International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 06 – Issue 02 || February 2021 || PP. 34-38

Anew ID-based multi-proxy signature

Nguyen Thi Hong Thuy
Trade Union University, Ha Noi, Vietnam

Abstract: In this paper, we proposes a new ID-based multi proxy signature is a solution of delegation of signing capabilities. Proxy signatures can combine other special signatures to obtain some new types of proxy signatures. Then only the cooperation of all signers in proxy group can generate multi-proxy multi-signatures. multi-proxy multi-signatures can play important roles in the following scenario: For a large building, there are some conflict among the constructors and the householders. All householders of the large building want to authorize a lawyer group as their agents. So a group of lawyers are authorized to act on behalf of all householders.

Keyword: Signature; multisignature; ID-Based, multi-proxy,

1. Introduction

The concept of proxy signature was first introduced by Mambo, Usuda and Okamoto in 1996 [9]. In the proxy signature scheme, an original signer is allowed to authorize a designated person as his proxy signer. Then the proxy signer is able to sign on behalf of the original signer. Since then, many proxy signature schemes have been proposed [7,8,10]. Proxy signatures can combine other special signatures to obtain some new types of proxy signatures. Till now, there are various kinds of proxy signature schemes have been proposed [1,2,5,6,13–15].The multi-proxy signature scheme was first proposed in 2000 [6]. In a multi-proxy signature scheme, an original signer could authorize a proxy group as his proxy agent. Then only the cooperation of all the signers in the proxy group can generate the proxy signatures on behalf of the original signer. It can be regarded as a special case of a (t, n) threshold proxy signature scheme for $t = n$. A contrary concept, proxy multi-signature was also introduced by Yi et al. in 2000 [14]. Another kind of proxy signature schemes is multi-proxy multisignature schemes proposed by Hwang [5]. In multi-proxy multi-signature schemes, an original group of signers can authorize a group of proxy signers under the agreement of all signers both in the original group and the proxy group. Then only the cooperation of all signers in proxy group can generate multi-proxy multi-signatures. multi-proxy multi-signatures can play important roles in the following scenario: For a large building, there are some conflict among the constructors and the householders. All householders of the large building want to authorize a lawyer group as their agents. So a group of lawyers are authorized to act on behalf of all householders. The paper will proceed as follows. In Section 2 we will give some prelimin- ary works. Section 3 recalls the general identity based signature schemes. We will present our identity based multi-proxy signature scheme in Section 4 and provide its security analysis in Section 5. ID-based proxy multi-signature scheme and its security analysis are presented in Sections 6 and 7, respectively. The paper ends with some concluding remarks.

2. Preliminaries

In this section, we will first 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 Z_q^*. We assume that the discrete logarithm problems (DLP) in both $G_1$and G_2 are hard. Abilinear pairings is a map ê: $G_1 \times G_1 \rightarrow G_2$ with the following properties:
(1) Bilinear: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$
(2) Non-degenerate: There exists P and $Q \in G_1$ such that $\hat{e}(P, Q) \neq 1$;
(3) Computable: There is an efficient algorithm to computa $\hat{e}(P, Q)$ for all $P, Q \in G_1$

In the proxy signature scheme, an original signer is allowed to authorize a designated person as his proxy signer.

Then the proxy signer is able to sign on behalf of the original signer. Basically, a secure proxy signature scheme should satisfy the following requirements [8].

Strong unforgeability: Only the legitimate proxy signer can generate a valid proxy signature; even the original signer cannot.

Verifiability: Anyone can verify the signature and the signed message should conform to the delegation warrant.

Strong identifiability: Anyone can determine the identity of the corresponding proxy signer.

Strong undeniability: The proxy signer cannot repudiate the signature which he ever generates. **Prevention of misuse:** The proxy key pair should be used in any place conforms to the warrant. Like the general proxy signature, an identity based proxy signature scheme should provide the properties as above.

