Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **2**, April **2014**

A Multi-function Password Mutual Authentication Key Agreement Scheme with Privacy Preservingg

Tian-Hua Liu[1], Qian Wang[2], Hong-Feng Zhu[3]

[1,2,3]Software College,
Shenyang Normal University,
No.253, HuangHe Bei Street, HuangGu District, Shenyang, 110034, China
liutianhua@sina.com[1], Janewang215@foxmail.com[2], zhuhongfeng1978@163.com[3]

Received December, 2012; revised October, 2013

Abstract. *Mutual authentication and key agreement is important for providing secure remote communication in client-server environment. In this paper, the authors show that the latest related schemes proposed by Shen and Du, and Jiang et al. are vulnerable to a strong variant of off-line guessing attack. Then introduce a novel multi-function password authentication key agreement scheme with smart card based on elliptic curve cryptosystem and one-way hash function. It can not only achieve privacy preserving, resist the strong variant of off-line guessing attack but also retain most previously proposed merits without timestamp. The functions of this kind of scheme are firstly classified into auxiliary function and essential function. By comparing the properties with other related schemes, our scheme satisfies more functionality features with normal computation and communication cost, and is practical in pervasive and ubiquitous computing environment.*

Keywords: Authentication, Key agreement, Smart card, Privacy preserving, Secure breach

1. **Introduction.** As is known to all, with the development of computer network technologies, various resources and services are shared across the Internet provided by remote servers. The worldwide proliferation of using wireless portable devices and mobile social network service help our life become more intelligent and convenient. Nevertheless, wireless client-server communication in the public insecure channels is facing more challenges in two aspects.

On one hand, the interaction and computation abilities of both client and adversary are enhanced at the same time. Legal registered clients request services from the remote server while adversaries may impersonate to login into the server or break down the scheme. In this way, mutual authentication and key agreement is an important issue of designing protocol especially in wireless communication. On the other hand, in a new era of cloud computing and big data, sensitive identity information of clients may be extracted from the transmission messages and mined for business marketing tactics or for password guessing attack. Population ageing also stimulates the research about privacy protection of healthcare information systems. Thus, from the point of view of privacy and security, client privacy as well as resistance of well-known attacks should be concerned to realize the communication scheme with multi-function. Smart card and password based remote authentication scheme is one of the most significant two-factor mechanisms to achieve the requirement mentioned above.

To preserve the user privacy, it is desirable that the users' identities are hidden while executing authentication procedure simultaneously. User authentication without revealing users identity can be divided into two categories, protocols with anonymous channels allow the users to be authenticated to the server, and anonymous authentication protocols allow users to prove the legitimacy to the server. Here we proposed an efficient anonymous authentication key agreement scheme that users sensitive information such as identities and passwords are protected by one-way hash function.

1.1. **Related Work.** The history of password authentication schemes with smart card can trace back to the remote user authentication environment. Since 1981, Lamport[1] proposed a remote authentication scheme with a password table for verifying the legitimacy of the login users over insecure communication. This scheme and its transformations were later discovered vulnerable to host-impersonate attack[2] and modification attack[3]. Hwang et al.[4] proposed an authentication scheme using smart cards based on the Shamir's ID-based signature scheme[5]. Since then, a variety of ID-based remote user authentication schemes were proposed based on bilinear pairings and elliptic curve cryptosystem [6-9].

In 2000, Hwang and Li.[10] proposed a new remote user authentication scheme using smart card based on the ElGamal's public key cryptosystem without a verification table to check the authenticity of the login request but the passwords were determined by the system. However, Chan and Cheng [11], Shen et al.[12] pointed out different attacks to Hwang and Li's scheme[10]. In 2002, Chien et al.[13] proposed a new efficient and practical solution to remedy the flaws in Sun's scheme[14] where it neither allow users freely choosing password nor achieving mutual authentication. In 2004, Ku and Chen[15], Hsu[16] pointed out reflection attack, insider attack, not reparable, and parallel session attack on Chien et al.'s scheme[13] and also proposed an improvement scheme. In the same year, Lee et al.[17] enhanced Chien et al.'s scheme[13] by eliminating parallel session attack. One year later, Yoon and Yoo[18] showed that Lee et al.'s scheme[17] was also vulnerable to some insidious attacks, such as masquerading server attack. Besides, Lee and Chiu[19] proposed a password authentication scheme which was claimed to be an improvement of Wu and Chieus[20]. In 2009, Xu et al.[21] put forward a forgery attack on Lee and Chiu's scheme[19] and a password guessing attack on Lee et al.'s scheme[22]. Soon after that, Song[23] detailed the potential attack on Xu et al.'s scheme[21] and suggested a new efficient strong smart card based password authentication protocol.

More recently, password authentication scheme with smart card based on elliptic curve cryptography (ECC) are proposed to be better than the previous research using bilinear pairings or RSA cryptosystem. Li et al.[24] showed several weaknesses in Kim et al.'s scheme[25] and designed a more secure, robust and practical scheme for portable devices based on the discrete logarithm on elliptic curve without timestamp. In 2013, Tang et al.[26] reviewed Awasthi et al.'s scheme[27], discussed attacks against it, and proposed a timestamp-based mutual authentication scheme using smart card and ECC with the clock synchronization problem unsolved. Shen and Du[28] also reviewed and cryptanalysed Kim et al.'s scheme[25], then improved Li et al.'s[29] scheme in which smart card security breach was proposed. Considering the auxiliary function, for instance, preserving user privacy, we show Jiang et al.'s scheme[30] doesn't resist the basic password guessing attack.

1.2. **Our Contributions.** In this paper, we classify the functions of password authentication key exchange scheme based on smart card into two types, essential function and auxiliary function . Then, we propose a strong off-line guessing attack called stealing card and eavesdropping off-line guessing attack, SEG attack for short. After pointing out

SEG attack flaws in recent schemes, we raise a strong multi-function scheme with privacy preserving more efficient and secure by comparing with the related research.

