International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Secure Multi Proxy Multi Signature Scheme based on Factoring and DLP

Pankaj Sarde[1], Amitabh Banerjee[2]

[1]Dept. of Mathematics, Rungta College of Engineering and Technology, Raipur, CG, India
[2]Dept. of Mathematics, Govt. D. B. Girlss PG College, Raipur, CG, India

Abstract: ***Multi-proxy signatures allow the original signer to delegate his/her signing power to n proxy signers such that all proxy signers must cooperatively generate a valid proxy signature on behalf of the original signer. In this paper, we propose a secure multi proxy multi signature scheme based on factoring and discrete logarithm problem. Our scheme is more secure as compare to Hwang and Chen's scheme.***

Keywords: Proxy-Signature, Multisignature, Factoring, discrete logarithm problem.

1. Introduction

The concept of proxy signature was first introduced by Mambo, Usuda and Okamoto [2] in 1996. In a proxy signature scheme, an original signer can delegate his/her signing capability to a proxy signer, and having the signing rights, the proxy signer can sign a message on behalf of the original signer. There are three types of delegation in proxy signature: full delegation; Partial delegation and delegation by warrant. In full delegation, the original signer gives its private key to the proxy signer. In partial delegation,the original signer produces a proxy signature key from its private key and gives it to the proxy signer. The proxy signer uses the proxy key to sign. As far as delegation by warrant is concerned, warrant is a certificate composed of a message part and a public signature key. The proxy signer gets the warrant from the original signer and uses the corresponding private key to sign. Since the conception of the proxy signature was brought forward, a lot of proxy signature schemes [4, 5, 6, 7, 10, 11] have been proposed. The proxy signature can be categorized in multi-proxy signature, proxy multi-signature and multi proxy multi signature. The multi-proxy signature scheme was first proposed in 2000 [3]. With deep insight into it, the multi-proxy signature scheme can be treated as a special case of the (t,n) threshold proxy signature scheme when $t=n$. In a multi-proxy signature scheme, a group of proxy signers can be authorized by an original signer, and the proxy group can make a proxy signature on behalf of the original signer. A contrary concept called proxy multi-signature was proposed by Yi et al in 2000 [8]. In Proxy multi-signature scheme [1, 12], a group of original signers can authorize a proxy signer. The proxy signer can sign a message on behalf of the group of the original signers. Proxy multi-signatures can play important role in the following scenario: A company releases a document that may involve the financial department, engineering department, and program office, etc. The document must by signed jointly by these entities, or signed by a proxy signer authorized by these entities. One solution to the later case of this problem is to use a proxy multi-signature scheme. Another type of signature, called multi-proxy multi signature, was proposed by Hwang and Chen [9]. A multi-proxy multi-signature is a signature, generated by a group of proxy signers on behalf of the group of original signers. 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 rest of paper is organized as follow: Properties of proxy signatures is described in section 2. In section 3, we brief review of Hwang and Chen's multi-proxy multi-signature schemes. In section 4, we propose a secure multi-proxy multi-signature scheme based on factoring and discrete logarithm problem in section 4. In section 5, we discuss its security analysis. Some conclusion are made in section 6.

2. Properties of Proxy Signature Scheme

A strong proxy signature should have the following properties:

From the proxy signature, the verifier can be convinced of the original signer's agreement on the signed message.
Anyone can determine the identity of the corresponding proxy signer from the proxy signature.
Once a proxy signer creates a valid proxy signature for the original signer, he can't repudiate the signature creation.
Proxy signatures are distinguishable from normal signature by everyone.
The proxy signer can't use the proxy key for other purpose than generating a valid proxy signature. That is, he can't sign, with the proxy key, messages that have not been authorized by the original signer.
A designated proxy signer can create a valid proxy signature for the original signer. But the original signer and other third parties who are not designated as a proxy signer, can't create a valid proxy signature.

3. Reviews of Hwang and Chen's Multi-proxy Multi-signature Schemes [9]

Hwang and Chen's divide multi-proxy multi signature into four phases:

3.1 The System Set Up Phase

In this scheme, there are three kinds of participants: the original signer, the proxy signer, and the clerk. The used notation are given as below:

An original signer, where the original signer group of n original signer is $\{u_1, u_2, u_3.....,u_n\}$

A proxy signer, where the proxy signer group of m proxy is $\{p_1, p_2, p_3....., p_m\}$ the clerk

A large prime number the large public prime factor of $(p-1)$

A public generator of order q in z_p^*

A public one way collision-resistant hash function.

