Abstract: A new concept called multi-proxy multi-signcryption is introduced in this paper. In a multi-proxy multi-signcryption scheme, a group of original signcrypters can authorize a group of proxy signcrypters under the agreement of all signcrypters in the original group. Then only the cooperation of all signcrypters in the proxy group could generate a multi-proxy multi-signcryption. We propose a multi-proxy multi-signcryption scheme based on bilinear pairings. The proposed scheme has the following characteristics: (i) the size of multi-proxy multi-signcryption is independent of the number of original and proxy signcrypters. (ii) it provides the fair protection for the original signcyrpter group and the proxy group. (iii) the key management problem is simplified because of using ID-based cryptography. Finally, we give an application of the proposed scheme in electronic commerce.

KeyWord: ID-based cryptography; signcryption; multi-proxy multi-signcryption; electronic commerce

I. INTRODUCTION


Signcryption, first proposed by Zheng [8] in 1997, is a cryptographic primitive that performs signature and encryption simultaneously, at lower computational costs and communication overheads than the signature-then-encryption approach. Several ID-based signcryption schemes were also proposed in [9]–[11]. In 1999, Gamage et al. [12] introduced a new notion called proxy signcryption by combining the concepts of proxy signature and signcryption together. In such a scheme, an original signcyrpter can delegate his signcryption power to a designated person, called the proxy signcyrpter who can generate signcryption on behalf of the original signcyrpter. Li and Chen [13] proposed an ID-based proxy signcryption scheme in 2004.

In this paper, we introduce a new conception called multi-proxy multi-signcryption which is a new kind of proxy signcryption. In a multi-proxy multi-signcryption scheme, a group of original signcrypters can authorize a group of proxy signcrypters under the agreement of all signcrypters in the original group. To realize this new kind of proxy signcryption scheme, we propose a multi-proxy multi-signcryption scheme based on bilinear pairings. The proposed scheme makes use of Chen and Malone-Lee’s scheme [11] as the basic scheme.

II. PRELIMINARY WORKS

In this section, we briefly describe the basic definition and properties of the bilinear pairings.

Let \( G_1 \) be a cyclic additive group generated by \( P \), whose order is a prime \( q \), and \( G_2 \) be a cyclic multiplicative group of the same order \( q \). Let \( a, b \) be elements of \( \mathbb{Z}_q^* \). A bilinear pairings is a map \( \hat{e} : G_1 \times G_1 \rightarrow G_2 \) with the following properties:

1) Bilinearity: \( \hat{e}(nP, bP) = (\hat{e}(P, Q))^{ab} \).

2) Non-degeneracy: There exists \( P \) and \( Q \in G_1 \) such that \( \hat{e}(P, Q) \neq 1 \).

3) Computability: There is an efficient algorithm to compute \( \hat{e}(P, Q) \) for all \( P, Q \in G_1 \).

The modified Weil pairing and the Tate pairing [4] are admissible maps of this kind. The security of our scheme described here relies on the hardness of the following problems.

Definition 1: Given two groups \( G_1 \) and \( G_2 \) of the same prime order \( q \), a bilinear map \( \hat{e} : G_1 \times G_1 \rightarrow G_2 \) and a generator \( P \) of \( G_1 \), the Bilinear Diffie-Hellman problem (BDHP) in \((G_1,G_2,\hat{e})\) is to compute \( h = \hat{e}(P,P)^{abc} \) given \((P,aP,bP,cP)\).

Definition 2: Given two groups \( G_1 \) and \( G_2 \) of the same prime order \( q \), a bilinear map \( \hat{e} : G_1 \times G_1 \rightarrow G_2 \) and a generator \( P \) of \( G_1 \), the Decisional Bilinear Diffie-Hellman problem (DBDHP) in \((G_1,G_2,\hat{e})\) is to decide whether \( h = \hat{e}(P,P)^{abc} \) given \((P,aP,bP,cP)\) and an element \( h \in G_2 \).

The decisional problem is of course not harder than the computational one. However, no algorithm is known to be able to solve any of them so far.

