Improvement of Efficient and Secure Smart Card Based Password Authentication Scheme

Jongho Moon[1], Donghoon Lee[1], Jaewook Jung[1], and Dongho Won[2]
(Corresponding author: Dongho Won)

Department of Electrical and Computer Engineering, Sungkyunkwan University[1]
Department of Computer Engineering, Sungkyunkwan University[2]
Suwon 16419, Korea
(Email: dhwon@securiry.re.kr)
(Received Aug. 31, 2016; revised and accepted Nov. 15 & Dec. 25, 2016)

Abstract

Remote user authentication scheme is one of the most convenient authentication schemes to deal with secret data over public communication channel. In order to satisfy the security requirements, the smart card has become an essential device, one that is widely used. This is because its low computational cost and expedient portability. Recently, Liu et al. pointed out some security weaknesses in Li et al.'s scheme, such as man-in-the middle attack and insider attack. They hence claimed that their scheme is more secure and practical remote user authentication scheme. However, we find that Liu et al.'s scheme is still insecure against outsider attack and off-line password guessing attack. To overcome these security vulnerabilities, we propose a new authentication and key agreement scheme using smart card. In addition, we demonstrate that proposed authentication scheme has strong resistance to the various attacks. Finally, we compare the performance and functionality of the proposed scheme with other related schemes.

Keywords: Authentication; Biometrics; Elliptic Curve Cryptosystem; Smart Card

1 Introduction

Since Lamport [14] proposed the first password-based authentication scheme over insecure communication in 1981, password-based authentication schemes [1, 9, 10, 22, 25] have been extensively investigated. However, a main problem of password-based remote user authentication scheme is that a server must maintain a password table for verifying the legitimacy of a remote user. Therefore, the server requires additional memory space for storing the password table for verifying user identity. Furthermore, password is generally simple and can be easily broken or forgotten. For this reason, many researchers has proposed a new remote user authentication scheme by using biological characteristics of persons such as fingerprint, iris and so on. The main property of using biometric is its uniqueness. In the view of the fact that many remote user authentication schemes using biological characteristics [3, 16, 19, 20] have been proposed. In 2009, Xu et al. [21] proposed a novel user authentication and claimed that their scheme is secure against various attacks. However, Song [23] and Sood et al. [24] found that Xu et al.'s scheme has some weaknesses, and Sood et al. proposed an improved schemes. Subsequently, Chen et al. [2] pointed out that there are vulnerabilities on Song and Sood et al.'s schemes. Chen et al. then presented an enhanced version to solve the weaknesses. Recently, Li et al. [15] claimed that Chen et al.'s scheme is still insecure and proposed a modified smart card based remote user password authentication scheme. Unfortunately, Liu et al. [17] found that there are weaknesses in Li et al.'s scheme, such as the man-in-the-middle attack and insider attack, and proposed a novel scheme to defend against these security weaknesses. However, we found that Liu et al.'s scheme is still insecure against the outsider attack and off-line password guessing attack.

In this paper, we find that the security weaknesses of the two-factor authentication scheme by Liu et al. After careful analysis, we demonstrated their scheme does not actually resist off-line password guessing and user impersonation attacks. To overcome these security vulnerabilities, we propose a new biometrics-based authentication and key agreement scheme using smart card. In addition, we demonstrate that the proposed authentication scheme has strong resistance to various attacks, and compare the performance and functionality with other related schemes.

The rest of this paper is organized as follows. In Section 2, we briefly introduce some cryptographic definitions. In Section 3, we briefly review Liu et al.'s smart card-based password authentication scheme, and Section 4 analyzes its weaknesses. In Section 5, we propose new authentication scheme. Section 6 and 7 gives security and performance analysis of the proposed scheme.

Finally, we present the conclusion in Section 8.

2 Preliminaries

In this section, we briefly introduce the Elliptic curve cryptosystem, threat assumptions and fuzzy-extractor.

2.1 Elliptic Curve Cryptosystem

The elliptic curve cryptosystem (ECC) was first proposed by Koblitz [11] and Miller [18] to design public key cryptosystem, and presently it is widely used in several cryptographic schemes to provide desired level of security and performance [13]. For example, 160-bit ECC and 1024-bit RSA have the same security level in practice [8]. An elliptic curve E_K defined over a field K of the characteristic $\neq 2$ or 3 is the set of solutions $(x, y) \in K^2$ to the equation:

$$y^2 = x^3 + ax + b, \quad a, b \in K, 4a^3+27b^2 \neq 0.$$

Cryptosystems based on GF$(q)^*$ can be translated to systems using the group E, where E is an elliptic curve defined over GF(q). The point multiplications $kP = (P + P + ... + P, k$ times) that means k times addition of point P. Given an elliptic curve E defined over GF(q) and two points $P, Q \in E$, find an integer x such that $Q = xP$ if such x exists. This problem proved to be more intractable than the typically discrete logarithm problem. The details of the ECC definitions can be found in [11].

