Secret Handshakes with Dynamic Expressive Matching Policy

Lin Hou[1], Junzuo Lai[1,2(✉)], and Lixian Liu[1]

[1] Department of Computer Science, Jinan Universisty, Guangzhou, China
linhou19@gmail.com, 944427149@qq.com
[2] The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China
laijunzuo@gmail.com

Abstract. Secret handshake is an important building block of private communication over public networks, which allows two members of the same group to secretly authenticate each other and agree on a shared key for further communication. Ateniese et al. [1] introduced attribute-based secret handshake, in which a group member Alice can complete the handshake protocol with another group member Bob by specifying the attributes Bob must have. In this paper, we propose the first efficient attribute-based secret handshake scheme which supports arbitrary matching policies with unlinkable and reusable credentials. Specifically, we first present a generic construction of attribute-based secret handshakes from *centralized* ciphertext-policy attribute-based encryption (CP-ABE). Based on the construction, we present a highly efficient attribute-based secret handshake scheme employing the CP-ABE scheme in [18].

1 Introduction

Given the pervasiveness and public nature of today's Internet, communication privacy is becoming a grave concern. Many techniques have been proposed in literatures for achieving communication privacy over public networks. Among them, privacy-preserving authentication protocols such as *secret handshake* schemes are important building blocks.

Secret handshakes, first introduced by Balfanz et al. [2], allow two members of the same group to secretly and privately authenticate each other and agree on a shared key for subsequent communication. Such a handshake is privacy-preserving in the sense that someone who is not in the group cannot perform the handshake. On the other hand, any two parties who are members of the same group could authenticate to each other. A common cited application of such interactions is mutual authentication of two CIA agents, in which they should be able to successfully complete the handshake while others should not be able to recognize the handshake.

Ateniese et al. [1] extended the framework of secret handshakes to include roles and support dynamic matching of attributes associated with the role in

J.K. Liu and R. Steinfeld (Eds.): ACISP 2016, Part I, LNCS 9722, pp. 461–476, 2016.
DOI: 10.1007/978-3-319-40253-6_28

a threshold way, which is also called attribute-based secret handshakes. This dynamic matching allows users to specify the group of person with whom they would like to perform a secret handshake, rather than a static group setting. Moreover, each member has a number of attributes (say n) associated with her membership. For instance, a depressed patient Alice wants to authenticate herself and reveal her illness only to others authenticated as psychologist. When setting up a handshake with some psychologist, Alice can specify what attributes the psychologist must have, such as (psychologist|female|$\cdots$|inLosAngeles). The handshake succeeds iff the credentials of the psychologist match d or more of the attributes specified by Alice for some threshold $d \leq n$.

Traditional secret handshake has many appealing applications, such as digital content protection and anonymous routing in ad-hoc networks. However, attribute-based secret handshake is used more broadly. Such as in online dating system, employing attribute-based secret handshake allows any two users to check whether each of them meets the expectations of the other without revealing any additional personal information beforehand.

Unfortunately, previous attribute-based secret handshakes in literatures only support simple matching policy, i.e. threshold favor, and there is no scheme that supports expressive matching policies before this paper. The difficulty in constructing such a scheme comes from its security requirements. A secure secret handshake must provide three basic properties. The first one is *impersonator resistance*, which means any adversary not satisfying the matching policy is unable to authenticate himself to an honest member. And *detector resistance* requires the adversary above cannot decide whether some honest party satisfies the rules or not. The last one, *unlinkability*, demands that it should be infeasible to tell whether two (successful) execution of handshake protocol were performed by the same party or not. Most attribute-based schemes may not possess detector resistance, thus making it a challenge to construct secret handshakes with a dynamic expressive matching policy.

1.1 Our Contributions

In this paper, we investigate the construction of attribute-based secret handshakes from ciphertext-policy attribute-based encryption (CP-ABE) schemes, and propose an efficient secret handshake protocol which supports attribute matching with more *flexible* or *expressive* access structures than the existing ones in literatures. Specifically, our contributions are as follows:

1. We first introduce a generic construction of attribute-based secret handshakes employing *centralized* CP-ABE with *partially hidden access structures*. Centralized CP-ABE is slightly modified from traditional CP-ABE with an extra **Init** algorithm, which runs by the System Administrator (SA). In centralized CP-ABE, SA publishes the global public parameter to all Private Key Generators (PKGs) before the setup procedure. The formal definition is described in Sect. 2.3. In *partially hidden access structure* model [18], each attribute includes two parts, i.e. attribute name and attribute value. If the set of

attributes associated with a user's private key does not satisfy the access structure associated with a ciphertext, attribute values in the access structure are hidden while the attribute names are still public. Since in many applications, specific attribute values carry much more sensitive information than the generic attribute names, this model is sufficient and plausible in practice.

2. Based on the generic construction of attribute-based secret handshakes from centralized CP-ABE, we present a concrete instantiation employing the partial hidden policy CP-ABE scheme proposed in [18]. Specifically, We first modify the scheme in [18] to a get a centralized CP-ABE scheme, and then use it to construct an efficient attribute-based secret handshake. The result handshake scheme not only supports dynamic expressive matching policy but also provides all the security properties in standard model.

1.2 Related Work

We only focus on closely related works, and refer the reader to [2,19,31] for discussions on some loosely related ones.

Secret Handshake. The concept of secret handshakes was first introduced by Balfanz et al. [2]. Several proposals on secret handshake schemes followed, based on bilinear maps [2], computational Diffie-Hellman [10,32], and RSA [28]. However, users in these schemes are *linkable*. Namely, an attacker can recognize two instances of a protocol executed by the same party. In order to achieve unlinkability, the scheme in [2] resorts to use one-time credentials.

Xu and Yung [31] presented secret handshake schemes that achieve unlinkability with reusable credentials instead of one-time credentials, but only offer a weak notion of privacy called k-anonymity. Unlinkable secret handshake schemes with strong notion of privacy were proposed later in [1,15].

