A SECURE AND EFFICIENT AUTHENTICATION WITH KEY AGREEMENT SCHEME BASED ON ELLIPTIC CURVE CRYPTOSYSTEM

Juan Qu

Yuming Feng

Yi Huang

School of Mathematics and Statistics
Chongqing Three Gorges University
Chongqing, 404100
China
e-mails: qulujuan@163.com (Juan Qu)
yumingfeng25928@163.com (Yuming Feng)

Abstract. Recently, Li et al. [20] proposed an improved authentication with key agreement scheme on elliptic curve cryptosystem for global mobility networks to remedy the weaknesses of Rhee et al.'s scheme. Li et al.'s scheme not only achieves mutual authentication, but also provides the procedure for key agreement and updates of secrets for users and servers. However, we find that Li et al.'s scheme is still insecure and vulnerable to insider attack, impersonation attack and unverifiable password change. In order to eliminate these pitfalls, we propose a new authenticated with key agreement scheme based on elliptic curve cryptosystem. The analysis shows that the proposed scheme is more secure and more suitable for global mobility networks.

Keywords: authentication, elliptic curve cryptosystem, key agreement, impersonation attack

2000 Mathematics Subject Classification: 20C15.

1. Introduction

Mutual authentication between a remote user and a server is the most common approach to ensure that the legal user can access the resources provided by remote systems over unreliable networks. In 1981, Lamport [1] first proposed a password-based authentication scheme to solve the secure communication problem. Since then, some password authentication schemes have been extensively investigated in [2], [3], [4], [5]. However, these schemes have security problems such as password attack, the system overhead of keeping the password tables. To avoid the above problems, smart-card-based password authentication schemes [6], [9], [10], [11], [12], [13], [14], [15] have been proposed. In a smart-card-based password authentication scheme, users insert their smart card into a card reader and input a password for the card. Then, the smart card generates the user's login request, and sends the request to the server. After the user and the server mutual authenticate the identity with each other, they share the common session key for future communication. Although the smart-card-based password authentication scheme improves the system security and solves many security attacks. However, most of user authentication schemes are subject to stolen smart card attack, off-line password guessing attack, impersonation attack and so on. Moreover, the smart-card-based password authentication schemes need the cards and readers which are increasing the cost of deployment.

In order to reduce the deployment cost, the memory device-aided (e.g., USB sticks, mobile phones, PDAs) password authentication protocol has been proposed. In 2009, Rhee et al. [16] first analyzed the security of the existing schemes using smart cards when the tamper-resistant property is eliminated from smart card. Then, Rhee et al. [16] proposed an enhanced scheme based on Khan-Zhang's scheme [17]. In 2012, Chen et al. [18] proposed a password-based remote user authentication and key agreement scheme without using smart cards. They pointed out that their scheme not only could resist off-line dictionary attack, replay, forgery and impersonation attacks but also guaranteed mutual authentication. But, in 2013, Jiang et al. [19] found that Chen et al.'s [18] scheme was insecure against off-line dictionary attacks. To remedy the security flaw, they proposed an improved password authentication protocol without using smart cards. Recently, Li et al. [20] pointed out Rhee et al.'s [16] authentication scheme is not secure against user impersonation attack caused by mathematical homomorphism computed in the finite field based upon the discrete logarithm. And Li et al. [20] proposed a new password-based authentication with key agreement scheme for portable devices on an elliptic curve cryptosystem. However, we find that Li et al.'s scheme is also existing some flaws, such as insider attack, impersonation attack, unverifiable password change. In this paper, to overcome these security flaws, we propose a secure and efficient authentication with key agreement scheme based on elliptic curve cryptosystem.

The rest of this paper is organized as follows. Some preliminaries are given in Section 2. In Section 3, we give a brief review of Li et al.'s scheme. Section 4 describes the cryptanalysis of Li et al.'s scheme. Our scheme is proposed in Section 5, its security is proved in Section 6. Finally, we draw our conclusion in Section 7.

2. Preliminaries

In this section, we will introduce the basic concepts of ECC. In all elliptic curve cryptosystem, the elliptic curve equation is defined as the form of $E_p(a,b)$: $y^2 = x^3 + ax + b(mod\ p)$. Given an integer $s \in F_p^*$ and a point $P \in E_p(a,b)$, the point-multiplication sP over $E_p(a,b)$ can be defined as $s \cdot P = P + P + P + \cdots + P$

(s times). Generally, the security of ECC relies on the difficulties of the following problems.