III. THE PROPOSED SCHEME

In this section, we propose an ID-based multi-proxy multi-signcryption scheme from bilinear pairings. The proposed
scheme uses the Chen and Malone-Lee’s scheme [11] as the basic scheme. Our scheme involves four roles: the PKG, a set of original signcrupters $D = \{O_1, O_2, \ldots, O_q\}$ with identity $ID_{O_1}, ID_{O_2}, \ldots, ID_{O_q}$, a set of proxy signcrupters $L = \{P_1, P_2, \ldots, P_l\}$ with identity $ID_{P_1}, ID_{P_2}, \ldots, ID_{P_l}$, and the message recipient Bob with identity $ID_B$. It consists of the following seven algorithms.

**Setup:** Given a security parameter $k$, the PKG chooses groups $G_1$ and $G_2$ of prime order $q$ (with $G_1$ additive and $G_2$ multiplicative), a generator $P$ of $G_1$, a bilinear map $\hat{\cdot}: G_1 \times G_1 \rightarrow G_2$ and hash functions $H_0: \{0, 1\}^{k} \rightarrow G_1$, $H_1: \{0, 1\}^{k_0+n} \rightarrow \mathbb{Z}_q^*$, $H_2: G_2 \rightarrow \{0, 1\}^{k_0+n}$ and $H_3: \{0, 1\}^{k_2+k_0} \rightarrow G_2^*$. Here $k_0$ is the number of bits required to represent an element of $G_1$; $k_1$ is the number of bits required to represent an identity; $k_2$ is the number of bits required to represent a warrant; and $n$ is the number of bits of a message to be signcrypted. The PKG also chooses a master-key $s \in Z_q^*$ and computes $P_{pub} = sP$. The PKG publishes system’s public parameters $(G_1, G_2, n, \hat{\cdot}, P, P_{pub}, H_0, H_1, H_2, H_3)$ and keeps the master-key $s$ secret.

**Extract:** Given a user $U$’s identity $ID_U \in \{0, 1\}^{k_1}$, the PKG computes the user’s public key $Q_U = H_0(ID_U)$ and private key $S_U = sQ_U$.

**Generation of the proxy key:** To delegate the signcryption capacity to the proxy group $L$, each original signcrupter $O_i$ follows the steps below to generate the signed warrant $m_w$ and each proxy signcrupter $P_j$ computes his proxy private key $S_{OP_j}$ and corresponding proxy public key $Q_{OP_j}$. The warrant $m_w$ specifies the delegation period, what kind of messages is delegated and identity information of the original signcrupters and the proxy signcrupters, etc.

1) Each original signcrupter $O_i$ chooses $x_i$ from $Z_q^*$ randomly, computes $U_i = x_iP$ and broadcasts $U_i$ to other $d - 1$ original signcrupters.
2) Each $O_i$ computes $U = \sum_{i=1}^{d} U_i$, $S_i = H_3(m_w || U)S_{O_i} + x_iP_{pub}$ and sends $(m_w, U, S_i)$ to the proxy group $L$.
3) When receiving all $(m_w, U, S_i)$, each proxy signcrupter $P_j$ computes $U = \sum_{i=1}^{d} U_i$, $Q_{OP_j} = H_0(ID_{O_j})$ and checks if the following equations hold:

$$\hat{\epsilon}(P, S_i) = \hat{\epsilon}(P_{pub}, Q_{O_i})H_3(m_w || U)\hat{\epsilon}(U, P_{pub}), i = 1, 2, \ldots, d.$$ 

If all $(m_w, U, S_i)$ are verified to be legal, $P_j$ computes $Q_{P_j} = H_0(ID_{P_j})$, his proxy private key $S_{OP_j} = H_3(m_w || U)S_{P_j} + \sum_{i=1}^{d} S_i$ and corresponding proxy public key $Q_{OP_j} = H_3(m_w || U)(Q_{P_j} + \sum_{i=1}^{d} Q_{O_i}) + U$; otherwise rejects it and requests a valid one.

**Multi-proxy multi-sign:** Suppose the proxy group $L$ wants to send a delegated message $m$ on behalf of the original group $D$ to Bob. Each proxy signcrupter $P_j$ generates the partial proxy signature and an appointed clerk $C$, who is one of the proxy signcrupters, combines the partial proxy signatures to generate the final multi-proxy multi-signature.