Tsudik and Xu [27] introduced the first scheme for group secret handshakes, which achieves unlinkability with reusable credentials; however, their scheme ensures successful authentication among group members only if every member holds the same most recently distributed group key, a condition which results in high real-time communication overhead between the group manager and group members. Jarecki et al. [13] presented another scheme for group secret handshakes which fits into the standard PKI setting and avoids having the group manager broadcasting key-update messages to group members; however, as in [2], the scheme uses one-time credentials to achieve unlinkability.

Jarecki et al. [14] considered a very strong notion of secret handshakes, referred to as affiliation-hiding authenticated key exchange, which guarantees security under arbitrary composition of protocol sessions.

Ateniese et al. [1] presented a secret handshake scheme with dynamic matching, in which each party can specify both the group and the role the other must have in order for the handshake to succeed. They also gave a novel extension of secret handshakes to include attributes, allowing the handshake to support

threshold-based matching on attributes, as we discussed at the beginning of this section.

As an independent research interest, revocation of credentials in secret handshakes was investigated in [15,26].

A related topic is oblivious signature-based envelope (OSBE), introduced by Li et al. [20]. Informally, an OSBE enables a sender to send an envelope (encrypted message) to a recipient, with the assurance that the latter will be able to open it only if he holds the signature on a prior agreed-upon message. Nasserian and Tsudik [21] observed that two symmetric instances of OSBE may yield a secret handshake.

Attribute-Based Encryption. The notion of ABE was first introduced by Sahai and Waters as an application of their fuzzy identity-based encryption (IBE) scheme [25], where both ciphertexts and secret keys are associated with sets of attributes. Decryption is enabled if and only if the ciphertext and secret key attribute sets overlap by at least a fixed threshold value d. There are two kinds of ABE schemes, key-policy and ciphertext-policy ABE schemes.

In a key-policy ABE scheme [12,24], every ciphertext is associated with a set of attributes, and every user's secret key is associated with an access structure on attributes. Decryption is enabled if and only if the ciphertext attribute set satisfies the access structure associated with the user's secret key. The notion of predicate encryption (PE) [16] is related to key-policy ABE. In a PE scheme, secret keys correspond to predicates and ciphertexts are associated with a set of attributes; the secret key SK_f corresponding to a predicate f can be used to decrypt a ciphertext associated with an attribute set I if and only if $f(I) = 1$. Katz, Sahai, and Waters [16] also introduced the idea of *attribute-hiding*, a security notion for PE that is stronger than the basic security requirement of *payload-hiding*. Roughly speaking, *attribute-hiding* requires that a ciphertext conceal the associated attributes as well as the plaintext, while *payload-hiding* only requires that a ciphertext conceal the plaintext.

In a ciphertext-policy ABE (CP-ABE) scheme [4,11,29], the situation is reversed. That is, attributes are associated with user's secret keys and access structures (also called ciphertext policies) with ciphertexts. Nishide et al. [22] proposed CP-ABE schemes where encryptor-specified access structures are hidden. Access structures in their schemes support AND operation, and the security of the schemes were only proved in a weak model, which can be considered to be analogous to the selective-ID model [5,9] used in IBE schemes. Lai et al. [18] proposed a partial hidden CP-ABE scheme which supports a wide range of access structures in standard model.

1.3 Organization

The rest of the paper is organized as follows. In Sect. 2, we review some standard notations and cryptographic definitions. We also formally define the notion of centralized CP-ABE and fully security notion. We then present the generic

construction of secure attribute-based secret handshake from fully secure centralized CP-ABE in Sect. 3. This generic construction ensures that the handshake scheme supports the same access structures on attributes as those supported by the underlying fully secure CP-ABE scheme. In Sect. 4, we present a concrete secret handshake with dynamic expressive matching policy. Finally, we state our conclusion in Sect. 5.

2 Preliminaries

If S is a set, then $s \xleftarrow{\$} S$ denotes the operation of picking an element s uniformly at random from S. Let $\mathbb{N}$ denote the set of natural numbers. If $\lambda \in \mathbb{N}$ then 1^λ denotes the string of λ ones. Let $z \leftarrow \mathsf{A}(x, y, \ldots)$ denote the operation of running an algorithm A with inputs $(x, y, \ldots)$ and output z. A function $f(\lambda)$ is *negligible* if for every $c > 0$ there exists a λ_c such that $f(\lambda) < 1/\lambda^c$ for all $\lambda > \lambda_c$.

2.1 Composite Order Bilinear Groups

Composite order bilinear groups were first introduced in [7]. We use bilinear groups whose order is the product of three distinct primes.

Let $\mathcal{G}$ be an algorithm that takes as input a security parameter 1^λ and outputs a tuple $(p, q, r, \mathbb{G}, \mathbb{G}_T, \hat{e})$, where p, q, r are distinct primes, $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order $N = pqr$, and $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a map such that

1. (Bilinear) $\forall g, h \in \mathbb{G}, a, b \in \mathbb{Z}_N, \hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$;
2. (Non-degenerate) $\exists g \in \mathbb{G}$ such that $\hat{e}(g, g)$ has order N in $\mathbb{G}_T$.

We further require that multiplication in $\mathbb{G}$ and $\mathbb{G}_T$, as well as the bilinear map $\hat{e}$, are computable in time polynomial in λ. We use $\mathbb{G}_p, \mathbb{G}_q, \mathbb{G}_r$ to denote the subgroups of $\mathbb{G}$ having order p, q, and r, respectively. Observe that $\mathbb{G} = \mathbb{G}_p \times \mathbb{G}_q \times \mathbb{G}_r$. Note also that if $h_p \in \mathbb{G}_p$ and $h_q \in \mathbb{G}_q$ then $\hat{e}(h_p, h_q) = 1$. A similar rule holds whenever $\hat{e}$ is applied to elements in distinct subgroups.

