JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 34, 155-170 (2018)
DOI: 10.6688/JISE.2018.34.1.10

Security and Efficiency Enhancement of Robust ID Based Mutual Authentication and Key Agreement Scheme Preserving User Anonymity in Mobile Networks*

CHUN-TA LI[1], CHENG-CHI LEE[2,3,+] AND CHI-YAO WENG[4]
[1]*Department of Information Management*
Tainan University of Technology
Tainan City, 71002 Taiwan
E-mail: th0040@mail.tut.edu.tw
[2]*Department of Library and Information Science*
Fu Jen Catholic University
New Taipei City, 24205 Taiwan
[+]*E-mail: cclee@mail.fju.edu.tw*
[3]*Department of Photonics and Communication Engineering*
Asia University
Taichung City, 41354 Taiwan
[4]*Department of Computer Science*
National Pingtung University
Pingtung City, 90003 Taiwan
E-mail: cyweng@mail.nptu.edu.tw

With the rapid development of wireless communication technologies, mobile networks will enable users to use personal mobile devices to access various network information services at anytime and anyplace. Recently, Lu *et al.* proposed a dynamic ID based mutual authentication and key agreement scheme using elliptic curve cryptography (ECC) which attempts to support better security properties and resists various well-known security attacks. However, we introduce some design flaws in Lu *et al.*'s scheme, such as server impersonation attacks by launching stolen-verifier attacks. Besides, their authentication scheme is unable to preserver user anonymity and the performance of authentication and key agreement phase is inefficiency. As a remedy, the main contribution of this study is to design an improved and efficient ECC-based authentication scheme with privacy protection. We analyze its security and performance, proving that our improved scheme not only prevents security weaknesses on Lu *et al.*'s scheme, but also enhances system efficiency such that it can be implemented to more electronic applications in mobile communication networks.

Keywords: elliptic curve cryptography, key agreement, mobile networks, mutual authentication, user anonymity

1. INTRODUCTION

Mobile communication means a mobile user can roam on Internet or wireless networks and perform online electroni transactions by using his/her personal mobile devices (*e.g.*, smart phones, notebooks tablet computers *etc.*). More and more mobil

Received April 24, 2016; revised May 18, 2016; accepted May 30, 2016.
Communicated by Hung-Min Sun.
[+] Corresponding author.
[*] This work was partially supported by the Ministry of Science and Technology, Taiwan, under Contract No. MOST 106-3114-E-030-001 and MOST 106-3114-C-165-001-ES

services (*e.g.*, online banking, online pay TV, online shopping, online instant messenger *etc.*) are implemented for a mobile user to access services and resources from a remote server. To gai popularity of mobile services, ensuring user privacy and system security are paramount [12-19]. User privacy assures that a legitimate user involved in various mobile services is not spied by any adversary [21, 23-25, 27, 28]. Furthermore, system security assures that unregistered users cannot fraudulently access mobile services and resources from remote servers [5-9]. As the mobile communication networks are public and insecure by nature, the mobile use and remote server have to verify the authenticity of each other and share a session key to protect the integrity of transmitted messages. Besides, it could damage user privacy when user's real identity is transmitted as a plaintext without any protection in mobile networks. By tracking the user's static identity, an adversary may successfully track his/her current location and recognize what kinds of mobile services the user accesses. To preserve user anonymity in mobile networks, a mobile user cannot be linked or traced by any adversaries and his/her real identity must be masked during the authentication session.

In recent years, in order to safeguard the security from network intrusions, many ID based user authentication and key agreement schemes using elliptic curve cryptography [11, 22] have been proposed. In the year of 2009, Yang and Chang [26] proposed an ECC-based solution to build a mutual authentication with key agreement scheme for mobile devices. However, in the year of 2011, Islam and Biswas [10] pointed out that Yang-Chang's solution is still susceptible to replay attacks, many logged-in users' and clock synchronization problems. Moreover, Yang-Chang's solution did not preserve user anonymity and session key forward secrecy. Islam and Biswas further proposed an improved version of Yang-Chang's scheme and their improved scheme can provide remote server and mobile users with a more secure and efficient Internet applications. Additionally, in the year of 2012, He *et al.* [4] proposed a new ID-based authentication scheme for mobile client-server environments and their authentication scheme uses general cryptographic hashing functions instead of MapToPoint functions. In the year of 2013, Chou *et al.* [2] pointed out that He *et al.*'s solution did not provide explicit key confirmation and the construction of a user's private key is time-consuming because the server needs to perform modular inversion operations. Therefore, Chou *et al.* further proposed an improved ID-based authenticated scheme with key agreement for mobile environments. However, in the year of 2014, Farash and Attari [3] showed that Chou *et al.*'s scheme is still vulnerable to two kinds of impersonation attacks. In order to remedy these design flaws in Chou *et al.*'s scheme, Farash and Attari propose a more secure and efficient ID based authenticated key exchange scheme using ECC for mobile client-server environments. Recently, in the year of 2016, Lu *et al.* [20] present a cryptanalysis on both Chou *et al.*'s and Farash-Attari's authentication schemes and they found that Farash-Attari's scheme is still susceptible to track and key-compromise impersonation attacks. To achieve security robustness in designing two-party authenticated key exchange scheme, Lu *et al.* present a simple enhancement on Farash-Attari's scheme, which not only retains the original merits of Farash-Attari's scheme but also resists security flaws for mobile networks.