1) Each $P_j$ chooses $r_j$ from $Z_q^*$ randomly, computes $X_j = r_jQ_{OP_j}$ and broadcasts $X_j$ to the other $l - 1$ co-signcrupters.
2) Each $P_j$ computes $X = \sum_{j=1}^{d} X_j$, $h = H_1(X || m)$, $Z_j = (r_j + h)S_{OP_j}$ and sends the individual proxy signature $(X_j, X, Z_j)$ to the clerk $C$.
3) The clerk $C$ verifies the individual proxy signatures by checking if the following equation holds:

$$\hat{\epsilon}(Z_j, P) = \hat{\epsilon}(P_{pub}, X_j + hS_{OP_j}), j = 1, 2, \ldots, l.$$ 

If all individual proxy signatures are verified to be legal, the clerk $C$ computes $Z = \sum_{j=1}^{d} Z_j$, otherwise rejects it and requests a valid one. The final multi-proxy multi-signature is $(m_w, U, X, Z)$.

**Encrypt:** To encrypt $m$ for recipient Bob, each $P_j$ generates the partial encryption key and the clerk $C$ combines these partial encryption keys to generate the ciphertext.

1) Each $P_j$ computes $Q_B = H_0(ID_B)$, $w_j = \hat{\epsilon}(r_jS_{OP_j}, Q_B)$ and sends $w_j$ to the clerk $C$.
2) The clerk $C$ computes $w = \prod_{j=1}^{l} w_j$.
3) The clerk $C$ computes $Y = H_2(w) \oplus (Z || ID_{P_1} || ID_{P_2} || \ldots || ID_{P_l} || m)$.
4) The clerk $C$ sends the ciphertext $(m_w, U, X, y)$ to Bob.

**Decrypt:** To decrypt a ciphertext $(m_w, U, X, y)$ from the proxy group $L$, Bob follows the steps below.

1) Compute $w = \hat{\epsilon}(X, S_B)$.
2) Compute $Z || ID_{P_1} || ID_{P_2} || \ldots || ID_{P_l} || m = y \oplus H_2(w)$.
3) Forward message $m$, multi-proxy multi-signature $(m_w, U, X, Z)$ and $P_j$’s identity $ID_{P_j}$ for $j = 1, 2, \ldots, l$ to Verify.

**Verify:** To verify the proxy group $L$’s multi-proxy multi-signature $(m_w, U, X, Z)$ on message $m$, any third party follows the steps below.

1) Compute $Q_{O_i} = H_0(ID_{O_i})$ for $i = 1, 2, \ldots, d$.
2) Compute $Q_{P_j} = H_0(ID_{P_j})$ and $Q_{OP_j} = H_3(m_w || U)(Q_{P_j} + \sum_{i=1}^{d} Q_{O_i}) + U$ for $j = 1, 2, \ldots, l$.
3) Compute $h = H_1(X || m)$.
4) Check if the following equation holds:

$$\hat{\epsilon}(Z, P) = \hat{\epsilon}(P_{pub}, X + h\sum_{j=1}^{l} Q_{OP_j}).$$

If it does, the third party accepts the multi-proxy multi-signature; otherwise rejects it.

**IV. ANALYSIS OF THE PROPOSED SCHEME**

In this section, we discuss the security and efficiency of the proposed multi-proxy multi-signcryption scheme.

**A. Security**

We show that our ID-based multi-proxy multi-signcryption scheme satisfies all the requirements should be have.

1) **Distinguishability:** This is obvious, because there is a warrant $m_w$ in a valid multi-proxy multi-signature, at the same time, this warrant $m_w$ and the public keys of the original signcrupters and the proxy signcrupters must occur in the verification equation of the multi-proxy multi-signature.
2) **Verifiability:** Because the warrant contains the identity information and the limit of the delegated signcryption capacity, the verifier can verify the multi-proxy multi-signature and check whether the signcrypted message conforms to the delegation warrant or not.

3) **Strong unforgeability:** We consider two types of attacks to the proposed scheme: the outsider forgery attack and the insider forgery attack.

   - **Outsider forgery attack:** An adversary \( A \), who is not in the proxy group \( L \) may attempt to forge a multi-proxy multi-signature for a chosen message. In this attack, we assume that all public information is available to \( A \).

   - **Insider forgery attack:** A co-signcyper in the proxy group \( L \) or the collusion of some co-signcypers may attempt to forge the multi-proxy multi-signature for the proxy group. In this attack, we assume that the number of malicious co-signcypers in the proxy group can be as many as \( l - 1 \).