We now state the complexity assumptions we use. The first assumption is just the subgroup decision problem in the case where the group order is a product of three primes. We justify these assumptions in Appendix A by proving that they hold in the generic group model assuming finding a non-trivial factor of the group order N is hard. Note that our assumptions are non-interactive (in contrast to, e.g., the LRSW assumption [8]) and of fixed size (in contrast to, e.g., the q-SDH assumption [6]).

Assumption 1. *Let $\mathcal{G}$ be as above. We define the following distribution:*

$$(p, q, r, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \mathcal{G}(1^\lambda),\ N = pqr,\ g_p \xleftarrow{\$} \mathbb{G}_p,\ g_r \xleftarrow{\$} \mathbb{G}_r,$$
$$D = (\mathbb{G}, \mathbb{G}_T, N, \hat{e}, g_p, g_r),$$
$$T_1 \xleftarrow{\$} \mathbb{G}_p \times \mathbb{G}_q,\ T_2 \xleftarrow{\$} \mathbb{G}_p.$$

The advantage of an algorithm $\mathcal{A}$ in breaking Assumption 1 is defined as

$$Adv^1_{\mathcal{A}} = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|.$$

Definition 1. *we say $\mathcal{G}$ satisfies Assumption 1 if for any polynomial time algorithm $\mathcal{A}$, $Adv^1_{\mathcal{A}}$ is negligible.*

Assumption 2. *Let $\mathcal{G}$ be as above. We define the following distribution:*

$$(p, q, r, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \mathcal{G}(1^\lambda),\ N = pqr,$$

$$g_p, X_1 \xleftarrow{\$} \mathbb{G}_p,\ X_2 \xleftarrow{\$} \mathbb{G}_q,\ g_r \xleftarrow{\$} \mathbb{G}_r,$$
$$D = (\mathbb{G}, \mathbb{G}_T, N, \hat{e}, g_p, X_1X_2, g_r),$$
$$T_1 \xleftarrow{\$} \mathbb{G}_p \times \mathbb{G}_q,\ T_2 \xleftarrow{\$} \mathbb{G}_p.$$

The advantage of an algorithm $\mathcal{A}$ in breaking Assumption 2 is defined as

$$Adv^2_{\mathcal{A}} = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|.$$

Definition 2. *we say $\mathcal{G}$ satisfies Assumption 2 if for any polynomial time algorithm $\mathcal{A}$, $Adv^2_{\mathcal{A}}$ is negligible.*

Assumption 3. *Let $\mathcal{G}$ be as above. We define the following distribution:*

$$(p, q, r, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \mathcal{G}(1^\lambda),\ N = pqr,$$

$$\omega, s \in \mathbb{Z}_N,\ g_p, Z_1 \xleftarrow{\$} \mathbb{G}_p,\ X_2, Y_2, Z_2 \xleftarrow{\$} \mathbb{G}_q,\ g_r \xleftarrow{\$} \mathbb{G}_r,$$
$$D = (\mathbb{G}, \mathbb{G}_T, N, \hat{e}, g_p, g_p^\omega X_2, g_p^s Y_2, Z_1Z_2, g_r),$$

$$T_1 = \hat{e}(g_p, g_p)^{\omega s},\ T_2 \xleftarrow{\$} \mathbb{G}_T.$$

The advantage of an algorithm $\mathcal{A}$ in breaking Assumption 3 is defined as

$$Adv^3_{\mathcal{A}} = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|.$$

Definition 3. *we say $\mathcal{G}$ satisfies Assumption 3 if for any polynomial time algorithm $\mathcal{A}$, $Adv^3_{\mathcal{A}}$ is negligible.*

Assumption 4. *Let $\mathcal{G}$ be as above. We define the following distribution:*

$$(p, q, r, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \mathcal{G}(1^\lambda),\ N = pqr,$$

$$a \in \mathbb{Z}_N,\ g_p \xleftarrow{\$} \mathbb{G}_p,\ g_q, Q_1, Q_2, Q \xleftarrow{\$} \mathbb{G}_q,\ g_r, R_0, R_1, R \xleftarrow{\$} \mathbb{G}_r,$$
$$D = (\mathbb{G}, \mathbb{G}_T, N, \hat{e}, g_pR_0, g_p^aR_1, g_pQ_1, g_p^{1/a}Q_2, g_q, g_r),$$

$$T_1 = g_p^aQR,\ T_2 \xleftarrow{\$} \mathbb{G}_T.$$

The advantage of an algorithm $\mathcal{A}$ in breaking Assumption 4 is defined as

$$Adv^4_{\mathcal{A}} = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|.$$

Definition 4. *we say $\mathcal{G}$ satisfies Assumption 4 if for any polynomial time algorithm $\mathcal{A}$, $Adv^4_{\mathcal{A}}$ is negligible.*

2.2 Attribute-Based Secret Handshake Scheme

An attribute-based secret handshake scheme (denoted by ABSH) consists of the following algorithms:

Setup. Given a security parameter 1^λ, the algorithm generates the public parameters params common to all subsequently generated groups.

CreateGroup. The group administrator GA in group G runs the algorithm on input of params, and outputs the group public information GPK_G and group secret key GSK_G.

AddUser. This is a protocol between GA and a user. On input of a set of attributes S_U of user U, GA outputs the user's group credential cred_U using GA's key pair $(\mathsf{GPK}_G, \mathsf{GSK}_G)$.

HandShake. This is an authentication protocol executed between users A and B, who may belong to different groups. At the end of the protocol, if A's target requirements are matched by B and vice versa, A and B will authenticate each other by sharing a common secret key for subsequent secure communication.

We consider the following core security properties for secret handshake schemes:

Impersonator resistance: An adversary not satisfying the requirements of the handshake protocol can not authenticate to an honest user.

Detector resistance: An adversary not satisfying the requirements of the handshake protocol can not decide whether an honest user satisfies the requirements or not.