Although Lu *et al.*'s ID-based mutual authentication and user anonymity scheme enhanced the security and efficiency of Chou *et al.*'s and Farash-Attari's schemes. Unfortunately, this study demonstrated that Lu *et al.*'s scheme has three design weaknesses:

1) the scheme fails to preserve user anonymity by launching eavesdrop attacks, 2) the scheme has stolen-verifier attacks in server side, 3) the scheme has server impersonation attacks when the verifier table of server is compromised by an adversary. Moreover, the performance of Lu *et al.*'s scheme is inefficiency during authentication and key agreement phase. In order to tackle above-mentioned weaknesses, we suggest a more reliable and efficient two-party authenticated key agreement scheme for protecting user privacy in mobile communication environments. From the experiment result shows, we demonstrate the efficiency of our improved scheme. Furthermore, we prove the robustness of our improved scheme through the Burrows-Abadi-Needham (BAN) logic analysis [1]. Formal security proof shows that our enhanced scheme seems to be more practical for implementation in various mobile services to ensure message confidentiality and user privacy.

The remainder of this study is organized as follows. Section 2 provides briefly overview of Lu *et al.*'s and demonstrates its design weaknesses in Section 3. Section 4 presents our improved scheme and proves the security of our scheme by using widely-accepted BAN logic in Sections 5 and 6. Section 7 gives a detailed experimental comparison between our improved scheme and Lu *et al.*'s scheme. Finally, the conclusions are provided in Section 8.

2. REVIEW OF LU *ET AL.*'S SCHEME

Lu *et al.*'s mutual authentication scheme [20] will be briefly reviewed in this section. Lu *et al.*'s scheme comprises two phases like registration and authentication and key agreement. Some terminologies and notations used throughout this study are listed below:

–U: The user.
–S: The server.
–ID_A: The identity of entity A.
–$h_1(\cdot)$: The one-way hash function $h_1(\cdot)$: $\{0,1\}^* \rightarrow Z_n^*$.
–$h_2(\cdot)$: The one-way hash function $h_2(\cdot)$: $\{0,1\}^* \rightarrow Z_p^*$, where p is a large prime.
–k_s, K_S: The private key and public key of S.
–k_U, Q_{ID_U}: The private key and public key of U.
–P: The point value on the elliptic curve.
–||: The concatenation operation.
–⊕: The XOR operation.

2.1 Registration Phase

Before registration, the server S publishes $\{E(a, b), K_S, h_1(\cdot), h_2(\cdot)\}$, where $K_S=k_sP$. The details of registration phase are described below:

Step 1: U chooses his/her identity ID_U and transmits it to S through a secure channel.
Step 2: S generates a random number r_{s1} and calculates $k_U=r_{s1}h_1(ID_U \oplus k_s)$ and $Q_{ID_U}=h_1(ID_U \oplus k_s)P$. Then S stores r_{s1} into its secret DB and returns $\{r_{s1}, k_U, Q_{ID_U}\}$ to U

through a secure channel.

Step 3: After receiving $\{r_{s_1}, k_U, Q_{ID_U}\}$ from S, U checks if $k_UP=r_{s_1}Q_{ID_U}$. If it holds, U keeps k_U secretly and releases Q_{ID_U}.

2.2 Authentication and Key Agreement Phase

Step 1: U chooses a random number r_u and calculates $P_1=r_{s_1}P\oplus ID_U$, $K=h_2(ID_U||r_{s_1})$, $P_2=K\oplus r_uP$, $P_3=h_2(K||r_uP||k_UP)$. Then U transmits the login request $\{P_1, P_2, P_3\}$ to S.

Step 2: After receiving $\{P_1, P_2, P_3\}$ from U, S reveals ID_U by computing $P_1\oplus r_{s_1}P$ and makes use of (ID_U, r_{s_1}) to compute $K'=h_2(ID_U||r_{s_1})$ and $r_uP=P_2\oplus K'$. Then S checks if $h_2(K'||r_uP||r_{s_1}Q_{ID_U})=P_3$. If it holds, S calculates the session key $SK=r_{s_2}r_uP$, $Q_1=K'\oplus r_{s_2}P$, $Q_2=h_2(K'||r_uP||SK)$ and transmits the response message $\{Q_1, Q_2\}$ to U through a public channel, where r_{s_2} is a random number chosen by S.

Step 3: After receiving $\{Q_1, Q_2\}$ from S, U reveals $r_{s_2}P$ by computing $Q_1\oplus K$ and calculates the session key $SK'=r_ur_{s_2}P$. Then U checks if $h_2(K||r_uP||SK')=Q_2$. If it holds, U calculates the acknowledgement message $P_4=h_2(K||r_{s_2}P||SK')$ and transmits it to S through a public channel.

Step 4: After receiving P_4 from U, S checks if $h_2(K'||r_{s_2}P||SK)=P_4$. If it holds, S and U successfully achieve mutual authentication and negotiate a common and secure session key $SK=SK'$ between them.

3. DESIGN WEAKNESSES ON LU *ET AL.*'S SCHEME

In this section, we show that Lu *et al.*'s scheme has some design weaknesses, which are described below:

3.1 Fail to Ensure User Anonymity

In authentication and key agreement phase of Lu *et al.*'s scheme, they claimed that the anonymity of every login session from U to S is guaranteed by keeping the secret random number r_{s_1}. However, in this study, we found that the anonymity property of Lu *et al.*'s scheme cannot be protected from message eavesdropping attacks during the authentication and key agreement phase. Using such an eavesdropping attack, an adversary U_A can un-intrusively monitor on the open communication channels between login users and the server and can discover some valuable information about the messages being transmitted over the public channels. Assume that U_A eavesdrops all the communication messages transmitted between U and S in mobile networks.