2.2 Threat Assumptions

We introduce the Dolev-Yao threat model [7] and consider the risk of side-channel attack [12] to construct the threat assumptions which are described as follows:.

1) An adversary $\mathcal{A}$ can be either a user or a server. A registered user can act as an adversary.

2) An adversary $\mathcal{A}$ can eavesdrop every communication in public channels. He/she can capture any message exchanged between user and server.

3) An adversary $\mathcal{A}$ has the ability to alter, delete or reroute the captured message.

4) Information can be extracted from the smart card by examining the power consumption of the card.

2.3 Fuzzy Extractor

We describe the basis of a biometric-based fuzzy extractor, which converts biometric information data into a random value. Based on Refs. [4, 5, 26], the fuzzy extractor is given by two procedures (Gen, Rep). The fuzzy extractor consists of two procedures (Gen, Rep).

- $Gen(BIO) \rightarrow \langle R, P \rangle$.
- $Rep(BIO^*, P) = R$ if BIO^* is reasonable close to BIO.

The function Gen is a probabilistic generation procedure, which on biometric input BIO outputs an "extracted" string $R \in \{0, 1\}^l$ and an auxiliary string $P \in \{0, 1\}^*$ and the function Rep is a deterministic reproduction procedure, which allows to recover R from the corresponding auxiliary string P and any vector BIO^* close to BIO. The detailed information about fuzzy extractor can be founded in literature [6].

3 Review of Liu et al.'s Scheme

In this section, we demonstrate Liu et al.'s smart card-based password authentication scheme [17] before demonstrating its weaknesses. Their scheme is an improvement of Li et al.'s scheme [15]. The notations used in Liu et al.'s scheme are listed in Table 1. Their scheme involves two entities, i.e., the user U_i and the server S, to communicate with each other to perform the following four phases: (1) The registration phase; (2) the login phase; (3) the authentication phase; and (4) the password change phase.

Table 1: The notations used in Liu et al.'s scheme

Term	Description
U_i	The i^{th} user
ID_i, PW_i	The identity and password of the user i
S	The server
x	The naster secret key stored in the S
T_i	The timestamp of the U_i
T_i'	The time of receiving the login request message
T_s	The timestamp of the server S
T_s'	The time of receiving the mutual authentication message
$h(\cdot)$	A secure hash function
$\oplus$	Exclusive-or operation
$\|$	Concatenation operation
sk	The shared session key

3.1 Registration Phase

At the beginning of the proposed scheme, the server S selects the master secret key x and a collision-free one-way hash function $h(\cdot)$. The user U_i then registers to the server S by the way below:

S1. The user U_i first selects his/her identity ID_i, password PW_i and a random number r, and then computes $h(r||PW_i)$. The U_i then submits $\{ID_i, h(r||PW_i)\}$ to the server S for registration over a secure channel.

S2. The server S computes the following parameters:

$$\begin{aligned} A_i &= h(ID_i \oplus x)||h(x), \\ B_i &= A_i \oplus h(r||PW_i), \\ C_i &= h(A_i||ID_i||h(r||PW_i)). \end{aligned}$$

S3. The server S stores the data $\{B_i, C_i, h(\cdot)\}$ on a new smart card and issues the smart card to the user U_i over a secure channel.

S4. The user U_i stores the random number r into the smart card.

3.2 Login Phase

This phase is invoked whenever the user U_i wants to login to the server S. These steps of the login phase are conducted as follows:

S1. The user U_i inserts his/her smart card into a card reader, and inputs his/her identity ID_i and password PW_i.

S2. The smart card first computes two parameters: $A_i' = B_i \oplus h(r||PW_i)$ and $C_i' = h(A_i'||ID_i||h(r||PW_i))$. Then, the smart card checks whether C_i' is equal to the stored C_i. If this holds, the smart card continues to perform the next step; otherwise, the smart card terminates this session.

S3. The smart card randomly generates a number α, and computes the following parameters:

$$\begin{aligned} D_i &= h(ID_i \oplus \alpha), \\ E_i &= A_i' \oplus \alpha \oplus T_i, \end{aligned}$$

where T_i is the current timestamp of the user U_i.