Unlinkability: It is not feasible to tell whether two executions of the handshake protocol were performed by the same users or not.

2.3 Centralized CP-ABE with Partially Hidden Access Structures

Centralized CP-ABE is slightly modified from traditional CP-ABE which consists of the following five algorithms:

Init(1^λ): It takes as input a security parameter λ, and output a global public parameter PP.

Setup(PP): It takes as input the global public parameter PP, and outputs a public key MPK and a master secret key MSK.

KeyGen$(\mathsf{MPK}, \mathsf{MSK}, S)$: It takes as input the public key MPK, the master secret key MSK and a set of attributes S. It outputs a secret key SK_S.

Encrypt$(\mathsf{MPK}, m, \mathbb{A})$: It takes as input the public key MPK, a message m and an access structure $\mathbb{A}$. It outputs a ciphertext c.

Decrypt$(\mathsf{MPK}, \mathsf{SK}_S, c)$: It takes as input the public key MPK, a secret key SK_S and a ciphertext c. It outputs a message m.

Let $(\mathsf{MPK}, \mathsf{MSK}) \leftarrow \mathsf{Setup}(1^\lambda), \mathsf{SK}_S \leftarrow \mathsf{KeyGen}(\mathsf{MPK}, \mathsf{MSK}, S)$, and c is the output of the algorithm $\mathsf{Encrypt}(\mathsf{MPK}, m, \mathbb{A})$. For correctness, we require the following to hold:

1. If the set S of attributes in a private key satisfies the access structure $\mathbb{A}$ in a ciphertext, then $m \leftarrow \mathsf{Decrypt}(\mathsf{MPK}, \mathsf{SK}_S, c)$;
2. Otherwise, with overwhelming probability, $\mathsf{Decrypt}(\mathsf{MPK}, \mathsf{SK}_S, c)$ outputs a random message.

Partially Hidden Access Structures. In the construction of CP-ABE with partially hidden access structures [18], each attribute includes two parts, i.e. *attribute name* and *attribute value*. It is assumed that there are n categories of attributes and every user has n attributes with each attribute belonging to a different category. Let i denote the attribute name of the i^{th} category attribute. A user's attribute set $\mathcal{S}$ is parsed as $(s_1, \cdots, s_n)$, where $s_i \in \mathbb{Z}_N$ is the value of attribute i. We express an access formula by $(\mathcal{A}, \rho, \mathcal{T})$, where $\mathcal{A}$ is $\ell \times n$ share-generating matrix, ρ is a map from each row of $\mathcal{A}$ to an attribute name, i.e. $\rho : \{1, \cdots, \ell\} \rightarrow \{1, \cdots, n\}$, and $\mathcal{T}$ can be parsed as $(t_{\rho(1)}, \cdots, t_{\rho(\ell)})$ and $t_{\rho(i)}$ is the value of attribute $\rho(i)$ specified by the access formula. A user's attribute set $\mathcal{S}$=$(s_1, \cdots, s_n)$ satisfies an access formula $(\mathcal{A}, \rho, \mathcal{T})$ if and only if there exist $\mathcal{I} \subseteq \{1, \cdots, \ell\}$ and constants $\{\omega_i\}_{i \in \mathcal{I}}$ such that

$$\textstyle\sum_{i \in \mathcal{I}} \omega_i A_i = (1, 0, \cdots, 0) \text{ and } s_{\rho(i)} = t_{\rho(i)} \text{ for } \forall i \in \mathcal{I},$$

where A_i denotes the i^{th} row of A.

Security Model. We now give the security model for centralized CP-ABE with partially hidden access structures, described as a game between a challenger and an adversary $\mathcal{A}$. The game proceeds as follows:

Setup. The challenger runs $\mathsf{Init}(1^\lambda)$ and $\mathsf{Setup}(\mathsf{PP})$ to obtain the public parameters MPK and a master secret key MSK. It gives the public parameters MPK to the adversary $\mathcal{A}$ and keeps MSK to itself.

Query phase 1. The adversary $\mathcal{A}$ adaptively queries the challenger for secret keys corresponding to sets of attributes $\mathcal{S}_1, \ldots, \mathcal{S}_q$. In response, the challenger runs $\mathsf{SK}_{\mathcal{S}_i} \leftarrow \mathsf{KeyGen}(\mathsf{MPK}, \mathsf{MSK}, \mathcal{S}_i)$ and gives the secret key $\mathsf{SK}_{\mathcal{S}_i}$ to $\mathcal{A}$, for $1 \leq i \leq q$.

Challenge. The adversary $\mathcal{A}$ submits two (equal length) messages M_0, M_1 and two access structures $(\mathbf{A}, \rho, \mathcal{T}_0)$, $(\mathbf{A}, \rho, \mathcal{T}_1)$, subject to the restriction that, $(\mathbf{A}, \rho, \mathcal{T}_0)$ and $(\mathbf{A}, \rho, \mathcal{T}_1)$ cannot be satisfied by any of the queried attribute sets. The challenger selects a random bit $\beta \in \{0, 1\}$ and encryptes M_β to get the challenge ciphertext $C = \mathsf{Encrypt}(\mathsf{MPK}, M_\beta, (\mathbf{A}, \rho, \mathcal{T}_\beta))$ and sends C to the adversary as its challenge ciphertext.
Note that, the LSSS matrix $\mathbf{A}$ *and* ρ *are the same in the two access structures provided by the adversary. In a CP-ABE scheme with partially hidden access structures, one can distinguish the ciphertexts if the associated access structures have different* $(\mathbf{A}, \rho)$*, since* $(\mathbf{A}, \rho)$ *is sent along with the ciphertext explicitly.*

Query phase 2. The adversary continues to adaptively query the challenger for secret keys corresponding to sets of attributes with the added restriction that none of these satisfies $(\mathbf{A}, \rho, \mathcal{T}_0)$ and $(\mathbf{A}, \rho, \mathcal{T}_1)$.