1.3. **Organization.** The structure of our paper is organized as follows. In next section, we introduce some preliminaries. In section 3, we recall and cryptanalyse Shen and Du's scheme[28] and Jiang et al.'s scheme[30]. Section 4 demonstrates our proposed scheme. Section 5 presents the evaluations of essential function and auxiliary function including security and performance of the proposed scheme. Finally, we present our conclusions in Section 6.

2. **Preliminaries.** In this section, we present some fundamental backgrounds.

2.1. **One-way Hash Function.** A secure cryptographic one-way hash function $h : a \to b$ has four main properties:

(1) The function h takes a message of arbitrary length as the input and produces a message digest of fixed-length as the output;
(2) The function h is one-way in the sense that given a, it is easy to compute $h(a) = b$. However, given b, it is hard to compute $h^{-1}(b) = a$;
(3) Given a, it is computationally infeasible to find a' such that $a' \neq a$, but $h(a') = h(a)$;
(4) It is computationally infeasible to find any pair a, a' such that $a' \neq a$, but $h(a') = h(a)$.

2.2. **Elliptic Curves Cryptography.** The security of ECC is based on the difficulty of solving the following problems, readers can get more about ECC refering to [31],:

(1) Elliptic curve discrete logarithm problem (ECDLP): Suppose that given a point element $Q = x \times G$, it is hard to find an integer $x \in Z_n^*$, where $x \times G$, means that the point G is added by itself for x times in the elliptic curve cryptosystem and x is chosen randomly and is smaller than n.
(2) Computational Diffie-Hellman problem (CDHP): Suppose that given three points G, $x \times G$, and $y \times G$, it is hard to calculate $x \times y \times G$, where x, $y \in Z_n^*$ are smaller than n.
(3) Elliptic curve Diffie-Hellman problem (ECDHP): Suppose that given a point $x \times y \times G$, the elliptic curve Diffie-Hellman problem is to find the two points $x \times G$ and $y \times G$.

2.3. **SEG Attack.** SEG attack is a strong variant of off-line guessing attack assuming that the adversary has full control over the insecure channel including eavesdropping, recording, intercepting, modifying the transmitted messages. Besides it could steal the smart card or other mobile devices for the stored information. Three instances of this kind of attack can be illustrated as: (1) Eavesdropping all the transmission messages, then the adversary steals or picks up any smart card for further guessing attack; (2) Eavesdropping certain users' transmission messages and then the adversary steals the corresponding smart cards for extracting and guessing sensitive information. After that, the adversary returns the smart cards without users' awareness; (3) Secretly adding small device in the card reader, the adversary can obtain both the information of the smart card and the transmission message of certain users. The more ability and secretiveness adversaries have the more practical significance it has to our proposed scheme.

In the final analysis, the capacity of adversaries is increasing and redundant information will help them acquire the secrets by guessing attack.

3. **Cryptanalysis of Shen and Du's Scheme and Jiang et al.'s Scheme.** In this section, we give a brief review and cryptanalysis of Shen and Du's Scheme[28] and Jiang et al.'s Scheme[30].

3.1. **Review of Shen and Du's Scheme.** The FIGURE 1 below shows registration phase, login and verification phase, and session key agreement phase in Shen and Du's Scheme[28] whose password changing phase is omitted.

3.2. **Attack in Shen and Du's Scheme.** As shown in FIGURE 1, the login and verification phase in Shen and Du's scheme[28], after verifying the validity of the current time of the server TS, user's smart card further checks if $H(H(D\oplus H(H(pw_i^*)\oplus s)\oplus E^{new})\oplus T_S)$, equals to the received M_2, Here, D and s can be extracted from the smart card by some physical methods[32-33]. E^{new}, M_2, and T_S are transmitted in plaintext whichcan be easily intercepted by the adversary. Then the adversary carries out SEG attack by checking if $M_2 \stackrel{?}{=} H(H(D \oplus H(H(pw_i^*) \oplus s) \oplus E^{new}) \oplus T_s)$, for each candidate password pw_i. Thus, Shen and Du's scheme couldn't satisfy the secure requirement, resistance of SEG attack without additional session key, of this kind of scheme.

3.3. **Review of Jiang et al.'s Scheme.** Jiang et al.'s Scheme[30] consists of five phases: parameter-generation, registration, authentication, password changing and smart card recocation. For the sake of simplicity, we show the first three phases in FIGURE 2.

3.4. **Weakness in Jiang et al.'s Scheme.** Similarly, the adversary can extract V from the smart card as in Jiang et al.'s scheme[30]. Only after the first transmission message $\langle IM_0, {G_C}'\rangle$ from user to the server in the authentication phase can ${G_C}'$ be intercepted by the adversary with ${G_C}' = r_C \times G$ which is the public parameter. Besides, $V' = V - h(pw)$, ${G_C}' = G_C + V'$, so that SEG attack can be carried out by checking if ${G_C}' - G_C \stackrel{?}{=} V - h(pw^*)$, pw^* is the adversary's guess of pw while other parameters are known to the adversary. Here, Jiang et al. prefer minus operation to the usual XOR operation maybe for increasing the efficiency in the parameter generation phase. However, it is easier for the adversary to attack the scheme under the same condition. Then it is even easier for the adversary to replace the old password by the new one as is descripted in the password changing phase.

With the above related work and cryptanalysis of the latest two schemes, it is not difficult to see that design a robust password authentication scheme with smart card is a nontrivial and challenging task.

4. **Our Proposed Scheme.** In this section, our proposed scheme is described in detail containing four phases: initialization phase; registration phase; authentication and key agreement phase; password changing phase. The notations used in our scheme are summarized as follows:

U_i: One of the legal users to communicate with the server.
S: The remote server.
ID_i: The identity of U_i.
r_i: The random number chosen by U_i.
r_s: The secret key maintained by S.
R_i/R_s: The public key of U_i/S.
K_i: The session key between U_i and S.
$\oplus$: The exclusive or operation.
$||$: The string concatenation operation.
$h(\bullet)$: A public collision - free one - way hash function with an arbitrary - length input and an output string $\{0,1\}^l$, where l is a secure parameter determining the length of the output.