S4. The smart card sends the login request message $\{ID_i, D_i, E_i, T_i\}$ to the server S.

3.3 Authentication Phase

After completing this phase, the user U_i and the server S can mutually authenticate each other and establish a shared session key for the subsequent secret communication. These steps of the authentication phase are shown as follows:

S1. The server S verifies whether ID_i is valid and $T_i' - T_i \leq \triangle T$, where T_i' is the time of receiving the login request message and $\triangle T$ is a valid time threshold. If both conditions are true, the server S continues to execute Step 2; otherwise, the server S rejects the login request.

S2. The server S then computes the following parameters:

$$\begin{aligned} A_i' &= h(ID_i \oplus x)||h(x), \\ \alpha' &= E_i \oplus A_i' \oplus T_i, \\ D_i' &= h(ID_i \oplus \alpha'). \end{aligned}$$

Then, the server S checks whether D_i' is equal to the received D_i. If this holds, the server S confirms that the user U_i is valid and the login request is accepted; otherwise, the login request is rejected.

S3. The server S randomly generates a number β, and computes the following parameters:

$$\begin{aligned} F_i &= h(ID_i \oplus \beta), \\ G_i &= A_i' \oplus \beta \oplus T_s, \end{aligned}$$

where T_s is the current timestamp of the server S.

S4. The server S sends the mutual authentication message $\{F_i, G_i, T_s\}$ to the user U_i.

S5. Upon receiving the message $\{F_i, G_i, T_s\}$ from the S, the user U_i checks the validity of the T_s. If $T_s' - T_s \leq \triangle T$, where T_s' is the time of receiving the mutual authentication message, the user U_i continues to perform Step 6; otherwise, the user U_i terminates this connection.

S6. The user U_i computes $\beta' = G_i \oplus A_i' \oplus T_s$ and $F_i' = h(ID_i \oplus \beta')$, then checks whether F_i' equals to the received F_i. If they are equal, the validity of the server S is authenticated; otherwise, the session is terminated.

S7. The user U_i and the server S construct a shared session key $sk = h(\alpha'||\beta||h(A_i \oplus ID_i))$ to ensure the secret communication.

3.4 Password Change Phase

S1. The user U_i inserts his/her smart card into a card reader, enters his/her old identity ID_i and password PW_i, and requests to change the password.

S2. The smart card computes $A_i^* = B_i \oplus h(r||PW_i)$ and $C_i^* = h(A_i^*||ID_i||h(r||PW_i))$, and then checks whether C_i^* is equal to C_i that is stored in the smart card. If the equation holds, the user U_i submits the new password PW_i^{new}; otherwise, the smart card rejects the password change request.

S3. The smart card computes $B_i^{new} = A_i^* \oplus h(r||PW_i^{new})$ and $C_i^{new} = h(A_i^*||ID_i||h(r||PW_i^{new}))$. Then, the smart card replaces B_i andC_i with B_i^{new} and C_i^{new}, respectively.

4 Security Analysis of Liu et al.'s Scheme

Liu et al. claimed that their scheme could resist the various attacks. However, we find that their scheme is still insecure against the outsider and off-line password guessing attacks. The following attacks are based on the threat assumptions that a malicious adversary $\mathcal{A}$ was completely monitored through the communication channel connecting the U_i and S in the login and authentication phases, and obtained the information saved in their own smart card [7]. Thus, the $\mathcal{A}$ can eavesdrop, modify, insert, or delete any message transmitted via a public channel [14]. We now reveal the details of these problems.

4.1 Outsider Attack

The outsider is the person who has registered with the server S, not the person who is not the user of the system. In the registration phase, the server S stores $\{B_i, C_i, h(\cdot)\}$ on a smart card, and submits them to the user U_i. After receiving the smart card, the U_i stores the random number r into the smart card. Let $\mathcal{A}$ be an active adversary who is a legal user and owns a smart card to extract information $\{B_{\mathcal{A}}, C_{\mathcal{A}}, r_{\mathcal{A}}, h(\cdot)\}$. The $\mathcal{A}$ then can easily obtain $h(x)$ which is the same for each legal user belonging to the S.

$$h(ID_{\mathcal{A}} \oplus x)||h(x) = B_{\mathcal{A}} \oplus h(r_{\mathcal{A}}||PW_{\mathcal{A}}).$$

4.2 Off-line Password Guessing Attack

Suppose that an adversary $\mathcal{A}$ intercepts the communication messages $\{ID_i, D_i, E_i, T_i, F_i, G_i, T_s\}$ between the user U_i and the S, and steals the smart card of the U_i after login and authentication phase. The $\mathcal{A}$ then can extract the data $\{B_i, C_i, r, h(\cdot)\}$, and now perform an off-line password guessing to obtain the current password of the user U_i.