Guess. The adversary $\mathcal{A}$ outputs its guess $\beta' \in \{0,1\}$ for β and wins the game if $\beta = \beta'$.

The advantage of the adversary in this game is defined as $|\mathsf{Pr}[\beta = \beta'] - \frac{1}{2}|$ where the probability is taken over the random bits used by the challenger and the adversary.

Definition 5. *The centralized CP-ABE scheme with partially hidden access structures is CPA secure if all polynomial time adversaries have at most a negligible advantage in this security game.*

Note that another stronger notion is *fully security* [19], which means that the ciphertext reveals no information about the underlying plaintext and completely hides the associated policy. However, the only known construction of fully secure CP-ABE schemes comes from Inner-product Predicate Encryption (IPE) [16], which causes a superpolynomial blowup in size for arbitrary access structures and is extremely impractical.

3 Attribute-Based Secret Handshake from Centralized CP-ABE

In this section, based on the secure centralized CP-ABE with partially hidden access structures, we propose a generic construction of attribute-based secret handshakes. Compared with the scheme proposed by Ateniese et al. [1], which only supports threshold-based access structures, our construction is more expressive thus the resulting handshake schemes support the same access structures on attributes as those supported by the underlying CP-ABE.

Suppose that Π is a centralized CP-ABE scheme with partially hidden access structures which contains algorithms Init, Setup, KeyGen, $\mathsf{Encrypt}$ and $\mathsf{Decrypt}$. We can construct a attribute-based secret handshake scheme by defining its corresponding algorithms in the following way.

ABSH.Setup(1^λ): Given a security parameter λ, the algorithm runs

$$\Pi.\mathsf{PP} \leftarrow \Pi.\mathsf{Init}(1^\lambda)$$

and sets the public parameter

$$\mathsf{params} = \Pi.\mathsf{PP}$$

ABSH.CreateGroup(params): Given the public parameter params, the group administrator GA first runs

$$(\Pi.\mathsf{MPK}, \Pi.\mathsf{MSK}) \leftarrow \Pi.\mathsf{Setup}(1^\lambda)$$

and then sets the group G's public information GPK_G and secret key GSK_G as

$$(\mathsf{GPK}_G, \mathsf{GSK}_G) = (\Pi.\mathsf{MPK}, \Pi.\mathsf{MSK}).$$

ABSH.AddUser(GSK_G, S_U): To add a user U with a set of attributes S_U to the group G, the group administrator GA runs

$$\Pi.\mathsf{SK}_{S_U} \leftarrow \Pi.\mathsf{KeyGen}(\mathsf{GPK}_G, \mathsf{GSK}_G, S_U),$$

and gives user U the secret credential $\mathsf{cred}_U = \Pi.\mathsf{SK}_{S_U}$.

ABSH.HandShake(A, B): Let A be a member of group G_A and B be a member of group G_B for generality. Suppose A with a secret credential cred_A, which is a private key on a set of attributes S_A, and B with a secret credential cred_B, which is a private key on a set of attributes S_B, engage in a handshake protocol. The protocol proceeds as follows:

1. A chooses a random k_1 and sends a ciphertext c_B to B, where

$$c_B \leftarrow \Pi.\mathsf{Encrypt}(\mathsf{GPK}_{G'_B}, k_1, \mathbb{A}_B),$$

and G'_B is the group that B must be in and $\mathbb{A}_B$ is the access structure on attributes that B must satisfy in order to complete the handshake.

2. Similarly, B chooses a random k_2 and sends a ciphertext c_A to A, where

$$c_A \leftarrow \Pi.\mathsf{Encrypt}(\mathsf{GPK}_{G'_A}, k_2, \mathbb{A}_A),$$

and G'_A is the group that A must be in and $\mathbb{A}_A$ is the access structure on attributes that A must satisfy in order to complete the handshake.

3. Upon receiving the ciphertext c_A, A runs

$$k_2 \leftarrow \Pi.\mathsf{Decrypt}(\mathsf{GPK}_{G_A}, \mathsf{cred}_A, c_A).$$

4. Upon receiving the ciphertext c_B, B runs

$$k_1 \leftarrow \Pi.\mathsf{Decrypt}(\mathsf{GPK}_{G_B}, \mathsf{cred}_B, c_B).$$

If $G_A = G'_A$, $G_B = G'_B$, S_A satisfies $\mathbb{A}_A$ and S_B satisfies $\mathbb{A}_B$, then at the end of the handshake, both A and B share the key $k = (k_1, k_2)$.

Theorem 1. *If the centralized CP-ABE scheme Π is secure in the model defined in Sect. 2.3, then the resulting secret handshake scheme is* impersonator resistant*,* detector resistant *and* unlinkable*.*

To keep the paper compact, we just give the core idea of the proof here.

Impersonator resistance: Let $\mathcal{A}$ be an adversary who attacks impersonator resistance of the secret handshake scheme. When $\mathcal{A}$ wants to authenticate to an honest user U, U chooses a random k and sends a ciphertext c to $\mathcal{A}$,

$$c \leftarrow \Pi.\mathsf{Encrypt}(\mathsf{GPK}_G, k, \mathbb{A}),$$

where G is the group that $\mathcal{A}$ must be in and $\mathbb{A}$ is the access structure on attributes that $\mathcal{A}$ must satisfy. If $\mathcal{A}$ is not a member of the group or $\mathcal{A}$ does not satisfy $\mathbb{A}$, because the CP-ABE scheme Π has plaintext privacy, then $\mathcal{A}$ cannot achieve any information about k and the handshake will fail.

Detector resistance: Let $\mathcal{A}$ be an activate adversary. When $\mathcal{A}$ engages in the secret handshake protocol with an honest user U, Since $\mathcal{A}$ does not satisfy the access structure specified by U and the underlying CP-ABE scheme Π has plaintext privacy, the handshake will fail and $\mathcal{A}$ can not decide whether U satisfies the access structure or not.

