A New Unlinkable Secret Handshakes Scheme based on ZSS

Preeti Kulshrestha and Arun Kumar
Department of Mathematics, Statistics and Computer Science
G.B. Pant University of Agriculture and Technology
Pantnagar, India
Emails: ibspreeti@gmail.com and arun_ pal1969@yahoo.co.in

Abstract

Secret handshakes (SH) scheme is a key agreement protocol between two members of the same group. Under this scheme two members share a common key if and only if they both belong to the same group. If the protocol fails none of the parties involved get any idea about the group affiliation of the other. Moreover if the transcript of communication is available to a third party, she/he does not get any information about the group affiliation of communicating parties. The concept of SH was given by Balfanz in 2003 who also gave a practical SH scheme using pairing based cryptography. The protocol proposed by Balfanz uses one time credential to insure that handshake protocol performed by the same party cannot be linked. Xu and Yung proposed SH scheme that achieve unlinkability with reusable credentials. In this paper, a new unlinkable secret handshakes scheme is presented. Our scheme is constructed from the ZSS signature and inspired on an identity based authenticated key agreement protocol, proposed by McCullagh et al. In recently proposed work most of unlinkable secret handshake schemes have either design flaw or security flaw, we proved the security of proposed scheme by assuming the intractability of the bilinear inverse Diffie-Hellman and k-CAA problems.

Keywords:Authentication, Bilinear Pairing, Secret Handshakes, Pairing based Cryptography, Unlinkability, ZSS Signature.

1 Introduction

The secret handshakes (SH) is a cryptographic primitive introduced by Balfanz et al [2] in 2003, as a mechanism to prove group membership secretly. Using the protocol participants establishes a secure, anonymous, unlinkable and unobservable communication channel only if they are valid members of the same group. In a SH protocol, two members of the same group identify and authenticate each other secretly and share a common key for further communication. If the handshake protocol fails, the group affiliation of the participants will not be revealed. Also, a third party observing the exchange between two legitimate group members learns nothing about the group affiliation of the parties. Hence SH protect the identity information of users and also provide a privacy preserving property on their affiliations. Performing the successful SH is essentially equivalent to computing a common key between two interactive members of the same group. Hence the SH change according to the group members involved. A SH scheme can include roles too which allow the handshake between members from only one society to similar society.

At first Balfanz et al [2] proposed a SH protocol which is based on bilinear maps and secure under the BDH assumption. After that, many SH schemes have been proposed using different cryptographic primitives such as RSA [11], ElGamal [23] and message recovery signature [12, 15]. All these schemes use one time pseudonyms to achieve the unlinkability. Unlinkability property has been recognized as a desirable security requirement in many applications such as group signatures, identity escrow, electronic-cash and unlinkable credentials. These one time pseudonyms based SH scheme requires more storage and computation cost. Xu -Yung [18] in 2004 present the first SH scheme that achieves unlinkability while allowing users to reuse their credentials. This scheme is not based on any shared secret, it only offers a weak version of the privacy property which is called k-anonymity, where k is an adjustable parameter indicating the desired anonymity assurance. Jarecki -Liu [5] in 2007 proposed an efficient unlinkable secret handshake scheme, with no information leakage due to certification revocation, with no reliance on single use certificates and with support of revocation. Their scheme uses a key private public key group key management, which is a version of the public key broadcast encryption. Although their construction is not very efficient as every party requires $O(logn)$ exponentiations where n is the upper bound on the number of players affiliated with a single organization.

Huang -Cao [4] in 2009 improved the jarecki [5] scheme and proposed an efficient unlinkable secret handshakes scheme and claimed that scheme achieve affiliation hiding and unlinkability later on which is proved by Su [10] and

Youn -Park [20] that Huang -Cao scheme have a design flaw and insecure. Gu -Xue [3] in 2011 proposed an improved secret handshakes scheme with unlinkability based on the Huang -Cao scheme. Yoon [19] in 2011 points out that Gu -Xue scheme is insecure to key compromise impersonation (K-CI) attack and cannot provide master key forward secrecy.

Ateniese et al [1] proposed the first efficient unlinkable secret handshake scheme without random oracles. Inspired on Ateniese et al's scheme [1], Kulshrestha et al [7] also proposed a similar concept of dynamic matching for the members of the same group based on ZSS [21]. Wen-Gong [17] in 2014 also proposed dynamic matching between members of different groups which achieves unlinkability and untraceability without random oracles. Ryu et al [9] in 2010 proposed an efficient unlinkable secret handshakes scheme for anonymous communications allowing arbitrary two communication parties with same role in either one single group or multiple groups to privately authenticate each other. Recently Kulshrestha et al [6] points out that Ryu et al [9] scheme is insecure to K-CI attack.