Consider that a user U would like to log into S and transmits the login request $\{P_1, P_2, P_3\}$ to S to access network services. However, in Step 1 of the authentication and key agreement phase, the login parameter P_1 transmitted from U to S is unchanging in every login session. Thus, the user anonymity will not be ensured even U's real identity ID_U is protected by an alias $P_1= r_{s_1}P\oplus ID_U$. In this way, U_A can easily trace down the login session from U to S by comparing P_1 with all of the collected messages. For example, if there is a login parameter transmitted between U and S containing P_1. This means that

specific user is involved in a login session. As a result, U_A can discover the relation of a connection between U to S as long as the login requests transmitted over the public channels contains P_1. To prevent this kind of attack, we suggest all the login parameters involved in U's login request $\{P_1, P_2, P_3\}$ should be different for each login session.

3.2 Suffer from Stolen-Verifier Attacks

In Lu *et al.*'s scheme, we observe that their scheme may suffer from stolen-verifier attacks. Assume that the verification table is compromised by an adversary U_A, then he/she can use it to break the property of user anonymity. The cryptanalysis steps are introduced as follows:

Step 1: U_A collects U's login request $\{P_1, P_2, P_3\}$ transmitted between U and S by launching eavesdropping attacks.
Step 2: U_A makes use of stolen (ID_U, r_{s1}) to calculate $ID_U \oplus r_{s1}P$.
Step 3: U_A checks if computed $ID_U \oplus r_{s1}P$ is equal to P_1 or not. If it holds, U_A knows that U is involved in a login session.

From the above steps, we conclude that U_A could know U's identity ID_U and Lu *et al.*'s scheme cannot prevent stolen-verifier attacks.

3.3 Suffer from Server Impersonation Attacks

Continued to the Sections 3.1 and 3.2, once an adversary U_A has compromised server's secret database and has learned a login user's identity ID_U, he/she could use the stolen (ID_U, r_{s1}) to forge a response message to impersonate as a legal server. The cryptanalysis steps are described as follows:

Step 1: U_A intercepts U's login request $\{P_1, P_2, P_3\}$ transmitted between U and S and makes use of stolen (ID_U, r_{s1}) to calculate $K''=h_2(ID_U||r_{s1})$ and $r_uP=P_2 \oplus K''$.
Step 2: U_A chooses a random number r_a and calculates r_aP and the common session key $SK''=r_ar_uP$.
Step 3: U_A calculates $Q_1'=K'' \oplus r_aP$ and $Q_2'=h_2(K''||r_uP||SK'')$ and transmits the malicious response $\{Q_1', Q_2'\}$ to the victim user U.
Step 4: After receiving $\{Q_1', Q_2'\}$ from U_A, the victim U reveals r_aP by computing $Q_1' \oplus K$ and calculates the session key $SK'=r_ur_aP$, where $K=K''$ and $SK'=SK''$. In addition, U checks if $h_2(K||r_uP||SK')=Q_2'$. If it holds, U convinces that he/she is interacting with a legal S. Then, U calculates the acknowledgement message $P_4=h_2(K||raP||SK')$ and transmits it to S.
Step 5: U_A intercepts U's acknowledgement P_4 transmitted between U and S. As a result, S is not aware of causing this security problem because it never received the messages from U.

From the above steps, we conclude that U_A not only fooled U into believing the authenticity of U_A but also cheated U into believing an insecure session key $SK'=SK''$. Finally, Lu *et al.*'s scheme cannot prevent server impersonation attacks.

3.4 Lack of Random Number in Registration Phase

In the end of registration phase of Lu *et al.*'s scheme, we observe that the U only keeps k_U in its memory without storing the secret random number r_{s1}. Consider that U generates the login request $\{P_1, P_2, P_3\}$ in Step 1 of authentication and key agreement phase, where $P_1 = r_{s1}P \oplus ID_U$. However, in fact, U cannot calculate (P_1, K, P_2, P_3) without having the random number r_{s1}.

3.5 Inefficiency of Authentication and Key Agreement Phase

In authentication and key agreement phase of Lu *et al.*'s scheme, we observe that their scheme exhibits an inefficiency problem in this phase. Consider that a user U transmits a login request $\{P_1, P_2, P_3\}$ to S. Then S makes use of all (ID_U, r_{s1}) stored in its secret database to verify the authenticity of the authorized identity ID_U by computing $P_1 \oplus r_{s1}P$. S first computes all the authorized random number $r_{s1}P$ stored in its secret database and compares $P_1 \oplus r_{s1}P$ with all the authorized identify ID_U stored in its secret database. Suppose that S needs to take j milliseconds to compute a $P_1 \oplus r_{s1}P$ and takes k milliseconds to compare a $P_1 \oplus r_{s1}P$ with an ID_U. Thus it may take $j*k*n$ milliseconds to confirm that U's login identity ID_U is valid or not, where n is the number of all authorized identities stored in S's secret database. If the number of n is a million identities and there are l registered users send login requests to S simultaneously, S must take $j*k*l*n$ milliseconds to confirm them and maybe the login user needs to wait a few minutes for a response message from S. In practice, it exhibits an inefficiency problem in the authentication process and it becomes infeasible for users to wait for the respondent results for such long time in mobile networks. To repair this flaw, we will propose an improved scheme to decrease the waiting time for access S and ensure a high rate of efficiency in the authentication procedures.