3. General Id-Based Signature Schemes

In 1984 Shamir introduced identity based cryptosystems [12] in which the user's public key can be generated from a publicly identifiable information such as his email address. For such a system to work there are Trusted Authorities (or Private Key Generators) that generate users' private key from their identity information. Many identity based signature schemes have been devised since 1984 [1,3,4,11,15]. Generally, an identity based signature scheme consists of four algorithms which are the following.
Setup: The PKG picks a security parameter k and generates the system's public parameters and the master-key.
Extraction: This algorithm is performed by the PKG when a user requests a secret key corresponding to his identity. The secret key is given to the user in a secure way. This step is done only once for every identity and uses the same Setup data for many different identities.
Signing: User Alice with identity ID_A and secret key d_{ID_A} uses this algorithm with input (m, ID_A) to produce a signature σ on m valid under the public key derived from ID_A
Verification: On input of (m, ID_A, σ) this algorithm outputs if $\sigma$is not $ID_{A'}$ signature on m and it outputs 1 otherwise.

4. Identity Based Multi –Proxy Signature Scheme

In this section, we propose an identity based multi-proxy signature scheme. Some initial settings of the scheme are assumed in identity based systems. Our multi-proxy signature scheme with the clerk architecture is divided into five phases: System setup phase, Extraction phase, Proxy key generation phase, Multi-proxy signature generation phase, and Verification phase.

[*System setup phase*] Given a security parameter k, the PKG chooses groups G_1 and G_2 of prime order q, a generator P of G_1
a bilinear map ê: $G_1 \times G_1 \rightarrow G_2$
and hash func- tions $H_1: \{0,1\}^* \rightarrow G_1$,

$$H_2 : \{0,1\}^* \rightarrow Z_q^*.$$
$$H_3: \{0,1\}^* \rightarrow Z_q^*.$$

It chooses a masterkey $s \in Z_q^*$. and computes $P_{pub} = sP \in G_1$
The PKG publishes system's

$$Params = \{k, G_1, G_2 q, \hat{e}, H_1, H_2, H_3, P, P_{pub}\}$$

and keeps the master-key *s*ssecret.
[*Extraction phase*]
Given an identity ID, the PKG computes his public key $Q_{ID}$and secret key d_{ID}as follows:

$$Q_{ID} = H_2(ID) \in G_1 d$$
$$ID = sQ_{ID} = ID_{B_i} \in G_1.$$

Thus, the original signer Alice has the public key Q_{ID_A} and private key d_{ID_A}
The proxy signers P_{S_i} with identity $ID_{P_{S_i}}$ have public keys $Q_{ID_{S_{P_i}}}$ and corresponding private keys $d_{ID_{P_{S_i}}}$.
Without loss of generality, assume that there are $n$proxy signers in the proxy group.
[*Proxy key generation phase*]

To delegate the signing capability to a group of proxy signers, the original signer Alice does the following to make the signed warrant mw. The warrant mw specifies the delegation period, what kind of messages is delegated, the identity information of the original signer and the proxy group member, etc. If the follow- ing process is finished successfully, each proxy signer P_{S_i} gets a proxy key d_{P_i}
• Alice chooses $x \leftarrow RZ_q^*$.
Computes:

$$U = xP;\ H = H_2(m)$$
$$d_{ap} = H_1(mw \| U)\, d_{ID_{B_i}} + xP_{pub}$$ sends (*m*w, *U*, d_{ap}) to the proxy group.

• Each proxy signer *PSi* in the proxy group accepts dap as a valid key only if the following equation is satisfied:

$$\hat{e}(P, d_{ap}) = \hat{e}(P_{pub}, Q_{ID_{B_i}} +)H_1(mw\|U)\,\hat{e}(U, P_{pub})$$

Then, he computes the proxy key pairs as:

$$d_{B_i} = d_{ap} + H_1(mw\|U)\, d_{ID_{P_{S_i}}}$$
$$Q_{B_i} = H_1(mw\|U)(Q_{ID_A} + Q_{B_{S_i}}) + U$$

Using $\{d_{P_i}\}$these proxy signers can cooperate to sign any message which conforms to mw on behalf of the original signer Alice.

