A Novel Multi-factor Authenticated Key Exchange Scheme With Privacy Preserving

Dexin Yang
Guangzhou City Polytechnic
Guangzhou, China, 510405
yangdexin@21cn.com

Bo Yang*
South China Agricultural University
Guangzhou, China, 510642
byang@scau.edu.cn

Abstract

In this paper, a new multi-factor authenticated key exchange scheme, which combines with biometrics, password and the smart card, is proposed. Compared with the previous schemes, this scheme has higher security in remote authentication and preserves privacy of biometrics , and most of the previous schemes rely on the smart card to verify biometrics. The advantage of these approaches is that the user's biometrics is not shared with the remote server, which can resist insider's attack and preserve the privacy of the biometrics. The disadvantage is that the remote server must trust the smart card to perform authentication, which leads to various vulnerabilities. To achieve multi-factor authentication, a new function called one-way function with distance-keeping, which is used to preserve privacy of user's biometrics, is introduced. This scheme has advantages as multi-factor authentication, privacy preserving and lower communication complexity etc. It is proven secure under the random oracle and is suitable to the environment which lacked communication resource and needed higher security.

Keywords: Multi-factor authentication Biometrics Passwords Smart cards Privacy Preserving

1 Introduction

Typically, user authentication based on something that a user knows (typically a PIN, a password) or something that a user has (a key, a token, a magnetic or smart card, a badge, a passport etc.). Unfortunately,these traditional methods of the user authentication do not authenticate the user as such. Traditional methods are based on properties that can be forgotten(password), disclosed, lost or stolen(smart card). Nowadays, password authentication is the most common authentication system. Passwords provide a convenient and inexpensive methodology. However, remembering multiple passwords and changing them frequently lead to the usage of lower entropy passwords which are susceptible to adversaries' guessing attacks. Moreover, passwords can be compromised without being detected and therefore do not defend well against repudiation. The smart card might be shared, lost or stolen. If a user's smart card is stolen, all the information stored in it can be lost. If more than one user share their smart cards, they can collude to deceive the remote server to get extra information.

Biometric authentication, the science of using physical or behavioral characteristics for identity verification, which provides a new authentication type which is based on who you are, is becoming a security mainstay in many areas. Recently, biometric authentication has become a new research focus in cryptography.

Biometric authentication has some advantages over traditional authentication methods: biometric information cannot be acquired by direct covert observation, it is impossible to share and difficult to reproduce and it is convenient for user by alleviating the need to memorize long and random passwords. Moreover, biometrics is one of the rare techniques that can be used for negative recognition through

Journal of Internet Services and Information Security, volume: 1, number: 2/3, pp. 44-56
*Corresponding author

which the system determines whether the person is who he or she denies to be. But biometrics is easily obtained and can never be changed, which makes biometric features unreliable as encryption keys. The server cannot verify the device captures a person's biometrics who is alive because the biometric capture devices are remotely located.

The single factor and two-factor authentication, which uses one of three factors or combines two of the three factors(what you know,what you have and who you are) have some drawbacks in security. The authentication scheme, which combines this three factors, has become a new direction in authentication because these three-factor authentication schemes can overcome some drawbacks compared with traditional one or two-factor authentication schemes.

1.1 Related Work

Several multi-factor authentication schemes have been proposed in literature [10, 12, 8, 13, 15, 6, 9, 14] since 2002. Lee et al [10]proposed a fingerprint-based remote user authentication scheme using smartcard in 2002. In this scheme, a user inserts his smart card to card reader and then scans his fingerprint and inputs his password in the login phase. In the authentication phase, a user inserts his smart card, submits his fingerprint and password, then the password is checked with the data stored in smart card and the fingerprint is checked with the fingerprint template stored in the smart card. This scheme was broken by Lin et al. Lin et al[5] found that a registered user could create many valid pairs of identities and passwords to masquerade as other legal users in 2003. Lin et al proposed an improvement scheme in [10], which allows a user changes his password offline. In 2005, Eun-Jun Yoon et al [16] found this scheme is insecure, because the password change operation is vulnerable, the smart card can not check the correctness of old password. In addition, the scheme is vulnerable to an impersonation attack. The most recent scheme above has not yet been broken, but it still, like other methods, lacks a means of checking on biometrics in the server side. Another drawback of this scheme is that it can not be proven secure. In 2010, Li, Chun-Ta and Hwang, Min-Shiang [14]propose a new efficient biometrics-based remote user authentication scheme using smart cards, the authors claimed that the computation cost of this scheme is lower than the related schemes, and the user can change their passwords freely and mutual authentication etc. It is the latest scheme that was found.

In 2008, Pointcheval, David et al [15]proposed a multi-factor authenticated key exchange scheme, which combines a password, a secure device and biometrics. This is the first multi-factor scheme which is proven secure under the random oracle model. Almost all of the instable biometrics are suitable to this scheme. A homomorphic encryption is used to encrypt every bits of biometric templates, so it has lower efficiency in computation and communication. Zero-knowledge proof is a necessary tool to build an authentication scheme, A. Bhargav-Spantzel et al [3] proposed a privacy preserving multi-factor scheme with biometrics in 2006, which combines password, biometrics, public-key encryption scheme and zero-knowledge proof. The biometrics is used to generate a biometric key in the first phase, and the key is kept secret, in order to preserve the confidentiality of the biometric data, while exploiting the advantages of biometric authentication. In the second phase, several authentication factors including password, biometrics and public key encryption scheme are combined to provide a strong authentication. The zero knowledge proof in this scheme is traditional zero knowledge proof which compares two biometric keys in accurately equal, not in approximately equal. Chun-I-Fan et al [6] proposed a provably secure three-factor authentication scheme with privacy protection on biometrics in 2009, which combines password, the smart card and biometrics. In the three rounds of this protocol, a public-key encryption scheme and symmetric encryption scheme are adopted to protect security of data transferred in the public channel. This scheme is proven secure under BR's model[1, 2]. Compared with Pointcheval, David et al's scheme, the computation complexity is lower, and the communication complexity of this scheme is higher.