Due to the employment of the basic scheme, the security of the proposed scheme is based on the robustness of the Chen and Malone-Lee’s scheme [11]. Besides, we assume that all hash functions used herein are secure for cryptographic usages. Below, we first prove the security of the individual proxy signature is equivalent to the signature in the Chen and Malone-Lee’s scheme. Subsequently, we show that the proposed scheme is secure against the outsider forgery attack and the insider forgery attack. Our proving method used here is similar to the one in [15].

**Theorem 1:** The security of the individual proxy signature is equivalent to the signature in the Chen and Malone-Lee’s scheme under the assumption that the hash function \( H_1 \) is secure.

**Proof.** In the Chen and Malone-Lee’s scheme, a valid signature for message \( m \) is \((X, Z)\), and its verification equation can be represented as

\[
\hat{e}(Z, P) = \hat{e}(P_{pub}, X + H_1(X|m)Q_A).
\]  

(3)

In the proposed scheme, a valid individual proxy signature for message \( m \) is \((X_j, X, Z_j)\), where \( X = \sum_{j=1}^{l} X_j \). The verification equation (1) can be represented as

\[
\hat{e}(Z_j, P) = \hat{e}(P_{pub}, X_j + H_1(X_j + X_{2j}|m)Q_{OP_j}).
\]  

(4)

where \( X_{2j} = X - X_j = \sum_{k=1, k \neq j}^{l} X_k \).

In Eq.(4), if \( X_{2j} \) is fixed in advance, then the construction of the Eq.(4) is related to Eq.(3), which implies that finding a valid proxy signature \((X_j, Z_j)\) for Eq.(4) will require the same knowledge as the case for Eq.(3). On the other hand, if \( Z_j \) is fixed prior to the computing of \((X_j, X_{2j})\) to satisfy the Eq.(4), the adversary will have to convert \( H_1 \) to attempting this. Under the assumption that \( H_1 \) is a secure hash function, the security of the individual proxy signature in the proposed schemes is equivalent to that of the signature in the Chen and Malone-Lee’s scheme, which is secure against adaptively chosen message attack in the random oracle model [11].

**Theorem 2:** The proposed scheme is secure against the outsider forgery attack.

**Proof.** For the outsider forgery attack, consider that an adversary \( A \), who is not in the proxy group \( L \) may attempt to forge a multi-proxy multi-signature of a chosen message \( m \) for the proxy group \( L \). That is, \( A \) knows all public information, including all the public keys \( Q_{P_j} \) and \( Q_{OP_j} \) for all \( P_j \), and wants to find \((X, Z)\) satisfying the verification equation (2). By letting the public verification key for \( Q \) as \( \sum_{j=1}^{l} Q_{OP_j} \), the construction of the multi-proxy multi-signature of the our scheme can be related to the construction of the signature in the Chen and Malone-Lee’s scheme. This implies that such attack is equivalent to the signature forgery in the Chen and Malone-Lee’s scheme. Since the Chen and Malone-Lee’s scheme is secure against existential forgery on adaptively chosen message attack in the random oracle model [11], the outsider forgery attack is infeasible in the our scheme. Even all the original signcypers cannot create a valid multi-proxy multi-signature since each proxy private key \( S_{OP_j} \) includes the private key \( S_{P_j} \) of proxy signcyper \( P_j \).

**Theorem 3:** The proposed scheme is secure against the insider forgery attack.

**Proof.** For the insider forgery attack, we assume there is at least one honest co-signcyper \( P_k \) in the proxy group \( L \). Considering that some malicious signcypers who want to generate the multi-proxy multi-signature of the message \( m \) for the proxy group \( L \). From Multi-proxy multi-sign, it can be see that all malicious co-signcypers have to obtain \( P_k \)’s individual proxy signature to attempt this. With all public information and individual proxy signatures generated by \( P_k \) regarding some messages different to \( m \), all malicious co-signcypers may try to deduce \( P_k \)’s proxy private key or forge \( P_k \)’s individual proxy signature for \( m \). However, deducing \( P_k \)’s proxy private key \( S_{OP_k} = H_3(m_w||U)S_{P_k} + \sum_{i=1}^{d} S_i \) from his proxy public key \( Q_{OP_k} = H_3(m_w||U)(Q_{P_k} + \sum_{i=1}^{d} Q_{S_i}) + U \) requires the knowledge of PKG’s private key \( s \) and finding \( s \) from PKG’s public key \( P_{pub} = sP \) requires solving discrete logarithm problem. On the other hand, the individual proxy signature \((X_k, Z_k)\) has the same security strength as the signature in the Chen and Malone-Lee’s scheme, which has been proven in Theorem 1. Therefore, the insider forgery attack is infeasible.