S1. The $\mathcal{A}$ selects a random password PW_i^*, calculates $h(ID_i \oplus E_i \oplus B_i \oplus h(r||PW_i^*) \oplus T_i)$, and compares it with D_i. If this holds, the adversary $\mathcal{A}$ infers that PW_i^* is the user U_i's password; otherwise, the $\mathcal{A}$ selects another password nominee, and performs the same processes, until he/she locates the valid password.

4.3 Not Support User Anonymity

Suppose an adversary $\mathcal{A}$ intercepts the communication messages $\{ID_i, D_i, E_i, T_i, F_i, G_i, T_s\}$, and then he/she can easily obtain the identity ID_i of the user U_i. We therefore concluded that Liu et al.'s scheme cannot provide user anonymity.

4.4 Not Support Perfect Forward Secrecy

Liu et al. claimed that even if an adversary obtained the server S's master secret key x, he/she cannot derive the previous session key sk because α and β are encrypted into the ciphertext D_i and F_i, respectively. Therefore, the $\mathcal{A}$ cannot obtain α and β. However, if the $\mathcal{A}$ obtain the server S's master secret key x, then he/she can easily obtain α and β. Suppose that an adversary $\mathcal{A}$ intercepts the communication messages $\{ID_i, D_i, E_i, T_i, F_i, G_i, T_s\}$. The $\mathcal{A}$ can then compute $\alpha = E_i \oplus (h(ID_i \oplus x)||h(x)) \oplus T_i$ and $\beta = G_i \oplus (h(ID_i \oplus x)||h(x)) \oplus T_s$.

5 The Proposed Scheme

In this section, we propose a new biometric-based password authentication scheme using smart card. In the proposed scheme, there are also two participants, the user U_i and the server S. The proposed scheme consists of four phases: registration, login, authentication, password changing phase. For convenience, some notations used in the proposed scheme are described in Table 2.

Table 2: The notations used in the proposed scheme

Term	Description
U_i	The i^{th} user
ID_i, PW_i	The identity and password of the user i
S	The server
x	The master secret key stored in the S
P	The base point of the elliptic curve E
rP	The point multiplication defined as $rP = \underbrace{P + P + \cdots + P}_{r \ times}$
T_i	The timestamp of the user U_i
T_i'	The time of receiving the login request message
T_s	The timestamp of the S
T_s'	The time of receiving the mutual authentication message
R_i, P_i	The U_i's nearly random binary string and auxiliary binary string
$h(\cdot)$	A collision-resistant hash function
$\oplus$	Exclusive-or operation
$\|\|$	Concatenation operation
sk	The shared session key

5.1 Registration Phase

At the beginning of the proposed scheme, the server S selects the master secret key x, the base point P of the elliptic curve E and a collision-resistant one-way hash function $h(\cdot)$. Then, the user U_i registers to the server S by the way below:

S1. The U_i imprints the personal biometric information BIO_i at the sensor. The sensor then scans the BIO_i, extracts (R_i, P_i) from $Gen(BIO_i) \rightarrow (R_i, P_i)$, and stores P_i in the memory. Next, the U_i selects the identity ID_i and password PW_i, and computes $RPW_i = h(PW_i||R_i)$. Lastly, the U_i sends the registration request message $\{ID_i, RPW_i\}$ to the S over a secure channel.

S2. After receiving the registration request message from the U_i, the server S verifies whether ID_i is valid, and computes the following parameters:

$$\begin{aligned} A_i &= h(ID_i \oplus x), \\ B_i &= h(A_i) \oplus RPW_i, \\ C_i &= h(ID_i||RPW_i), \\ D_i &= x \oplus A_i \oplus h(x). \end{aligned}$$

S3. The server S stores the data $\{B_i, C_i, D_i, h(\cdot), P\}$ on a new smart card and issues the smart card to the user U_i over a secure channel.

S4. The user U_i stores the random string P_i into the smart card.

5.2 Login Phase

This phase is invoked whenever the user U_i wants to login to the server S. The steps of this phase are conducted as follows.

