A Dynamic Matching Secret Handshake Scheme without Random Oracles*

Yamin Wen[1] and Zheng Gong[2,3,**]

[1] School of Mathematics and Statistics
Guangdong University of Finance & Economics
Guangzhou 510320, P.R. China
yamin.wen@gmail.com
[2] School of Computer Science
South China Normal University
Guangzhou 510631, P.R. China
cis.gong@gmail.com
[3] Shanghai Key Laboratory of Integrate Administration Technologies
for Information Security, Shanghai 200240, China
cis.gong@gmail.com

Abstract. Secret handshake schemes allow mutually anonymous authentication between members of organizations. In this paper, a new unlinkable secret handshake scheme with dynamic matching is proposed (which is named USH-DM). Considering the existence of multiple different groups, the implementation of USH-DM achieves dynamic matching between members among completely different groups. In particular, USH-DM enhances the privacy of group members, which enables the transcripts of group members to remain unlinkable and untraceable. Without using the random oracle, USH-DM is proved secure by assuming the intractability of the decisional bilinear Diffie-Hellman and subgroup decision problems.

Keywords: Anonymity, Secret handshakes, Unlinkability, Dynamic matching.

1 Introduction

With the amazing development of online applications via open communication networks, privacy-preserving techniques are increasingly significant for the future growth of web services. Privacy-preserving authentication plays an indispensable role among the whole privacy concerns. A promising cryptosystem,

* This work is supported by the Natural Science Foundation of China (No.61300204, 61100201), the Natural Science Foundation of Guangdong (No.S2012040006711), the Foundation for Distinguished Young Teachers in Higher Education of Guangdong (Yq2013051) and the Project of Science and Technology New Star of Guangzhou Pearl Rivel (2014J2200006).

** The corresponding author.

M.H. Au et al. (Eds.): NSS 2014, LNCS 8792, pp. 409–420, 2014.

which is named *secret handshake*, was first introduced by Balfanz *et al.* [2] for mutually anonymous authentication. Roughly speaking, secret handshakes require that one user will only discover his/her affiliation to the other user if they belong to the same organization. Thus participants only recognize that they are members of the same organization, without leaking their true identities in this organization. As suggested in [1,2], secret handshakes have many interesting applications. A typical example is that members of FBI secretly authenticate each other. The prover will reveal his affiliation (FBI) if and only if the verifier holds the same one, and vice versa. Moreover, a practical secret handshake scheme can also be used in networking protocols, such as the devices with legitimate credentials can be mutually authenticated for sharing secret keys. For instance, Li and Ephremides [12] proposed that secret handshakes are available for realizing the anonymous routing protocol in *ad hoc* networks.

To match up the security requirements of real-life applications, many extensions of secret handshakes have been proposed. One of the extensions is to include roles, so that users can authenticate with the members who hold specific roles in the same group [2]. Furthermore, Ateniese *et al.* [1] proposed the dynamic matching model which allows users to make more flexible authentication policies. The new model aims to allow secret handshakes between members from sister organizations instead of the same organization. For instance, an online game operator administers a distributed social networks on two cities. The two cities can be considered as sister groups and named as "City-A" and "City-B". Each registered user can designate his favorite attributes that his partner must satisfy, such as the city and the grade. And then users from the two cities can execute a successful secret handshake only if their attributes are matching. In other words, users from City-A can play with other users from City-B, without restricting to the same city.

The secret handshake scheme proposed by Ateniese *et al.* in [1] can realize above application well. However, Ateniese *et al.*'s scheme only realizes limited dynamic matching. Since the different sister groups are created and distinguished by group name in Ateniese *et al.*'s scheme, the different groups still share the same group public/private keys which are actually managed by an upper operator. And hence, the limited dynamic matching model still relies on a single Group Authority (GA) for different groups. In real-life applications, users may expect to authenticate with other partners from different groups with the assumption of multiple self-governed group authorities. In such a setting, more dynamic matching is possible. One of the most appealing applications would be the authentication between members from different Secret Interest Groups(SIGs) in online social networks. SIGs are self-managed groups which have independent Group Authorities (GAs). Two registered users (e.g., Alice and Bob) from different SIGs can secretly authenticate with each other if their polices can be matched. Therefore, it is necessary to search for a practical secret handshake scheme which can achieve the real dynamic matching in multiple-groups environment.

