A New ID-based Designated Verifier Proxy Multi-Signature Scheme

Shenjun Cui and Fengtong Wen

Abstract—Proxy multi-signature allows a proxy signer to generate signatures on behalf of a group of original signers. In a designated verifier signature scheme, the signature only can be verified by a designated person. In this paper, we give the model of ID-based designated verifier proxy multi-signature and present a new ID-based designated verifier proxy multi-signature scheme. Its security is based on the computational Diffie-Hellman (CDH) problem and it is highly efficient.

Index Terms—proxy multi-signature, designated verifier, ID-based

I. INTRODUCTION

The concept of identity(ID)-based cryptosystem was first introduced by Shamir [1] in 1984 where, a user’s public key is derived from his/her identity such as his/her name, address or E-mail, etc. The user’s private key is generated by a private key generator (PKG). Application of identity-based crypto-system can avoid the use of public key certificates, so it can save system resources and improve the efficiency. In 2001, Boneh and Franklin [2] proposed a secure and efficient ID-based encryption scheme on the random oracle model. At present, there are many types of ID-based signature schemes, such as ID-based ring signature [3], ID-based aggregate signature [4].

In 1996, Jakobsson et al. [5] presented the concept of designated verifier signature. In designated verifier signature, only the designated verifier specified by the signer can check the validity of the signature. This kind of signature mechanism can be widely used in e-commerce and e-government, because it can solve the collision of the authentication and the privacy effectively. Sadeenia et al. [6] proposed the strong designated verifier signature scheme, which forces the designated verifier to use his/her private key in verification phase. Then, many designated verifier signature schemes were proposed where many ID-based signature schemes [7-9]. Recently, Kang et al. [10] pointed out Zhang-Mao’s scheme [9] can not satisfy the strong property.

The proxy signature primitive and first efficient solution were first introduced by Mambo et al. [11] in 1996, which allows the original signer to delegate his/her signing right to the proxy signer. Afterwards, a lot of proxy signature schemes and some ID-based proxy signature schemes with special features were proposed by scholars at home and abroad. Such as identity-based multi-proxy signature [12], identity-based strong designated verifier proxy signature [13], [14].

Proxy multi-signature is a special case of the proxy signature, and it was first proposed in [15]. A proxy multi-signature allows a signer to generate a valid signature on behalf of multiple original signers. Currently, there are many proxy multi-signature schemes based on identity [16], [17].

In this paper, based on the work of Kang et al. [10], we construct a new ID-based designated verifier proxy multi-signature scheme, then we analyze its security and efficiency. The rest of this paper is organized as follows. Some preliminary works are described in the next section. We give a model of ID-based designated verifier proxy multi-signature in section III. In section IV, we propose a new and efficient designated verifier proxy multi-signature scheme. The analysis of security and efficiency of the scheme is given in section V. Finally, we conclude the paper in section VI.

II. RELATED WORK

In this section, we review some basic primitives and constructions related to our scheme.

A. Bilinear Pairings

Let $G_i$ be a cyclic additive group generated by $P$, whose order is a prime $q$ ($q$ is a large prime), $G_i$ be a multiplicative cyclic group of the same order. Let $e: G_i \times G_i \rightarrow G_{t}$ be a bilinear mapping with the following properties:

1) Bilinear: For any $P, Q \in G_i$, $a, b \in Z_q^*$, $e(aP, bQ) = e(aP, Q)^b = e(P, abQ) = e(abP, Q)$

2) Non-degenerate: There exists $P \in G_i, Q \in G_i$ such that $e(P, Q) \neq 1$.

3) Computable: There exists an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G_i$. Submit your manuscript electronically for review.