S1. The U_i inserts his/her smart card into the card reader and enters the identity ID_i and password PW_i, and imprints the biometrics BIO_i^* at the sensor. The sensor then sketches BIO_i^* and recovers R_i from $Rep(BIO_i^*, P_i) \rightarrow R_i$.

S2. The smart card first computes two parameters: $RPW_i = h(PW_i||R_i)$ and $C_i' = h(ID_i||RPW_i)$. The smart card then examines whether C_i' is equal to the stored C_i. If this holds, the smart card continues to perform Step 3; otherwise, the smart card terminates this session.

S3. The smart card randomly generates a number α and n_i, and computes the following parameters:

$$\begin{aligned} h(A_i) &= B_i \oplus RPW_i, \\ AID_i &= ID_i \oplus h(A_i), \\ E_i &= \alpha P, \\ F_i &= h(ID_i||h(A_i)||E_i||T_i), \end{aligned}$$

where T_i is the current timestamp of the user U_i.

S4. The smart card sends the login request message $\{AID_i, D_i, E_i, F_i, T_i\}$ to the server S.

5.3 Authentication Phase

Upon completing this phase, the user U_i and the server S can mutually authenticate each other and establish a shared session key for the subsequent secret communication. These steps of the authentication phase are shown as follows:

S1. The server S verifies whether $T_i' - T_i \leq \triangle T$, where T_i' is the time of receiving the login request message and $\triangle T$ is a valid time threshold. If both conditions are true, the server S continues to execute Step 2; otherwise, the server S rejects the login request.

S2. The server S computes the following parameters:

$$\begin{aligned} A_i' &= D_i \oplus x \oplus h(x), \\ ID_i' &= AID_i \oplus h(A_i'), \\ F_i' &= h(ID_i'||h(A_i')||E_i||T_i). \end{aligned}$$

The server S then compares whether F_i' is equals F_i. If this holds, the server S confirms that the user U_i is valid and the login request is accepted; otherwise, the server S rejects the login request.

S3. Next, the server S randomly generates a number β and computes the following parameters:

$$\begin{aligned} F_i &= \beta P, \\ G_i &= h(ID_i'||h(A_i')||F_i||T_s), \end{aligned}$$

where T_s is the current timestamp of the server S.

S4. The server S sends the mutual authentication message $\{F_i, G_i, T_s\}$ to the user U_i.

S5. Upon receiving the message $\{F_i, G_i, T_s\}$ from the S, the user U_i checks the validity of the T_s. If $T_s' - T_s \leq \triangle T$, where T_s' is the time of receiving the mutual authentication message, the user U_i continues to perform Step 6; otherwise, the user U_i terminates this connection.

S6. The user U_i computes $G_i' = h(ID_i||h(A_i)||F_i||T_s)$, then checks whether G_i' is equal to the received G_i. If this holds, the validity of the server S is authenticated; otherwise, the session is terminated.

S7. Finally, the user U_i and the server S construct a shared session key $sk = \alpha\beta P$ to ensure the secret communication.

5.4 Password Change Phase

During the password change phase, U_i updates the password without any assistance from server S_j. This phase consists of the following steps:

S1. The U_i enters the identity ID_i and password PW_i, and imprints the biometrics BIO_i^* at the sensor. The sensor then scans BIO_i^*, and recovers R_i from $Rep(BIO_i^*, P_i) \rightarrow R_i$.

S2. Next, the SC_i calculates $RPW_i = h(PW_i||R_i)$, and checks whether $h(ID_i||RPW_i)$ is equal to the stored C_i. If this holds, the smart card asks the U_i for a new password; otherwise, the SC_i immediately terminates the password change phase.

S3. The U_i inputs new password PW_i^{new}, and the smart card further computes $RPW_i^{new} = h(PW_i^{new}||R_i)$, $B_i^{new} = B_i \oplus RPW_i \oplus RPW_i^{new}$ and $C_i^{new} = C_i \oplus RPW_i \oplus RPW_i^{new}$.

S4. Finally, the smart card replaces B_i with B_i^{new} and C_i with C_i^{new} in memory.

6 Security Analysis of The Proposed Scheme

In this section, we demonstrate that the proposed scheme, which retains the merits of Liu et al.'s scheme, can withstand several types of possible attacks; and we also show that the proposed scheme supports several security properties. The security analysis of the proposed scheme was conducted with the threat assumptions made in the Section 2.