Definition 1. Given two points P and Q over $E_p(a,b)$, the elliptic curve discrete logarithm problem (ECDLP) is to find an integer $s \in F_p^*$ such that $Q = s \cdot P$.

Definition 2. Given three points P, $s \cdot P$, and $t \cdot P$ over $E_p(a,b)$ for s, $t \in F_p^*$, the computational Diffie-Hellman problem(CDLP) is to find the point $(st)P$ over $E_p(a,b)$.

Definition 3. Given two points P and $Q = s \cdot P + t \cdot P$ over F_p^* for s, $t \in F_p^*$, the elliptic curve factorization problem(ECFP) is to find two points $s \cdot P$ and $t \cdot P$ over $E_p(a,b)$.

3. Review of Li et al.'s scheme

In this section, we briefly review Li et al.'s scheme [20]. The notations used in Li et al.'s scheme are defined in Table 1.

Table 1: Some important notations used in Li et al.'s scheme

p	a large prime number
$E_p(a,b)$	an elliptic curve in the prime finite field F_p
P	the generator of order n
$H(\cdot)$	a key derivation function
ID_i	the identity of the client U_i
pw_i	the password of the client U_i
x_S	server S's secret key
n_i	a large unique number generated by S
m	session identifier
$\|\|$	concatenation operation

3.1. Registration phase

1. A client U_i chooses his/her valid identifier ID_i with password pw_i, then sends ID_i and pw_i to S over a secure channel.
2. Upon receiving the registration request message ID_i and pw_i from U_i, S computes U_i's authentication information $Y_i = (Y_{i,1}, Y_{i,2}) = (ID_i \cdot r_i \cdot n_i \cdot x_S \cdot P + pw_i \cdot P, r_i \cdot P)$ where r_i is a random number only used once in this phase and n_i is a large unique number generated randomly by S for every user.

3. S sends $\{H(\cdot), p, E_p(a,b), P, Y_i\}$ to U_i over a secure(or public) channel and stores the list $ID_i - n_i$ in its database privately.
4. Upon receiving the authentication information, U_i stores it in his/her storage device and remembers his/her ID_i with pw_i.

3.2. Login phase

U_i can perform the following operations to login in to the authentication server:

1. U_i inputs his/her ID_i with pw_i into his/her device.
2. The device chooses temporary secret random numbers $a, b, c, d, k_1 \in F_p^*$. The random numbers mentioned in the scheme are only used once and will not be dropped until the scheme is terminated.
3. Computes $Y'_{i,1} = Y_{i,1} - pw_i \cdot P = ID_i \cdot r_i \cdot n_i \cdot x_S \cdot P$, $C_1 = a \cdot Y'_{i,1} = a \cdot ID_i \cdot r_i \cdot n_i \cdot x_S \cdot P$, $C_2 = a \cdot Y_{i,2} = a \cdot r_i \cdot P$, $C_3 = b \cdot Y_{i,2} = b \cdot r_i \cdot P$, $C_4 = c \cdot Y_{i,2} = c \cdot r_i \cdot P$, $C_5 = c \cdot Y'_{i,1} + k_1 \cdot P = c \cdot ID_i \cdot r_i \cdot n_i \cdot x_S \cdot P + k_1 \cdot P$, $C_6 = d \cdot Y_{i,2} = d \cdot r_i \cdot P$.
4. U_i sends to S the login request message $M_1 = \{ID_i, Y_{i,2}, C_1, C_2, C_3, C_4, C_5, C_6\}$.

3.3. Authentication with key agreement phase

1. Upon receiving the login request message, S checks whether the ID_i is valid in the registration table at first and extracts n_i corresponding to ID_i in its database, then verifies if the equation $ID_i \cdot n_i \cdot x_S \cdot C_2 = C_1$ holds. If it holds, S accepts $U_i^{;}$ s login request; otherwise it rejects.
2. S computes $k_1 \cdot P = C_5 - ID_i \cdot n_i \cdot x_S \cdot C_4$. Then S can get the session key $sk = H(K_x)$, where K_x is the x-coordinate of the point $K = k_1 \cdot k_2 \cdot P$ on $E_p(a,b)$, $k_2 \in F_p^*$ is a random number generated by S.
3. S computes $C_7 = ID_i \cdot n_i \cdot x_S \cdot C_3 = ID_i \cdot n_i \cdot x_S \cdot b \cdot r_i \cdot P$, $C_8 = ID_i \cdot n_i \cdot x_S \cdot C_6 + k_2 \cdot P$, $C_9 = E_{sk}(ID_i \parallel m \parallel S)$, where m is a session identifier.
4. Finally, S sends to U_i the message $M_2 = \{C_7, C_8, C_9\}$ for mutual authentication and key confirmation.