U_i the user	SC_i smart card	S the server
Registration phase:		
chooses ID_i	ID_i, registration request — secure channel →	chooses random numbers r, b, master key x; computes $E = H(ID_i \oplus x \oplus r) \oplus b$, $\overline{D} = H(ID_i \oplus x \oplus b)$
chooses password pw_i	← $\langle ID_i, r, E, \overline{D} \rangle$ to SC_i; SC_i to U_i — secure channel; pw_i — secure channel →	chooses random number s; computes $D = \overline{D} \oplus H(H(pw_i) \oplus s)$; keeps $\langle ID_i, r, E, D, s \rangle$
Login and verification phase:		
pw_i — secure channel →	takes current timestamp T_{U_i}; computes $M_1 = H(H(D \oplus H(H(pw_i) \oplus s) \oplus E) \oplus T_{U_i})$	
	$\langle ID_i, r, E, M_1, T_{U_i} \rangle$ →	verifies T_{U_i}; derive b from $b = E \oplus H(ID_i \oplus x \oplus r)$; checks $H(H(H(ID_i \oplus x \oplus r) \oplus E) \oplus T_{U_i}) \stackrel{?}{=} M_1$; chooses new random numbers r^{new}, b^{new}; takes current timestamp T_S; computes $E^{new} = H(ID_i \oplus x \oplus r^{new}) \oplus b^{new}$, $\overline{D}^{new} = H(H(ID_i \oplus x \oplus b) \oplus r^{new}) \oplus H(ID_i \oplus x \oplus b^{new})$, $M_2 = H(H(H(ID_i \oplus x \oplus b) \oplus E^{new}) \oplus T_S)$, $M_3 = H(H(H(ID_i \oplus x \oplus b) \oplus \overline{D}^{new}) \oplus T_S)$
	verifies T_S ← $\langle r^{new}, E^{new}, \overline{D}^{new}, M_2, M_3, T_S \rangle$	
	checks $H(H(D \oplus H(H(pw_i) \oplus s) \oplus E^{new}) \oplus T_S) \stackrel{?}{=} M_2$, $H(H(D \oplus H(H(pw_i) \oplus s) \oplus \overline{D}^{new}) \oplus T_S) \stackrel{?}{=} M_3$; chooses new random number s^{new} replace s; computes $D^{new} = H(D \oplus H(H(pw_i) \oplus s) \oplus r^{new}) \oplus \overline{D}^{new} \oplus H(H(pw_i) \oplus s^{new})$; changes E, D, r, s into $E^{new}, D^{new}, r^{new}, s^{new}$	
Session key agreement phase: Suppose the server and smart cards share a cyclic group G of large enough order l with generator $g \in G$		
		chooses random number $\alpha \in [1, l-1]$; computes $K = H(H(ID_i \oplus x \oplus b^{new}) \oplus r^{new}) \oplus g^{\alpha}$
	derive g^{α} from $H(H(ID_i \oplus x \oplus b^{new}) \oplus r^{new}) \oplus K$ ← $\langle K \rangle$	
	chooses random number $\beta \in [1, l-1]$; computes $K' = H(D^{new} \oplus H(H(pw_i) \oplus s^{new}) \oplus r^{new}) \oplus g^{\beta}$	
	$\langle K' \rangle$ →	
	session key: $g^{\alpha\beta}$	