1.2 Our Contribution

In this paper, we formalize the definition of one-way function with distance-keeping, which is used to keep biometric privacy in [6] and our scheme, and a new multi-factor authenticated key exchange scheme is proposed. Compared with the scheme in [6], this scheme is more efficient in communication complexity. The scheme in [6] is a key distribution scheme, and the proposed scheme is a key exchange scheme. Rough speaking, in a key distribution scheme, a session key is picked by one party, and it is transferred to another party in a secure manner, but in a key exchange scheme, a session key is computed by two parties in a secure manner, the key exchange scheme has advantages in security.

1.3 Organization of this work

The remainder of this paper is organized as follows: Section 2 Preliminary, Section 3 Formal security model, Section 4 The proposed scheme, Section 5 Securities of our scheme, Section 6 Performance, and finally, Conclusion.

2 Preliminary

2.1 Definitions

Definition 1. *A function δ_k is called a one-way function with distance-keeping. If it satisfies:*
(1)$\Delta(S_i, S_i') = \Delta(\delta_k(S_i), \delta_k(S_i'))$, where $\Delta()$ is a distance function in a metric space;
(2)$Pr[S_i|\delta_k(S_i)] \leq \varepsilon$.
Namely, the probability to compute δ^{-1} given $\delta_k(S_i)$ is negligible without secret information k, where k is secret key, ε is negligible, and S_i, S_i' are elements in the metric space.

In definition 1, property (1) means the distance of S_i, S_i' is kept under δ, and property (2) means one-wayness. In our scheme, we use function δ_k to keep privacy of users' biometrics. For example, the simplest one-way function with distance-keeping is $\delta_k(S_i) = S_i \oplus k$.

Definition 2. *[4] A biometric template $b \in B$ is the result of a measurement from someone's biometrics thanks to a sensor. For a specific user whose biometrics is β, we note $b \leftarrow \beta$ the fact that b is a measure of β. Two different measures of the same user $b, b' \leftarrow \beta$ have with overwhelming probability $\Delta(b, b') \leq t$; measures of different users $b_1 \leftarrow \beta_1, b_2 \leftarrow \beta_2$ have with high probability $\Delta(b_1, b_2) > t$, where t is a threshold of error-correcting code.*

Definition 2 means biometric templates captured from the same user can always be accepted by the authentication system and biometric templates captured from the different users can always be rejected by the authentication system.

Definition 3. *Consider a group G of order q, g is a generator of G. The DDH assumption states that, let D be an algorithm that takes as input triples of G's elements, and outputs a bit. We define the $DDH-advantage$ of D to be*

$$|Pr[x, y \in_R Z_q : D(g^x, g^y, g^{xy}) = 1] - |Pr[x, y, z \in_R Z_q : D(g^x, g^y, g^z) = 1]|$$

The DDH assumption(for G) is that any efficient algorithm's $DDH-advantage$ is negligible.

Triples of the first kind are often called DDH triples.

Juels and Wattenberg [11] proposed the definition of the fuzzy commitment scheme. They suggested that the biometric templates acquired from the same user at different time(for example, enrollment and authentication)could be treated as data transmitted and received over a noisy channel.

Definition 4. *[7] A commitment scheme (for a message space M) is a triple* $(Setup, Commit, Decommit)$ *such that:*

(1)$CK \leftarrow Setup(1^k)$*: generates the public commitment key.*

(2)$\forall m \in M$, $(c,d) \leftarrow Commit_{CK}(m)$ *is the commitment/decommitment pair for m.* $c = c(m)$ *serves as the commitment value, and* $d = d(m)$ *as the decommitment value.*

(3)$Decommit_{CK}(c,d) \rightarrow \tilde{m} \in M \cup \perp$*, where* $\perp$ *is returned if c is not a valid commitment to any message.*

(4)Correctness: $\forall m \in M$, $Decommit_{CK}(Commit_{CK}(m)) = m$.

We can define fuzzy commitment scheme based on Definition 4 as follows.

Definition 5. *A commitment scheme is a fuzzy commitment scheme, if it satisfies:*

$\forall m \in M$, $Pr[Decommit_{CK'}(Commit_{CK}(m)) = m | dis(CK, CK') \leq t] = 1$,

where $dis()$ *is the distance of some metric space, t is the error threshold of error-correcting code.*

In literature [11], a fuzzy commitment scheme is constructed as follows. Let $\mathscr{F}$ be a field, and $\mathscr{C}$ be the set of codewords for some error-correcting code, assume that codewords lie in $\mathscr{F}^n$. To commit to a value $x \in \mathscr{F}^n$, the user selects a codeword c uniformly at random from $\mathscr{C}$ and computes an offset of the form $\delta = c - x \in \mathscr{F}^n$, i. e. , the difference over individual field elements. The commitment then consists of the pair $(\delta; y)$, where $y = h(c)$ for some suitable one-way function h. To decommit using key x', the user computes $\delta + x'$ and, if possible, decodes to the nearest codeword c'. The decommitment is successful iff $h(c') = y$. The above scheme is used to protect random number r in our scheme, which is the key of one-way function with distance-keeping(Definition 1).

