(\pi) > \varepsilon$$

which is still non-negligible. This contradicts the *ECDLP* assumption, and therefore, we can derive that $Adv_{P'}^{\Lambda'}(\kappa, q_{fake})$ must be negligible. This concludes the theorem.

5. **Conclusions.** In this paper, we have demonstrated that Choi and Jung's scheme is still vulnerable to a man-in-the-middle attack. To remedy the weakness, we propose an improved version with the novel and efficient architecture. We focus on preserving the efficient handover authentication with robust security. The proposed scheme has several attractive characteristics as follows: the mutual authentication can be achieved between a mobile user and a visited access point; the access point does not need to store the long term keys shared with mobile users which is scalable in wireless networks; and the established session key would only be shared with the communication parties rather than others. Eventually, we analyze the security property of the proposed scheme and it is well-suited for the low power devices in wireless networks.

REFERENCES

[1] 3GPP, Wireless local area network (WLAN) interworking security, *3GPP TS 33.234*, 2007.

[2] 3GPP, Formal analysis of the 3g authentication protocol, *3GPP TR 33.902*, 2000.

[3] M. Bellare, and P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, *Proc. of The 1st ACM Conference on Computer and Communications Security*, pp. 62-73, 1993.

[4] D. Boneh, and M. Franklin, Identity-based encryption from the weil pairing, *Proc. The 21st Annual International Cryptology Conference on Advances in Cryptology*, pp. 213-229, 2001.

[5] J. Choi, and S. Jung, A secure and efficient handover authentication based on light-weight Diffie-Hellman on mobile node in FMIPv6, *IEICE trans. communications*, vol. 91, no. 2, pp. 605-608, 2008.

[6] J. Choi, and S. Jung, A handover authentication using credentials based on chameleon hashing, *Journal of IEEE Communications Letters*, vol. 14, no. 1, pp. 54-56, 2010.

[7] Y. J. Choie, E. Jeong, and E. Lee, Efficient identity-based authenticated key agreement protocol from pairings, *Journal of Applied mathematics and computation*, vol. 162, no. 1, pp. 179-188, 2005.

[8] W. Diffie, and M. Hellman, New directions in cryptography, *IEEE Trans. Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[9] A. M. Johnston, and P. S. Gemmell, Authenticated key exchange provably secure against the man-in-the-middle attack, *Journal of cryptology*, vol. 15, no. 2, pp. 139-148, 2002.

[10] Y. Kim, W. Ren, J. Y. Jo, Y. T. Jiang, and J. Zheng, SFRIC: a secure fast roaming scheme in wireless LAN using ID-based cryptography, *Proc. of IEEE International Conference on Communications*, pp. 1570-1575, 2007.

[11] N. Koblitz, Elliptic curve cryptosystem, *Journal of MATHEMATICS of COMPUTATION*, vol. 48, pp. 203-209, 1987.

[12] H. Krawczyk, and T. Rabin, Chameleon signatures, *Proceedings of NDSS*, pp. 143-154, 2000.

[13] A. Mishra, M. H. Shin, N. L. Petroni, Jr, T. C. Clancy, and W. A. Arbaugh, Proactive key distribution using neighbor graphs, *Journal of IEEE Wireless Communications*, vol. 11, no. 1, pp. 26-36, 2004.

[14] S. Pack, and Y. Choi, Fast handoff scheme based on mobility prediction in public wireless LAN systems, *Journal of IEE Proceedings - Communications*, vol. 151, no. 5, pp. 489-495, 2004.

[15] H. Wang, and A. R. Prasad, *Fast authentication for inter-domain handover*, LNCS 3124, Springer, pp. 973-982, 2004.

[16] C. Zhang, R. Lu, P. H. Ho, and A. Chen, A location privacy preserving authentication scheme in vehicular networks, *Proc. of Wireless Communications and Networking Conference*, pp. 2543-2548, 2008.