FIGURE 1. Part of Shen and Du's scheme

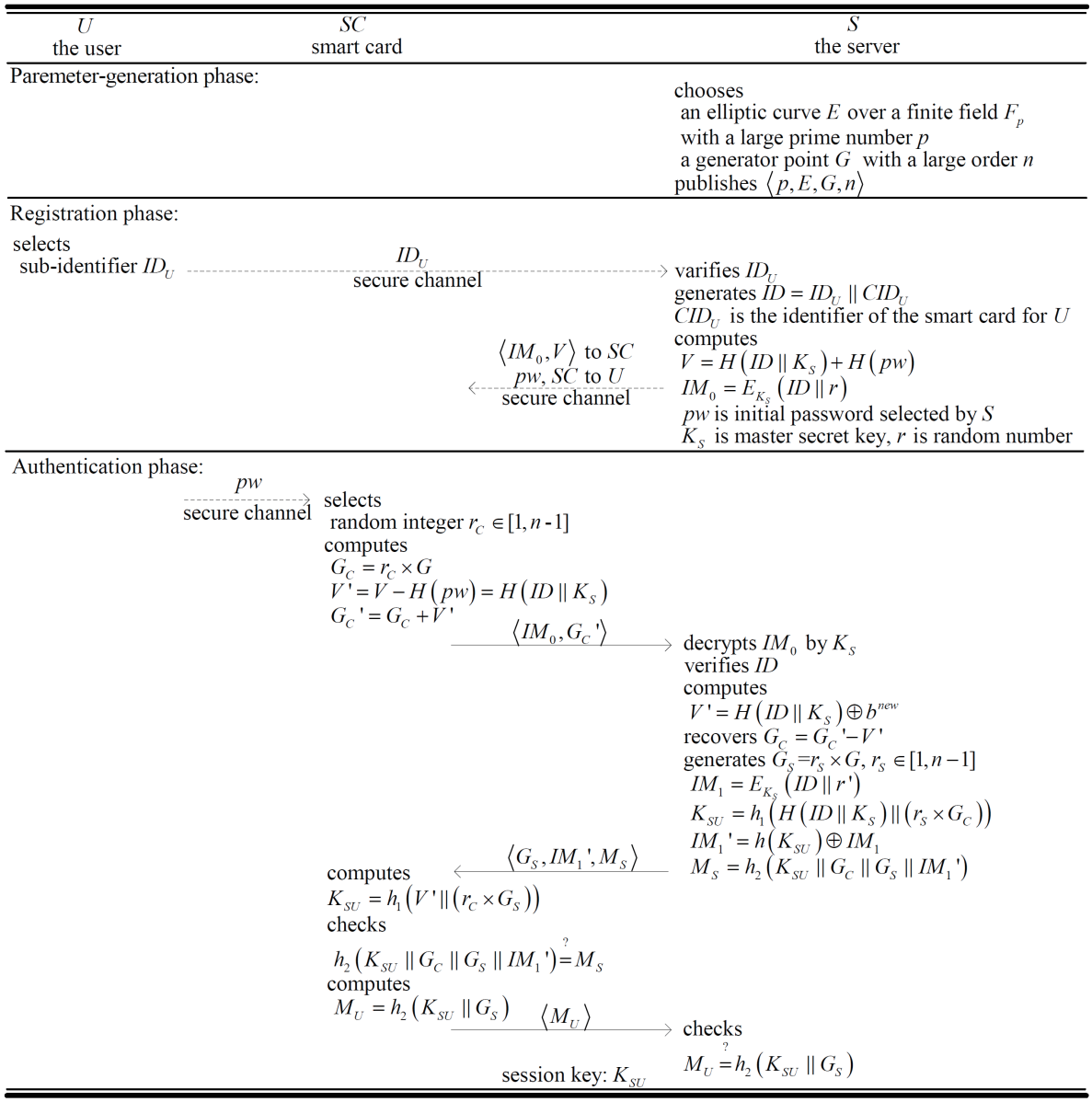

FIGURE 2. Part of Jiang et al.'s scheme

E_K/D_K: The secure symmetric encryption/decryption algorithm with the secret key K_i.

4.1. **Initialization Phase.** To initialize the scheme, the following steps will be completed by the server S.

Step 1. The server S selects a large prime q and two integer elements a and b, where $q > 2^{160}$ and $4a^3 + 27b^2 \bmod q \neq 0$ so that the employed elliptic curve E_q is over finite field $q : y^2 = x^3 + ax + b \bmod q$. This condition prevents E_q from generating repeated factors, and a finite abelian group based on the set E_q can be defined.

Step 2. Let G be a base point of the elliptic curve with a prime order q. An elliptic curve has a point O at infinity as identity element which is the third point intersected by a straight line with this curve. The intersection points are (x, y), $(x, -y)$, and O.

Step 3. The server S chooses a random nonce $r_s \in_R Z_n^*$ as the public key. And $n = 2q + 1$

and computes $R_s = r_s \times G$ as the public key. And $r_s \times R_s$ also also maps to $\{0,1\}^l$ so that it can achieve exclusive or operation with the value of $h(\bullet)$.

4.2. **Registration Phase.** We suppose that only the legal users can reach the secure channel. If the user U_i would like to register with the trustworth server S, he can choose its identity ID_i and the corresponding password pw_i to perform the following steps as depicted in FIGURE 3.

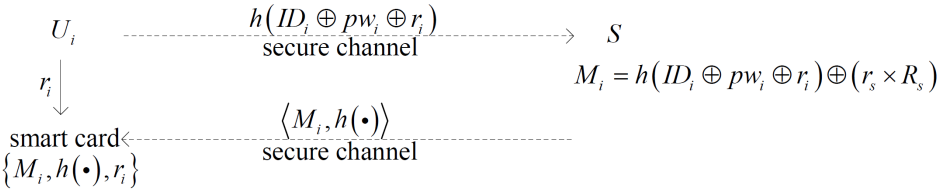

FIGURE 3. Registration phase

Step 1. The user U_i chooses an identity information as ID_i, a password pwi appropriate for memorization and a random number r_i. Then the user U_i computes $h(ID_i \oplus pw_i \oplus r_i)$ and submits it to the server S for registration over a secure channel;

Step 2. After receiving $h(ID_i \oplus pw_i \oplus r_i)$ from the user U_i, the server Scomputes $M_i = h(ID_i \oplus pw_i \oplus r_i) \oplus (r_s \times R_s)$ where r_s is the master key of the server S.

Step 3. The server S stores the data $\langle M_i, h(\bullet) \rangle$ into a new smart card, and issues the smart card to the user U_i through a secure channel. Meanwhile, S stores each legal user's subscript as the index to a status-bit in a write protected file which contains $\langle i, status - bit \rangle$. The status-bit indicates the login status of the user to prevent many logged-in attack;

The user U_i stores the random number r_i into the smart card.

4.3. **Authentication and Key Agreement Phase.** After completing this phase, the user U_i and the server S can achieve the goal of mutual authentication and session key agreement which can be used for secure subsequent communication without revealing user's identity. The authentication and key exchange phase is depicted in FIGURE 4.

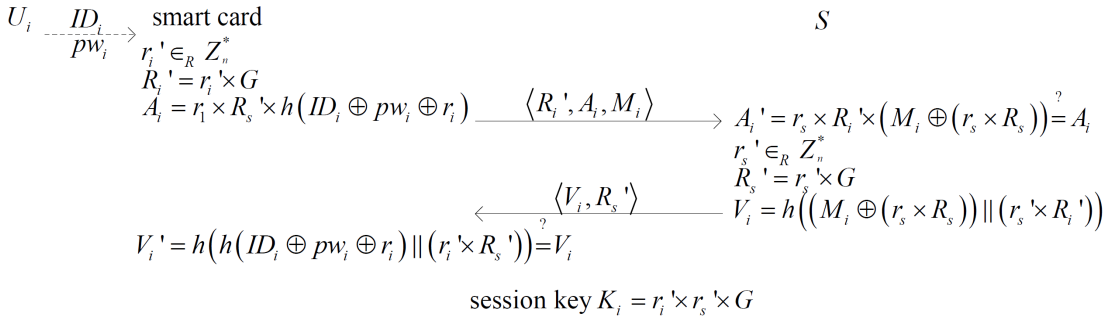

FIGURE 4. Authentication and key agreement phase

Step 1. The user U_i inserts his smart card into a card reader and inputs ID_i and pw_i;

Step 2. The smart card selects a random number $r'_i \in_R Z_n^*$ and computes $R'_i = r'_i \times G$, $A_i = r_i' \times R_s \times h(ID_i \oplus pw_i \oplus r_i)$. Then sends $\langle R_i', A_i, M_i \rangle$ to the server S.