6.1 Resisting Outsider Attack

The outsider is the person who has registered with the server S, not the person who is not the user of the system. Suppose an outsider adversary $\mathcal{A}$ extracts all of the information $\{B_{\mathcal{A}}, C_{\mathcal{A}}, D_{\mathcal{A}}, h(\cdot), P, P_{\mathcal{A}}\}$ from own smart card by side channel attack [12]. However, he/she cannot obtain any secret information of the S. The $\mathcal{A}$ can compute $h(A_{\mathcal{A}}) = B_{\mathcal{A}} \oplus RPW_{\mathcal{A}}$. However, the value x is a master secret key stored in the server S. Therefore, $\mathcal{A}$ does not know, and the proposed scheme can resist outsider attack.

6.2 Resisting Insider Attack

The insider is the authorized users of the server who access data or resources. In the registration phase, the user conceals the password in a ciphertext from the server S to resist an insider attack. More specifically, the user U_i first selects their password PW_i, and then submits $RPW_i = h(PW_i||R_i)$ to the server S for the registration over a secure channel. The S cannot retrieve the password PW_i or biometrics BIO_i from $RPW_i = h(PW_i||R_i)$. In addition, the S does not store RPW_i in the database. The proposed scheme therefore can resist insider attack.

6.3 Resisting User Impersonation Attack

Suppose an adversary $\mathcal{A}$ intercepts all of the message $\{D_i, E_i, F_i, T_i, F_i, G_i, T_s\}$ transmitted in public channel between the U_i and S, and steals the smart card of the U_i, then extracts the all of the information $\{B_i, C_i, D_i, h(\cdot), P, P_i\}$. However, the $\mathcal{A}$ cannot generate the legal login request message $\{AID_i, D_i, E_i, F_i, T_i\}$, where $AID_i = B_i \oplus h(A_i)$, $D_i = x \oplus A_i \oplus h(x)$, $E_i = \alpha P$, and $F_i = h(ID_i||h(A_i)||E_i||T_i)$. This is because the value $h(A_i)$ is protected by $RPW_i = h(PW_i||R_i)$, and the A_i is protected by server S's master key x. The user U_i's password is protected by collision resistant one-way hash function, such as, $h(PW_i||R_i)$, where R_i possesses high entropy. Moreover, there is no the same biometric templates between any two people. The $\mathcal{A}$ cannot generate the mutual authentication message $\{F_i, G_i, T_s\}$ without the value $h(A_i)$. The proposed scheme can therefore resist user impersonation attack.

6.4 Providing Perfect Forward Secrecy

The perfect forward secrecy means that if one of long-term keys is compromised, a session key which is derived from these long-term keys will not be compromised in the future [27]. In the proposed scheme, a session key between the user U_i and server S is calculated as follows:

$$\begin{aligned} E_i &= \alpha P, \\ F_i &= \beta P, \\ sk &= \alpha\beta P. \end{aligned}$$

Even if the server S's long-term key x is compromised, the adversary $\mathcal{A}$ cannot retrieve α and β to generate the session keys between the U_i and S. The session key of the proposed scheme is based on elliptic curve discrete logarithm problem. The adversary $\mathcal{A}$ cannot obtain $\alpha\beta P$ from the αP and βP. Above all, the scheme achieves the perfect forward secrecy.

7 Performance Analysis

In this section, we compare the functionality between the proposed scheme and the other recent schemes [2, 10, 15, 16, 17, 23, 25]. From Table 4, we can see that all of other existing schemes involve some time-consuming operations, such as modulus exponential operations, symmetric encryption/decryption operations, multiplication/division operations and scalar multiplication. From this comparison, we can see that the hash operation costs of the proposed scheme are slightly lower than the authentication scheme by Liu et al., and the proposed scheme performs four further scalar multiplication functions and four fuzzy-extraction functions than Liu et al.'s scheme to accomplish mutual authentication and key agreement; however, the proposed scheme archives perfect forward secrecy.

Table 3: Functionality comparison of the proposed scheme and other related schemes

	F1	F2	F3	F4	F5	F6	F7	F8	F9
Juang et al. [10]	○	○	○	○	○	○	×	○	○
Sun et al. [25]	○	○	×	○	○	○	○	○	○
Li et al. [16]	○	○	○	○	○	○	○	○	○
Song [23]	○	○	○	○	×	○	×	○	○
Chen et al. [2]	○	○	○	○	×	○	×	○	○
Li et al. [15]	○	○	○	×	×	○	○	○	○
Liu et al. [17]	○	○	○	○	○	○	×	○	×
The proposed	○	○	○	○	○	○	○	○	○

F1: Mutual authentication; F2: Session key agreement; F3: Freely chosen and exchanged password; F4: Withstanding man in the middle attack; F5: Withstanding insider attack; F6: Withstanding replay attack; F7: Providing perfect forward secrecy; F8: Satisfying known-key security; F9: User impersonation attack.