[*Multi-proxy signature generation phase*]
To generate a multi-proxy signature on a message m that conforms to the warrant mwone proxy signer in the proxy group is designated as a clerk, whose task is to combine partial proxy signatures to generate the final multi-proxy signature.
• Each proxy signer P_{S_i}, for $i = 1, 2, \ldots, n$ chooses : $x_i \epsilon Z_q^*$
Computes:

$$h_3 = H_3(m, w) \text{ and } U_i = x_i P$$

broadcasts his U_i to the other $n - 1$ proxy signers
• Each proxy signer P_{S_i},, for $i = 1, 2, \ldots, n$
computes:

$$U_p = \sum_{i=1}^{n} U_{p_i}$$
$$S_{P_i} = h_3 S_p^{k_i} + x_i P_{pub}$$

Sends (U_p, S_{P_i}) to the clerk as his partial proxy signature on the message m.
• The clerk verifies the partial proxy signatures by the equation

$$\hat{e}(P, S_{P_i})) = \hat{e}(P_{pub}, h' Q_p^{k_i} + U_{P_i})$$

Once all partial proxy signatures are correct, the multi-proxy signature of message m can be generated as(U_p, S_p, m, U) by computing
[*Verification phase*]
After receiving the multi-proxy signature (U_p, S_p, m, U) and the message m, the verifier operates as follows.
(1) Check whether or not the message m conforms to the warrant mw. If not, stop. Otherwise, continue.
(2) Check whether or not the n proxy signers are authorized by the original signer Alice in the warrant mw. If not, stop.
Otherwise, continue.
(3) Recover the proxy public key $Q_{B_i}, for\ i = 1, \ldots, n$:

$$d_{B_i} = d_{ap} + H_1(mw\|U)\, d_{ID_{B_{S_i}}}$$
$$Q_{B_i} = H_1(mw\|U)(Q_{ID_A} + Q_{B_{S_i}}) + U$$

(4) Accept the multi-proxy signature if and only if the following equalityholds:
$\hat{e}(P, d_{ap}) = \hat{e}(P_{pub}, Q_{ID_{B_i}})H_1(mw\|U)\,\hat{e}(U, P_{pub},)$;

$$c = H_1(m\|r)\ ;\ r = \hat{e}(P, P)x;\ S = xP - c_{dp}$$

5. Analysis of the Proposed Scheme

5.1. Correctness

The property of correctness is satisfied. In effect, if the multi-proxy signature is correctly generated, then:
$r = \hat{e}(P, S)\hat{e}(P_{pub}, Q_{ID_{B_i}} + \sum_{i=1}^{n} Q_{ID_{B_i}})^c\, H_1(mw\|U)\,\hat{e}(U, P_{pub})^c$
$r = \hat{e}(P, P)^x$
$= \hat{e}(P, S + c_{dp})$
$= \hat{e}(P, S)\hat{e}(P, dp)^c$
$= \hat{e}(P, S)\hat{e}(P, H_1(mw \| U) d_{ID_{B_i}} + \sum_{i=1}^{n} d_{ap\ i})^c$
$= \hat{e}(P, S)\hat{e}(P_{pub}, Q_{ID_{B_i}})^c\, H_1(mw\| U)\,\hat{e}(P, \sum_{i=1}^{n} H_1(mw\| U) = 1 d_{ID_{B_i}} + (x_i P_{pub})^c$
$= \hat{e}(P, S)\hat{e}(P_{pub}, Q_{ID_{B_i}})^c\, H_1(mw\| U)\,\hat{e}(P, \sum_{i=1}^{n} d_{ID_{B_i}} = 1 + (x_i P_{pub})^c\, H_1(mw\| U)\,\hat{e}(P, \sum_{i=1}^{n} x_i P_{pub})^c$