Step 3. Upon receiving $\langle R_i', A_i, M_i \rangle$, S checks the validity of the user U_i. If the status-

bit in the database corresponding to i is equal to one, S aborts the session, rejects the login request, and informs the user about it. Otherwise S sets the status-bit from zero to one and computes $A_i{}' = r_s \times R_i{}' \times (M_i \oplus (r_s \times R_s)) \stackrel{?}{=} A_i$, checks if $A'_i = A_i$. If it holds, the server S selects a random number $r'_s \in_R Z_n^*$ and computes $R_s{}' = r_s{}' \times G$, $V_i = h((M_i \oplus (r_s \times R_s))||(r_s{}' \times R_i{}'))$ Finally, S sends $\langle V_i, R_s{}' \rangle$ back to the user U_i.

Step 4. The user U_i computes $V_i = h(h(ID_i \oplus pw_i \oplus r_s)||(r_s{}' \times R_i{}'))$ with the received $\langle V_i, R_s{}' \rangle$ and checks if $V'_i \stackrel{?}{=} V_i$. The user U_i and the server S are authenticated successfully if it holds; Otherwise, U_i terminates this phase. After the authentication and key agreement phase, both the user U_i and the server S can compute the session key $K_i = r_i{}' \times r_s{}' \times G$.

Here the random numbers against replay attack. $r_i{}'$ and $r_s{}'$ vary in different sessions in order to make the scheme secure against replay attack.

4.4. **Password Changing Phase.** 5 shows the password changing phase of our scheme. If a user suspects that his password has been stolen, he can change the password in this phase. However, he has to go through the above authentication and key agreement procedures and achieve the common session key with the server S first aiming to mutual authentication.

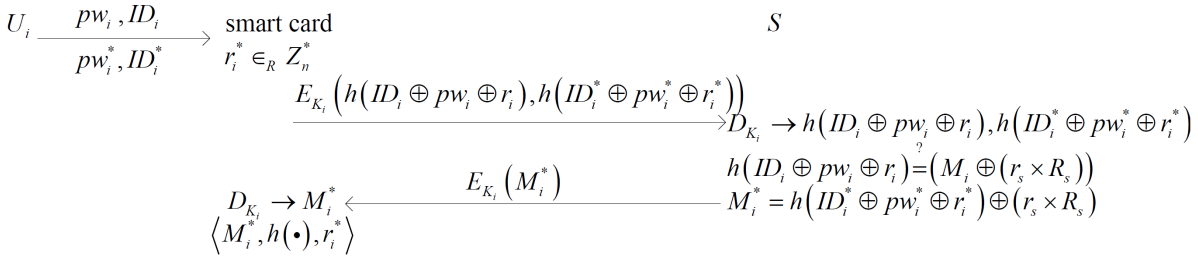

FIGURE 5. Password changing phase

Step 1. After negotiating the common session key with the server S, the user U_i inputs the old parameters pw_i, ID_i and the new parameters pw_i^*, ID_i^* to the smart card.

Step 2. The corresponding smart card selects a random number r_i^* and encrypts $h(ID_i \oplus pw_i \oplus r_i)$ and $h(ID_i^* \oplus pw_i^* \oplus r_i^*)$ with the common session key K_i. And then it sends $E_{K_i}(h(ID_i \oplus pw_i \oplus r_i), h(ID_i^* \oplus pw_i^* \oplus r_i^*))$ to the server S.

Step 3. After decrypting the receiving message, the server S checks if $h(ID_i \oplus pw_i \oplus r_i)$ is equal to $M_i \oplus (r_s \times R_s)$. If the equation holds, the server S continues to compute $M_i^* = M_i \oplus h(ID_i \oplus pw_i \oplus r_i) \oplus h(ID_i^* \oplus pw_i^* \oplus r_i^*)$ and sends the encrypted information $E_{K_i}(M_i^*)$ to the smart card.

Step 4. The smart card decrypts the message from the server S and replaces M_i and r_i with the new values M_i^* and r_i^*, respectively. Finally, the smart card sends back the successful message to the user U_i.

We require the user inputs the old parameters once more after authentication and key agreement phase for preventing known key attack or replay attack without timestamp. Although symmetric cryptosystem is used in this phase, its operating frequency is far less than the former initialization phase, authentication and key agreement phase. So its complexity can be ignored as higher security and privacy is achieved.

5. **Multi-function Analysis of Our Scheme.** Assume that all the mentioned three problems, ECDLP, ECDHP, and CDHP cannot be solved in polynomial-time. Assume

that the adversary has full control over the insecure channel including eavesdropping, recording, intercepting, modifying the transmitted messages. After that it could steal the smart cards or other mobile devices for the stored information. However, the adversary could neither get the temporary values chosen in the local machine nor guess ID_i, pw_i, and r_i correctly at the same time.

In this section, we classify the functions of authentication key agreement scheme based on password and smart card into two types, auxiliary function and essential function. We also prove that our proposed scheme achieves the security and efficiency goals.

5.1. **Auxiliary Function.** .

Privacy preserving

In our protocol, the users' sensitive information such as identities and passwords is private to both the server and the adversaries. During the whole scheme, the privacy is protected by the one-way hash function for transferring over insecure channel and cannot be retrieved from the transmission messages. The user's identity and password are always combined with a random number as $h(ID_i \oplus pw_i \oplus r_i)$ transmitting to the server. Neither the server nor the adversaries can achieve the exact value of ID_i and pw_i. By the way, we think user untraceablity is not achieved in our scheme for tracing the trails of someone communicating through the Internet is still feasible.