2.2 Security Against an Adaptively Chosen Ciphertext Attack of a Encryption Scheme

An adaptive chosen-ciphertext attack (abbreviated as CCA2) is an interactive form of chosen-ciphertext attack in which an attacker sends a number of ciphertexts to be decrypted, then uses the results of these decryptions to select subsequent ciphertexts. It is to be distinguished from an indifferent chosen-ciphertext attack (CCA1).

Firstly, we introduce the adaptively chosen ciphertext attack in a public-key encryption system. Let $\Gamma = \{K, E, D\}$ be a public-key encryption scheme, where K is the key generation algorithm taking a security parameter k as a input and outputs a key pair(pk, sk), E is a probabilistic encryption algorithm, and D is a deterministic decryption algorithm. An adaptively chosen attack including five steps.

(1)The K generates a key pair (pk, sk). An adversary gets pk only.

(2)The adversary makes a series of decryption queries by sending a sequence of ciphertexts $y_0, y_1, ..., y_i$ to the decryption oracle. The decryption oracle decrypts these ciphertext using sk and returns the corresponding plaintext to the adversary.

(3)The adversary selects two message x_o, x_1 and sends them to the encryption oracle. The encryption oracle chooses $b \in \{0,1\}$ by coin toss, and then encrypts x'_b and returns y'_b to the adversary.

(4)The adversary perfroms (2) again by making a series of decryption queries $y_{i+1}, y_{i+2} ... y_n$ where $y'_b \notin \{y_{i+1}, y_{i+2} ... y_n\}$.

(5)Finally, the adversary outputs $b' \in \{0,1\}$ as his guess of the b.

We say a public-key encryption scheme is secure against the adaptively chosen ciphertext attack if, for any polynomial-time adversary, $Pr[b' = b] - 1/2$ is negligible, where $Pr[b' = b]$ is the probability of $b' = b$.

In literature [6], the author introduces the adaptively chosen ciphertext attack in a symmetric encryption system. It has some differences from asymmetric encryption scheme as follows: the adversary makes a series of encryption/decryption queries by sending a sequence of plaintexts/ciphertexts, such

as $(y_o,''decrypt''),(y_1,''encrypt''),...,(y_i,''encrypt'')$ to the encryption/decryption oracle in symmetric encryption scheme, rather than the adversary makes a series of decryption queries by sending a sequence of ciphertexts $y_0,y_1,...,y_i$ to the decryption oracle in asymmetric encryption scheme.

2.3 Security Against Existential Forgery Under Chosen-message Attack of a Digital Signature Scheme

Existential forgery under chosen-message attack of a digital signature scheme $(KeyGen,Sign,Verify)$ is defined as the following games between a challenger $\mathscr{C}$ and an adversary $\mathscr{A}$. The challenger runs algorithm *KeyGen* to generate a key pair (pk,sk), the adversary $\mathscr{A}$ is given pk at first. Then the adversary $\mathscr{A}$ requests signatures with pk at most q_s messages of his choice $M_1,M_2,...,M_{q_s}\in\{0,1\}^*$,the challenger responds each query with a signature $\sigma_i=Sign_{sk}(M_i)$. These queries are proceeding adaptively. Eventually, $\mathscr{A}$ outputs a pair (M,σ) and wins the game if (1)$M\notin\{M_1,M_2,...M_q\}$, and (2) $Verify(pk,M,\sigma)=true$.

We say a signature scheme is secure against existential forgery under chosen-message attack if, for any polynomial time $\mathscr{A}$, the probability of $\mathscr{A}$ forging the signature of M successfully is negligible.

3 Formal Security Model

We now describe the formal security model for our multi-factor scheme, and then present a security proof for the improved scheme.

3.1 Security Model

We introduce a formal security model, which is mainly adopted from Bellare et al [1]. In addition, we formally define the special security requirements of multi-factor authentication schemes.

Protocol Participants: $\prod_{A,B}^{i}$ denotes the client oracle which plays the role A to interact with B in the ith session, and $\prod_{B,A}^{j}$ denotes the server oracle which plays the role to interact with A in the jth session. Let $\mathscr{P}$ be the proposed multi-factor authentication protocol. During the execution of $\mathscr{P}$, there exists an adversary E, who is a probabilistic polynomial time Turing machine. In protocol $\mathscr{P}$, there are two partners $\prod_{A,B}^{i}$ and $\prod_{B,A}^{j}$ oracles , and an adversary E who can control the entire network and obtain the transmitted data in the past processes. Let us define the capability of adversary which can be captured by the following queries:

· Execute($\prod_{A,B}^{i}$, $\prod_{B,A}^{j}$): This query simulates adversaries passive attacks. An adversary can eavesdrop all transmitted data between $\prod_{A,B}^{i}$ and $\prod_{B,A}^{j}$) in the protocol $\mathscr{P}$.