The unique identity of the original signer u_i

The unique identity of the proxy signer p_j

The private key of the original signer u_i, where $x_{u_i} \in z_q$

The certified public key of the original signer u_i, where $y_{u_i} = g^{x_{u_i}} \bmod p$

The private key of proxy signer p_j, where $x_{p_j} \in z_q$

The certified public key of the proxy signer p_j where $y_{p_j} = g^{x_{p_j}} \bmod p$

The proxy warrant which specifies the details including $ID_{u_i}, ID_{p_j}, y_{u_i}, y_{p_j}$

3.2 The proxy certificate generation phase

In this phase, for $i = 1,2,3.....n$, all the original signer u_i randomly select an integer $k_{u_i} \in Z_q^*$, computes $K_{u_i} = g^{k_{u_i}} \bmod p$,and broadcasts K_{u_i} the other (n-1) original signers, m proxy signers, and the clerk C. Meanwhile, for $j = 1,2,3,.....m$ the proxy signer p_j randomly select an integer $k_{p_j} \in z_q^*$, computes $K_{p_j} = g^{k_{p_j}} \bmod p$, and broadcasts K_{p_j} to n original signers, the other $(m-1)$ proxy signers, and the clerk C.

The clerk C and all of the proxy signers and the original signers compute $K = \prod_{i=1}^{n} K_{u_i} \prod_{j=1}^{m} K_{p_j} \bmod p$

For $i = 1,2,3,.....,n$, the original signer u_i computes $V_{u_i} = h(w)x_{u_i} y_{u_i} + k_{u_i} K \bmod q$ and sends V_{u_i} to C.

For $j = 1,2,3,.....,m$, the proxy signer p_j computes $V_{p_j} = h(w)x_{p_j} y_{p_j} + k_{p_j} K \bmod q$ and sends V_{p_j} to the clerk C.

The clerk C verifies V_{ui} by checking whether $g^{V_{u_i}} \equiv y_{u_i}^{y_{u_i}^{h(w)}} K_{u_i}^{K} \bmod p$ holds or not and verifies V_{p_j} by checking if $g^{V_{p_j}} \equiv y_{p_j}^{y_{p_j}^{h(w)}} K_{p_j}^{K} \bmod p$ holds for $i = 1,2,3.....,n$ and $j = 1,2,3.....m$.

If all V_{u_i}'s and V_{p_j}'s are valid, the clerk C computes $V = \sum_{i=1}^{n} V_{u_i} \sum_{j=1}^{m} V_{p_j} \bmod q$ and broadcasts V to n original signers and m proxy signers. Finally, the proxy signer group $\{p_1, p_2,....., p_m\}$ is authorized to act as the agent of the original signer group $\{u_1, u_2,....., u_n\}$. The proxy certificate key is (K, V).

3.3 The multi-proxy multi-signature generation phase

Once the proxy signer group wants to sign the document M on behalf of the original signer group, the following steps are performed.

For $j = 1,2,3,.....,m$, the proxy signer p_j randomly select an integer $t_j \in Z_q^*$, computes $r_j = g^{t_j} \bmod p$, and broadcasts r_j to the (m-1) proxy signers

For $j = 1,2,3,.....m$, p_j computes $R = \prod_{j=1}^{m} r_j \bmod p$ and $s_j = (Vt_j + x_{p_j} y_{p_j}^{Rh(M)}) \bmod q$, and then the partial proxy signature (r_j, s_j) of M is generated.

For $j = 1,2,3,.....,m$ p_j sends (r_j, s_j) to C, and the chairman of the proxy signer group p_1 sends $(w,(K,V),M)$ to C

After getting (r_j, s_j)'s and $(w,(K,V),M)$, C first checks the validity of the proxy certificate by checking if $g^V = K^K (\prod_{i=1}^{n} y_{u_i}^{y_{u_i}} \prod_{j=1}^{n} y_{p_j}^{y_{p_j}})^{h(w)} \bmod p$. If it does not hold, C reject the proxy certificate, otherwise phase continue.