Resist SEG attack

Upon the assumption about the adversary like stealing the smart card and eavesdropping, it's similar to a more powerful smart cart security breach attack mentioned in Shen and Du's scheme[28]. Here in our scheme, that is to say, $\langle M_i, h(\bullet), r_i, A_i, R_i', R_s', V_i\rangle$ are visible to the adversary. But the successful mutual authentication is based on $h(ID_i \oplus pw_i \oplus r_i)$ which cannot be revealed by the adversary, because the server's master key r_s is kept secret. Without knowing any information about ID_i and pw_i, general password guessing attack or brute-force attack is infeasible.

No clock synchronization

The proposed scheme solves the clock synchronization problem with no timestamp mechanism. Instead, we introduce fresh random number r_i' and r_s' to provide the challenge response security mechanism so that replay attack cannot threaten the proposed scheme while no clock synchronization is needed.

TABLE 1 lists the auxiliary function comparison between the latest related schemes. In this paper, symbols in the table denote the following meaning. Y: the scheme achieves the function or resists the attack, N: we found it not satisfy the property, and I: not mentioned in the corresponding paper which we think the function is indeterminate.

Table 1. Comparison of auxiliary function

	User anonymity	SEG attack	No clock synchronization	Server spoofing attack	DoS attack/ Many logged-in users' attack
Li et al.'s[24]	N	N	Y	I	Y
Tang et al.'s[26]	N	I	N	I	Y
Shen and Du's[28]	N	Y	N	I	I
Jiang et al.'s[30]	Y	N	Y	I	N
Ours	Y	Y	Y	Y	Y

From TABLE 1, it can be seen that not all the auxiliary function mentioned above can achieve in the related work except ours. Although different operating environments require different functions, it's obvious that multi-function mutual authentication scheme is more flexible and adjustable. In fact, with the development of the technology and the

increase of the computation capacity, these auxiliary functions may even become essential while more new functions may be proposed. The proof of resisting server spoofing attack and denial of service(DoS) attack is shown in 5.2 pertaining to the well-known attack.

5.2. **Essential Function.** .

Mutual authentication and key agreement

Mutual authentication is crucial to ensure legal users to access services provided by legitimate server. The proposed scheme allows the server S to authenticate the user U_i by checking whether $A_i{}' = r_s \times R_i{}' \times (M_i \oplus (r_s \times R_s)) \stackrel{?}{=} A_i = r_i{}' \times R_s \times h(ID_i \oplus pw_i \oplus r_i)$. It is because only the correct $h(ID_i \oplus pw_i \oplus r_i)$ can be computed when the user inputs the correct identity information ID_i and password pw_i. On the other hand, the user U_i authenticates the server S by checking if $V_i{}' = h(h(ID_i \oplus pw_i \oplus r_i)||(r_i{}' \times R_s{}')) \stackrel{?}{=} V_i = h((M_i \oplus (r_s \times R_s)||(r_s{}' \times R_i{}'))$ where $V_i{}'$ and V_i can be computed only by the legal user U_i and server S respectively. Therefore, no one can impersonate a legal user or the server in our proposed scheme. After mutual authentication, user U_i and server S negotiate a session key $K_i = r_i \times R_s{}' = r'_s \times R_i{}'$. Thus, this essential function is achieved in the proposed scheme.

Mutual authentication and key agreement

(1) Privileged insider attack

The privileged insider of the server cannot derive the password or the identity of the user from $h(ID_i \oplus pw_i \oplus r_i)$. In that ID_i and pw_i are not guessable without any correlative information. Meanwhile, the security of sensitive information is based on one-way hash function.

(2) Stolen-verifier attack

When the adversary steals verifiers from the database of the server, it cannot get any sensitive information of the server because we only store $\langle i, status - bit \rangle$ as a table which is write protected.

(3) Lost smart card attack

After picking up the smart card of U_i (unknow the identity of U_i), the adversary uses the physical technique to extract value M_i and r_i from the smart card. It may try to select a candidate password from the dictionary but find it hard to guess the ID_i and pw_i.

(4) Impersonation attack/ Man-in-the-middle attack

An adversary cannot impersonate the user U_i to cheat the server S, because it is not able to construct the message $A_i = r_i{}' \times R_s \times h(ID_i \oplus pw_i \oplus r_i)$ without the knowledge of ID_i and pw_i. It either cannot masquerade as the server S to cheat U_i for the same reason. In this sense, impersonation attack is similar to the man-in-the-middle attack.

(5) Replay attack

An adversary cannot start a replay attack against our scheme because of the freshness of $R_i{}'$ in each session and the write protected table $\langle i, status - bit \rangle$ If $R_i{}'$ has appeared before or the status shows in process, the server rejects the login request. If the adversary wants to launch the replay attack successfully, it must compute and modify $A_i = r_i{}' \times R_s \times h(ID_i \oplus pw_i \oplus r_i)$ correctly which is impossible.

(6) Password guessing attack

The general password guessing attack has two classes. One is the on-line guessing attack which can be prevented easily by limiting the number of failed verification times while the other is off-line guessing attack on $h(ID_i \oplus pw_i \oplus r_i$ to obtain ID_i and pw_i with no relative information. Besides, in our scheme, the password of hashing table is not stored in the server so that the adversary cannot get $h(ID_i \oplus pw_i \oplus r_i$ to obtain ID_i or pw_i using an off-line guessing attack.

(7) Modification attack

An adversary cannot modify the message $\langle R_i', A_i, M_i \rangle$ and $\langle V_i, R_s' \rangle$ because the user and the server always detect anomalous by checking the correctness of A_i and V_i, respectively.