· Send($\prod_{A,B}^{i},m$): This query models adversaries active attacks. An adversary sends a message m which is forged, modified etc. to $\prod_{A,B}^{i}$. The adversary gets response message according to m in protocol $\mathscr{P}$. The adversary can also initiate a session by setting $m=\lambda$, where λ is empty string.

· Send($\prod_{B,A}^{j}$, m): This query models adversaries active attacks. An adversary sends a message m which is forged, modified etc. to $\prod_{B,A}^{j}$. The adversary gets response message according to m in protocol $\mathscr{P}$.

· Corruption($\prod_{A,B}^{i}$): This query models leakage of two of the three factors from client. When an adversary makes this query, the client oracle $\prod_{A,B}^{i}$ will respond two of three factors to the adversary into three cases.

Case 1: The leakage of the password and the data stored in the smart card.

Case 2: The leakage of the biometrics and the data stored in the smart card.

Case 3: The leakage of the password and biometrics.

· Reveal($\prod_{A,B}^{i}$): This query models disclosure of the session key of instance i. This query is only valid to A when the role actually holds a session key.

· Test($\prod_{A,B}^{i}$): When $\prod_{A,B}^{i}$ accepts and shares a session key with the partner oracle $\prod_{B,A}^{j}$, an adversary can make this query and try to distinguish a real session key from a random number. This query models the adversary's queries of the test oracle. It will return the real session key or a randomly chosen number to the adversary according the values of coin toss.

3.2 Security Definitions

Any secure mutual authentication protocol must guarantee that neither the server nor the client can accept each other unless both the server and the client accept each other. When two conversations accept each other, we call these two conversations matching conversation[2]. Additionally, a multi-factor authentication scheme has more strict requirements. The server accepts if and only if all of the factors pass authentication.

Definition 6. *[6] A protocol $\mathscr{P}$ is a secure multi-factor(n factors) mutual authentication protocol if, for any polynomial time adversary E:*

(1)If oracles $\prod_{A,B}^{i}$ and $\prod_{B,A}^{j}$ have matching conversations, both oracles accept.

(2)$\prod_{A,B}^{i}$ acceptance implies the probability of $No-Matching^{E}(k)$ is negligible.

(3)$\prod_{B,A}^{j}$ acceptance implies the probability of $No-Matching^{E}(k)$ is negligible even if any $n-1$ of n factors are leaked from the client, where k is a security parameter and $No-Matching^{E}(k)$ is the event that exists i, j, P and Q, such that $\prod_{P,Q}^{i}$ accepts and there is no $\prod_{Q,P}^{j}$ engaged in a matching conversation.

Definition 7. *[6] A protocol $\mathscr{P}$ is a secure multi-factor mutual authenticated key exchange protocol if $\mathscr{P}$ is a secure multi-factor mutual authentication protocol and satisfies:*

(1)An adversary engages in the execution of $\mathscr{P}$ with $\prod_{A,B}^{i}$ and its partner $\prod_{B,A}^{j}$. The both oracles $\prod_{A,B}^{i}$ and $\prod_{B,A}^{j}$ always share the same session key.

(2)For any polynomial-time adversary E, $advantage^{E}(k) = (Pr[Good-Guess^{E}(k)] - 1/2)$ is negligible where k is the security parameter and $Good-Guess^{E}(k)$ is the event that an adversary E guesses the right answer to the test query $Test(\prod_{B,A}^{j})$.

4 The proposed scheme

In general, an authenticated key exchange scheme includes three stages: initialization, registration and authentication and key exchange.

4.1 Initialization

In this stage, a user U_i chooses his identity ID_i, password PW_i and two hash functions $h(.)$ and $H(.)$. A fuzzy commitment scheme $(Commit, Decommit)$ is created by the user, where $Commit$ and $Decommit$ are commitment and decommitment algorithm, respectively.

The server S generates its symmetric encryption key x and asymmetric key pair (pk, sk), which are used in a public-key encryption scheme and a digital signature scheme. (E_x, D_x) represents symmetric encryption and decryption algorithm, (E_{pk}, D_{sk}) represents asymmetric encryption and decryption algorithm, respectively, and $Sign_{sk}(m)$ and $Verify_{pk}(m, \delta)$ represent algorithm of signing and verifying, respectively.