B. Computational Diffie-Hellman (CDH) Problem and the CDH Assumption

**Definition 1.** Given a group $G_i$ of prime order $q$ with generator $P$ and elements $aP, bP \in G_i$ where $a, b$ are selected at random from $Z_q^*$, the CDH problem in $G_i$ is to compute $abP$. 
The private key choses a random number \( I \) and signs the warrant

They have the identities \( I \)

The multi-signature scheme is a tuple \( \text{Setup}, \text{Extract}, \text{KGen}, \text{Sign}, \text{Veri} \)

In this section, we present an ID-based designated verifier proxy multi-signature scheme.

In an ID-based designated verifier proxy multi-signature scheme, there are \( n \) original signers, a proxy signer, and a designated verifier. Let \( A_1, A_2, ..., A_n \) be the original signers, \( B \) be the proxy signer, and \( C \) be the designated verifier. They have the identities \( ID_{A_i} (i = 1, ..., n), ID_B, ID_C \) respectively.

**Definition 3.** An ID-based designated verifier proxy multi-signature scheme is a tuple \( \langle \text{Setup}, \text{Extract}, \text{KGen}, \text{Sign}, \text{Veri} \rangle \)

1. \( \text{Setup} (k) \rightarrow (\text{params}, S): \) Given a security parameter \( k \), this algorithm outputs the public parameters \( \text{params} \) of the scheme and a master secret key \( S \). The private key generator PKG stores the master secret key securely and publishes the public parameters \( \text{params} \).
2. \( \text{Extract} (\text{params}, S, ID) \rightarrow (S_{ID}, Q_{ID}): \) Given \( \text{params}, \) the master secret key \( S \) and an identity \( ID \), this algorithm outputs the private-public key pair \( (S_{ID}, Q_{ID}) \).
3. \( \text{KGen} (\text{params}, w, S_{ID}, S_{ID_B}) \rightarrow s_p: \) All original signers and the proxy signer input their identities \( ID_{A_1}, ..., ID_{A_n}, ID_B \) and their private keys \( S_{ID_{A_1}}, ..., S_{ID_{A_n}}, S_{ID_B} \), the original signers also input the delegation warrant \( w \). This algorithm outputs the proxy key \( s_p \).
4. \( \text{Sign} (\text{params}, m, s_p) \rightarrow \sigma: \) This is a randomized algorithm. Set \( m \) as the message to be signed, it inputs \( \text{params} \) and the proxy key \( s_p \), and outputs a designated verifier proxy multi-signature \( \sigma \).
5. \( \text{Veri} (\text{params}, \sigma, S_{ID}) \rightarrow \{0,1\}: \) This is a deterministic algorithm. Given a signature tuple \( \sigma \), the designated verifier uses his/her private key \( S_{ID} \) to check its validity, and outputs 1 if \( \sigma \) is valid, otherwise outputs 0.

**IV. PROPOSED ID-BASED DESIGNATED VERIFIER PROXY MULTI-SIGNATURE SCHEME**

In this section, we present an ID-based designated verifier proxy multi-signature scheme. The participants are \( n \) original signers \( A_1, A_2, ..., A_n \), a proxy signer \( B \), and a designated verifier \( C \). The details are described as follows:

**A. Setup**

1. Assume \( k \) is a security parameter. \( G_1 \) and \( G_2 \) are cyclic additive group and cyclic multiplicative group of prime order \( q \) respectively, and \( e: G_1 \times G_1 \rightarrow G_2 \) is a bilinear map.
2. \( \text{PKG} \) picks a master secret key \( s \in R \mathbb{Z}_q^* \) and computes \( Q = sp \).
3. \( \text{PKG} \) chooses hash function \( H_i: \{0,1\}^* \rightarrow G_1 \). \( H_2: \{0,1\}^* \times G_2 \rightarrow G_1 \)
4. All public system parameters \( \text{params} \) are \( (G_1, G_2, q, e, P, Q, H_1, H_2) \).