Table 4: Computational cost comparison of the proposed scheme and other related schemes

	C1	C2	C3	C4	C5	C6	Total
Juang et al. [10]	1H	2H+3S	3H+3S	4H+6S+1M	1H+5S	1H+5S	12H+22S+1M
Sun et al. [25]	-	2H+1S	4H+2M	4H+1S+2M	2H	-	12H+2S+4M
Li et al. [16]	1H	2H+3S	8H+4S	10H+10S+1M	1H+6S	1H+9S	23H+32S+1M
Song [23]	-	2H+1E	3H+1S	3H+1S+1E	-	-	8H+2S+2E
Chen et al. [2]	-	1H+1E	2H+2M+4E	1H+1M+4E	3H+2M+2E	3H+2M+3E	10H+14E+7M
Li et al. [15]	-	2H+2E	4H+1M+4E	3H+3E	3H+2M+4E	-	12H+3M+13E
Liu et al. [17]	1H	3H	6H	6H	4H	-	20H
The proposed	1H+1F	4H	4H+1F+2P	3H+1F+2P	3H+1F	-	15H+4F+4P

C1: Computational cost of the user in registration phase; C2: Computational cost of the server in registration phase; C3: Computational cost of the user in login and authentication phases; C4: Computational cost of the server in login and authentication phases; C5: Computational cost of the user in password change phase; C6: Computational cost of the server in password change phase; H: Hashing operation; E: Modulus exponential operation; S: Symmetric encryption/decryption operation; M: Multiplication/division operation; Null: P: Scalar multiplication; F: Fuzzy extraction; Null: Cannot provide this functionality.

8 Conclusions

In this paper, we proposed a biometrics-based user authentication scheme using smart card to overcome the security weaknesses of Liu et al.'s scheme. The proposed scheme can achieve mutual authentication and perfect forward secrecy, and users can freely choose and change their password. We prove that the proposed scheme can resist various attacks, such as the outsider attack and user impersonation attack.

Acknowledgments

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.R0126-15-1111, The Development of Risk-based Authentication·Access Control Platform and Compliance Technique for Cloud Security)

References

[1] N. Anwar, I. Riadi, A. Luthfi, "Forensic SIM card cloning using authentication algorithm," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 71–81, 2016.

[2] B. L. Chen, W. C. Kuo and L. C. Wuu, "Robust smart-card-based remote user password authentication scheme," *International Journal of Communication Systems,* vol. 27, no. 2, pp. 377–389, 2014.

[3] Y. Choi, Y. Lee and D. Won, "Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction," *International Journal of Distributed Sensor Networks,* vol. 2016, pp. 1–16, 2016.

[4] A. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *International Journal of Communication Systems,* vol. 30, no. 1, pp. 1–25, 2017.

[5] Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin and A. Smith, "Robust fuzzy extractors and authenticated key agreement from close secrets," *IEEE Transactions on Information Theory,* vol. 58, no. 9, pp. 6207–6222, 2012.

[6] Y. Dodis, L. Reyzin and A. Smith, "Fuzzy extractors:How to generate strong keys from biometrics and other noisy data," *Advances in Cryptology (EUROCRYPT'04),* LNCS 3027, pp. 523–540, Springer, 2004.

[7] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory,* vol. 29, no. 2, pp. 198–208, 1983.

[8] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, Berlin, 2004.

[9] W. Jeon, J. Kim, J. Nam, Y. Lee and D. Won, "Two-round password-only authenticated key exchange in the three-party setting," *IEICE Transactions on Communications,* vol. 95, no. 5, pp. 1819–1821, 2012.

[10] W. S. Juang, S. T. Chen and H. T. Liaw, "Robust and efficient password-authenticated key agreement using smart card," *IEEE Transactions on Industrial Electronics,* vol. 55, no. 6, pp. 2551–2556, 2008.

[11] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 117, pp. 203–209, 1987.

[12] P. Kocher, J. Jaffe, B. Jun and P. Rohatgi, "Introduction to differential power analysis," *Journal of Cryptographic Engineering,* vol. 1, no. 1, pp. 1–23, 2011.

[13] A. V. N. Krishna, A. H. Narayana, K. M. Vani, "Window method based cubic spline curve public key cryptography," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 94–102, 2016.

[14] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM,* vol. 24, no. 11, pp. 770–772, 1981.