4. OUR IMPROVED SCHEME

In this section, we propose a simple improvement on Lu *et al.*'s authentication scheme, in which user anonymity and performance efficiency are preserve and stolen-verifier attacks are obviated in the improved scheme. Fig. 1 shows the entire schematic of our enhanced scheme in mobile networks.

4.1 Registration Phase

Before registration, the server S publishes $\{E(a, b), K_S, h_1(\cdot), h_2(\cdot)\}$, where $K_S = k_sP$. The details of registration phase are as follows:

Step 1: U selects his/her identity ID_U and transmits it to S through a secure channel.

Step 2: S checks whether ID_U is already registered or not. If ID_U is not registered, S generates a random number r_{s1} and calculates $k_U = r_{s1}h_1(ID_U \oplus k_s)$ and $Q_{ID_U} = h_1(ID_U \oplus k_s)P$. Then S stores (ID_U, r_{s1}) into its secret DB and returns $\{r_{s1}, k_U, Q_{ID_U}\}$ to U through a secure channel.

Step 3: After receiving $\{r_{s1}, k_U, Q_{ID_U}\}$ from S, U checks if $k_UP = r_{s1}Q_{ID_U}$. If it holds, U keeps (r_{s1}, k_U) secretly and releases Q_{ID_U}.

4.2 Authentication and Key Agreement Phase

Step 1: U chooses a random number r_u and calculates $P_1=r_uK_S\oplus ID_U$, $K=h_2(ID_U||r_{s_1})$, $P_2=r_uP$, $P_3=h_2(K||P_2||k_UP)$. Then U transmits the login request $\{P_1, P_2, P_3\}$ to S.

Step 2: After receiving $\{P_1, P_2, P_3\}$ from U, S reveals ID_U by computing $ID_U=P_1\oplus k_sP_2$ and makes use of (ID_U, r_{s_1}) to compute $K'=h_2(ID_U||r_{s_1})$, where k_s means S's private key. Then S checks if $h_2(K'||P_2||r_{s_1}Q_{ID_U})=P_3$. If it holds, S calculates the session key $SK= r_{s_2}r_uP$, $Q_1=K'\oplus r_{s_2}P$, $Q_2=h_2(K'||r_{s_1}Q_{ID_U}||SK)$ and transmits the response message $\{Q_1, Q_2\}$ to U through a public channel, where r_{s_2} is a random number chosen by S.

Step 3: After receiving $\{Q_1, Q_2\}$ from S, U reveals $r_{s_2}P$ by computing $Q_1\oplus K$ and calculates the session key $SK'=r_ur_{s_2}P$. Then U checks if $h_2(K||k_UP||SK')=Q_2$. If it holds, U calculates the acknowledgement message $P_4=h_2(K||r_{s_2}P||P_2||SK')$ and transmits it to S through a public channel.

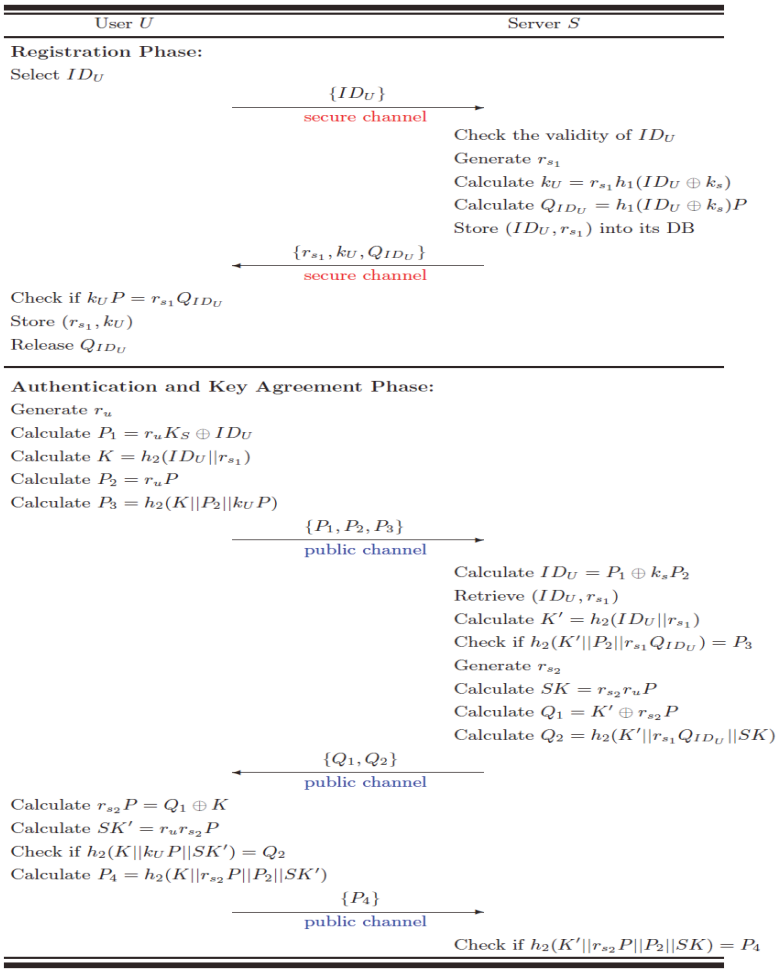

Fig. 1. The schematic of our improved scheme in mobile networks.

Step 4: After receiving P_4 from U, S checks if $h_2(K'||r_{s_2}P||P_2||SK)=P_4$. If it holds, S and U successfully achieve mutual authentication and negotiate a common and secure session key $SK=SK'$ between them.

5. SECURITY ANALYSIS

In this section, we analyze the security of our improved scheme and show that it is able to prevent above-mentioned weaknesses in Lu *et al.*'s scheme.