**B. Extract**

1. Given identities \( ID_{A_i} (i = 1, ..., n) \) of \( n \) original signers, \( \text{PKG} \) generates \( S_{ID_{A_i}} = sH_i(ID_{A_i}) \) and sends them to the \( n \) original signers respectively as their private keys and \( Q_{ID_{A_i}} = H_i(ID_{A_i}) \) are the public keys of them.
2. Given the identity \( ID_B \) of the proxy signer, \( \text{PKG} \) generates \( S_{ID_B} = sH_i(ID_B) \) and sends it to the proxy signer as his/her private key, and \( Q_{ID_B} = H_i(ID_B) \) is the public key of him/her.
3. Given the identity \( ID_C \) of the designated verifier, \( \text{PKG} \) generates \( S_{ID_C} = sH_i(ID_C) \) and sends it to the designated verifier as his/her private key, and \( Q_{ID_C} = H_i(ID_C) \) is the public key of him/her.

**C. KGen**

1. The warrant \( w \) contains the identity information of \( n \) original signers \( A_1, A_2, ..., A_n \), the proxy signer \( B \), the designated verifier \( C \), delegation range, delegation period, and other information of delegation.
2. Every original signer \( A_i \) signs the warrant \( w \) through the following method:
   \( A_i \) chooses a random number \( r \in \mathbb{Z}_q^* \), and computes \( U_i = rQ_{ID_{A_i}} \).
   \( \sigma_i = H_2(w, e(rQ_{ID_{A_i}}, S_{ID_{A_i}})) \),
   then, sends \( w \) and \((U_i, \sigma_i)\) to the proxy signer \( B \).
3. \( B \) checks whether the following \( n \) equations hold:
   \( \sigma_i = H_2(w, e(U_i, S_{ID_{A_i}})) \).
4. If the above \( n \) equations hold, \( B \) computes proxy key \( s_p \) as follows:
   \( B \) picks a random number \( t \in \mathbb{Z}_q^* \) and computes \( \sigma = \sum \sigma_i, \)
   \( U = tQ_{ID_B} \),
   \( s_p = tr^{-1}\sigma + S_{ID_B} \).

**D. Sign**

The proxy signer \( B \) generates a designated verifier proxy multi-signature on message \( m \):
\( V = H_1(m, w, e(Q_{ID_B}, s_p)) \).
Finally, the designated verifier proxy multi-signature is \( (m, w, \sigma, U, V) \), and \( B \) sends it to the designated verifier \( C \).
E. Veri

After receiving the signature \((m, w, \sigma, U, V)\), the designated verifier \(C\) processes as follows:

1) Verifies whether \(m\) and the identities of original signers and proxy signer meet the restrictions in the warrant \(w\).
   - If not, stops the protocol, else continues.
2) Checks whether the following equation holds:
   \[
   V = H_2(m, w, e(Q_{id}, \sigma)e(S_{id}, U)).
   \]
   If the equation holds, he/she accepts the proxy signature, otherwise, rejects it.

V. ANALYSIS OF OUR SCHEME

A. Correctness

1) The proxy signer checks \((w, U, \sigma, \cdot)\) from \(A\) through \(\sigma_i = H_2(w, e(U_i, S_{id}))\), and it is valid because of the following:
   \[
   \sigma_i = H_2(w, e(r_iQ_{id}, S_{id})).
   \]
   \[
   = H_2(w, e(r_iQ_{id}, S_{id})).
   \]
   \[
   = H_2(w, e(r_iQ_{id}, S_{id})).
   \]
   \[
   = H_2(w, e(U_i, S_{id})).
   \]
2) The verification of the designated verifier proxy multi-signature is correct by the following equations:
   \[
   V = H_2(m, w, e(Q_{id}, \sigma)).
   \]
   \[
   = H_2(m, w, e(Q_{id}, r_i\sigma + S_{id})).
   \]
   \[
   = H_2(m, w, e(Q_{id}, \sigma)).
   \]
   \[
   = H_2(m, w, e(Q_{id}, \sigma)).
   \]
   \[
   = H_2(m, w, e(Q_{id}, \sigma)).
   \]

B. Efficiency

Let \(M\) represent the point scalar multiplication operation in \(G_1\), \(E\) represent the exponentiation operation in \(G_1\), \(P\) represent the pairing operation, and \(I\) represent the inverse operation. We omit the cost of integer addition, integer comparison and hash operation. In the table 1, we analyze the efficiency of our scheme, and it is easy to see our scheme is highly efficient, because there is no exponentiation operation in our scheme.