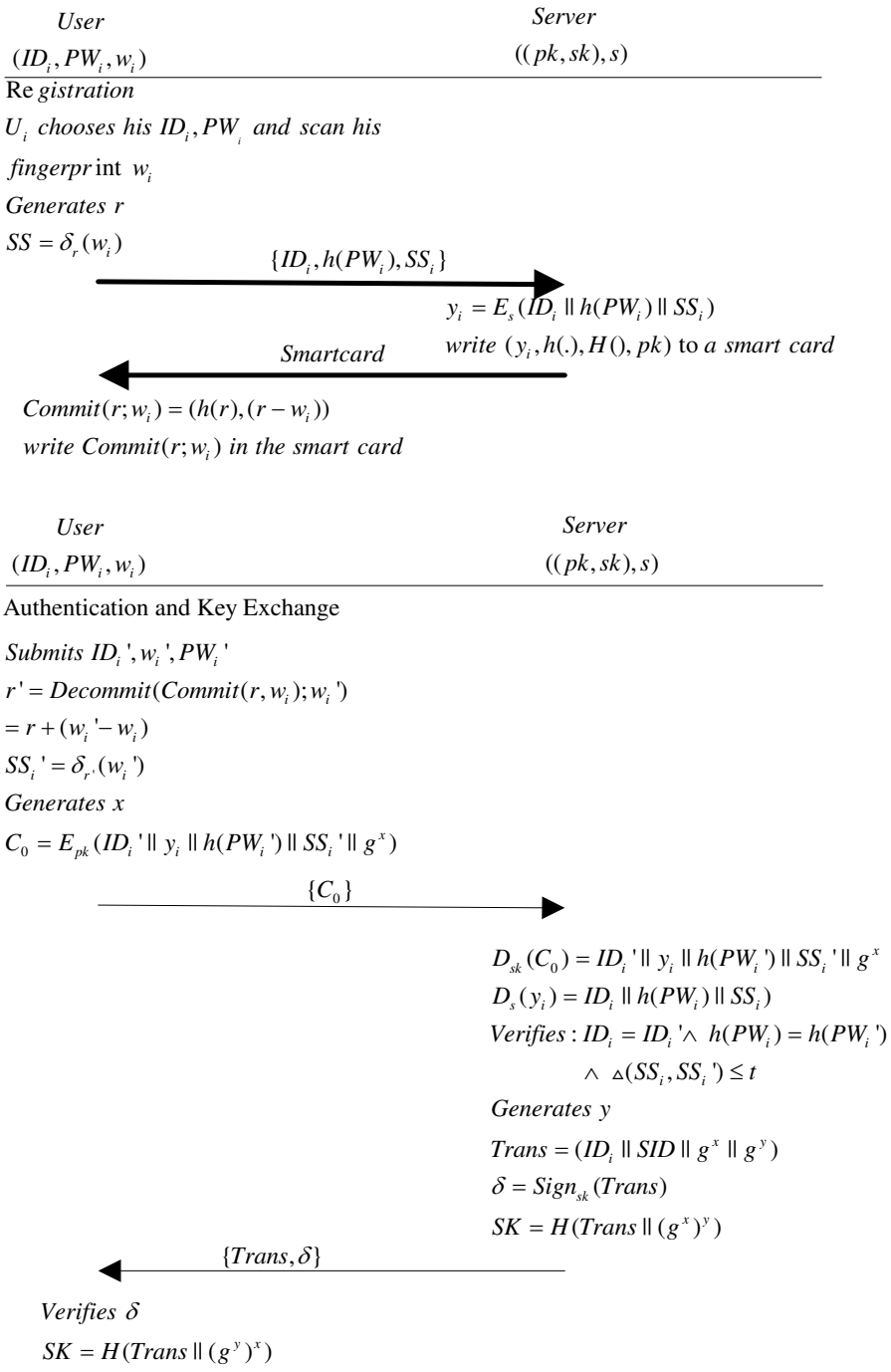

Figure 1: The proposed scheme

In our scheme, the symmetric encryption scheme and the asymmetric encryption scheme are secure against adaptively chosen ciphertext attack, and the digital signature scheme is secure against existential forgery under chosen message attack.

4.2 Registration

Let's consider a new user U_i with an identity ID_i and a password $PW_i \in D$, where D is the password space.

(1)U_i submits his ID_i, PW_i, scans his biometrics(fingerprint, iris etc.), generates a template w_i, and chooses a random number r. U_i computes $SS_i = \delta_r(w_i) = PW_i \oplus w_i$. Then U_i sends $(ID_i, h(PW_i), SS_i)$ to the server S in a secure manner, where $h(.)$ is a public one-way function.

(2)The server S computes $y_i = E_s(ID_i \| h(PW_i \| SS_i))$, writes $(ID_i, y_i, h(.), pk)$ to a smart card, and then sends the smart card to the user U_i in a secure manner.

(3)Upon receiving the smart card from the server, U_i generates $r \in_R Z_q^*$, commits r using w_i: $Commit(r; w_i) = (h(r); r - w_i)$, and writes $Commit(r; w_i)$ in his smart card.

4.3 Authentication and Key Exchange

(1)U_i inputs his identity ID_i', password PW_i', and allows biometrics scan. Lets w_i' be the fingerprint template. U_i retrieves r successfully by decommitting the fuzzy commitment using w_i' if $dis(w_i, w_i') \leq t$, $r = Decommit(Commit(r; w_i); w_i') = r + (w_i' - w_i)$, where dis is the hamming distance and t is a threshold of error-correcting code. Then U_i generates a $x \in Z_q^*$ and computes $SS_i' = \delta_r(w_i')$, $C_0 = E_{pk}(ID_i \| y_i \| h(PW_i' \| SS_i' \| g^x))$. Finally, U_i sends (C_0, y_i) through a public channel.

(2)Upon receiving (C_0, y_i) from the user, the server decrypts C_0 vis the private key sk to obtain $ID_i' \| y_i \| h(PW_i') \| SS_i' \| g^x$, and then decrypts y_i via key s to obtain $ID_i \| h(PW_i) \| SS_i$. The server verifies $(ID_i = ID_i') \wedge (h(PW_i) = h(PW_i')) \wedge (\Delta(SS_i, SS_i') \leq t)$. If it satisfies, the protocol instance continues, otherwise the server aborts and terminates the execution of this protocol instance. Then the server S generates a $y \in Z_q^*$ and computes $\sigma = g^{xy}$, $Trans = ID_i \| SID \| g^x \| g^y$, $\delta = Sign_{sk}(Trans)$, $SK = H(Trans \| g^{xy})$. The server sends $(Trans, \delta)$ to the user via a public channel.