Related Works. After Balfanz *et al.*'s initial work [2], many secret handshake schemes have been proposed from different cryptographic primitives, such as

pairing [2], CA-oblivious encryption [6] and ElGamal [27]. According to the lifetime of credentials, the rich literature can be sorted as the following two types.

- **Secret handshakes with one-time pseudonyms.** The pioneering publication is derived from Balfanz *et al.* [2] based on pairing. It uses one-time pseudonyms to ensure that the instances of the secret handshake protocol, which were performed by the same parties, cannot be linked. Subsequently, Castelluccia *et al.* [6] proposed a new secret handshake scheme using a novel tool so-called *CA-oblivious public-key encryption*. Since any Oblivious Signature Based Envelope (OSBE) scheme can easily be converted to a secret handshake scheme [13], Zhou *et al.* [27] constructed an improved scheme by using of ElGamal and DSA signature. These schemes are slightly more efficient than Balfanz *et al.*'s original scheme, but still does not satisfy unlinkability unless members use one-time pseudonyms. However, one-time pseudonyms based schemes require more storage and computation cost owing to the single-use of pseudonyms for achieving unlinkability in practice. Since Group Authority (GA) has all secret information of group users, GA can impersonate or frame one user with malicious behaviors. Accordingly, the unlinkability against GA can unlikely be achieved by using one-time pseudonyms.

- **Unlinkable secret handshakes with reusable credentials.** Xu and Yung [25] first offers scheme which achieves unlinkability with reusable credentials in a weaker way. By using the blinding technique, Huang and Cao proposed a novel and efficient unlinkable secret handshake scheme [8] based on Balfanz *et al.*'s scheme [2]. Subsequently, Su [18] pointed out a successful impersonation attack on Huang and Cao's proposal [8]. And hence Gu and Xue[7] proposed an improved efficient secret handshake scheme with unlinkability by amending Huang and Cao's proposal [8]. Wen *et al.*[22] also presented a new unlinkable secret handshake scheme with reusable credentials under the random oracle. Based on the construction of identity-based encryption [20], Ateniese *et al.* [1] proposed the first efficient unlinkable secret handshake scheme without random oracles. However, there only needs selecting a name for the group when creating a new group in their scheme. Different groups are distinguished just through each name, while all groups share a pair of group keys in the whole secret handshake system. From the AddMember algorithm, we can see that the scheme treats a set of members with identical attributes as an entity instead of different individual. It is essentially a group key agreement scheme between different sub-group members in a large group environment and thus limits the popularization of secret handshakes. Due to the less efficiency of Ateniese *et al.*'s scheme [1], Zhao *et al.* [26] constructed an efficient unlinkable secret handshake protocol without random oracles. But Zhao *et al.*'s proposal [26] still cannot carry out dynamic matching in multiple-groups environment. Therefore, it is meaningful to realize a new unlinkable secret handshake scheme with dynamic matching without random oracles, which can be adapted to more practical applications.

Subsequently, Jarecki *et al.* [9] proposed an unlinkable secret handshake scheme with revocation by using central key management (broadcast encryption). But it strongly assumes that all groups have the same numbers of group users and revoked users. Also the group public key will increase linearly with the numbers of group users, which is impractical in large-scale applications (e.g., online social network). Based on Ateniese *et al.*'s scheme [1], Sorniotti and Molva [14,16] proposed revocable secret handshake schemes. Their proposals provide the revocation checking of the participants who have initiatively left their groups during handshakes. Nevertheless, they are still unable to trace and revoke malicious group members for complete unlinkability and untraceability. Moreover, their proposals still have the same weakness of Ateniese *et al.*'s scheme [1].

Our Contributions. A new construction of unlinkable secret handshake scheme with dynamic matching without random oracles, which is named USH-DM, is presented in this paper. Our new proposal USH-DM aims to fix the weakness of Ateniese *et al.*'s scheme. The enhancements of USH-DM are three-fold. Firstly, we apply a new technique of full domain subgroup hiding to realize a practical secret handshake scheme, which enables USH-DM can be applied to the real multiple-groups environment. Secondly, the authentication policies can be flexible for matching more complicated attributes based on different groups. USH-DM also achieves efficient and unlinkable with reusable credentials. Finally, USH-DM is provably secure without random oracles by assuming the intractability of Decisional Bilinear Diffie-Hellman and Subgroup Decision problems.