In the case that $\mathcal{A}$ is a passive adversary, due to hidden policy privacy of the CP-ABE scheme Π, the ciphertexts sent during the handshake protocol do not reveal the attribute value information in the access structure and $\mathcal{A}$ also cannot decide whether an honest user satisfies the access structure or not.

Unlinkability: In our secret handshake scheme, the messages exchanged during the handshake protocol are the ciphertexts of the CP-ABE scheme Π. Because Π has ciphertext-policy privacy, protocol messages do not reveal any information about the access structures on attributes; therefore, it is impossible to distinguish whether two different executions of the protocol were performed by the same user or not.

It is apparent that the secret handshake scheme obtained from our generic construction preserves the access structures of the underlying CP-ABE scheme, which will support dynamic and expressive matching policies.

4 An Efficient Instantiation

Based on the construction above, we describe a concrete instantiation of attribute-based secret handshake employing the CP-ABE scheme proposed in [18]. We first modify the scheme to a centralized CP-ABE, and then obtain the attribute-based secret handshake as follows.

Setup(1^λ): The setup algorithm firt runs $\mathcal{G}(1^\lambda)$ to obtain $(p_1, p_2, p_3, p_4, \mathbb{G}, \mathbb{G}_T, e)$ with $\mathbb{G} = \mathbb{G}_{p_1} \times \mathbb{G}_{p_2} \times \mathbb{G}_{p_3} \times \mathbb{G}_{p_4}$, where $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order $N = p_1p_2p_3p_4$. Next it chooses $g \in \mathbb{G}_{p_1}$, $X_3 \in \mathbb{G}_{p_3}$, $X_4 \in \mathbb{G}_{p_4}$ uniformly at random. The public parameters are published as

$$\mathsf{params} = (N, g, X_3, X_4)$$

CreateGroup(params): The group administrator GA of a group G takes the public parameter params as input and chooses $h, u_1, ..., u_n \in \mathbb{G}_{p_1}$, $Z \in \mathbb{G}_{p_4}$, $\alpha, a \in \mathbb{Z}_N$ uniformly at random. Then outputs group G's public information

$$GPK_G = (g^a, e(g,g)^\alpha, u_1, ..., u_n, H = h \cdot Z).$$

The master secrete key is $GSK_G = (h, \alpha)$.

AddUser(GSK_G, S_U): To add a member U with a set of attributes S_U to the group G, the group administrator GA takes input GPK_G, GSK_G and S_U, and chooses $t \in \mathbb{Z}_N$, $R, R', R_1, \ldots, R_n \in \mathbb{G}_{p_3}$ uniformly at random. Then the credential $\mathsf{cred}_U = (\mathcal{S}_U,\ K_U, K'_U, \{K^i_U\}_{1 \le i \le n})$ is computed as

$$K_U = g^\alpha g^{at} R,\ K'_U = g^t R',\ K^i_U = (u_i^{s_i} h)^t R_i.$$

HandShake(A, B): Let A be a member of group G_A and B be a member of G_B. Suppose A with a secret credential cred_A of attributes S_A, and B with a secret credential cred_B corresponding to attributes S_B, are engaging in a handshake protocol. The protocol proceeds as follows:

1. A sets a policy $\mathbb{A} = (\mathbf{M}, \rho, \mathcal{T}_B)$ that can be satisfied by S_B, in which $\mathbf{M}$ is an $\ell \times n$ matrix, ρ is a map from each row M_x of $\mathbf{M}$ to an attribute name and $\mathcal{T}_B = (t_{\rho(1)}, \ldots, t_{\rho(\ell)}) \in \mathbb{Z}_N^\ell$. Then A randomly chooses $k_1 \in \mathbb{G}_T$, $r_{1x}, r'_{1x} \in \mathbb{Z}_N$, $v_1, v'_1 \in \mathbb{Z}_N^n$, where $v_1 = (s_1, v_{10}, \ldots, v_{1n})$ and $v'_1 = (s'_1, v'_{10}, \ldots, v'_{1n})$. For $1 \le x \le \ell$, it picks $Z_{1,x}, Z'_{1,x}, Z_{2,x}, Z'_{2,x} \in \mathbb{G}_{p_4}$. Finally, A utilizes $GPK_{G_{B'}} = (g^{a_1}, e(g,g)^{\alpha_1}, u_1, ..., u_n, H = h \cdot Z)$ to compute

$$\tilde{C}_1 = k_1 \cdot e(g,g)^{\alpha_1 s_1},\ C'_1 = g^{s_1},$$
$$C_{1,x} = g^{a_1 M_x \cdot v_1} (u_{\rho(x)}^{t_{\rho(x)}} H)^{-r_{1x}} \cdot Z_{1,x},\ D_{1,x} = g^{r_{1x}} \cdot Z'_{1,x},$$
$$\tilde{C}_2 = e(g,g)^{\alpha_1 s'_1},\ C'_2 = g^{s'_1},$$
$$C_{2,x} = g^{a_1 M_x \cdot v'_1} (u_{\rho(x)}^{t_{\rho(x)}} H)^{-r'_{1x}} \cdot Z_{2,x},\ D_{2,x} = g^{r'_{1x}} \cdot Z'_{2,x}.$$

and sends the ciphertext $C_B = ((\mathbf{M}, \rho),\ \tilde{C}_1, C'_1, \{C_{1,x}, D_{1,x}\}_{1 \le x \le \ell}, \tilde{C}_2, C'_2, \{C_{2,x}, D_{2,x}\}_{1 \le x \le \ell})$ to B. Note that $G_{B'}$ is the group that B must be in order to complete the handshake.