5.1 Resistance to Stolen-Verifier Attacks

We assume that all the verifier (ID_U, r_{s1}) stored in S's secret database is compromised by an adversary U_A. Moreover, U_A could collect U's login request $\{P_1, P_2, P_3\}$ transmitted between U and S. In the authentication and key agreement phase of our improved scheme, U's real identity ID_U is embedded in the encrypted message $P_1=r_uK_S\oplus ID_U$ and ID_U is well-protected via r_uK_S. Without knowing the knowledge of U's random number r_u, r_u could not be calculated by U_A due to the infeasibility of deriving r_u from r_uK_S by solving elliptic curve discrete logarithm problem (ECDLP). In addition, without knowing the knowledge of S's private key k_s, U_A could not compute k_sr_uP from P_2. As a result, U_A could not successfully derive ID_U from P_1 by computing $ID_U=P_1\oplus k_sP_2$ and the stolen-verifier attack is prevented in the improved scheme.

5.2 Resistance to Server Impersonation Attacks

Here, we analyze why our improved scheme can withstand our server impersonation attacks in Section 3.3. In Step 2 of authentication and key agreement phase of the improved scheme, U_A needs to response $Q_1'=K''\oplus r_aP$ and $Q_2'=h_2(K'||r_{s1}Q_{ID_U}||SK'')$ to the user for verification, where r_a is a random number chosen by U_A and the forged session key $SK''=r_ar_uP$. However, without knowing U's secret parameter $Q_{ID_U}=h_1(ID_U\oplus k_s)P$, it is computational infeasible for U_A to generate a correct Q_2'. As a result, U_A could not impersonate as a legal server to response a correct Q_2' to convince the user and we prove the improved scheme is robust against server impersonation attacks.

5.3 Resistance to User Impersonation Attacks

Continued to the stolen-verifier attacks, once user's verifier (ID_U, r_{s1}) is compromised by U_A, he/she may use it to impersonate as a legal U to log into S. However, in Step 1 of authentication and key agreement phase of the improved scheme, U_A needs to generate a valid login request $P_1'=r_aK_S\oplus ID_U$, $K''=h_2(ID_U||r_{s1})$, $P_2'=r_aP$ and $P_3'=h_2(K''||r_aP||k_UP)$ to the server for verification, where r_a is a random number chosen by U_A and the secret parameter K'' is legal one. However, without knowing U's another secret parameter $k_UP=r_{s1}Q_{ID_U}$, it is computational infeasible for U_A to forge a correct P_3'. Although the login parameters P_1' and P_2' are successfully forged, U_A could not forge a correct login parameter P_3' to convince the server. Finally, the improved authentication scheme is secure against user impersonation attacks.

5.4 Resistance to Replay Attacks

In the authentication and key agreement phase of the improved scheme, since the transmitted messages $\{P_1, P_2, P_3\}$ and $\{Q_1, Q_2\}$ contains freshly generated random numbers r_u and r_{s_2}. Therefore, U and S could check the freshness of random numbers received and verifies whether these the same as random numbers present in transmitted messages. Finally, this design discards the possibility of replay attacks in our improved scheme.

5.5 Provision of User Anonymity

Based on the design of our improved scheme, the property of user anonymity can be ensured in authentication and key agreement phase. We cleverly mask the real identity of U via a public channel and the adversary U_A could not compromise U's real identity ID_U by launching security attacks. First, in authentication and key agreement phase, U's real identity is included in $P_1=r_uK_S \oplus ID_U$ and $P_3=h_2(K||P_2||k_UP)$, where $K=h_2(ID_U||r_{s_1})$. Thus U_A cannot reveal ID_U without knowing r_u. In addition, we assume that the secret parameter r_{s_1} is compromised by U_A. Thus U_A could guess a candidate ID_U' and compute $K'=h_2(ID_U'||r_{s_1})$. However, U_A could not verify the validity of K' from P_3 without knowing k_U, where $k_U=r_{s_1}h_1(ID_u \oplus k_s)$. That is to say, all the identities are transmitted in cipher format instead of plaintext and these random numbers will be randomized at each new session. Finally, the property of user anonymity can be guaranteed in our improved scheme.

5.6 Provision of Mutual Authentication

In authentication and key agreement phase of the improved scheme, only the legitimate user can know the secret parameters (r_{s_1}, K, k_U) to generate a legal login request $\{P_1, P_2, P_3\}$. Therefore, in Step 2 of this phase, S can authenticate U by checking if the computed $h_2(K'||P_2||r_{s_1}Q_{ID_U})$ is equal to the received P_3. Moreover, in Step 3 of this phase, only the legal server S can embed U's secret parameter k_U into Q_2, where $Q_2=h_2(K'||r_{s_1}Q_{ID_U}||SK)$ and $r_{s_1}Q_{ID_U}=k_UP$. As a result, U can authenticate S by computing $h_2(K||k_UP||SK')$ and checking if the secret parameter k_UP is involved in Q_2. Finally, the property of mutual authentication is satisfied in the improved scheme.

5.7 Provision of Session Key Security

Since the common session key SK is only shared and established among the user U and the server S. In order to establish a secure and authenticated channel for late successive transmission, the session key SK not only ensures confidentiality but also achieves authenticity of participants and messages. Based on the design of session key $SK=r_{s_2}r_uP=r_ur_{s_2}P=SK'$, where r_u and r_{s_2} are used for preventing possible replay attacks. Moreover, due to the protection of elliptic curve Diffie-Hellman problem, the adversary U_A could not derive the session key $SK=SK'$ by collecting r_uP and $r_{s_2}P$. Finally, the excellent properties of session key security and data confidentiality can be guaranteed in our improved authentication scheme.