Zhao et al [22] in 2010 proposed a new unlinkable SH scheme with reusable credentials which is based on symmetric pairing group and secure without random oracles under the truncated $q-ABDHE$ assumption. Their scheme possesses an advantage that it can be extended to the situation with roles and dynamic matching. Wen-Zhang [13] in 2011 proposed revocable SH scheme which supports revocation with backward unlinkability and impersonation against malicious GA. Wen -Gong [16] in 2013 proposed an unlinkable secret handshake with fuzzy matching for social networks which is secure under the assumption intractability of the decisional bilinear Diffie -Hellman problems. As several unlinkable secret handshakes scheme have been proposed in recent years, but most of them are fail to achieve the security requirement or have design flaw. In this paper we proposed a new role based unlinkable secret handshakes scheme from bilinear pairing. Our scheme is constructed from Bilinear Inverse Diffie- Hellman. Our scheme is based on ZSS signature [21] and is inspired by identity based authenticated key agreement by McCullagh et al [8]. We also give security proofs for the new scheme by under random oracle model.

Organization: The remainder of this paper is organized as follows. Section 2 recalls the preliminaries related to our work. Section 3 describes definitions and security requirements of a secret handshakes scheme. In Section 4 we give our unlinkable secret handshakes scheme based on ZSS signature and the security analysis of our proposed scheme. In section 5 we discuss efficiency issues. Finally we draw our conclusion in Section 6.

2 Preliminaries

2.1 Bilinear Pairing

Let G_1 and G_2 be two cyclic groups of the same large prime order q. G_1 is denoted as an additive group and G_2 as a multiplicative group. Let P denote a generator of G_1. A Bilinear Pairing is a function $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:

(1) [Bilinearity] for $P \in G_1$ and $a, b \in \mathbb{Z}_q^*$,
$e(aP, bP) = e(P, P)^{ab}$.

(2) [Non-degeneracy] $e(P, P) \neq 1$.

(3) [Computability] e can be efficiently computed in polynomial time.

2.2 Complexity Assumptions

Definition 1. Bilinear Inverse Diffie-Hellman (BIDH): Let G_1 and G_2 be a finite cyclic groups of same order q, and P is a generator of G_1. Let $a, b \in \mathbb{Z}_q^*$, the BIDH problem is to compute the value of bilinear pairing $e(P, P)^{a^{-1}b}$, when given $P, aP, bP \in G_1$.

Definition 2. The k-CAA problem is to compute $\frac{1}{s+h}P$ for some $h \in \mathbb{Z}_q^*$ when given $P, sP, h_1, h_2, ..., h_k \in \mathbb{Z}_q^*, \frac{1}{s+h_1}P, \frac{1}{s+h_2}P, ..., \frac{1}{s+h_k}P$.

2.3 ZSS Signature

ZSS Signature was proposed by Zhang et al [21] in 2004. The signature scheme consists of four algorithms a parameter generation algorithm $ParamGen$, a key generation algorithm $KeyGen$, a signature generation algorithm $Sign$ and a signature verification algorithm Ver.

Signature scheme is as follows:

ParamGen: Given a security parameter the algorithm generates the system parameter $\{G_1, G_2, e, q, P, H\}$ where G_1 and G_2 are the two cyclic groups of same order q, and P is a generator of G_1, e is the bilinear map and $H : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ is the cryptographic hash function.

KeyGen: Randomly selects $s \in_R \mathbb{Z}_q^*$ as the secret key and computes $P_{pub} = sP$ as the public key.

Sign: Given a secret key s, and a message m, computes the signature $S = \frac{1}{H(m) + s}P$.

Ver: Given a public key P_{pub}, a message m, and a signature S, verifies if $e(H(m)P + P_{pub}, S) = e(P, P)$.