(8) Many logged-in users' attack/ DoS attack

Firstly, we set the status-bit to indicate the user's login status which can resist many logged-in users' attack. Secondly, the adversary cannot start the DoS attack during the password changing phase since we check the correctness of the old ID_i and pw_i by executing the authentication and key agreement phase before.

(9) Server spoofing attack

In this attack, an adversary may try to cheat the requesting user. However, without knowing the ID_i and pw_i, an adversary cannot cheat the requesting user for failing to forge a valid response message in Step 2 of authentication and key agreement phase. It is infeasible to obtain the master key of the server to compute $M_i \oplus (r_s \times R_s)$ as well.

The comparison of the resist well-known attack function in related work is depicted in TABLE 2.

Table 2. The comparison of the well-known attack

	Privileged insider attack	Stolen-verifier attack	Lost smart card	Impersonation/Man-in-the-middile	Replay attack	Password guessing attack	Modification attack
Li et al.'s[24]	I	Y	I	Y	Y	Y	I
Tang et al.'s[26]	Y	Y	Y	Y	Y	Y	Y
Shen and Du's[28]	Y	Y	Y	Y	Y	Y	Y
Jiang et al.'s[30]	Y	Y	Y	I	I	Y	Y
Ours	Y	Y	Y	Y	Y	Y	Y

Comparisons of well-known attack between the proposed scheme and the previous related schemes are given in TABLE 2. These essential well-known attacks are almost achieved in these protocols, privileged insider attack, lost card attack, and modification attack are not illustrated in[24]. Whether impersonation attack, and replay attack are achieved in[30] is unknown.

Forward security

The forward security of the session key is one of the basic properties of key agreement scheme. Our scheme could preserve the forward security of the session key because of the freshness and the independence with other session keys generated in the past or in the future no matter whether it is used or not. In our proposed scheme, $K_i = r'_i \times R_s' = r'_s \times R_i' = r_i' \times r_s' \times G$ is generated by fresh random number r_i' and r_s' chosen by U_i and S respectively for each session. Firstly, the adversary has no ability to intercept r_i' and r_s' from previous sessions. Secondly, even the correct session key is known, r_i' and r_s' are still concealed because of CDHP which is polynomial-time equivalent to ECDLP. Thus, even if a session key is known, no previous session key will be compromised. The proposed scheme ensures perfect forward security.

No sensitive information table

In our proposed scheme, no password or verification table is kept by the server S. Thus an adversary cannot destroy the system security by manipulating.

Practical in pervasive and ubiquitous computing environment

Since smart card and other mobile devices are constrained by computational capability and low bandwidth, complicated computation operations should be avoided in these authentication schemes. Compared to RSA, ECC offers smaller key sizes, faster computation, as well as memory, energy and bandwidth savings and is thus better suited for small devices[34-35]. The security level of 160-bit key in elliptic curve cryptosystem is the

same as 1024-bit key in RSA cryptosystem. Because ECC is employed in the proposed scheme, this function is achieved.

TABLE 3. The comparison of computation cost and communication cost of the login and authentication key agreement phases

	Round number	Hash	Exclusive or	Symmetric en/decryptio	Modular multiplicatio	Modular exponent	Elliptic curve multiplication	Elliptic curve addition
Li et al.'s[24]	5	5	0	4	3	0	11	2
Tang et al.'s[26]	2	6	1	0	0	0	3	0
Shen and Du's[28	4	22	45	0	0	4	0	0
Jiang et al.'s[30]	3	11	2	2	0	0	4	0
Ours	2	4	6	0	0	0	7	0

For performance analysis, we compare the computation cost and communication cost in authentication and key agreement phase with the others, and tabulate the result in TABLE 3. The number of rounds, hash operation, exclusive or operation, symmetric encryption/decryption, modular multiplication, modular exponent and elliptic curve addition considered, our scheme is better than the others. Shen and Du's scheme is the only one need four more modular exponent to achieve session key agreement and only by additional session key can it resist the SEG attack. Our scheme only needs four more elliptic curve multiplication operation than[26] which is negligible for adding privacy preserving, resistance of SEG attack, and solving clock synchronization problem.

6. **Conclusions.** We analyze that Shen and Du's scheme and Jiang et al.'s scheme are vulnerable to the password guessing attack and put forward a strong and multi-function mutual authentication key agreement scheme to remedy the security flaw and adding auxiliary functions. Achieving privacy preserving, solving clock synchronization problem with nonce, and resist a more powerful smart cart security breach attack without increasing high computation cost are the dominating characteristics of our scheme. Security analysis for well-known attacks and efficiency analysis are included in the multi-function analysis. Next we will extend the proposed scheme to the multi-server environment and further enhance the password mutual authentication group key agreement protocol achieving more functions in the future.

Acknowledgement. This research is supported by Liaoning Provincial Natural Science Foundation of China (Grant No. 20102202, 201102201) and Liaoning Baiqianwan Talents Program(2011921046).

REFERENCES

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

[2] C. J. Mitchell, and l. Chen, Comments on the S/KEY user authentication scheme, *ACM SIGOPS Operating Systems Review*, vol. 30, no. 4, pp. 12-16, 1996.

[3] C. M. Chen, and W. C. Ku, Stolen-verifier attack on two new strong-password authentication protocol, *IEICE Trans. Communications*, vol. E85-B, no. 11, pp. 2519-2521, 2002.

[4] T. Hwang, Y. Chen, and C. S. Laih, Non-interactive password authentications without password tables, *Proc. of IEEE Region 10 Conference on Computer and Communication Systems*, pp. 429-431, 1990.

[5] A. Shamir, Identity Based Cryptosystems and Signature Schemes, *Proceedings of Crypto*, LNCS 196, pp. 47-53, 1985.

[6] D. Boneh, and M. Franklin, Identity-based encryption from theWeil pairing, *Proc. of the 21st Annual International Cryptology Conference on Advances in Cryptology*, LNCS 2139, pp. 213-229, 2001.