6. FORMAL SECURITY PROOF

In this section, we adopt the formal tool to analyze the security of the session key between user U and server S namely BAN logic [1]. Some notations used in BAN logic analysis are described as follows:

– $A \mid\equiv X$: It means that A believes the formula X is true.
– $A \lhd X$: It means that A sees the formula X.
– $A \mid\Rightarrow X$: It means that A has complete control over the formula X.
– $A \mid\sim X$: It means that A has once said the formula X.
– $\#(X)$: It means that X is fresh. The formula X has not been used before or X is a nonce.
– $A \overset{K}{\longleftrightarrow} B$: It means that principals A and B may use the shared key K to communicate.

Note that K will never be discovered by any principals except A and B.
– $\langle X\rangle_Y$: It means that formula X is combined with a secret parameter Y.
– $(X)_K$: It means that formula X is hashed with a key K.
– $\frac{Rule\,1}{Rule\,2}$: It can infer *Rule* 2 from *Rule* 1. For example, $\frac{A \text{ creates random } X}{A \mid\equiv \#(X)}$ means that principal A creates X, so A believes X is fresh.
– SK: A session key established in each session.

In order to describe logical postulates of BAN logic in formal terms, we list four rules as follows:

(Rule 1) Message meaning rule: $\dfrac{A \mid\equiv A \overset{K}{\longleftrightarrow} B, A \lhd (X)_K}{A \mid\equiv B \mid\sim X}$

If A believes that K is shared with B and sees X hashed with K, then A believes that B once said X.

(Rule 2) Nonce verification rule: $\dfrac{A \mid\equiv \sharp(X), A \mid\equiv B \mid\sim X}{A \mid\equiv B \mid X}$

If A believes that X has been uttered recently (freshness) and A believes that B once said X, and then A believes that B believes X.

(Rule 3) The jurisdiction rule: $\dfrac{A \mid\equiv B \mid\equiv X . A \mid\equiv B \mid\Rightarrow X}{A \mid\equiv X}$

If A believes that B has jurisdiction over X, and A believes that B believes a message X, then A believes X.

(Rule 4) The freshness conjuncatenation rule: $\dfrac{A \mid\equiv \sharp(X)}{A \mid\equiv \sharp(X, Y)}$

If one part known to be fresh, then the entire formula is fresh.

According to the analytic procedures of BAN logic, two participators U and S co-operatively run the improved scheme and we list the verification goals of our scheme as follows:

Goal 1: $U \mid\equiv U \overset{SK}{\leftrightarrow} S$
Goal 2: $S \mid\equiv U \overset{SK}{\leftrightarrow} S$

Next, we use BAN logic to transform our protocol, illustrated in Fig. 1 into the idealized form. The protocol generic types are shown in the following:

Message 1: $U \rightarrow S$: $r_u K_S \oplus ID_U$, $r_u P$, $h_2(K||P_2||k_U P)$
Message 2: $S \rightarrow U$: $K \oplus r_{s_2} P$, $h_2(K||r_{s_1} Q_{ID_U}||SK)$
Message 3: $U \rightarrow S$: $h_2(K||r_{s_2} P||r_u P||SK)$

Idealize form of the proposed protocol:

Message 1: $U \rightarrow S$: $< ID_U) >_{r_u K_S}$, $r_u P$, $(K, r_u P)_{k_U}$
Message 2: $S \rightarrow U$: $< r_{s_2} P >_K$, $(K, SK)_{k_U}$
Message 3: $U \rightarrow S$: $(K, r_{s_2} P, r_u P)_{SK}$

To analyze the proposed protocol, the following assumptions are also required:

(A.1): $U|\equiv\#(r_u)$
(A.2): $S|\equiv\#(r_{s_2})$
(A.3): $U \mid\equiv (U \overset{k_U}{\longleftrightarrow} S)$
(A.4): $S \mid\equiv (U \overset{k_U}{\longleftrightarrow} S)$
(A.5): $U \mid\equiv S \mid\equiv (U \overset{k_U}{\longleftrightarrow} S)$
(A.6): $S \mid\equiv U \mid\equiv (U \overset{k_U}{\longleftrightarrow} S)$
(A.7): $U \mid\equiv (U \overset{K}{\longleftrightarrow} S)$
(A.8): $S \mid\equiv (U \overset{K}{\longleftrightarrow} S)$
(A.9): $U \mid\equiv S \mid\equiv (U \overset{K}{\longleftrightarrow} S)$
(A.10): $S \mid\equiv U \mid\equiv (U \overset{K}{\longleftrightarrow} S)$

Based on the above-mentioned assumptions, the preliminary procedures of BAN logic are well prepared and we show the main steps of the verification proof as follows:

According to the Message 1, we could obtain:

(V.1): $S \triangleleft < ID_U >_{r_u K_S,} r_u P$, $(K, r_u P)_{k_U}$
According to the assumption **(A.4)** and **(A.6)**, we apply the message meaning rule to obtain:
(V.2): $S|\equiv U|\sim r_u P$
According to the assumption **(A.1)**, we apply the freshness conjuncatenation rule to obtain:
(V.3): $S\#(K, r_u P)_{k_U}$
According to **(V.2)** and **(V.3)**, we apply the nonce verification rule to obtain:
(V.4): $S|\equiv U|\equiv (K, r_u P)_{k_U}$
According to **(A.8)** and **(V.4)**, we apply the jurisdiction rule to obtain:
(V.5): $S|\equiv r_u P$
According to $SK=r_{s_2} r_u P=r_u r_{s_2} P$ and assumption **(A.2)**, we could obtain:
(V.6): $S \mid\equiv U \overset{SK}{\longleftrightarrow} S$ (Goal 2)