The verification works because

$$\begin{aligned} e(H(m)P + P_{pub}, S) &= e(H(m)P + sP, (H(m) + s)^{-1}P) \\ &= e(P, P). \end{aligned}$$

3 Secret Handshakes Scheme

A secret handshakes scheme consists of the following probabilistic polynomial time algorithms:
Setup: It takes security parameter k as input and generates the public parameters *params*.
Create Group: This is an algorithm run by a group administrator GA, which takes *params* as input and generates a group public key GP_k and group secret key GS_k.
Add User: This is an algorithm between a user U and the GA of some group G. It takes *params* and GA's secret GS_k as input and generates a credential *cred* for the user U and makes U a valid member of the group. The group member keeps the *cred* secret.
Handshake: This is the authentication protocol. It is executed between users A and B, who want to authenticate each other on the public inputs ID_A, ID_B and *params*. The private input of each party is their secret credential and the output of the protocol for either party is either *reject* or *accept*.
A secret handshakes scheme must have the following security properties:
Completeness/Correctness: If two honest members belonging to the same group and run handshake protocol with valid credentials then both members always output *accept*.
Impersonator Resistance: An adversary not satisfying the rules of the handshake protocol is unable to successfully authenticate to an honest member.
Member impersonation game:
Init: The challenger C simulates setup, create group and add user protocol and sends group public key and params to adversary $\mathcal{A}$.
Corruption queries: $\mathcal{A}$ can make create group and add user queries for the secret information for some groups and members, let $U_{\mathcal{A}}$ denote the users that $\mathcal{A}$ controls.
Select: $\mathcal{A}$ select a target user U_t of a target group G_t such that $U_t \notin U_{\mathcal{A}}$, whom he would like to impersonate also $\mathcal{A}$ cannot corrupt the GA of U_t's group.

Interaction: $\mathcal{A}$ interacts with user $U_t \notin U_{\mathcal{A}}$, in which case C acts as the member of the group and execute handshake protocol with the adversary $\mathcal{A}$. $\mathcal{A}$ attempts to convince C that $\mathcal{A}$ is legitimate member of group G_t.
Output: If $\mathcal{A}$ succeeds in performing successful handshake then $\mathcal{A}$ wins the game but only if $\mathcal{A}$ never queried about the secret information of any of user U_t of group G_t in corruption queries and then the output of game is "1"otherwise the output is "0".
Detector Resistance: An adversary not satisfying the rules of the handshake protocol cannot decide whether some honest party satisfies the rule or not.
Member detection game:
Init: The challenger C simulates setup, create group and add user protocol and sends group public key and params to adversary $\mathcal{A}$.
Corruption queries: $\mathcal{A}$ can make create group and add user queries for the secret information for some groups and members, let U_A denote the users that $\mathcal{A}$ controls.
Select: $\mathcal{A}$ select a target user U_t of a target group G_t s.t. $U_t \notin U_{\mathcal{A}}$, whom he would like to detect also $\mathcal{A}$ cannot corrupt the GA of U_t's group.
Interaction: The challenger C acts as the member U_t of the group G_t or a simulator R and execute handshake protocol with $\mathcal{A}$. $\mathcal{A}$ attempts to detect whether $U_t \in G_t$. Challenger C flipped a random bit $b \leftarrow \{0, 1\}$. If $b = 1$, A interacts with U_t and $U_t \in G_t$. If $b = 0$, A interacts with R.
Output: The adversary $\mathcal{A}$ output a guess b^* for b and wins the game if $b^* = b$ and also $\mathcal{A}$ never queried about the secret information of user U_t and other member of group G_t in corruption queries. Otherwise $\mathcal{A}$ abort with "0".
Unlinkability: It is not feasible to tell whether two execution of the handshake protocol were performed by the same party or not, even if both of them were successful.
Linking game:
Init: The challenger C simulates setup, create group and add user protocol and sends group public key and params to adversary $\mathcal{A}$.
Corruption queries: $\mathcal{A}$ can make create group and add user queries for the secret information for some groups and members, let U_t denote the users that $\mathcal{A}$ controls.
Select: $\mathcal{A}$ select a target user U_t of a target group G_t s.t. $U_t \notin U_{\mathcal{A}}$ such that $\mathcal{A}$ cannot corrupt the GA of U_t's group and engages in a handshake protocol with U_t.
Interaction: The challenger C acts as the member U_t of the group G_t and execute handshake protocol with $\mathcal{A}$. $\mathcal{A}$ attempts to learn whether he engages in a handshake protocol with the same member or any other whom he did not

corrupt. Challenger C flipped a random bit $b \leftarrow \{0, 1\}$. If $b = 1$, $\mathcal{A}$ interacts with the same member and if $b = 0$, $\mathcal{A}$ interacts with different member.
Output: The adversary $\mathcal{A}$ output a guess b^* for b and wins the game if $b^* = b$ and also $\mathcal{A}$ never queried about the secret information of user U_t and other member of group G_t in corruption queries. Otherwise $\mathcal{A}$ abort with "0".