Organization. The remainder of this paper is organized as follows. In Section 2, we recall the preliminaries related to our work, including the definitions and security properties of secret handshake schemes. In Section 3, a new unlinkable secret handshake scheme with dynamic matching named USH-DM is described. Section 4 gives the security and performance analyses of our proposal. Section 5 concludes the paper.

2 Preliminaries

In this section, we recall the notions and definitions of bilinear pairings of composite order and complexity assumptions, which will be used in later sections. The definition and security requirements of secret handshakes are also briefly reviewed.

2.1 Bilinear Pairings of Composite Order

Composite order bilinear pairings were first introduced in [4], which will be used in our proposal. We first review some general notions about bilinear groups and pairings. Most of cryptosystems based on pairings are based on bilinear groups with prime order for simplicity. In our case, we define $\mathbb{G}$ is a (multiplicative)

cyclic group of composite order N, where $N = pq$ is the product of two different primes p and q. Let g is a generator of $\mathbb{G}$. A one-way map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a bilinear pairing if the following conditions hold.

- **Bilinear:** For all $g \in \mathbb{G}$, s.t., g is a generator of $\mathbb{G}$, and $a, b \in \mathbb{Z}_N$, $e(g^a, g^b) = e(g, g)^{ab}$.
- **Non-degeneracy:** $e(g, g) \neq 1$, i.e., if g generates $\mathbb{G}$, then $e(g, g)$ generates $\mathbb{G}_T$ with order N.
- **Computability:** There exists an efficient algorithm for computing $e(.,.)$.

2.2 Complexity Assumptions

Definition 1. (Decisional Bilinear Diffie-Hellman (DBDH) Problem [20]) *Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order q along with a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, and let $g \in \mathbb{G}$ be generator of $\mathbb{G}$. The challenger flips a fair binary coin β and outputs the tuple $(g, A = g^a, B = g^b, C = g^c, Z = e(g, g)^{abc})$ when $\beta = 1$. Otherwise, the challenger outputs the tuple $(g, A = g^a, B = g^b, C = g^c, Z = e(g, g)^d)$ where $d \leftarrow_R \mathbb{Z}_p^*$. The DBDH problem is to output a guess β' of β.*

DBDH Assumption: We say that the (t, ϵ)-DBDH assumption holds if there exists no algorithm can solve the DBDH problem with a non-negligible advantage ϵ in a polynomial time bound t. In other words, for $g \in \mathbb{G}$ and $a, b, c, d \leftarrow_R \mathbb{Z}_p^*$, distinguish between tuples of the form $(g, g^a, g^b, g^c, e(g, g)^{abc})$ and $(g, g^a, g^b, g^c, e(g, g)^d)$ is infeasible.

Definition 2. (Subgroup Decision (SD) Problem [4,21]) *Given a tuple $(p, q, \mathbb{G}, \mathbb{G}_T, e)$, in which p and q are independent secure primes, $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups of order $N = pq$ with efficiently computable group operations and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a bilinear map. Let $\mathbb{G}_q \subset \mathbb{G}$ be the q-order subgroup of $\mathbb{G}$. Given an element x which is selected randomly either from $\mathbb{G}$ or from $\mathbb{G}_q$, the subgroup decision problem is to distinguish whether x is in $\mathbb{G}_q$.*

The Subgroup Decision Assumption: Let the success probability of solving the subgroup decision problem is defined as $Adv_{sd} = \frac{1}{2} + \varepsilon$, we say that the subgroup decision assumption holds if ε is negligible.

2.3 Secret Handshakes: Definition and Security Requirements

A secret handshake scheme (denoted by SHS) operates in an environment which consists of a set of groups managed by a set of group authorities, and a set of users $U_1, \cdots, U_n$ registered into some groups. Based on the definitions in [1,2], an unlinkable SHS without traceability and revocation consists of the following probabilistic polynomial-time algorithms:

- SHS.Setup: The Setup algorithm selects high-enough security parameter κ to generate the public parameters `params` common to all subsequently generated groups.