$= \hat{e}(P, S)\hat{e}(P_{pub}, Q_{ID_{B_i}})^c H_1(mw \| U)\, \hat{e}(P_{pub}, \sum_{i=1}^{n} Q_{ID_{B_i}})^c H_1(mw \| U)\, \hat{e}(U, P_{pub})^c$

$= \hat{e}(P, S)\hat{e}(P_{pub}, Q_{ID_{B_i}} + \sum_{i=1}^{n} Q_{ID_{B_i}})^c H_1(mw \| U)\, \hat{e}(U, P_{pub})^c$

5.2. Security

In this section, we will show that the multi-proxy signature scheme satisfies all the requirements stated in Section 2.

Unforgeability: As for multi-proxy signature, there are mainly three kinds of attackers: outsiders, who do not participate the issue of the multi-proxy signature; some proxsigner, who play an active in the signing process; and the signature owner. Firstly, since we use a modified Hess's scheme, which is proven secure, to generate the multi-proxy signature, any third party who can even get Alice's signature on the warrant mwcannot forge the multi-proxy signature. On the other hand, the original signer Alice cannot generate a valid multi-proxy signature since those proxy signers' private keys $\{d_{ID_{B_{S_i}}}\}$are used in the multi-proxy signature generation algorithm. Secondly, even the clerk, who has more power than other proxy signers in the proxy group, cannot forge a multi-proxy signature. To see this, suppose that the clerk wants the proxy group to sign a false message m'. Of cause, he can change his own U_i, therefor U_p.

Then he tries to compute S_p. such that the equation:

$$\hat{e}(P, d_{ap}) = \hat{e}(P_{pub} Q_{ID_{B_i}}) H_1(mw \| U)\, \hat{e}(U, P_{pub})$$ holds.

But it is equivalent to solve the bilinear pairing inversion problem, which is defined as: given $P \in G_1$and $(P, S) \in G_2$, find $S \in G_1$. Since the bilinear pairing inversion problem is reducible to computational Diffie–Hellman problem in G_2,. and can be reduced to DLP in G_2, and CDHP and DLP are intracta- ble in G_2, the clerk cannot forge a valid multi-proxy signature by this way. Lastly, since the signature owner cannot obtain more information than the clerk, he cannot generate a valid multi-proxy signature.

From the above discussion, we conclude that our scheme is unforgeable.

Verifiability: Because the warrant contains the identity information and the limit of the delegated signing capacity, the verifier can verify the signature and check whether the signed message conforms to the delegation warrant or not.

Identifiability: Since there is the warrant in a valid proxy signature, anyone can determine the identity of the corresponding proxy signer from mw.

Undeniability: The clerk owns other proxy signers' partial signature on message m, and validates them by checking whether or not the equation:

$\hat{e}(P, S)\, \hat{e}(P_{pub} Q_{ID_{B_i}} + \sum_{i=1}^{n} Q_{ID_{B_i}})^c H_1(mw \| U)\, \hat{e}(U, P_{pub})^c$ holds.

So no one can deny his signa-ture of earlier session.

Prevention of misuse: There is the warrant that has an explicit description of delegated signing capability, so the proxy signers cannot sign any messages that has not been authorized by Alice.

6. Discussions on the Multi – Proxy Multi-Signature Scheme

Our scheme is based on the multi-proxy signature scheme proposed in Section 4 The proxy certificate must be generated by the cooperation of the original group and the proxy group. Thus, the proxy certificate is verified by the equation:

$\hat{e}(P, S)\, \hat{e}(P_{pub}, Q_{ID_{B_i}} + \sum_{i=1}^{n} Q_{ID_{B_i}})^c H_1(mw \| U)$

Which uses the public keys of all original signers and all proxy signers. The original group is not able to arbitrarily announce that some group is its proxy agent without the agreement of the proxy group. Therefore, the scheme provides the protec- tion for the proxy group. On the other hand, the proxy group cannot deny they are the proxy agent, since they had agreed the proxy authorization. Therefor, the original signers' rights are also protected. No one can create the multi- proxy multi-signature without the authorization of the original group. Moreover, since the proxy signers' private keys are required in the multiproxy multi-signature generation phase, the multi-proxy multi-signature has to be generated by the cooperation of all members in the proxy group.