According to the Message 2, we could obtain:

(V.7): $U \triangleleft < r_{s_2}P >_K, (K, SK)_{kU}$

According to the assumption **(A.3)**, **(A.5)**, **(A.7)** and **(A.9)**, we apply the message meaning rule to obtain:

(V.8): $U|\equiv S|\sim r_{s_2}P$

According to the assumption **(A.2)**, we apply the freshness conjuncatenation rule to obtain:

(V.9): $U\#< r_{s_2}P >_K$

According to **(V.8)** and **(V.9)**, we apply the nonce verification rule to obtain:

(V.10): $U|\equiv S|\equiv < r_{s_2}P >_K$

According to **(A.7)** and **(V.10)**, we apply the jurisdiction rule to obtain:

(V.11): $U|\equiv r_{s_2}P$

According to $SK = r_{s_2}r_uP = r_ur_{s_2}P$ and assumptions **(V.11)** and **(A.1)**, we could obtain:

(V.12): $U \mid\equiv U \xleftrightarrow{SK} S$ (Goal 1)

According to the Message 3, we could obtain:

(V.13): $S \triangleleft (K, r_{s_2}P, r_uP)_{SK}$

According to **(V.6)** and **(V.12)**, we have proven the improved scheme achieves the verification goals as well as establishes a common session key *SK* between *U* and *S*.

7. EXPERIMENT RESULT

To demonstrate the efficiency, we show the experiment results of our improved scheme and compare it with Lu *et al.*'s authentication scheme [20] in terms of computational overhead. For example in our experimental environment (Pentium IV 3.2 GHz CPU and 6.0 GB RAM), we have run thousand rounds to take the arithmetic mean. The outcome showed that the average time of performing a one-way hash function and an elliptic curve point multiplication are approximately 0.01 ms and 1.15 ms, respectively. Here, we neglect the computational overhead for XOR and concatenate operations, we only consider one-way hash function and elliptic curve point multiplication in our experiment and performance comparisons are done only for authentication and key agreement phase because this phase is frequently executed. According to the computational time of Lu *et al.*'s scheme and our improved scheme, we can get the performance comparisons as shown in Fig. 2.

On the sides of mobile user and remote server, the computational time of all these two authentication schemes are approximately identical for one communication session when the total number of registered user stored in the server is only one. As illustrated in Fig. 2, we learn that our improved scheme executes only 8 one-way hashing operations and 8 elliptic curve point multiplication operations and takes 9.23 ms a session on average, without respect to total numbers of registered users stored in remote server side. Additionally, for performing an authentication session, Lu *et al.*'s scheme requires much more computational time especially for scenarios of increasingly registered users stored in remote server side. From the implementation point of view, our improved scheme requires less computational cost compared with Lu *et al.*'s scheme and the feature of performance efficiency makes our new scheme more suitable for implementation in mobile communication networks.

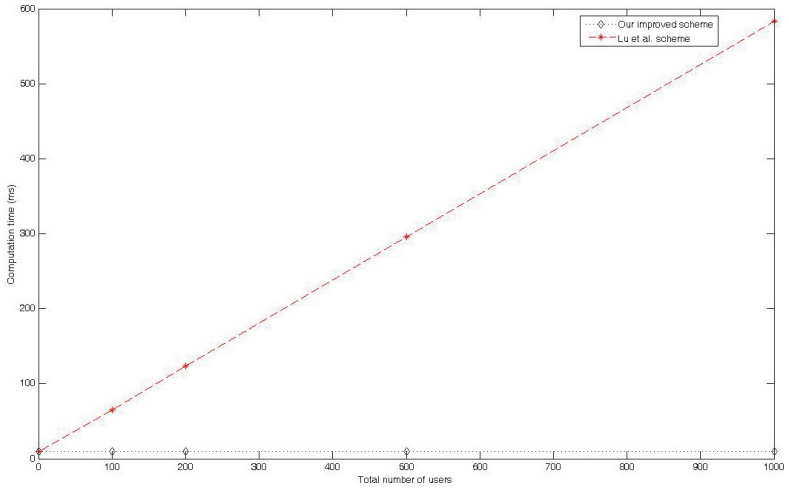

Fig. 2. Performance comparisons.

8. CONCLUSIONS

In this study, we have analyzed the security aspects of Lu *et al.*'s mutual authentication and key agreement scheme with user anonymity for mobile networks. However, we have demonstrated that Lu *et al.*'s authentication scheme has redundancy in protocol design and still failed to preserve user anonymity. Moreover, we have presented that their authentication scheme is susceptible to server impersonation attacks while having a problem of stolen-verifier in remote server side. To address these design weaknesses, we present an improved scheme and demonstrate the robustness of our improved scheme through BAN logic. According to the formal verification and experimental comparison, our improved scheme has protected network security during the service delivery session and has less computational overhead compared with Lu *et al.*'s authentication scheme.