(3)Upon receiving $(Trans, \delta)$ from the server, the user U_i verifies the validity of signature δ using the server's public key pk, if the signature passes verification, the protocol instance continues, otherwise the user U_i aborts and terminates the execution of this protocol instance. Then he computes $Trans = (ID_i \| SID \| g^x, g^y)$, $SK = H(Trans \| g^{xy})$, SK is the shared key between the user and the server.

5 Security of The Scheme

In this section, we show that the proposed multi-factor authentication protocol is provably secure.

Lemma 1 (Server Authentication)If the digital signature scheme, which protects the data transmitted in second message of protocol $\mathscr{P}$, is secure against existential forgery under chosen ciphertext attack, then the client cannot accept without the server involved.

Proof. If there exists an adversary E that is accepted by the client but the client is not accepted by the server, we prove that the probability of this event is negligible.

Let $Succ$ be the event that an adversary E is accepted by the client where the client is not accepted by the server. Let $T_E(k)$ denote a polynomial bound on the number of oracle calls made by E.

Fix A, B, s, $\prod_{A,B}^s$ is an initiator oracle, and at time τ_0 the oracle sent flow C_0. If $\prod_{A,B}^s$ with both A, B not corrupted is to accept, then at some time $\tau_2 > \tau_0$ it must receive:

$$Trans, \delta$$

for some *Trans*. If no oracle previously outputs this flow, the probability the adversary can compute it correctly is negligible, because of the security of signature scheme.

So suppose some oracle does not output this flow. The form of the flow implies it must be a $\prod_{B,A}^{t}$ oracle which received C_0 as its own first flow. The probability that this event happens before time τ_0 is at most $2^{-f(k)}(T_E(k)-1) \leq \varepsilon(k)$, which is negligible. If it happens after time τ_0, $\prod_{A,B}^{s}$ would have a matching conversation.

We conclude that the probability that such a $\prod_{A,B}^{s}$ accepts without a matching conversation is negligible. Thus the probability

$$Pr[Succ] \leq \varepsilon(k)$$

is a negligible amount, where $\varepsilon(k)$ is a negligible function of k.

□

Lemma 2 (Client Authentication)If the symmetric encryption scheme, which encrypts the card data in $\mathscr{P}$, is secure against the adaptively chosen ciphertext attack, and the fuzzy commitment scheme is perfect hiding in protocol $\mathscr{P}$, the server cannot accept without the client even though any two of three factors are leaked.

Proof. Let E be an adversary that interacts with oracle $\prod_{B,A}^{t}$, if E passes server's authentication without client with just two factors are leaked, there must exist a matching conversation between E and the server oracle $\prod_{B,A}^{t}$. Then we can show the symmetric encryption scheme which encrypts the data stored in the smart card and the one-way function with distance- keeping which protects privacy of biometrics is insecure. The leakage of two factors leads to three cases as follows.

Case 1: The server cannot accept without the client even though the password and the data stored in the card are leaked.

If the password and the data stored in the card are leaked and there exists an adversary E who can let the server accept without the client, then we can prove the fuzzy commitment scheme is not perfect hiding and the one-way function with distance-keeping is insecure.

There exists a matching conversation between E and the server oracle $\prod_{B,A}^{j}$ if the following occurs. After obtaining the card data and the password by a Corruption query(Case 1), sending the first message to $\prod_{B,A}^{j}$. If E can pass the authentication process performed by $\prod_{B,A}^{j}$(Server's authentication), then there must exist a matching conversation between E and the server oracle $\prod_{B,A}^{j}$. The adversary E can query Execute($\prod_{A,B}^{i}$, $\prod_{B,A}^{j}$), Send($\prod_{B,A}^{j}$, m), Corruption($\prod_{A,B}^{i}$).

If there exists a matching conversation between E and $\prod_{A,B}^{t}$, this means that the adversary E successfully forges the first information C_0 of P. If the adversary wants to forge C_0, he need to get $y_i, h(PW_i'), SS_i'$ and g^x. The adversary has already known $h(PW_i), y_i$ through Corruption query(Case 1), but he can not obtain SS_i' directly. Let's assume that the adversary has already obtained SS_i', there is only one way in which he obtains SS_i is one-way function δ. If he computes δ successfully, this means that he has already retrieved r and W_i', and this means that he had broken up the one-way function δ. This is contradiction to definition 1 and 4, the probability that an adversary can break the one-wayness of δ and perfect hiding of commitment scheme is negligible.

Case 2: The server cannot guess the password by offline dictionary attack even though the biometric data and the data stored in the card are leaked.

If the data stored in the smart card and biometrics are leaked, and there exists an adversary E who can let the server accept without the client, then we can prove the symmetric encryption scheme which encrypts the data of the smart card is not secure against chosen ciphertext attack.

There exists a matching conversation between E and the server oracle $\prod_{B,A}^{j}$ if the following occurs. After obtaining the card data and the biometric data by a Corruption query(case 2), sending the first

message to $\prod_{B,A}^{t}$. If E passes the authentication process performed by $\prod_{B,A}^{t}$ without asking the partner oracle $\prod_{A,B}^{s}$, then there exists a matching conversation between E and $\prod_{B,A}^{t}$. The adversary E can query Execute($\prod_{A,B}^{i}$, $\prod_{B,A}^{j}$), Send($\prod_{B,A}^{j}$, m),Corruption($\prod_{A,B}^{i}$).