4) **Strong identifiability:** It contains the warrant \( m_w \) in a valid multi-proxy multi-signature, so anyone can determine the identity of the corresponding proxy signcypers from the warrant \( m_w \).

5) **Strong undeniability:** The clerk \( C \) verifies the individual proxy signature of each proxy signcyper, so no one can be deniable of his signature.
6) Prevention of misuse: Due to using the warrant $m_w$, the proxy signcryption schemes can only signcrypt messages that have been authored by the original group.

7) Message confidentiality: We can prove that the message confidentiality of the our scheme is equivalent to that of the Chen and Malone-Lee’s scheme.

**Theorem 4:** The message confidentiality of the our scheme is equivalent to that of the Chen and Malone-Lee’s scheme.

**Proof.** In the Chen and Malone-Lee’s scheme, a valid ciphertext for message $m$ is $(X, y)$, where

$$y = H_2(w) \oplus (Z||DA||m).$$

(5)

In the proposed scheme, a valid ciphertext for message $m = (m_w, U, X, y)$ and $y$ can be represented as

$$y = H_2(w_y + w_z) \oplus (Z||ID_{P_1}||ID_{P_2}|| \ldots ||ID_{P_l}||m),$$

(6)

where $w_y = w - w_z = \sum_{k=1}^{l} w_k$.

In Eq.(6), if $w_y$ is fixed in advance, then the Eq.(6) is related to Eq.(5), which implies that finding a valid $m$ for Eq.(6) will require the same knowledge as the case for Eq.(5). Therefore, the message confidentiality of the proposed scheme is equivalent to that of the Chen and Malone-Lee’s scheme, which is secure against adaptively chosen ciphertext attack in the random oracle model [11].

**B. Efficiency**

We compare the computational costs and communication overheads (CommOver for short) of our multi-proxy multi-signcryption scheme with those of the multi-proxy multi-signature-then-encryption approach in Table I. From Table I, we can see that both the computational costs and communication overheads of our scheme are lower than those of LC+BF.

**TABLE I
THE COMPUTATIONAL COSTS AND COMMUNICATION OVERHEADS COMPARISONS**

<table>
<thead>
<tr>
<th></th>
<th>LC+BF</th>
<th>Our scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-proxy multi-sign</td>
<td>Encrypt: $3M + 3E$</td>
<td>Encrypt: $2M + 1E$</td>
</tr>
<tr>
<td></td>
<td>Decrypt: $D$</td>
<td>Decrypt: $P$</td>
</tr>
<tr>
<td></td>
<td>Verify: $3P + E$</td>
<td>Verify: $2P + (l+1)M$</td>
</tr>
<tr>
<td></td>
<td>CommOver: $5k_0 + k_2 + n$</td>
<td>CommOver: $3k_0 + l_k + k_2 + n$</td>
</tr>
</tbody>
</table>

**V. APPLICATIONS**

We now present an application of the above multi-proxy multi-signcryption scheme in electronic commerce. A company signs some important contracts that may involve several departments, such as the financial department, the marketing department and the production office. To guarantee the confidentiality, integrity, non-repudiation and authentication of contracts, some signcryption are necessary. Usually, several directors represent a directorate to delegate their signcrypting power to the managers of all departments. Then, several of these managers represent the company to signcrypt a contract with another company through computer network. In such a case, we can exploit the above multi-proxy multi-signcryption scheme.

**VI. CONCLUSIONS**

We have proposed a new kind of proxy signcryption scheme called multi-proxy multi-signcryption from bilinear pairings with less computational costs and communication overheads.

**ACKNOWLEDGEMENT**

We thank the anonymous references for their valuable comments on this paper. This work is supported by the National High-Tech Development 863 Program of China (2009AA012415), the National Natural Science Foundation of China (60773175), the Doctor Foundation by the Ministry of Education (200806140010) and Youth Science and Technology Foundation of UESTC.

**REFERENCES**