<table>
<thead>
<tr>
<th>Table 1. Computational Cost of Our Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>KGen</td>
</tr>
<tr>
<td>Sign</td>
</tr>
<tr>
<td>Veri</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

C. Security

1) Verifiability

After the designated verifier obtains the proxy signature \((m, w, \sigma, U, V)\), he/she can identify the identities of original signers and proxy signer from the warrant \(w\), obviously, the verifier can check the signature through the verification equation.

2) Unforgeability

Any attacker wants to imitate the proxy signer \(B\) to forge a signature delegated by \(n\) original signers, he/she needs the private key \(S_{id}\) of \(B\), because the generation of the proxy signature needs the proxy key \(s_p\), but \(s_p = r\sigma + S_{id}\) contains the private key \(S_{id}\) of \(B\). Due to the private key \(S_{id}\) is kept secretly by \(B\), if the attacker wants to get it from \(S_{id} = sH_1(ID_b)\), it is not feasible according to the CDH assumption, so the attacker can not forge the signature. Moreover, on the basis of the CDH problem, and the difficulties of the inverse operation on bilinear pairings and the one-way hash function, if the attacker randomly chooses a message \(m\) he/she can’t generate a signature through \(V' = H_2(m, w, e(Q_{id}, \sigma)^{(s_{id}U)}\) without knowing the proxy key \(s_p\) and the private key \(S_{id}\) of the designated verifier.

3) Identifiability

The designated verifier can determine the identity of the proxy signer from the signature because the signature contains the warrant \(w\) which includes the information of the proxy signer.

4) Prevention of misuse

The proxy signer can’t use the proxy key to generate a designated verifier proxy multi-signature for the purpose other than the \(n\) original signers delegated, because of the use of warrant signed by \(n\) original signers \(w\).

5) Designated verification

The designated verifier \(C\) uses his/her private key to check the validity of the proxy multi-signature, hence, except the designated verifier, anyone can’t check the validity of signature. Even any third party gains the private key of the designated verifier he/she can’t be convinced by the validity of the signature because the designated verifier \(C\) can simulate the same transcripts in an indistinguishable way. To generate a designated verifier proxy multi-signature for any message \(m'\) which is corresponding to the warrant \(w'\), \(C\) chooses two random number \(r, r'\), and computes \(\sigma = r'Q_{U'} = tQ_{d_{id}}, V' = H_2(m, w, e(S_{id}, rP)e(S_{id}, U'))\), that is, the designated verifier can simulate the transcripts indistinguishable from the signer’s. Therefore, the new scheme is a strong designated verifier proxy multi-signature.

VI. Conclusion

In this paper, we constructed a new and efficient ID-based designated verifier proxy multi-signature. We analyzed its security and showed that the new scheme satisfied all the security requirements for designated verifier proxy multi-signature. In addition, our scheme is more computationally efficient.

ACKNOWLEDGMENT

The authors would like to thank the Natural Science Foundation of shandong province (No.Y2008A29), the Science and Technique Foundation of shandong province...
REFERENCES


Shenjun Cui female, born in 1988, bachelor's degree of information and computing science in the University of Jinan, Jinan, P R China. She is a master student now. Her paper “Improvement of a forward-secure proxy signature scheme” was published in Computer Engineering and Technology (ICCET), 2010 2nd International Conference, 2010, 1, pp. 441-444. Current interests are cryptography, digital signature, proxy signature, etc.