- SHS.CreateGroup: CreateGroup is a key generation algorithm executed by GA to establish a group G. It inputs `params`, and outputs a pair of group public key gpk_G and group secret key gsk_G.
- SHS.AddMember: AddMember is a two-party protocol run by GA and a user. GA plays a role of the administrator for the group, which issues credential for a legitimate member of the group. After verifying the user's real identity(U), GA outputs the user's group credential $\mathsf{cred_U}$ using GA's group keys (gpk_G, gsk_G). Thus, the user becomes a valid member of the group after the protocol.
- SHS.Handshake: Handshake is a two-party authenticate protocol executed by two anonymous users (A, B), who may belong to different groups. This protocol inputs the anonymous users' secrets $(\mathsf{cred_A}, \mathsf{cred_B})$ and public parameters. The output of the protocol for each member is either "1" or "0" depending on whether the authentication policies of participants are matched. If A's target requirements including group and properties are matched by B and vice versa, A and B will share a common session key K for subsequent secure communication and the protocol outputs "1". Otherwise, the output is "0".

A secret handshake scheme must satisfy the basic security requirements: *Completeness, Impersonator Resistance, Detector Resistance* and *Unlinkability.* The formal definition can be referred to [23,11]

Completeness: The SHS protocol will succeed with overwhelming probability, if the interactive participants satisfy the authentication policy of the counterparty.

Impersonator Resistance: An adversary who attempts to impersonate a legitimate user of one group cannot succeed with a non-negligible probability. In other words, any adversary not satisfying the authentication policies cannot accomplish a successful secret handshake.

Detector Resistance: An adversary will not succeed with non-negligible probability when he activates an SHS.Handshake with one honest member in order to determine whether he satisfies the authentication policies or not.

Unlinkability: This requirement implies that any adversary cannot find any relation between two instances of the Handshake algorithm, which involved with the same honest members.

3 A New Unlinkable Secret Handshake Scheme with Dynamic Matching

Developed from the idea of secret handshake [1], a new unlinkable secret handshake scheme (USH-DM) which supports dynamic matching in multiple-groups environment is designed as follows.

- Setup: Given a security parameter κ, the algorithm runs $Setup(1^\kappa) \rightarrow \mathtt{params}$. The public parameters $\mathtt{params} = (N, \mathbb{G}, \mathbb{G}_T, e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T, g, u, h, H_1, v_0, \cdots, v_n, F)$, which are shared by all participants in the scheme. Here g is a generator of a group $\mathbb{G}$ of composite order $N = pq$, where p and q are

random primes. Let $\mathbb{G}_p$ and $\mathbb{G}_q$ be the cyclic subgroups of $\mathbb{G}$ with respective order p and q. The algorithm picks a generator h of $\mathbb{G}_q$. Other generators of $\mathbb{G}$ $u, v_0, \cdots, v_n$ are selected randomly from $\mathbb{G}$. In addition, $H_1 : \{0,1\}^* \to \mathbb{Z}_N^*$ is a cryptographic hash function. F is a function which represents attribute. Suppose that one attribute P is represented by n-bits string $(\mu_1, \mu_2, \cdots, \mu_n)$, $F(P)$ is denoted by $v_0 \prod_{i=1}^{i=n} v_i^{\mu_i}$.

- CreateGroup: The GA chooses $t \leftarrow_R \mathbb{Z}_N^*$, and generates $T = g^t$. GA outputs its group secret key $gsk = t$ and group public key $gpk = T$.
- AddMember: If a user U with property P wants to join the group, GA issues attribute credential for the user U. GA randomly selects $s \leftarrow_R \mathbb{Z}_N^*$, and computes attribute credential $cred_{U,P} = (C_{U1}, C_{U2}) = (u^t \cdot F(P)^s, g^{-s})$. The user verifies that the credential is valid by testing $e(C_{U1}, g) \cdot e(F(P), C_{U2}) \stackrel{?}{=} e(u, gpk)$.
- Handshake: Supposing A and B are two parties who want to execute a secret handshake protocol to authenticate each other without leaking their privacy. Participant A runs the protocol with $cred_{A,P_A}$ and (tpk_A, P_{AT}) which are the target group public key and target property (i.e., authentication policy) of the participant A, and participant B runs it with $cred_{B,P_B}$ and (tpk_B, P_{BT}) which are the target group public key and target property (i.e., authentication policy) of the participant B. For example, A who is a lawyer of insurance company wants to handshake with a professor (P_{AT}) of higher university (tpk_A), and simultaneously B who is a professor of higher university wants to handshake with a lawyer (P_{BT}) of insurance company (tpk_B). The protocol proceeds as follows:

  1. $\mathsf{A} \to \mathsf{B} : \{\sigma_{A1}, \sigma_{A2}, \pi_A\}$
     (a) A chooses $t_{A1}, t_{A2}, r_A \leftarrow \mathbb{Z}_N^*$.
     (b) A computes
     $$\sigma_{A1} = C_{A1} \cdot h^{t_{A1}} \cdot u^{r_A},$$
     $$\sigma_{A2} = C_{A2} \cdot h^{t_{A2}},$$
     $$\pi_A = g^{-t_{A1}} \cdot F(P_A)^{-t_{A2}}.$$
     Finally, A sends σ_{A1}, σ_{A2} and π_A to B.

  2. $\mathsf{B} \to \mathsf{A} : \{\sigma_{B1}, \sigma_{B2}, \pi_B, V_B\}$
     (a) B chooses $t_{B1}, t_{B2}, r_B \leftarrow \mathbb{Z}_N^*$.
     (b) B computes
     $$\sigma_{B1} = C_{B1} \cdot h^{t_{B1}} \cdot u^{r_B},$$
     $$\sigma_{B2} = C_{B2} \cdot h^{t_{B2}},$$
     $$\pi_B = g^{-t_{B1}} \cdot F(P_B)^{-t_{B2}}.$$
     (c) B will compute k'_A according to tpk_B and P_{BT}
     $$k'_A = \frac{e(\sigma_{A1}, g) \cdot e(F(P_{BT}), \sigma_{A2}) \cdot e(h, \pi_A)}{e(u, tpk_B)}.$$

(d) B generates the following verification value V_B such that

$$V_B = H_1((k'_A)^{r_B}||e(u,g)^{r_B}||0).$$

Finally, B sends both $\sigma_{B1}, \sigma_{B2}, \pi_B$ and V_B to A.

3. $\mathsf{A} \rightarrow \mathsf{B} : \{V_A\}$

(a) A also computes k'_B according to tpk_A and P_{AT}

$$k'_B = \frac{e(\sigma_{B1}, g) \cdot e(F(P_{AT}), \sigma_{B2}) \cdot e(h, \pi_B)}{e(u, tpk_A)}.$$

(b) A verifies the V_B with the equation $V_B \stackrel{?}{=} H_1((k'_B)^{r_A}||k'_B||0)$. If the above equation holds, A will output "1" and send $V_A = H_1((k'_B)^{r_A}||e(u,g)^{r_A}||1)$ to B. Else A outputs "0" and also responds a random value $V_A \leftarrow_R \mathbb{Z}_N^*$ to B.

(c) B verifies V_A with the following equation $V_A \stackrel{?}{=} H_1((k'_A)^{r_B}||k'_A||1)$. B outputs "1" only if the above equation holds, else B outputs "0".

Completeness. If the authentication policy of A and B are matching, it implies that $tpk_A = gpk_B, P_{AT} = P_B$ and $tpk_B = gpk_A, P_{BT} = P_A$. Namely, both A and B can recover the original message $k'_A = e(u,g)^{r_A}$ and $k'_B = e(u,g)^{r_B}$. The completeness of USH-DM can be verified as follows.