[7] M. L. Das, A. Saxena, V. P. Gulati, and D. B. Phatakb, A novel remote user authentication scheme using bilinear pairings, *Journal of Computers & Security*, vol. 25, no. 3, pp. 184-189, 2006.
[8] J. H. Yang, and C. C. Chang, An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, *Journal of Computers & security*, vol. 28, no. 3, pp. 138-143, 2009.
[9] S. K. 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, no. 11, pp. 1892-1898, 2011.
[10] M. S. Hwang, and L. H. Li, A new remote user authentication scheme using smart cards, *IEEE Trans. Consumer Electronics*, vol. 46, no. 1, pp. 28-30, 2000.
[11] C. K. Chan, and L. M. Cheng, Cryptanalysis of a remote user authentication scheme using smart cards, *IEEE Trans. Consumer Electronics*, vol. 46, pp. 992-993, 2000.
[12] J. J. Shen, C. W. Lin, and M. S. Hwang, A modified remote user authentication scheme using smart cards, *IEEE Trans. Consumer Electronics*, vol. 49, no. 2, pp. 414-416, 2003.
[13] H. Y. Chien, J. K. Jan and Y. M. Tseng, An efficient and practical solution to remote authentication: smart card, *Computer & Security*, vol. 21, no. 4, pp. 372-375, 2002.
[14] H. M. Sun, An efficient remote user authentication scheme using smart cards, *EEE Trans. Consumer Electronic*, vol. 46, no. 4, pp. 958-961, 2000.
[15] W. C. Ku, and S. M. Chen, Weaknesses and improvements of an efficient password based user authentication scheme using smart cards, *IEEE Trans. Consumer Electronic*, vol. 50, no. 1, pp. 204-207, 2004.
[16] C. L. Hsu, Security of Chien et al.'s remote user authentication scheme using smart cards, *Journal of Computer Standards & Interfaces*, vol. 26, no. 3, pp. 167-169, 2004.
[17] S. Lee, H. Kim, and K. Yoo, Improved efficient remote user authentication scheme using smart cards, *IEEE Trans. Consumer Electronics*, vol. 50, no. 2, pp. 565-567, 2004.
[18] E. Yoon, and K. Yoo, More efficient and secure remote user authentication scheme using smart cards, *Proc. of 11th International Conference on Parallel and Distributed System*, pp. 73-77, 2005.
[19] N. Y. Lee, and Y. C. Chiu, Improved remote authentication scheme with smart card, *ournal of Computer Standards & Interfaces*, vol. 27, no. 2, pp. 177-180, 2005.
[20] S. T. Wu, and B. C. Chieu, A user friendly remote authentication scheme with smart cards, *Journal of Computer & Security*, vol. 22, no.6, pp. 547-550, 2003..
[21] J. Xu, W. T. Zhu, and D. G. Feng, An improved smart card based password authentication scheme with provable security, *Journal of Computer Standards & Interfaces*, vol. 31, no. 4, pp. 723-728, 2009.
[22] S. W. Lee, H. S. Kim, and K. Y. Yoo, Improvement of Chien et al.'s remote user authentication scheme using smart cards, *Journal of Computer Standards & Interfaces*, vol. 27, no. 2, pp. 181-183, 2005.
[23] R. Song, Advanced smart card based password authentication protocol, *Journal of Computer Standards & Interfaces*, vol. 32, no. 5, pp. 321-325, 2010.
[24] X. Li, F. Wen, and S. Cui. A strong password-based remote mutual authentication with key agreement scheme on elliptic curve cryptosystem for portable devices, *Journal of Applied Mathematics & Information Sciences*, vol. 6, no. 2, pp. 217-222, 2012.
[25] S. K. Kim, and M. G. Chung, More secure remote user authentication scheme, *Journal of Computer Communications*, vol. 32, no. 6, pp. 1018-1021, 2009.
[26] H. B. Tang, X. S. Liu, and L. Jiang, A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance, *International Journal of Network Security*, vol. 15, no. 6, pp. 360-368, 2013.
[27] A. K. Awasthi, K. Srivastava, and R. C. Mittal, An improved timestamp-based remote user authentication scheme, *Computers and Electrical Engineering*, vol. 37, no. 6, pp. 869-874, 2011.
[28] J. Shen, and Y. Du. Improving the password-based authentication against smart card security breach, *Journal of Software*, vol. 8, no. 4, pp. 979-986, 2013.
[29] C. T. Li, and C. C. Lee, A robust remote user authentication scheme against smart card security breach, *Proc. of the 25th annual IFIP WG 11.3 conference on Data and applications security and privacy*, pp. 231-238, 2011.
[30] Q. Jiang, J. Ma, G. Li, and L. Yang, Robust two-factor authentication and key agreement preserving user privacy, *International Journal of Network Security*, vol. 16, no. 4, pp. 321-332, 2014.
[31] V. S. Miller, Use of elliptic curves in cryptography, *Proc. of CRYPTO*, LNCS 218, pp. 417-426, 1986.

[32] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, Examining smart-card security under the threat of power analysis attacks, *IEEE Trans. Computers*, vol. 51, no. 5, pp. 541-552, 2002.
[33] S. P. Skorobogatov, and R. J. Anderson, Optical fault induction attacks, *Proc. of Cryptographic Hardware and Embedded Systems*, LNCS 2523, pp. 2-12, 2003.
[34] N. Gura, A. Patel, A. Wander, A. Wander, and H. Eberle, Comparing elliptic curve cryptography and RSA on 8-bit CPUs, *Proc. of Cryptographic Hardware and Embedded Systems*, LNCS 3156, pp. 119-132, 2004.
[35] V. Gupta, D. Stebila, S. Fung, S. C. Shantz, N. Gura, and H. Eberle, Speeding up secure web transactions using elliptic curve cryptography, *Proc. of the Network and Distributed System Security Symposium*, NDSS 2004, 2004.