4 Secret Handshake protocol

4.1 Proposed Scheme

In this section we propose a role based unlinkable secret handshakes scheme based on of ZSS [21] signature.
Setup: Given a security parameter k the GA generates the system parameters $\langle G_1, G_2, e, q, P, H, H_1\rangle$ where G_1 and G_2 are the two cyclic groups of same order q, P is the generator of G_1, e is the bilinear map $e : G_1 \times G_1 \rightarrow G_2$, and two cryptographic hash functions $H : (0, 1)^* \rightarrow \mathbb{Z}_q^*$, $H_1 : (0, 1)^* \rightarrow (0, 1)^l$. We assume that GA for each group is associated with a unique group master key $s \in_R Z_q^*$ and public key $P_{pub} = sP$.
Create Group: There is no computation associated with creating a new group other than selecting a name for the group to which we refer to as $groupID$. We presuppose that $groupID$ is known to GA and group member as well and can't leak.
Add User: For each user U in the group is assumed to be associated with group secret key
$S = (H(groupID||role) + s)^{-1}P$, consequent to the group identity $groupID$ and the given $role$ to the user.
Handshake: The protocol is a 3-round interactive communication algorithm which executed between two arbitrary communicating parties A and B. Let A with secret S_A which correspond with $(groupID_A||role_A)$ and B with secret S_B which correspond with $(groupID_B||role_B)$ engage in a handshake protocol. They should successfully complete the protocol if both belong to the same group and possessing the same role in group. $ini, res, resp$, and $agree - on$ are predefined constant values which represent initiator, responder, respective (of A or B), and agree on (if the both verification succeeds) respectively.
The protocol proceeds as follows:
Round 1: $A \rightarrow B : X_A$

1. A Choose unique random nonce $r_A \in_R Z_q^*$.

2. Compute $X_A = r_A((H(groupID_A||role_A))P + P_{Pub})$.

Round 2: $B \to A : X_B, resp_B$

1. B Choose unique random nonce $r_B \in_R Z_q^*$.
2. Compute $X_B = r_B((H(groupID_B||role_B))P + P_{Pub})$ and $K_B = e(X_A, S_B)^{r_B}$.
3. Compute $resp_B = H_1(K_B||X_A||X_B||res)$

Round 3: $A \to B : resp_A$

1. Compute $K_A = e(X_B, S_A)^{r_A}$ and verify
   $resp_B = H_1(K_A||X_A||X_B||res)$
2. If verification succeeds compute
   $resp_A = H_1(K_A||X_A||X_B||ini)$

Upon receiving $resp_A$, B verifies it using it own key K_B, in the exactly same way as A.
If the both verification succeeds A and B can compute the shared key for the further communication as:

$$
\begin{aligned}
SK_A &= H_1(K_A||X_A||X_B||agree - on) \\
SK_B &= H_1(K_B||X_A||X_B||agree - on)
\end{aligned}
$$

respectively.
Correctness: If A and B are in the same group with the same role then

$$
\begin{aligned}
S_A &= (H(groupID_A||role_A) + s)^{-1}P \\
&= (H(groupID_B||role_B) + s)^{-1}P \\
&= S_B
\end{aligned}
$$

To see that $K_A = K_B$, we observe that

$$
\begin{aligned}
K_A &= e(X_B, S_A)^{r_A} \\
K_A &= e(r_B((H(groupID||role))P + P_{Pub}), \\
&\quad (H(groupID||role) + s)^{-1}P)^{r_A} \\
K_A &= e(P, P)^{r_A r_B}.
\end{aligned}
$$

Similarly for B.

4.2 Security of our protocol

An adversary $\mathcal{A}$ who can forge a valid signature can surely attack the SH protocol just as an honest member. Hence the probability to attack SH scheme cannot be smaller than the probability to forge a valid signature. The proof of security of the proposed scheme relies on the conjectured intractability of the Bilinear Inverse Diffie- Hellman Problem ($BIDHP$) and also depend upon complex assumption that there is no polynomial time algorithm for the collusion of attack algorithm with k traitors (k-CAA).

Lemma 1:

If an adversary $\mathcal{A}$ has a non null advantage $AdvIR_{\mathcal{A}} = Pr[\mathcal{A} wins the game IR]$ then another adversary B can be used which uses $\mathcal{A}$'s advantage to forge ZSS signature.

Proof:

If an adversary $\mathcal{A}$ is able to violate the impersonate resistant property of unlinkable secret handshakes scheme with a non negligible property ϵ then $\mathcal{A}$ who does not hold the credentials of the group will succeed in authenticating with other legitimate user of the group. Let P be the generator of the bilinear group G_1 with prime order q. Let e be the bilinear map and H be the hash function in ZSS signature.