If there exists a matching conversation between E and $\prod_{B,A}^{t}$, this means the adversary E successfully forges the first message C_0 of the protocol $\mathscr{P}$. The adversary has already known w_i', y_i through Corruption query(Case 2), he decommits r using w_i', then he computes SS_i', but he can not obtain $h(PW_i)$ directly. If the adversary wants to forge C_0, he must extract $h(PW)$ from y_i, the data stored in the smart card. If this occurs, this means that the adversary has already broken up the security against chosen ciphertext attack of symmetric encryption scheme. This is contradiction to the definition in section 2.2.

Case 3: The server cannot accept without the client even though the password and the biometrics are leaked.

If password and biometrics are leaked, and there exists an adversary E who can let the server accept without the client, then we can prove the symmetric encryption scheme which encrypts the data of the smart card is not secure against chosen ciphertext attack.

There exists a matching conversation between E and the server oracle $\prod_{B,A}^{t}$ if the following occurs. After obtaining the password and the biometric data from the Corruption query(case 3), E sends the first message to $\prod_{B,A}^{t}$. If E can pass the authentication process performed by $\prod_{B,A}^{t}$ without asking the partner oracle $\prod_{A,B}^{s}$, then there exists a matching conversation between E and $\prod_{B,A}^{t}$.The adversary E can query Execute($\prod_{A,B}^{i}$, $\prod_{B,A}^{j}$), Send($\prod_{B,A}^{j}$, m),Corruption($\prod_{A,B}^{i}$).

If there exists a matching conversation between E and $\prod_{B,A}^{t}$, this means that the adversary successfully forges the first message C_0 of the protocol P, if E wants to forge C_0, he needs to know $ID_i, y_i, h(PW_i), SS', g^x$. He obtains w' and $h(pw_i)$ by Corruption(Case 3) queries, and extracts r by decommitting the fuzzy commitment using w', then he computes SS_i'. Because y_i is stored in the smart card, the E can not obtain it directly. This means that the adversary E has already forged a y_i' which can pass the server's authentication. If this occurs, this means the adversary has already broken up the symmetric encryption scheme which encrypts the data stored in the smart card. This is contradiction to the security against chosen ciphertext attack of symmetric encryption scheme(definition in section 2.2). □

Theorem 1. *(Mutual Authentication)If the public-key encryption scheme and symmetric encryption scheme are secure against adaptively chosen ciphertext attack, the signature scheme is secure against existential forgery under chosen-message attack, the fuzzy commitment scheme is perfect hiding, and the one-way function with distance keeping is secure, then $\mathscr{P}$ is a secure mutual authentication scheme.*

Proof. By lemma 1 and Lemma 2, theorem 1 holds. □

Theorem 2. *(Secure Key Agreement)If the computational Diffie-Hellman problem is hard in G, then $\mathscr{P}$ is a secure key agreement scheme.*

Proof. Let E be an adversary that interacts with two partner orales $\prod_{A,B}^{s}$ and $\prod_{B,A}^{t}$ in the execution of the protocol $\mathscr{P}$. At the end of the execution of $\mathscr{P}$, E submits a *Test* query to $\prod_{A,B}^{s}$, then the real session key sk or a random string is returned to E according the value of coin-flipping b. If $b = 0$, the session key is returned to E, otherwise, a random string is returned. Finally, E outputs a bit b', if $b = b'$, we say that E wins the game.

In order to simulate the environment of the game, a polynomial time machine T prepares all parameters in the protocol $\mathscr{P}$ to simulate both oracles $\prod_{A,B}^{i}$, $i \neq s$ and $\prod_{B,A}^{j}$, $j \neq t$, and answer the *Execute*, *Send*, and *Corruption* queries.

We now construct an algorithm T from E,which solves the computational Diffie-Hellman problem(CDH) in G with non-negligible probability. That is, given $g^x, g^y \in G$, $T's$ task is to compute and output the value of g^{xy}.

T simulates a challenger with E. T sets up the game with the group G and a generator $g \in G$. T generates a set of participants of size n_P. For each participants I, T sets $I's$ private key to be $x_I \in_R Z_q$ and sets their public key to be $X_I = g^{x_I}$. However for some participant P, T sets $P's$ public key is $X_p = g^x$. T also picks a random participant $Q \neq P$, a session number $t \in \{1,2,...,n_S\}$ and a number $l \in 1,2,...,n_H$. T starts $\mathscr{P}$ and answers $E's$ queries as follows.

The probability that E queries oracle $\prod_{B,A}^{t}$ for the *Test* session and that $pid_B = X_P$ is $1/(n_P^2 n_S)$. In this case, we note that E could not have corrupted participant P, and so T would not aborted.