3.4. Mutual authentication and key confirmation

Upon receiving the message M_2 from S, U_i performs the following steps:

1. U_i verifies whether the equation $b \cdot Y'_{i,1} = C_7$ holds. If so, U_i believes the response of the message is correct from the responding server; otherwise it rejects.

2. After the mutual authentication process, U_i computes $k_2 \cdot P = C_8 - d \cdot Y'_{i,1}$ and contains the session key $sk = H(K_x)$. Then, U_i can decrypt the message C_9 with sk and confirm the session key if S and ID_i are correct in C_9.
3. U_i computes $C_{10} = E_{sk}(ID_i \parallel m \parallel S)$ and sends $M_3 = \{C_{10}\}$ to S.
4. At the end of the scheme S should execute the final key confirmation by decrypting C_{10} with sk. If the information is correct in C_{10}, the scheme is finished successfully; otherwise it terminates in failure.

3.5. Secret update phase

1. Password update phase: the client U_i could change his/her password offline anytime and anywhere by computing $Y_i^* = (Y_{i,1}^*, Y_{i,2}) = (Y_{i,1} - pw_i \cdot P + pw_i^* \cdot P, Y_{i,2})$ and replacing Y_i by Y_i^* with a new password pw_i^*.
2. Secret number update phase: the server S could change its secret number x_S online by interacting with its client. This phase is executed after the authentication with key agreement procedures and a secure channel based on the session key sk. Thus S and the user U_i can communicate with each other securely using symmetric cryptography algorithm, i.e. all of the following information is encrypted by sk using the symmetric cryptography algorithm. U_i sends the update request. Then S computes the new $Y'^{*}_{i,1} = ID_i \cdot r_i^* \cdot n_i \cdot x_S^* \cdot P$, $Y'^{*}_{i,2} = r_i^* \cdot P$ and sends these new values to U_i. Finally, U_i computes $Y_{i,1}^* = Y'^{*}_{i,1} + pw_i \cdot P$ and replaces the original authentication information $Y_i = (Y_{i,1}, Y_{i,2})$ by $Y_i^* = (Y_{i,1}^*, Y_{i,2}^*)$.

4. Comments on Security Pitfalls of Li et al.'s scheme

In this section, the security of Li et al.'s scheme has been analyzed carefully and we have found some security pitfalls such as insider attack, impersonation attack and unverifiable password change. Now we are going to explore these security flaws.

4.1. Insider attack

The insider attack is defined that any manager of system purposely leaks the secret information, and then leads to serious security flaws of authentication scheme. In the registration phase of Li et al.'s scheme, U_i sends his/her password pw_i to the server S in plain text. Thus, the password of the user U_i will be revealed to the remote system. If the user offers the same password to access the other remote servers for the convenience, it is possible that the privileged insider of the remote server S can successfully impersonate U_i to login to the other remote servers by using pw_i.

4.2. Impersonation attack

In the secure analysis section of Li et al.'s scheme, he said that impersonation attack could not be effective in their scheme. However, we find that a malicious user U_A can be authenticated to remote system even if he or she does not have the valid password pw_i. Assume that the malicious user U_A has intercepted of the legal user U_i's previous login message $\{ID_i, Y_{i,2}, C_1, C_2, C_3, C_4, C_5, C_6\}$ from the public channel. An impersonation attack can be performed as given below:

1. The malicious user U_A computes $C_1' = a' \cdot C_1 = a' \cdot a \cdot ID_i \cdot r_i \cdot n_i \cdot x_S \cdot P$, $C_2' = a' \cdot C_2 = a' \cdot a \cdot r_i \cdot P$.
2. The malicious user sends the fabricated login message $M_1' = \{ID_i, Y_{i,2}, C_1', C_2', C_3, C_4, C_5, C_6\}$ to the S.
3. When the S receives the login request message $M_1' = \{ID_i, Y_{i,2}, C_1', C_2', C_3, C_4, C_5, C_6\}$, S checks whether the ID_i is valid in the registration table at first and extracts n_i corresponding to ID_i in its database, then verifies if the equation $ID_i \cdot n_i \cdot x_S \cdot C_2' = ID_i \cdot n_i \cdot x_S \cdot a \cdot a' \cdot r_i \cdot P$ is equal to C_1'. It is obvious that the equation holds. So, the server S accepts U_i' s login request. From the description above, we know that Li et al.'s scheme suffers from impersonation attack.