Challenger C will interact with $\mathcal{A}$ as follows:

Setup: Challenger C starts by setting the master public key $P_{Pub} = sP$ where $s \in_R Z_q^*$ and sets the system parameters as params $\{G_1, G_2, e, q, P, H\}$. The adversary $\mathcal{A}$ is given params.

Add User: When adversary $\mathcal{A}$ querying for private information of some users U_i, Challenger C answer as follows: Chooses $y_i \in_R Z_q^*$ and creates public keys as $u_iP = y_iP - sP$, $y_iP = u_iP + sP$ and computes the private key as $y_i^{-1}P$.

Select: Adversary $\mathcal{A}$ declared the target user U_t of group G_t such that $U_t \notin U_i$.

Handshake: The challenger then picks αP as a outgoing message from user U_t and send it to $\mathcal{A}$. Then $\mathcal{A}$ outputs $k' \in Z_q^*$.

Forgery: The adversary wins the game if
$e(P, P)^{k'} = e(y_i^{-1}P, \alpha P)$. Since the credentials of the users are constructed from the ZSS signature so given an attacker $\mathcal{A}$ that wins the above game with probability ε. We construct another attacker $\mathcal{B}$ that can successfully forge the ZSS signature with probability ε.

1. $\mathcal{B}$, when given the ZSS public parameters $\{G_1, G_2, e, q, P, H\}$ send to $\mathcal{A}$.

2. $\mathcal{A}$ respond with target user U_t.

3. $\mathcal{B}$ then chooses αP and send to $\mathcal{A}$.

4. Then $\mathcal{A}$ outputs $k' \in Z_q^*$ and send to $\mathcal{B}$.

5. Since $e(y_i^{-1}P, \alpha P) = e(P, P)^{k'}$.

Hence this can be viewed as the ZSS signature on the message k' in $\{G_1, G_2, e, q, P, H\}$. Then $\mathcal{B}$ succeeds in forging the signature if and only if $\mathcal{A}$ wins the above game. Thus, if $\mathcal{A}$ can impersonate a user with valid credential, a polynomial time algorithm can be constructed to forge the ZSS signature. But the assumption is that ZSS signature is existentially unforgeable. So we can see that if this assumption holds, the probability ε that $\mathcal{A}$ can impersonate a valid user in the protocol should be negligible in value.
Lemma 2:
If an adversary $\mathcal{A}$ has a non null advantage $AdvDR_{\mathcal{A}} = Pr$ [$\mathcal{A}$ wins the game DR], then a probabilistic polynomial time adversary $\mathcal{B}$ can be create which use's $\mathcal{A}$'s advantage to solve $BIDH$ problem.
Proof:
The proposed SH scheme is detector resistant if no polynomially bounded adversary wins the following game against the challenger with non-negligible probability:
Setup: Challenger C starts by setting the master public key $P_{Pub} = sP$ where $s \in_R Z_q^*$ and sets the system parameters as params $\{G_1, G_2, e, q, P, H\}$. The adversary $\mathcal{A}$ is given params.
Add User: When adversary $\mathcal{A}$ querying for private information of some users U_i, Challenger C answer as follows: Chooses $y_i \in_R Z_q^*$ and creates public keys as $u_iP = y_iP - sP$, $y_iP = u_iP + sP$ and computes the private key as $y_i^{-1}P$.
Select: Adversary $\mathcal{A}$ announces a target user U_t of group G_t such that $U_t \notin U_i$, which is not included in any of the above queries.
Handshake: When $\mathcal{A}$ declared the target user U_t challenger answers αP as a message of user U_t. Since $\mathcal{A}$ does not know α, it cannot calculate $\alpha^{-1}P$ the correct private key for the user U_t. $\mathcal{A}$ needs to send a message for U_t, he chooses βP for an unknown β which is $x(\alpha P)$, where $x \in_R Z_q^*$. In response it will get a value from U_t as the value δP. This is genuine value from U_t.
Forgery: $\mathcal{A}$ outputs $y' \in Z_q^*$. The adversary wins the game if $y' = y$.
Given an adversary $\mathcal{A}$ that wins the above game with probability ε. We construct another attacker $\mathcal{B}$ that can successfully break the $BIDH$ assumption with probability ε.