2. B also chooses a policy $\mathbb{A}' = (\mathbf{M}', \rho', \mathcal{T}_A)$ that can be satisfied by S_A, in which $\mathbf{M}'$ is an $\ell \times n$ matrix, ρ' is a map from each row M'_x of $\mathbf{M}'$ to an attribute name and $\mathcal{T}_A = (t_{\rho'(1)}, \ldots, t_{\rho'(\ell)}) \in \mathbb{Z}_N^\ell$. Then B randomly chooses $k_2 \in \mathbb{G}_T$, $r_{2y}, r'_{2y} \in \mathbb{Z}_N$, $v_2, v'_2 \in \mathbb{Z}_N^n$, where $v_2 = (s_2, v_{20}, \ldots, v_{2n})$ and $v'_2 = (s'_2, v'_{20}, \ldots, v'_{2n})$. For $1 \le y \le \ell$, it picks $Z_{3,y}, Z'_{3,y}, Z_{4,y}, Z'_{4,y} \in \mathbb{G}_{p_4}$. Finally, B uses $GPK_{G_{A'}} = (g^{a_2}, e(g,g)^{\alpha_2}, u'_1, ..., u'_n, H' = h' \cdot Z')$ to compute

$$\tilde{C}_3 = k_2 \cdot e(g,g)^{\alpha_2 s_2},\ C'_3 = g^{s_2},$$
$$C_{3,y} = g^{a_2 M'_y \cdot v_2} (u'^{t_{\rho'(y)}}_{\rho'(y)} H')^{-r_{2y}} \cdot Z_{3,y},\ D_{3,y} = g^{r_{2y}} \cdot Z'_{3,y},$$
$$\tilde{C}_4 = e(g,g)^{\alpha_2 s'_2},\ C'_4 = g^{s'_2},$$
$$C_{4,y} = g^{a_2 M'_y \cdot v'_2} (u'^{t_{\rho'(y)}}_{\rho'(y)} H')^{-r'_{2y}} \cdot Z_{4,y},\ D_{4,y} = g^{r'_{2y}} \cdot Z'_{4,y}.$$

and sends $C_A = ((\mathbf{M}', \rho'),\ \tilde{C}_3, C'_3, \{C_{3,y}, D_{3,y}\}_{1 \le y \le \ell},\ \tilde{C}_4, C'_4, \{C_{4,y}, D_{4,y}\}_{1 \le y \le \ell})$ to A. Note that $G_{A'}$ is the group that A must belong to in order to complete the handshake.

3. Upon receiving the ciphertext C_A, A parses C_A as $((\mathbf{M}', \rho'),\ \tilde{C}_3, C'_3, \{C_{3,y}, D_{3,y}\}_{1 \le y \le \ell},\ \tilde{C}_4, C'_4, \{C_{4,y}, D_{4,y}\}_{1 \le y \le \ell})$, and uses $(GPK_{G_A}, \mathsf{cred}_A)$ to calculate $\mathrm{I}_{\mathbf{M}', \rho'}$ from $(\mathbf{M}', \rho')$, where $\mathrm{I}_{\mathbf{M}', \rho'}$ denotes the set of minimum subsets of $\{1, \ldots, \ell\}$ that satisfies $(\mathbf{M}', \rho')$. It then checks if there exists a $\mathcal{I}' \in \mathrm{I}_{\mathbf{M}', \rho'}$ that satisfies

$$\tilde{C}_4 = e(C'_4, K_A) / \left(\prod_{i \in \mathcal{I}'} (e(C_{4,i}, K'_A) \cdot e(D_{4,i}, K_A^{\rho'(i)}))^{\omega'_i} \right),$$

where $\sum_{i\in\mathcal{I}'}\omega_i' A_i' = (1,0,\ldots,0)$. If no element in $\mathrm{I}_{\mathbf{M}',\rho'}$ satisfies the above equation, it outputs $\perp$. When $G_A = G_{A'}$, A can recover

$$e(C_3', K_A)/\left(\prod_{i\in\mathcal{I}'}(e(C_{3,i}, K_A') \cdot e(D_{3,i}, K_A^{\rho'(i)}))^{\omega_i'}\right) = e(g,g)^{\alpha_2 s_2}.$$

and compute k_2 as $\tilde{C}_3/e(g,g)^{\alpha_2 s_2}$.

4. Upon receiving the ciphertext C_B, B parses C_B as $((\mathbf{M},\rho), \tilde{C}_1, C_1', \{C_{1,x}, D_{1,x}\}_{1\le x\le \ell}, \tilde{C}_2, C_2', \{C_{2,x}, D_{2,x}\}_{1\le x\le \ell})$, and uses $(GPK_{G_B}, \mathsf{cred}_B)$ to calculate $\mathrm{I}_{\mathbf{M},\rho}$ from $(\mathbf{M},\rho)$, where $\mathrm{I}_{\mathbf{M},\rho}$ denotes the set of minimum subsets of $\{1,\ldots,\ell\}$ that satisfies $(\mathbf{M},\rho)$. It then checks if there exists a $\mathcal{I} \in \mathrm{I}_{\mathbf{M},\rho}$ that satisfies

$$\tilde{C}_2 = e(C_2', K_B)/\left(\prod_{i\in\mathcal{I}}(e(C_{2,i}, K_B') \cdot e(D_{2,i}, K_B^{\rho(i)}))^{\omega_i}\right),$$

where $\sum_{i\in\mathcal{I}}\omega_i M_i = (1,0,\ldots,0)$. If no element in $\mathrm{I}_{\mathbf{M},\rho}$ satisfies the above equation, it outputs $\perp$. When $G_B = G_{B'}$, B can recover

$$e(C_1', K_B)/\left(\prod_{i\in\mathcal{I}}(e(C_{1,i}, K_B') \cdot e(D_{1,i}, K_B^{\rho(i)}))^{\omega_i}\right) = e(g,g)^{\alpha_1 s_1}.$$

and compute k_1 as $\tilde{C}_1/e(g,g)^{\alpha_1 s_1}$.