4.3. Unverifiable password change

In the secret update phase of Li et al.'s scheme, when U_i wants to change his/her password, he/she chooses a new password pw_i^* by himself/herself, and computes $Y_i^* = (Y_{i,1}^*, Y_{i,2}) = (Y_{i,1} - pw_i \cdot P + pw_i^* \cdot P, Y_{i,2})$, and there is no authentication procedure in password change phase. If the malicious user U_A obtains U_i' s storage device, U_A may arbitrarily key in new and obsolete passwords. Then the storage device will replace Y_i by Y_i^*. Thereupon, even if the original legal user U_i uses his/her own the storage device, he or she cannot access the remote server S anymore.

5. Our proposed scheme

According to our cryptanalysis, some of the cryptanalysis attacks cannot be prevented in Li et al.'s scheme. Therefore, we propose a more secure remote authentication scheme using elliptic curve cryptosystem to remove the security weaknesses existing in Li et al.'s scheme. The proposed scheme has five phases: system initialization phase, the registration phase, the login phase, the authentication with key agreement phase and secret update phase. The details of these phases are as follows.

5.1. System initialization phase

The system initialization phase consists of two steps in our proposed scheme:

1. Let $p > 3$ be a large prime number, and $E_p(a, b)$ be an elliptic curve in the prime finite field F_p. P is a generator of order n and n must be large enough so that the ECDLP is difficult in the cyclic subgroup $< P >$.
2. The server S chooses three one-way secure hash functions $H_1 : \{0,1\}^* \to G_p$, $H_2 : \{0,1\}^* \times G_p \to \{0,1\}^k$, $H_3 : G_p \times G_p \to \{0,1\}^k$, $H_4 : \{0,1\}^* \times \{0,1\}^* \times G_p \times G_p \to \{0,1\}^k$ and the server S selects a random number x_S (which is the master secret of the server S) from $[1, n-1]$.
3. The server S publishes $\{p, E_p(a,b), P, H_1(\cdot), H_2(\cdot), H_3(\cdot), H_4(\cdot)\}$ as system parameters and keep the master key x_S secret.
4. All the operation are in F_p, and it omits mod p for the sake of simplicity.

5.2. Registration phase

1. A client U_i chooses his/her ID_i, pw_i and a random number b, then U_i submits ID_i, $H_1(pw_i \parallel b) \cdot P$ to S over a secure channel.
2. Upon receiving the registration request message $\{ID_i, H_1(pw_i \parallel b) \cdot P\}$ from U_i, S computes $X_i = H_2(ID_i \parallel H_1(pw_i \parallel b) \cdot P)$, $Y_i = (Y_{i,1}, Y_{i,2}) = (ID_i \cdot r_i \cdot n_i \cdot x_S \cdot P + H_1(pw_i \parallel b) \cdot P, r_i \cdot P)$, where r_i is a random number only used once in this phase.
3. S sends (X_i, Y_i) to U_i over a secure(public) channel and stores the list $ID_i - n_i$ in its database privately.
4. Upon receiving the authentication information, U_i stores it in his/her storage device and enters b into his/her storage device.

5.3. Login phase

When the client U_i wants to login the authentication server, the user U_i perform the following steps to generate a valid login request message.

1. U_i inputs his/her ID_i, pw_i into his/her device.
2. The device computes $X_i' = H_2(ID_i \parallel H_1(pw_i \parallel b) \cdot P)$ and checks whether $X_i' = X_i$. If it is not equal, the session is terminated. Otherwise, the user's identity ID_i and password pw_i are verified, and the device performs the next steps.
3. The device chooses temporary secret random numbers $a, b, c, d, k_1 \in F_p^*$ and computes $Y_{i,1}' = Y_{i,1} - H_1(pw_i \| b) \cdot P$, $C_1 = H_3(a \cdot Y_{i,1}')$, $C_2 = a \cdot Y_{i,2}$, $C_3 = b \cdot Y_{i,2}$, $C_4 = c \cdot Y_{i,2}$, $C_5 = c \cdot Y_{i,1}' + k_1 \cdot P$, $C_6 = d \cdot Y_{i,2}$.
4. U_i sends to S the login request message $M_1 = \{ID_i, Y_{i,2}, C_1, C_2, C_3, C_4, C_5, C_6\}$.