1. For above define game actual key can be compute by $e(P, P)^{\alpha^{-1}\beta + \delta y_i^{-1}}$.

2. Given $({}_iP, \alpha P, \beta P, \delta P)$, $\mathcal{B}$ have non negligible advantage in calculating $e(P,P)^{\alpha^{-1}\beta+\delta y_i^{-1}}$, because $\mathcal{B}$ does not know private key $\alpha^{-1}P$ of U_t.
3. $\mathcal{B}$ set $\gamma = e(P,P)^{\alpha^{-1}\beta+\delta y_i^{-1}}$.
4. Since $\mathcal{B}$ know $(y_i^{-1}P, \delta P)$, so it calculate $\eta = e(P,P)^{\delta y_i^{-1}}$.
5. $\mathcal{B}$ can compute $e(P,P)^{\alpha^{-1}\beta}$, as $e(P,P)^{\alpha^{-1}\beta} = \dfrac{\gamma}{\eta}$.

Then $\mathcal{B}$ has successfully broken the $BIDH$ assumption with probability ε. Thus if $BIDH$ assumption holds the probability ε that $\mathcal{B}$ can violate the detector resistance property should be a negligible value.

Lemma 3:

If an adversary $\mathcal{A}$ has a non null advantage $Advlink_{\mathcal{A}} = Pr[\mathcal{A}$ wins the game Linking], then their exist an algorithm B can be solve $k-CAA$ in polynomial time.

Proof:

Let an adversary $\mathcal{A}$ is able to violate the unlinkability property of unlinkable secret handshakes scheme with a non negligible property ε using an adaptive chosen message attack then there exist an algorithm $\mathcal{B}$ to solve the $k-CAA$ in polynomial time with a non negligible probability ε'. Suppose $\mathcal{A}$ is given a challenge to compute $(h+s)^{-1}P$ for some $h \notin (h_1, h_2, ..., h_{q\mathcal{A}})$ for given $P \in G_1, P_{Pub} = sP, h_1, h_2, ..., h_{q\mathcal{A}} \in \mathbb{Z}_q^*$ and $(h_1+s)^{-1}P, (h_2+s)^{-1}P, ..., (h_{q\mathcal{A}}+s)^{-1}P$.

Setup: $\mathcal{A}$ plays the role of the GA and setting the master public key $P_{Pub} = sP$ where $s \in_R Z_q^*$ and sets the system parameters as params $\{G_1, G_2, e, q, P, H\}$.

Add User: $\mathcal{B}$ answer add user queries itself. $\mathcal{A}$ never repeats add user query. When $\mathcal{A}$ makes add user query on identity ID_i for $1 \le i \le q_{\mathcal{A}}$. $\mathcal{B}$ respond α_i to $\mathcal{A}$ as the response of the hash oracle query on ID_i.

$\mathcal{A}$ makes a secret key query for α_i. If $\alpha_i = h_k$, $\mathcal{B}$ returns $(h_k+s)^{-1}P$ to $\mathcal{A}$. Otherwise the process stop and $\mathcal{B}$ has failed.

Handshakes: Finally $\mathcal{A}$ halts and outputs secret key S for identity ID. Here the hash value of ID is some α_k.

Forgery: (ID, S) is a valid forgery and $H(ID) = \alpha_n$ and $\alpha_n \notin (h_1, h_2, ..., h_{q_{\mathcal{A}}})$, it satisfies $e(H(ID)P + P_{Pub}, S) = e(P,P)$. $\mathcal{A}$ cannot distinguish between $\mathcal{A}$'s simulation and real life because the hash function behaves as a random oracle. So $\mathcal{A}$ outputs $S = (\alpha_n + s)^{-1}P$ as solution of challenge.

5 Comparison of efficiency and security issues

In this section we compare our proposed scheme with some previous schemes in terms of computation cost and security properties. As successful secret handshakes is equivalent to a key agreement between two members of the same group. So it is necessary for a secret handshakes scheme to fulfill security requirement of secret handshakes protocol as well as key agreement protocol as define in [4]. In the following table we list the number of multiplications (M), the number of exponentiation (E), and the number of pairing (Pr) are done to complete the respective schemes and the security properties unlinkable (UL), AKE security (AKE), perfect forward security (PFS), key independency (KI), affiliation hiding (AH), mutual authentication (MA), and key compromise impersonation ($K-CI$). For each scheme we show the computation cost per party. In case of computation cost our scheme is as good as known schemes.