$$\begin{aligned}
k'_A &= \frac{e(\sigma_{A1}, g) \cdot e(F(P_{BT}), \sigma_{A2}) \cdot e(h, \pi_A)}{e(u, tpk_B)} \\
&= \frac{e(\sigma_{A1}, g) \cdot e(F(P_A), \sigma_{A2}) \cdot e(h, \pi_A)}{e(u, gpk_A)} \\
&= \frac{e(C_{A1}, g) \cdot e(h^{t_{A1}}, g) \cdot e(u^{r_A}, g) \cdot e(F(P_A), C_{A2}) \cdot e(F(P_A), h^{t_{A2}}) \cdot e(h, g^{-t_{A1}} F(P_A)^{-t_{A2}})}{e(u, gpk_A)} \\
&= \frac{e(C_{A1}, g) \cdot e(u^{r_A}, g) \cdot e(F(P_A), C_{A2})}{e(u, g^{t_A})} \\
&= \frac{e(u^{t_A} \cdot F(P_A)^s, g) \cdot e(F(P_A), g^{-s}) \cdot e(u^{r_A}, g)}{e(u, g^{t_A})} \\
&= \frac{e(u^{t_A}, g) \cdot e(u^{r_A}, g)}{e(u, g^{t_A})} \\
&= e(u,g)^{r_A}.
\end{aligned}$$

Simultaneously, A can get $k'_B = e(u,g)^{r_B}$ by similar method and verify the corresponding responses V_B as follows.

$$\begin{aligned}
V_B &= H_1((k'_A)^{r_B}||e(u,g)^{r_B}||0) = H_2((e(u,g)^{r_A})^{r_B}||e(u,g)^{r_B}||0) \\
&= H_2(e(u,g)^{r_B})^{r_A}||e(u,g)^{r_B}||0) = H_1((k'_B)^{r_A}||k'_B||0).
\end{aligned} \tag{1}$$

By using the above method, B can check the corresponding response V_A. Hence A and B complete a successful secret handshake protocol. A session key $K = H_1(e(u,g)^{r_A \cdot r_B})$ is agreed between A and B for the following two-party communications, without leaking their affiliations.

4 Security and Performance Analysis

Now we provide the security results on the new construction USH-DM with respect to the impersonator resistance, detector resistance and unlinkability. Due to the limitation of the length, the proofs of the theorems are described in brief and the details can be referred to the full version.

4.1 Security

Theorem 1. USH-DM *is a secure unlinkable secret handshake scheme with dynamic matching under the decisional BDH and SD assumption.*

Proof (Sketch). We show that USH-DM satisfies the security requirements of secret handshakes in brief. Since the completeness has been analyzed in the above section, the proofs of impersonator resistance, detector resistance and unlinkability are described as follows.

- **Impersonator Resistance(IR).** If an adversary $\mathcal{A}$ breaks the IR property with a non-negligible probability ϵ, one can use $\mathcal{A}$ to derive a simulator $\mathcal{B}$ that solves an instance of the decisional BDH problem with a non-negligible probability related to ϵ. $\mathcal{B}$ is given an challenge of the decisional BDH problem such that $(g, A = g^a, B = g^b, C = g^c, Z)$ and is asked to output a guess β' of β that determine whether Z is equal to $e(g,g)^{abc}$ or $e(g,g)^d, d \leftarrow_R \mathbb{Z}_p$.
- **Detector Resistance(DR).** Assuming $\mathcal{A}$ breaks the DR property with a non-negligible probability, $\mathcal{A}$ has to distinguish a handshake instance with a true group member from an instance with a simulator SIM. During the handshake in our proposed scheme, we notice that the group member (e.g., A) sends only the blinded credential proof $(\sigma_{A1}, \sigma_{A2}, \pi_A)$ for authentication, which can provide the privacy of his identity. Since the transcript of a participant during the handshake seems to be random, $\mathcal{A}$ cannot determine whether it was generated by a true group member or a simulator.
- **Unlinkability.** Assuming $\mathcal{A}$ breaks the unlinkability property with a non-negligible probability $\frac{1}{2} + \epsilon$, $\mathcal{A}$ has to distinguish whether two handshake instances are related to the same participant or not. The implementation of attackers against unlinkability is similar to the parallel executions of two attack instances against Detector Resistance. Thus, the proof of unlinkability can be described by a similar way as in the proof of Detector Resistance. And hence the detailed proof is not provided here for brief.