At the end of the handshake, both A and B share the key $k = (k_1, k_2)$.

According to Theorem 1, the secret handshake protocol is secure as long as the underlying modified CP-ABE scheme with partially hidden access structures is CPA secure. We now state the security theorem of the modified CP-ABE scheme.

Theorem 2. *If Assumptions 1, 2, 3 and 4 hold, then the modified centralized CP-ABE is CPA secure and the access structures is partially hidden.*

The proof employs the dual system technology proposed in [30] which is similar with the proof in [18]. In the underlying CP-ABE scheme, the encryption algorithm encrypts both the sharing key k_i and a constant message '1' to get the ciphertext without the information of attribute-values in the access structure. When decrypting the ciphertext, the decryption algorithm first decrypts the second part of ciphertext to check whether the result equals to '1', if so, the first part ciphertext could be decrypted correctly, otherwise, it means the access structure cannot be satisfied by the attributes associated with the key. We note that, the modification of the global parameters is intended to guarantee that users running the secret handshake protocol are using parameters in the same group, thus the adversary cannot tell whether say Alice is shaking with Bob or Carol.

5 Conclusions

In this paper, we studied attribute-based secret handshakes which support dynamic flexible or expressive matching policies on attributes compared to the threshold policy in previous schemes.

We first introduced a notion of fully secure centralized CP-ABE and then proposed a generic construction of attribute-based secret handshakes based on the primitive. Our handshake schemes support the same access structures on attributes as those supported by the underlying CP-ABE and achieves unlinkability with reusable credentials.

Then we proposed an efficient attribute-based secret handshake scheme employing CP-ABE scheme with partial hidden access structure. Our construction supports dynamic flexible matching policy and can provide impersonator resistance, detector resistance and unlinkability secure properties.

Acknowledgement. This work was supported by National Natural Science Foundation of China (Nos. 61572235, 61300226), Research Fund for the Doctoral Program of Higher Education of China (No. 20134401120017), Guangdong Natural Science Funds for Distinguished Young Scholar (No. 2015A030306045), ISN Research Fund (No. ISN15-04) and Pearl River S&T Nova Program of Guangzhou.

References

1. Ateniese, G., Kirsch, J., Blanton, M.: Secret handshakes with dynamic and fuzzy matching. In: Proceedings of the 14th Annual Network and Distributed System Security Symposium, NDSS (2007)
2. Balfanz, D., Durfee, G., Shankar, N., Smetters, D.K., Staddon, J., Wong, H.C.: Secret handshakes from pairing-based key agreements. In: IEEE Symposium on Security and Privacy 2003, pp. 180–196. IEEE Computer Society (2003)
3. Bellare, M., Rogaway, P.: Random oracles are practical: a paradigm for designing efficient protocols. In: Proceedings of ACM CCS 1993, pp. 62–73. ACM Press, New York (1993)
4. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy 2007, pp. 321–334. IEEE Computer Society (2007)
5. Boneh, D., Boyen, X.: Efficient selective-id secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
6. Boneh, D., Boyen, X.: Short signatures without random oracles and the SDH assumption in bilinear groups. J. Crypt. **21**(2), 149–177 (2008)
7. 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)
8. Camenisch, J.L., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Heidelberg (2004)

9. Canetti, R., Halevi, S., Katz, J.: A forward-secure public-key encryption scheme. In: Biham, E. (ed.) Advances in Cryptology — EUROCRYPT 2003. LNCS, vol. 2656, pp. 255–271. Springer, Heidelberg (2003)
10. 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)
11. Cheung, L., Newport, C.: Provably secure ciphertext policy ABE. In: Proceedings of ACM CCS 2007, pp. 456–465. ACM Press, New York (2007)
12. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of ACM CCS 2006, pp. 89–98. ACM Press, New York (2006)
13. Jarecki, S., Kim, J.H., Tsudik, G.: Authentication for paranoids: multi-party secret handshakes. In: Zhou, J., Yung, M., Bao, F. (eds.) ACNS 2006. LNCS, vol. 3989, pp. 325–339. Springer, Heidelberg (2006)
14. Jarecki, S., Kim, J.H., Tsudik, G.: Beyond secret handshakes: affiliation-hiding authenticated key exchange. In: Malkin, T. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 352–369. Springer, Heidelberg (2008)
15. 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)
16. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008)
17. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. Cryptology ePrint Archive, Report 2007/404 (2007)
18. Lai, J.Z., RH. D, YJ. Li,: Expressive CP-ABE with partially hidden access structures. In: 7th ACM Symposium on Information, Compuer and Communications Security (2012)
19. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010)
20. Li, N., Du, W., Boneh, D.: Oblivious signature-based envelope. In: ACM Symposium on Principles of Distibuted Computing (PODC 2003), pp. 182–189. ACM Press, New York (2003)
21. 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)
22. Nishide, T., Yoneyama, K., Ohta, K.: Attribute-based encryption with partially hidden encryptor-specified access structures. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 111–129. Springer, Heidelberg (2008)
23. Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 214–231. Springer, Heidelberg (2009)
24. Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: Proceedings of ACM CCS 2007, pp. 195–203. ACM Press, New York (2007)
25. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)

26. 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)
27. Tsudik, G., Xu, S.: Brief announcement: a flexible framework for secret handshakes. In: PODC 2005, p. 39. ACM Press, New York (2005)
28. Vergnaud, D.: RSA-based secret handshakes. In: Ytrehus, Ø. (ed.) WCC 2005. LNCS, vol. 3969, pp. 252–274. Springer, Heidelberg (2006)
29. Waters, B.: Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. Cryptology ePrint Archive, Report 2008/290 (2008). http://eprint.iacr.org/
30. Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009)
31. Xu, S., Yung, M.: k-anonymous secret handshakes with reusable credentials. In Proceedings of ACM CCS 2004, pp. 158–167. ACM Press, New York (2004)
32. 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)