E finally outputs a session key of the form (a,b,c) where $a,b \in G$ and $c \in G^4$. If $\prod_{A,B}^{S}$ was an initiator, then T outputs a as its guess. It is now easy to see that T solves *CDH* problem on input (g^x, g^y) with probability $\eta' = \eta \cdot (1/(n_P^2 n_S))$. □

6 Performance

In this section, we compare our scheme with the other two authentication schemes [15, 6], which can be proven secure. (Table 1)

Table 1 Performance

	computation complexity	rounds of communication
Pointcheval et al [15]	*N*hash+*N*asym	4
Fan et al [6]	4hash+4sym+1asym	4
Our scheme	4hash+1sym+1asym+1sign	2

Where N is the bit-length of biometrics.

hash denotes computation of hash function or one-way function.

sym denotes symmetric encryption and decryption

asym denotes asymmetric encryption and decryption

sign denotes signing and verifying of signature scheme.

Compared with the schemes [15, 6], our scheme has lower communication complexity than the schemes in [15, 6]. The computation complexity of our scheme is more than the scheme in [6] and less than the scheme in [15].

7 Conclusion

In this paper, a new multi-factor authenticated key exchange scheme, which combines with biometrics, password and smart card, is proposed. This scheme provides higher security in remote authentication and privacy preserving in biometrics.Compared with the previous schemes, our scheme has advantages such as multi-factor authentication, privacy preserving and lower communication complexity etc. In the future, we will propose new multi-factor authenticated key exchange scheme which can be proven secure under the standard model.

Acknowledgement This work is supported by the National Natural Science Foundation of China under Grants 60573043 and 60773175 and the Foundation of National Laboratory for Modern Communications under Grant 9140c1108010606.

References

[1] Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. In *Proc. of the 19th International Conference on the Theory and Application of Cryptographic*

Techniques (EUROCRYPT'00), Bruges, Belgium, LNCS, volume 1087, pages 139–155. Springer-Verlag, May 2000.

[2] Mihir Bellare and Phillip Rogaway. Entity authentication and key distribution. In *Proc. of the 13th Annual International Cryptology Conference (CRYPTO'93), Santa Barbara, California, USA, LNCS*, volume 773, pages 232–249. Springer-Verlag, August 1993.

[3] Abhilasha Bhargav-Spantzel, Anna Squicciarini, and Elisa Bertino. Privacy preserving multi-factor authentication with biometrics. In *Proc. of the 2nd ACM workshop on Digital identity management (DIM'06), Alexandria, VA, USA*, pages 63–72. ACM Press, October-November 2006.

[4] Julien Bringer, Hervé Chabanne, and Bruno Kindarji. Identification with encrypted biometric data made feasible. In *Proc. of the International Conference on Communications 2009 (ICC'09), Dresden, Germany*. IEEE, June 2009.

[5] Lin Chu-Hsing and Lai Yi-Yi. A flexible biometrics remote user authentication scheme. *Computer Standards Interfaces*, 27(1):19–23, November 2004.

[6] Fan Chun-I and Lin Yi-Hui. Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics. *Trans. Info. For. Sec.*, 4(4):933–945, December 2009.

[7] Yevgeniy Dodis. Introduction to cryptography(commitment scheme). G22.3033-003, December 2001.

[8] Eun-JunYoon. Secure fingerprint-based remote user authentication scheme using smartcards. In *Proc. of the 1st International Workshop on Internet and Network Economics 2005 (WINE'05), Hong Kong, China, LNCS*, volume 3828, pages 405–413. Springer-Verlag, December 2005.

[9] JingXu, Wen-Tao Zhu, and Deng-Guo Feng. An improved smart card based password authentication scheme with provable security. *Computer Standards and Interfaces*, 31(4):723–728, June 2009.

[10] Lee J.K. and Ryu S.R. . Fingerprint-based remote user authentication scheme using smart cards. *Electronics Letters*, 38(12):554–555, June 2002.

[11] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In *Proc. of the 6th ACM conference on Computer and communications security (CCS'99), Singapore*, pages 28–36. ACM Press, November 1999.

[12] Hyun-Sung Kim, Sung-Woon Lee, and Kee-Young Yoo. ID-based password authentication scheme using smart cards and fingerprints. *SIGOPS Oper. Syst. Rev.*, 37(4):32–41, October 2003.

[13] Kwon Youngkwon Lee and Taekyoung. An improved fingerprint-based remote user authentication scheme using smart cards. In *Proc. of the 6th International Conference on Computational Science and Its Applications (ICCSA'06,), Glasgow, UK, LNCS*, volume 3981, pages 915–922. Springer-Verlag, May 2006.

[14] Chun-Ta Li and Min-Shiang Hwang. An efficient biometrics-based remote user authentication scheme using smart cards. *J. Netw. Comput. Appl.*, 33(1):1–5, January 2010.

[15] David Pointcheval and Sébastien Zimmer. Multi-factor authenticated key exchange. In *Proc. of the 6th international conference on Applied cryptography and network security (ACNS'08), New York, USA, LNCS*, volume 5037, pages 277–295. Springer-Verlag, June 2008.

[16] Eun-Jun Yoon and Kee-Young Yoo. A new efficient fingerprint-based remote user authentication scheme for multimedia systems. In *Proc. of the 9th International Conference on Knowledge-Based Intelligent Information and Engineering Systems (KES'05), Melbourne, Australia, LNCS*, volume 3683, pages 332–338. Springer-Verlag, September 2005.

Dexin Yang received his Ph.D. degree at South China Agricultural University. Now he is a lecturer of Guangzhou City Polytechnic. His main research topics are cryptography and information security.

Bo Yang received received his Ph.D. degree at Xidian University in China. Now he is a professor of South China Agricultural University. His main research topics are cryptography and information security.