Schemes	**Computations**	**Assumption**	**Remark**
Huang-Cao[4]	$1M + 1Pr + 1E$	BDH	Design flaw and insecure
Gu-Xue [3]	$1M + 1Pr$	BDH	not K-CI, not MFS
Ryu[9]	$1M + 1Pr + 1E$	BDH	not K-CI
Proposed	$1M + 1Pr + 1E$	$BIDH$	UL, AH, AKE, PFS, KI, MA, K-CI

In Huang-Cao scheme an adversary doesn't register himself as a group member can established a successful and unlinkable secret handshake with legitimate group users due to a design flaw in scheme and the scheme also suffer with the security flaw as it not provide affiliation hiding property and AKE security. Gu-Xue scheme achieved strong unlinkability against an adversary but cannot provide $K-CI$ resilience and master key forward secrecy (MFS), as Gu-Xue scheme is based on ID- based AKE scheme therefore $K-CI$ and MFS are important security requirement. Due to this reason, Gu-Xue scheme is insecure for practical application. As recently Kulshrestha et al. pointed out that Ryu et al s scheme also be unsuccessful to provide $K-CI$ resilience security.

6 Conclusion

In this paper we proposed an unlinkable secret handshake scheme based on ZSS signature inspired on the McCullagh et al. We also compared the computational complexity and security attributes of the new scheme with other known secret handshakes schemes. We observed that the proposed scheme is comparable to known schemes in case of computation cost and better for security attributes.

Acknowledgment

The authors express sincere thanks to Professor Sunder Lal and Mr. Manmohan Singh Chauhan for their help and encouragement.

References

[1] G. Ateniese, M. Blanton and J. Kirsch, "Secret Handshakes with Dynamic and Fuzzy Matching". In Network and Distributed System Security Symposium, NDSS, pages. 159-177, 2007.

[2] D. Balfanz, G. Durfee, N. Shankar, D. Smetters, J. Staddon, and H.C. Wong, "Secret Handshakes from Pairing based Key Agreement". In IEEE Symposium on Security and Privacy, pages. 180-196, 2003.

[3] J. Gu and Z. Xue, "An Improved Efficient Secret Handshakes Scheme with Unlinkability". IEEE Communications Letters, vol. 15, no. 2, pages 259-261, 2011.

[4] H. Huang and Z. Cao, "A Novel and Efficient Unlinkable Secret Handshakes Scheme". IEEE Communications Letters, vol. 13, no. 5, pages 363-365, 2009.

[5] S. Jarecki and X. Liu, "Unlinkable Secret Handshakes Scheme and Key Private Group Key Management Schemes". In ACNS-2007, LNCS 4521, Springer Verlag, pages 270-287, 2007.

[6] P. Kulshrestha, A. K. Pal, and M. S. Chauhan, "Cryptanalysis of Efficient Unlinkable Secret Handshakes for Anonymous Communications". IOSR Journal of Computer Engineering, vol. 17, issue II, pages 71-74, 2015.

[7] P. Kulshrestha and A. K. Pal, "A New Secret Handshakes Scheme with Dynamic Matching based on ZSS". International Journal of Network Security and its Applications, vol. 7, no. 1, pages 67-78, 2015.

[8] N. McCullagh and Paulo S. L. M. Barreto, "A New Two Party Identity based Authenticated Key Agreement". Topics in Cryptology CT-RAS-2005, LNCS Volume 3376, pages 262-274, 2005.

[9] E. K. Ryu, K. Y. Yoo and K. S. Ha, "Efficient Unlinkable Secret Handshakes for Anonymous Communications". Journal of Security Engineering, vol. 17, no. 6, pages 619-626, 2010.

[10] R. Su, "On the Security of a Novel and Efficient Unlinkable Secret Handshakes Scheme". IEEE Communications Letters, vol. 13, no. 9, pages 712-713, 2009.

[11] D. Vergnaud, "RSA-based Secret Handshakes".In WCC 2005, LNCS 3969, Springer Verlag, pages 252-274, 2005.

[12] Y. Wen, F. Zhang and L. Xu,"Unlinkable Secret Handshakes from Message Recovery Signature".Chinese Journal of Electronics, vol.19, no.4, pages 705-709, 2010.

[13] Y. Wen and F. Zhang, "A New Revocable Secret Handshakes Scheme with Backward Unlinkability". Euro PKI-2010, LNCS 6711, Springer Verlag, pages 17-30, 2011.

[14] Y. Wen and F. Zhang, "Delegatable Secret Handshakes Scheme". The journal of System and Software, Elsevier, vol. 84, issue 12, pages 2284-2292, 2011.

[15] Y. Wen, F. Zhang and L. Xu, "Secret Handshakes from ID-Based Message Recovery Signatures: a Generic Approach". Computers and Electrical Engineering, vol. 38, pages 96-104, 2012.