[15] X. Li, J. Niu, M. K. Khan, and J. Liao, "An enhanced smart card based remote user password authentication scheme," *Journal of Network and Computer Applications,* vol. 36, no. 5, pp. 1365–1371, 2013.

[16] X. Li, W. D. Qiu, D. Zheng, K. F. Chen, and J. H. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," *IEEE Transactions on Industrial Electronics,* vol. 57, no. 2, pp. 793–800, 2010.

[17] Y. Lin, C. C. Chang and S. C. Chang, "An efficient and secure smart card based password authentication scheme," *International Journal of Network Security,* vol. 19, no. 1, pp. 1–10, 2017.

[18] V. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology (CRYPTO'85)*, vol. 218, pp. 417–426, 1985.

[19] J. Moon, Y. Choi, J. Jung and D. Won, "An improvement of robust biometrics-based authentication and key agreement scheme for multi-server environments using smart cards," *Plos One,*, vol. 10, no. 12, pp. 1–15, 2015.

[20] J. Moon, Y. Choi, J. Kim and D. Won. "An improvement of robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps," *Journal of Medical Systems*, vol. 40, no. 3, pp. 1–11, 2016.

[21] J. Moon, J. Kim and D. Won, "An improvement of user authentication framework for cloud computing," *Journal of Conputers,* vol. 11, no. 6, pp. 446–454, 2016.

[22] J. Nam, K. K. R. Choo, S. Han, J. Paik and D. Won, "Two-round password-only authenticated key exchange in the three-party setting," *Symmetry,* vol. 7, no. 1, pp. 105–124, 2015.

[23] R. Song, "Advanced smart card based password authentication protocol," *Computer Standards and Interfaces*, vol. 32, no. 5, pp. 321–325, 2010.

[24] S. K. Sood, A. K. Sarje, and K. Singh, "An improvement of Xu et al.'s authentication scheme using smart cards," in *Proceedings of the Third Annual ACM Bangalore Conference,* pp. 17–22, Bangalore, Karnataka, India, 2010.

[25] D. Z. Sun, J. P. Huai, J. Z. Sun, J. X. Li, J. W. Zhang, and Z. Y. Feng, "Improvements of Juang et al.'s password-authenticated key agreement scheme using smart cards," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 6, pp. 2284–2291, 2009.

[26] C. Wang, X. Zhang and Z. Zheng, "Cryptanalysis and improvement of a biometric-based multi-server authentication and key agreement scheme," *Plos One,* vol. 11, no. 2, pp. 1–25, 2016.

[27] H. Zhu and X. Hao, "A provable authenticated key agreement protocol with privacy protection using smart card based on chaotic maps," *Nonlinear Dynamics,* vol. 81, no. 1, pp. 311–321, 2015.

Biography

Jongho Moon received the B.S. degree in electrical and computer engineering from Sungkyunkwan University, Suwon, Korea, in 2012 and the M.S. degree in electrical and computer engineering from Sungkyunkwan University, Suwon, Korea, in 2014. He also worked as a malware analyzer in SECUI between 2014 and 2015. He is currently pursuing the Ph.D. degree in electrical and computer engineering at Sungkyunkwan University,

Suwon, Korea. His current research interest includes cryptography, malware, forensic, and authentication or key management protocols.

Donghoon Lee received the B.S. degree in Computer Science from National Institute for Lifelong Education(NILE), Korea, in 2009 and the M.S. degree in Information Security Engineering from Sungkyunkwan University, Korea, in 2011. He is currently undertaking a Ph.D. course on Electrical and Computer Engineering in Sungkyunkwan University. His current research interest is in the area of software security, cryptography, authentication protocol, and network security.

Jaewook Jung received the B.S. degree in Electrical and Computer Engineering from Korea Aerospace University, Goyang, Korea, in 2010 and the M.S. degree in Electrical and Computer Engineering from Sungkyunkwan University, Suwon, Korea, in 2012. He is currently undertaking a Ph.D. course on Electrical and Computer Engineering in Sungkyunkwan University, Suwon, Korea. His current research interest is in the area of cryptography, forensic, authentication protocol, and mobile security.

Dongho Won received B.S., M.S. and Ph.D. in Electronic Engineering from Sungkyunkwan University, Suwon, Korea. After working in Electronics and Telecommunication Research Institute for two years, he joined Sungkyunkwan University, where he is currently a leader professor at Information and Communication Engineering. He also served as a President of Korea Institute of Information Security and Cryptography. His research interests are cryptology and information security.