□

4.2 Performance Analysis

Here the performance of USH-DM will be analyzed by considering its computation costs. In the literatures, most of secret handshake schemes are provably secure under the random oracle. Only a few secret handshake schemes are implemented without random oracles, which are basically derived from the scheme

Table 1. A comparison of related secret handshake schemes

	Balfanz *et* al. [2]	Ateniese *et al.*[1]	USH-DM
Setup	0	$(2n+3)T_e$	0
CreateGroup	T_e	T_e	T_e
AddMember	T_e	$2T_e$	$2T_e$
Handshake	$4T_p$	$6T_p + 6T_e$	$8T_p + 8T_e$
Traceability	Yes	No	No
Dynamic Matching	No	Yes(Limited in a large group)	Yes
Rounds	3	2	3
One-time credentials	Need	Not Need	Not Need
Underlying Assumption	BDH	SXDH and BDH	DBDH and SD
Random Oracles	with	without	without

proposed by Ateniese *et al* [1]. For clarity, we describe the performance comparison among some representative schemes selected from the existing literatures. According to the related experiments' findings, one pairing operation and modular exponentiation are the most time-consuming computations in the cryptography schemes. Hence, we focus on giving the computation costs about the pairing and modular exponentiation operations. By using Barreto's ECC Pairing Library [5], we calculate the computational costs of the pairing and the modular exponential operations with respect to the schemes in our comparison. T_p denotes time for one bilinear pairing operation in the elliptic curve groups which costs about 12.23ms. T_e denotes time for one modular exponential operation which costs about 2.42ms. The experiments are based on Intel Pentium-4 2.8GHz with 512MB RAM. For clarity, the computational costs are considered with respect to the different phases of secret handshake schemes, which are described in Table 1.

From Table 1, we can see that Balfanz *et al.*'s scheme [2] achieve traceability and unlinkability using one-time credentials. But the scheme is proven secure in the random oracle model. For the Ateniese *et al*'s scheme [1], since it distinguishes different groups through group identities which are all assumed to be n-bits strings, $2n + 3$ modular exponentiations need to be computed in the Setup phase and every group must know and maintain $n+2$ modular exponentiations as the private values to issue group credentials in the CreateGroup phase. Towards the proposed scheme USH-DM, different groups are self-governed which have respective group public and private keys without needing the group identities for distinction. And hence the computation costs of USH-DM are reduced in both of the Setup and CreateGroup phases. By issuing attribute credentials, USH-DM also achieves the dynamic matching for flexible authentication policies about designated groups and concrete attributes. Specially, the advantage of our proposed scheme is that its applications can be extended to the more practical multiple-groups environment. In addition, we note that the Ateniese *et al*'s scheme [1] also needs three rounds in order to implement a complete secret handshake protocol instead of only realizing a secret key agreement. Thus

the corresponding computational costs are increased. Therefore, Ateniese *et al*'s scheme [1] can only be applied to the handshakes between departments from the same group instead of individual members from different groups.

5 Conclusion

In this paper, we have proposed a new unlinkable secret handshake scheme supports dynamic matching policy. Our new proposal extends the functionality of Ateniese *et al*'s scheme, which can be applied to the multiple-groups environment where each group is really different and independent. Combining the technique of full-domain subgroup hiding with attribute-base encryption, our new scheme not only achieves the strong unlinkability against GA, but also more flexible authentication policy including affiliation and attributes. The formal security reduction of our proposal is proven in the standard model by assuming the intractability of the decisional bilinear Diffie-Hellman and subgroup decision problems. An interesting future work is to find more practical secret handshake schemes from other public key cryptosystems, such as Lattice and Multivariate PKC.

References

1. Ateniese, G., Blanton, M., Kirsch, J.: Secret handshakes with dynamic and fuzzy matching. In: Network and Distributed System Security Symposium, NDSS, pp. 159–177 (2007)
2. Balfanz, D., Durfee, G., Shankar, N., Smetters, D., Staddon, J., Wong, H.: Secret handshakes from pairing-based key agreements. In: IEEE Symposium on Security and Privacy, pp. 180–196 (2003)
3. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
4. Boneh, D., Goh, E.-J., Nissim, K.: Evaluating 2-DNF formulas on ciphertexts. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 325–341. Springer, Heidelberg (2005)
5. Barreto, P.: The η_T approach to the Tate pairing, and supporting (supersingular) elliptic curve arithmetic in characteristic 3, `http://www.larc.usp.br/~pbarreto/Pairings.GPL.zip`
6. Castelluccia, C., Jarecki, S., Tsudik, G.: Secret handshakes from CA-oblivious encryption. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 293–307. Springer, Heidelberg (2004)
7. Gu, J., Xue, Z.: An improved efficient secret handshakes scheme with unlinkability. IEEE Communications Letters 15(2), 486–490 (2011)
8. Huang, H., Cao, Z.: A novel and efficient unlinkable secret handshake scheme. IEEE Communications Letters 13(5), 363–365 (2009)
9. Jarecki, S., Liu, X.: Unlinkable secret handshakes and key-private group key management schemes. In: Katz, J., Yung, M. (eds.) ACNS 2007. LNCS, vol. 4521, pp. 270–287. Springer, Heidelberg (2007)
10. Jarecki, S., Liu, X.: Private mutual authentication and conditional oblivious transfer. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 90–107. Springer, Heidelberg (2009)