[16] Y. Wen and Z. Gong, "An Unlinkable Secret Handshake with Fuzzy Matching for Social Networks". Eighth International Conference on P2P, Parallel Grid, Cloud and Internet Computing, vol. 59, pages 347-352, 2013.

[17] Y. Wen and Z. Gong, "A Dynamic Matching Secret Handshake Scheme without Random Oracle". In NSS-2014, LNCS 8792, Springer Verlag, pages 409-420, 2014.

[18] S. Xu and M. Yung, "K- anonymous Secret Handshakes with reusable Credentials". In Proc. CCS'04: 11th ACM Conference on Computer and Communications Security, page 158-167, 2004.

[19] E. J. Yoon, "Cryptanalysis of an Efficient Secret Handshakes Scheme with Unlinkability". International Conference on Advances in Engineering, vol. 24 pages 128-132, 2011.

[20] T. Y. Youn and Y. H. Park, "Security Analysis of an Unlinkable Secret Handshakes Scheme". IEEE Communications Letters, vol. 14, no. 1, pages 4-5, 2010.

[21] F. Zhang, R. Safavi, W. Susilo, "An Efficient Signature Scheme from Bilinear Pairing and Its Application". Proceeding in LNCS, Springer Verlag, pages 277-290, 2004.

[22] G. Zhao and C. Tan, "An Efficient Unlinkable Secret Handshake Protocol without ROM". In IEEE Conference on Wireless Communication, Networking and Information Security WCNIS-2010, pages 486-490, 2010.

[23] L. Zhou, W. Susilo and Y. Mu, "Three-Round Secret Handshakes Based on ElGamal and DSA". ISPEC-2006, LNCS 3903, Springer Verlag, pages 332-342, 2006.

Appendix

1. Resistance to the attack described in [10] and [20]: Remember the attack described by Su [10], and Youn-Park [20] on Huang-Cao [4] scheme. An adversary $\mathcal{A}$ who obtains the group public key PK can break the AKE security of the scheme [4] as follows:
Adversary $\mathcal{A}$ chooses $r \in_R Z_q^*$ and computes $Q_{\mathcal{A}} = rP$ and $S_{\mathcal{A}} = rPK$. $Q_{\mathcal{A}}$ and $S_{\mathcal{A}}$ satisfies the equation $S_{\mathcal{A}} = sQ_{\mathcal{A}}$, since $S_{\mathcal{A}} = rPK = r(sP) = s(rP) = sQ_{\mathcal{A}}$. This show a non registered illegal user $\mathcal{A}$ can successfully perform a handshake with register user of her choice. However, this situation will not occur in our proposed scheme because in our scheme exchanged information is
$X_A = r_A((H(groupID_A||role_A))P + P_{Pub})$
Since $groupID$ and group secret s is exclusively for the group member. So adversary $\mathcal{A}$ who wish to initiate a secret handshake protocol with valid user is not able to compute $X_{\mathcal{A}}$ due to lack of information about the target group $groupID$ and group secret s. Therefore $\mathcal{A}$ is not able to relate public

information as defined above to compute X_A. So our scheme is $AKE - Secure$. Furthermore in this case $\mathcal{A}$ cannot generate a valid $resp_A$ and makes legitimate user accept except for negligible probability. So our scheme also fulfills *Mutual Authentication*.

2. Resistance to the attack described in [19]: Remember the key compromise impersonation (K-CI) attack described by Yoon [19] on Gu-Xue scheme [13]. An adversary $\mathcal{A}$ who obtain the private key of user U_A can impersonate as U_B to U_A and can break the K-CI security of the scheme [3]. Now we show this situation will not occur in our proposed scheme. Let private key of user U_A is $S_A = (H(groupID_A||role_A) + s)^{-1}P$, which disclosed to the adversary $\mathcal{A}$. Even then he cannot impersonate as U_B to U_A as follows: User U_A chooses $x \in_R Z_q^*$ and Compute $X_A = x((H(groupID_A||role_A))P + P_{Pub})$ and then send X_A to A, now using X_A and private key of U_A adversary can compute $e(X_A, S_A) = e(P, P)^{r_A}$ we claim that even possessing the secret of user U_A adversary cannot generate $Y = y((H(groupID_A||role_A))P + P_{Pub})$, $y \in_R Z_q^*$ due lake of knowledge of $groupID$ and due to hardness of $BIDH$. So our scheme is $K - CI$ *secure*.