5.4. Authentication with key agreement phase

1. Upon receiving the login request message, S checks whether the ID_i is valid in the registration table at first and extracts n_i corresponding to ID_i in its database, then verifies if the equation $H_3(ID_i \cdot n_i \cdot x_S \cdot C_2) = C_1$ holds. If it holds, S accepts $U_i^{’}$ s login request; otherwise it rejects.

2. S computes $k_1 \cdot P = C_5 - ID_i \cdot n_i \cdot x_S \cdot C_4$, $C_7 = ID_i \cdot n_i \cdot x_S \cdot C_3 = ID_i \cdot n_i \cdot x_S \cdot b \cdot r_i \cdot P$, $C_8 = ID_i \cdot n_i \cdot x_S \cdot C_6 + k_2 \cdot P$, $C_9 = H_4(ID_i \parallel m \parallel k_1 \cdot P \parallel k_2 \cdot P)$, where m is a session identifier, $k_2 \in F_p^*$ is a random number generated by S.

3. Finally, S sends to U_i the message $M_2 = \{C_7, C_8, C_9\}$ for mutual authentication and key confirmation.

4. Upon receiving the message M_2 from S, U_i performs the following steps: U_i verifies whether the equation $b \cdot Y'_{i,1} = C_7$ holds. If so, U_i computes $k_2 \cdot P = C_8 - d \cdot Y'_{i,1}$, $H_4(ID_i \parallel m \parallel k_1 \cdot P \parallel k_2 \cdot P)$ and verifies whether $H_4(ID_i \parallel m \parallel k_1 \cdot P \parallel k_2 \cdot P) = C_9$. If it is equal, the server S is authenticated by the user U_i. At the end of the scheme, the user U_i and server S can share a session key $sk = k_1 \cdot k_2 \cdot P$ for future confidentiality communication.

5.5. Secret update phase

1. Password update phase: the client U_i inputs his/her ID_i, pw_i into his/her storage device, and request to change his/her password. The device computes $X'_i = H_2(ID_i \parallel H_1(pw_i \parallel b) \cdot P)$ and checks whether $X'_i = X_i$. If it is not equal, the password change request is rejected. Otherwise, the user's identity ID_i and password pw_i are verified, and the user inputs a new password pw_i^*. The device computes $X_i^* = H_2(ID_i \parallel H_1(pw_i^* \parallel b) \cdot P)$, $Y_i^* = (Y_{i,1}^*, Y_{i,2}) = (Y_{i,1} - H_1(pw_i \parallel b) \cdot P + H_1(pw_i^* \parallel b) \cdot P, Y_{i,2})$ and replaces X_i, Y_i by X_i^*, Y_i^* .

2. Secret number update phase: the server S could change its secret number x_S online by interacting with its client. This phase is executed after the authentication with key agreement procedures and a secure channel based on the session key sk. Thus S and the user U_i can communicate with each other securely using symmetric cryptography algorithm, i.e. all of the following information is encrypted by sk using the symmetric cryptography algorithm. U_i sends the update request. Then S computes the new $Y_{i,1}^{\prime *} = ID_i \cdot r_i^* \cdot n_i \cdot x_S^* \cdot P$, $Y_{i,2}^{\prime *} = r_i^* \cdot P$ and sends these new values to U_i. Finally, U_i computes $Y_{i,1}^* = Y_{i,1}^{\prime *} + H_1(pw_i^* \parallel b) \cdot P$ and replaces the original authentication information $Y_i = (Y_{i,1}, Y_{i,2})$ by $Y_i^* = (Y_{i,1}^*, Y_{i,2}^*)$.

6. Security analysis and discussion

In this section, we discuss the security properties of our proposed scheme, and make comparisons with some related schemes in functionality and computation cost.

6.1. Insider attack

In the proposed scheme, the server S cannot obtain the user U_i's password pw_i. Since in the registration phase, the user U_i chooses his/her ID_i, pw_i and a random number b, then U_i submits ID_i, $H_1(pw_i \parallel b) \cdot P$ to the server S. It is computationally impossible that to derive the password pw_i from $H_1(pw_i \parallel b) \cdot P$, because of the difficulties of elliptic curve discrete logarithm problem(ECDLP) and the hardness of inverting hash function $H_1(\cdot)$. Therefore, the proposed scheme is secure against insider attack.