REFERENCES

1. M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, Vol. 8, 1990, pp. 8-36.
2. C. H. Chou, K. Y. Tsai, and C. F. Lu, "Two ID-based authenticated schemes with key agreement for mobile environments," *Journal of Supercomputing*, Vol. 66, 2013, pp. 973-988.
3. M. S. Farash and M. A. Attari, "A secure and efficient identity-based authenticated key exchange protocol for mobile client-server networks," *Journal of Supercomputing*, Vol. 69, 2014, pp. 395-411.
4. D. He, J. Chen, and J. Hu, "An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security," *Information Fusion*, Vol. 13, 2012, pp. 223-230.
5. D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual

authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Information Sciences*, Vol. 321, 2015, pp. 263-277.
6. D. He and S. Zeadally, "Authentication protocol for ambient assisted living system," *IEEE Communications Magazine*, Vol. 35, 2015, pp. 71-77.
7. D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, DOI: 10.1109/JSYST.2016.2544805, 2016.
8. D. He, N. Kumar, H. Shen, and J. H. Lee, "One-to-many authentication for access control in mobile pay-TV systems," *Science China Information Sciences*, DOI: 10.1007/s11432-015-5469-5, 2016.
9. W. H. Ho, S. W. Shieh, and C. C. Tseng, "RAKA: revocable authenticated key agreement system for mobile social networks," *Journal of Information Science and Engineering*, Vol. 32, 2016, pp. 731-746.
10. S. H. Islam and G. P. Biswas, "A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Journal of Systems and Software*, Vol. 84, 2011, pp. 1892-1898.
11. K. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, Vol. 48, 1987, pp. 203-209.
12. C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, Vol. 33, 2010, pp. 1-5.
13. C. T. Li and C. C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications," *Mathematical and Computer Modelling*, Vol. 55, 2012, pp. 35-44.
14. C. T. Li, C. C. Lee, C. Y. Weng, and C. I. Fan, "A secure dynamic identity based authentication protocol with smart cards for multi-server architecture," *Journal of Information Science and Engineering*, Vol. 31, 2015, pp. 1975-1992.
15. C. T. Li, C. C. Lee, and C. Y. Weng, "A dynamic identity-based user authentication scheme for remote login systems," *Security and Communication Networks*, Vol. 8, 2015, pp. 3372-3382.
16. C. T. Li, C. Y. Weng, and C. C. Lee, "A secure RFID tag authentication protocol with privacy preserving in telecare medicine information systems," *Journal of Medical Systems*, Vol. 39, 2015, Article No. 77, pp. 1-8.
17. C. T. Li, C. Y. Weng, C. C. Lee, and C. C. Wang, "A hash based remote user authentication and authenticated key agreement scheme for the integrated EPR information system," *Journal of Medical Systems*, Vol. 39, 2015, Article No. 144, pp. 1-11.
18. C. T. Li, C. C. Lee, and C. Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *Journal of Medical Systems*, Vol. 40, 2016, Article No. 117, pp. 1-15.
19. C. T. Li, "A secure chaotic maps-based privacy-protection scheme for multi-server environments," *Security and Communication Networks*, DOI:10.1002/sec.1487, 2016.
20. Y. Lu, L. Li, H. Peng, and Y. Yang, "Robust ID based mutual authentication and key agreement scheme preserving user anonymity in mobile networks," *KSII Transactions on Internet and Information Systems*, Vol. 10, 2016, pp. 1273-1288.
21. R. Madhusudhan and R. C. Mittal, "Dynamic ID-based remote user password au-

thentication schemes using smart cards: A review," *Journal of Network and Computer Applications*, Vol. 35, 2012, pp. 1235-1248.
22. V. S. Miller, "Use of elliptic curves in cryptography," in *Proceedings of the Advances in Cryptology*, 1985, pp. 417-426.
23. D. Wang, D. He, P. Wang, and C. H. Chu, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, Vol. 12, 2015, pp. 428-442.
24. Y. Wang, H. Zhong, Y. Xu, and J. Cui, "ECPB: efficient conditional privacy-preserving authentication scheme supporting batch verification for VANETs," *International Journal of Network Security*, Vol. 18, 2016, pp. 374-382.
25. K. Y. Wu, K. Y. Tsai, T. C. Wu, and K. Sakurai, "Provably secure anonymous authentication scheme for roaming service in global mobility networks," *Journal of Information Science and Engineering*, Vol. 31, 2015, pp. 727-742.
26. 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, 2009, pp. 138-143.
27. S. Zeng, Y. Huang, and X. Liu, "Privacy-preserving communication for VANETs with conditionally anonymous ring signature," *International Journal of Network Security*, Vol. 17, 2015, pp. 135-141.
28. M. Zhang, J. S. Zhang, and W. R. Tan, "A secure sketch-based authentication scheme for telecare medicine information systems," *Journal of Information Science and Engineering*, Vol. 32, 2016, pp. 389-402.

Chun-Ta Li (李俊達) received the Ph.D. degree in Computer Science and Engineering from National Chung Hsing University, Taiwan, in 2008. He is currently an Associate Professor with the Department of Information Management at Tainan University of Technology, Taiwan. His research interests include information and network security, wireless sensor networks, mobile computing, and security protocols for RFID, IoTs and cloud computing.

Cheng-Chi Lee (李正吉) received the Ph.D. degree in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He is currently a Professor with the Department of Library and Information Science at Fu Jen Catholic University. His current research interests include data security, cryptography, network security, mobile communications and computing, wireless communications.

Chi-Yao Weng (翁麒耀) received the Ph.D. degree in Computer Science from National Tsing Hua University, Hsinchu, Taiwan, in 2011. He is currently an Assistant Professor with the Department of Computer Science at National Pingtung University. His current research interests include data analysis, mobile security, multimedia security, digital right management and information forensics.