7. Conclusions

In electronic world, proxy signature is a solution of delegation of signing capabilities. Proxy signatures can combine other special signatures to obtain some new types of proxy signatures. Various type proxy

signatures are important in many applications. In this paper, we proposes a new ID-based multi proxy signature is a solution of delegation of signing capabilities. Proxy signatures can combine other special signatures to obtain some new types of proxy signatures.

References

[1]. X. Chen, F. Zhang, K. Kim, ID-based multi-proxy signature and blind multisignature from bilinear pairings, in: Proceeding of KIISC Conference 2003, Korea, 2003, pp. 11–19
[2]. J. Dai, X. Yang, J. Dong, Designated-receiver proxy signature scheme for electronic commerce, in: Proceedings of IEEE International Conference on Systems, Man and Cybernetics, vol. 1, October 5–8, 2003, pp. 384–389.
[3]. F. Hess, Efficient identity based signature schemes based on pairings, in: Proceedings of 9th Workshop on Selected Areas in Cryptography—SAC2002. Lecture Notes in Computer Science. Springer-Verlag.
[4]. F. Hess, Exponent group signature schems and efficient identity based signature schemes based on pairings. Cryptology ePrint Archive, Report 2002/012,2002.
[5]. S. Hwang, C. Chen, New multi-proxy multi-signature schemes, Appl. Math. Comput. 147 (2004) 57–67.
[6]. S. Huang, C. Shi, A simple multi-proxy signature scheme, in: Proceedings of the 10th National Conference on Information Security, Hualien, Taiwan, ROC, 2000, pp. 134–138.
[7]. S. Kim, S. Park, D. Won, Proxy signatures, revisited, in: Proceedings of ICICS'97, International Conference on Information and Communications Security, LNCS 1334, 1997, pp. 223–232.
[8]. B. Lee, H. Kim, K. Kim, Strong proxy signature and its applications, in: Proceedings of SCIS, 2001, pp. 603–608.
[9]. M. Mambo, K. Usuda, E. Okamoto, Proxy signature: delegation of the power to sign messages, IEICE Trans. Fundamentals E79–A (9) (1996) 1338–1353.
[10]. M. Mambo, K. Usuda, E. Okamoto, Proxy signature for delegating signing opertion, in: Proceedings of 3rd ACM Conference on Computer and Communications Security, ACM Press, New York, 1996, pp. 48–57.
[11]. K. Paterson, ID-based signatures from pairings on elliptic curves, Electron. Lett. 38487 (January) (1999) 1020–1025.
[12]. A. Shamir, Identity-based cryptosystems and signature schemes, in: Advances in Cryptology—CRYPTO'84, Lecture Notes in Computer Science, vol. 196, Springer-Verlag, 1984, pp. 47–53.
[13]. G. Wang, Designated-verifier proxy signatures for e-commerce, in: The IEEE 2004 International Conference on Multimedia and Expo (ICME 2004), Taipei, Taiwan, June 27– 30, 2004.
[14]. L. Yi, G. Bai, G. Xiao, Proxy multi-signature scheme: a new type of proxy signature scheme, Electron. Lett. 36 (6) (2000) 527–528.
[15]. F. Zhang, R. Safavi-Naini, C. Lin, New proxy signature, proxy blind signature, proxy ring signature schemes from bilinear pairings. Cryptology ePrint Archive, Report 2003/104.

Authors Biography (Mandatory)

Nguyen Thi Hong Thuy
Graduated Masters in Military Technical Academy
Research area: Areas of Study: Password Security and Security, Cryptography, Machine Learning, Network.