6.2. Quickly detect the authorized login

In the login phase of our proposed scheme, when the user inputs identity ID_i and password pw_i, the validity of identity ID_i and password pw_i can be verified by checks whether $X_i' = X_i$. If it is not equal, it means that the user inputs a wrong identity and password, then the storage device terminates the session. On the contrary, if it holds, the device performs the next steps. Thus, our proposed scheme can be quickly detect the wrong password by the device at the beginning of the login phase.

6.3. Impersonation attack

In our proposed scheme, if an adversary U_A wants to impersonation as the legal user U_i to pass the authentication of the server S, he/she must get $Y_{i,1}' = ID_i \cdot r_i \cdot n_i \cdot x_S \cdot P$ to compute the valid authentication message C_1 and C_2. However, an adversary U_A cannot derive $Y_{i,1}'$ without knowing the valid password pw_i of the user U_i. On the other hand, an adversary U_A cannot get $Y_{i,1}'$ from $C_1 = H_3(a \cdot Y_{i,1}')$, since it is protected by ECDLP and hash functions. Therefore, the proposed scheme is secure against impersonation attack.

6.4. Off-line password guessing attack

In the proposed scheme, there is no way for an adversary U_A to guess the user U_i's password based on $X_i = H_2(ID_i \parallel H_1(pw_i \parallel b) \cdot P)$ and $Y_i = (Y_{i,1}, Y_{i,2}) = (ID_i \cdot r_i \cdot n_i \cdot x_s \cdot P + H_1(pw_i \parallel b) \cdot P, r_i \cdot P)$ which are from the storage device. Due to hardness of ECDLP, the adversary U_A cannot obtain U_i's password pw_i from the value X_i . Besides, the adversary U_A cannot launch off-line dictionary attack without the secret random number, the server S's secret key.

6.5. Replay attack

In the proposed scheme, the random numbers a, b, c, d, k_1, k_2 are different in each new session, which make all messages dynamic and valid for that session only. Thus, our proposed scheme is secure against replay attack.

6.6. Server spoofing attack

If an adversary U_A wants to masquerade as the server S to cheat the user U_i. He/She needs to generate the valid response message $M_2 = \{C_7, C_8, C_9\}$. However, he/she cannot correctly compute C_7,C_8,and C_9 without the server's secret key x_S. Therefore, our scheme is secure against server spoofing attack.

6.7. Performance analysis

We analyze the functionary of the proposed scheme and make comparisons with other related schemes. Table 2 shows that our scheme is more secure and robust than other related schemes and achieves more functionality features. Table 3 summarizes the computation cost between our scheme and some related schemes. The following notations are used in Table 3. Besides, Table 3 demonstrates that our scheme does not need symmetric encryption/decryption operations, only needing point multiplication, point addition on ECC and hashing function operations. Hence, our proposed scheme is more secure and efficient than other authentication schemes.

Table 2: Functionality comparisons

	our scheme	Rhee's	Yang's	Li's
Achieves mutual authentication	Yes	No	Yes	Yes
Resist insider attack	Yes	No	Yes	No
Resist replay attack	Yes	No	No	Yes
Resist impersonation attack	Yes	No	No	No
Resist off-line dictionary attack	Yes	No	N/A	Yes
Resist the device stolen attack	Yes	No	N/A	Yes
Resist server spoofing attack	Yes	No	Yes	Yes
Quickly detect the unauthorized login	Yes	No	N/A	No

Table 3: Comparisons of computation cost

	T_{Exp}	T_{ECMul}	T_{ECAdd}	T_h	T_{Sym}	T_{Mul}	Total
our scheme	0	34	9	14	0	0	$31T_{ECMul}$ $+9T_{ECAdd}+11T_h$
Rhee's	7	0	0	6	0	2	$7T_{Exp}+6T_h$ $+2T_{Mul}$
Yang's	0	9	5	9	0	0	$9T_{ECMul}$ $+5T_{ECAdd}+9T_h$
Li's	0	34	9	2	4	0	$34T_{ECMul}+9T_{ECAdd}$ $+2T_h+4T_{Sym}$

T_h : the time complexity of hashing operations;
T_{Exp} : the time complexity of modular exponentiation in the finite field;
T_{ECAdd} : the time complexity of point multiplication on ECC;
T_{ECMul} : the time complexity of point addition on ECC;
T_{Sym} : the time complexity of symmetric encryption/decryption;
T_{Mul} : the time complexity of inverting operation in finite field.