11. Kawai, Y., Yoneyama, K., Ohta, K.: Secret handshake: strong anonymity definition and construction. In: Bao, F., Li, H., Wang, G. (eds.) ISPEC 2009. LNCS, vol. 5451, pp. 219–229. Springer, Heidelberg (2009)
12. Li, S., Ephremides, A.: Anonymous routing: a cross-layer coupling between application and network layer. In: Conference on Information Science and Systems, CISS, pp. 783–788 (2006)
13. Nasserian, S., Tsudik, G.: Revisiting oblivious signature-based envelopes. In: Di Crescenzo, G., Rubin, A. (eds.) FC 2006. LNCS, vol. 4107, pp. 221–235. Springer, Heidelberg (2006)
14. Sorniotti, A., Molva, R.: Secret handshakes with revocation support. In: Lee, D., Hong, S. (eds.) ICISC 2009. LNCS, vol. 5984, pp. 274–299. Springer, Heidelberg (2010)
15. Sorniotti, A., Molva, R.: Secret interest groups (SIGs) in social networks with an implementation on Facebook. In: SAC 2010, pp. 621–628. ACM Press (2010)
16. Sorniotti, A., Molva, R.: Federated secret handshakes with support for revocation. In: Soriano, M., Qing, S., López, J. (eds.) ICICS 2010. LNCS, vol. 6476, pp. 218–234. Springer, Heidelberg (2010)
17. Sorniotti, A., Molva, R.: A provably secure secret handshake with dynamic controlled matching. Computers & Security 29(5), 619–627 (2010)
18. Su, R.: On the security of a novel and efficient unlinkable secret handshakes scheme. IEEE Communications Letters 13(9), 712–713 (2009)
19. Vergnaud, D.: RSA-based secret handshakes. In: Ytrehus, Ø. (ed.) WCC 2005. LNCS, vol. 3969, pp. 252–274. Springer, Heidelberg (2006)
20. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
21. Boyen, X., Waters, B.: Full-domain subgroup hiding and constant-size group signatures. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 1–15. Springer, Heidelberg (2007)
22. Wen, Y., Zhang, F., Xu, L.: Unlinkable secret handshakes from message recovery signature. Chinese Journal of Electronics 19(4), 705–709 (2010)
23. Wen, Y., Zhang, F.: A new revocable secret handshake scheme with backward unlinkability. In: Camenisch, J., Lambrinoudakis, C. (eds.) EuroPKI 2010. LNCS, vol. 6711, pp. 17–30. Springer, Heidelberg (2011)
24. Zhang, F., Chen, X., Susilo, W., Mu, Y.: A new signature scheme without random oracles from bilinear pairings. In: Nguyên, P.Q. (ed.) VIETCRYPT 2006. LNCS, vol. 4341, pp. 67–80. Springer, Heidelberg (2006)
25. Xu, S., Yung, M.: K-anonymous secret handshakes with reusable without random oracles from bilinear pairings. In: ACM CCS 2004, pp. 158–167. ACM (2004)
26. Zhao, G., Tan, C., Ren, Y., Fang, L.: An efficient unlinkable secret handshake protocol without ROM. In: IEEE International Conference on WCNIS 2010, pp. 486–490 (2010)
27. Zhou, L., Susilo, W., Mu, Y.: Three-round secret handshakes based on ElGamal and DSA. In: Chen, K., Deng, R., Lai, X., Zhou, J. (eds.) ISPEC 2006. LNCS, vol. 3903, pp. 332–342. Springer, Heidelberg (2006)