7. Conclusions

We have identified security flaws in the authentication with key agreement scheme on elliptic curve cryptosystem of Li et al.'s scheme. To compensate for these shortcomings, we propose a novel authentication with key agreement scheme. According to our analysis and discussion, the proposed scheme can withstand various attacks and has a lower computation cost.

Acknowledgement. This work is supported by the Scientific and Technological Research Program of Chongqing Municipal Education Commission (Nos. KJ1401006, KJ1401019) and the Fundamental Research Funds for the Central Universities (No. XDJK2015D004).

References

[1] Lamport, L., *Password authentication with insecure communication*, Communications of the ACM, 24 (11) (1981), 770-772.

[2] Peyravian, M., Zunic, N., *Methods for protetcting password transmission*, Computers and Security, 19 (5) (2000), 466-469.

[3] Lee, C.C, Li, L.H., Hwang, M.S., *A remote user authentication scheme using hash functions*, ACM SIGOPS Operating System Review, 36 (4) (2002), 23-29.

[4] Lin, C.L, Hwang, T., *A password authentication scheme with secure password updating*, Computers and Security, 22 (1) (2003), 68-72.

[5] Yoon, E.J., Ruy, E.K., Roo, K.Y., *A secure user authentication scheme using hash functions*, ACM Operating Systems Review, 38 (2) (2004), 62-68.

[6] Chang, C., Wu, T., *Remote Password Authentication with Smart Cards*, IEE Proceedings – E Computers & Digital Techniques, 138 (3) (1991), 165-168.

[7] Sun, H.M., *An efficient remote user authentication scheme using smart cards*, IEEE Transactions on Consumer Electronics , 46 (4) (2000), 958-961.

[8] Yeh, K., Su, C., Lo, N., Li, Y., Hung, Y., *Two robust remote user authentication protocols using smart cards*, Journal of Systems and Software, 83 (12) (2010), 2556-2565.

[9] Yang, J.H., Chang, C., *An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem*, Computers & Security, 28 (3) (2009), 138-143.

[10] Wen, F.T., Li, X.L., *An improved dynamic ID-based remote user authentication with key agreement scheme*, Computers and Electrical Engineering, 38 (2) (2012), 381-87.

[11] Fan, C.I., Lin, Y.H., *Provably Secure Remote Truly Three-Factor Authentication Scheme With Privacy Protection on Biometrics*, Transactions On Information Forensics and Security, 4 (4) (2009), 933-945.

[12] Awasthi, A. K., Srivastava, K., Mittal, R.C., *An improved timestamp-based remote user authentication scheme*, Computers and Electrical Engineering, 37 (6) (2011), 869-874.

[13] Liao, C.H., Chen, H.C., Wang, C.T., *An exquisite mutual authentication schemes with key agreement using smart card*, Informatica, 33 (2009), 125-132.

[14] Shin, S., Kim, K., Kim, K.H., Yeh, H.J., *A remote user authentication scheme with anonymity for mobile devices*, International journal of advanced robotic systems, DOI: 10.5772/50912, 2012.

[15] Khan, M.K., Kim, S.K., Alghathbar, K., *Cryptanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme*, Computer Communications, 34 (3) (2011), 305-09.

[16] Rhee, H.S., Kwon, J.Q., Lee, D.H., *A remote user authentication scheme without using smart cards*, Computer standards & interfaces, 31 (1) (2009), 6-13.

[17] Khan, M.K., Zhang, J., *Improving the security of a flexible biometrics remote user authentication scheme*, Computer Standards & Interfaces, 29 (1) (2007), 82-85.

[18] Chen, B.L., Kuo, W.C., Wuu, L.C., *A secure password-based remote user authentication scheme without smart cards*, Information Technology and Control, 41 (1) (2012), 53-59.

[19] Jiang, Q., Ma, J.F., Li, G.S., Ma, Z., *An improved pssword-based remote user authentication protocol without smart cards*, Information technology and control, 42 (2) (2013), 150-158.

[20] Li, X.L., Wen, Q.Y., Zhang, H., Jin, Z.P., *An improved authentication with key agreement scheme on elliptic curve cryptosystem for global mobility networks*, International journal of network management, DOI: 10.1002/nem.1827, 2013.

Accepted: 29.09.2014