C computes $R = \prod_{j=1}^{m} r_j \bmod p$ and verifies (r_j, s_j) by checking if $g^{s_j} \equiv r_j^V y_{p_j}^{Ry_{P_j}^{h(m)}} \bmod p$ for $j = 1,2,3.....,m$. If all hold, C computes

$S = \sum_{j=1}^{m} s_j \bmod q$. Finally, the multi-proxy multi-signature of the message M is generated to be $(w,(K,V),M,(R,S))$.

3.4 The multi-proxy multi-signature verification phase

Once waiting to verify the multi-proxy multi-signature $(w,(K,V),M,(R,S))$., the verifier executes the followings:

The verifier first checks the validity of the proxy certificate w by checking $g^V \equiv K^K (\prod_{i=1}^{n} y_{u_i}^{y_{u_i}} \prod_{j=1}^{m} y_{p_j}^{y_{p_j}})^{h(w)} \bmod p$. If it does not hold, the verifier rejects the proxy certificate; otherwise, the phase continues.

The verifier checks if $g^S \equiv R^V (\prod_{j=1}^{m} y_{p_j}^{y_{p_j}})^{Rh(w)} \bmod p$. If it holds, it is ensured that $(w,(K,V),M,(R,S))$ is the valid multi-proxy multi-signature of M.

4. Our Proposed Scheme

We divide our scheme into four phases: (i) The system set up phase, (ii) The proxy certificate generation phase, (iii) The multi-proxy multi-signature generation phase (iv) The multi-proxy multi-signature verification phase.

4.1 The System Setup Phase

p is large prime and n is factor of $p-1$ that is product of two large prime p_1 and q_1 such that $n = p_1 q_1$
$\phi(n) = (p_1 - 1)(q_1 - 1)$ is a phi-Euler function.
A public generator of order n in z_p^*
A public one-way collision-resistant hash function.

Original signers and proxy signers agree on $e, d \in z_{\phi(n)}^*$ such that $ed \equiv 1 \bmod n$ Here e is public key.
The unique identity of the original signer u_i
The unique identity of the proxy signer p_j
The private key of the original signer u_i, where $x_{u_i} \in z_n^*$
The certified public key of the original signer u_i, where $y_{u_i} = g^{x_{u_i}} \bmod p$
The private key of proxy signer p_j, where $x_{p_j} \in z_n^*$
The certified public key of the proxy signer p_j where $y_{p_j} = g^{x_{p_j}} \bmod p$
The proxy warrant which specifies the details including $ID_{u_i}, ID_{p_j}, y_{u_i}, y_{p_j}$
The clerk C (one of the proxy signer)

4.2 The proxy certificate generation phase

In this phase, the original signers, proxy signers and clerk C co-operate to generate the proxy certificate which are given as below:

For $i = 1,2,3,.....n$, original signer u_i randomly select an integer $k_i \in z_n^*$ such that $K_{u_i} = g^{k_i} \bmod p$, $K'_{u_i} = g^{k_i x_{u_i}} \bmod p$ and broadcast to $n-1$ signers, m proxy signers and clerk C. Similarly for $j = 1,2,3,.....m$ proxy signers randomly select an integer $l_j \in z_n^*$ such that $K_{p_j} = g^{l_j} \bmod p$, $K'_{p_j} = g^{l_j x_{p_j}} \bmod p$ broadcasts to $m-1$ proxy signers, n original signers and clerk C.

The clerk C, all of the original signers and proxy signers computes $K = \prod_{i=1}^{n} K_{u_i} \prod_{j=1}^{m} K_{p_j}$ and $s = H(m_w \| \prod_{i=1}^{n} K'_{u_i} \prod_{j=1}^{m} K'_{p_j})$ sends to n original and m proxy signers.

Now For $i = 1,2,3,.....,n$, original signer u_i computes $v_i = (sk_i - x_{u_i} k'_i)^d \bmod n$ where $k'_i = K - k_i \bmod n$ and sends to clerk C. Similarly for $j = 1,2,3.....,m$, proxy signer p_j computes $w_j = (sl_j - x_{p_j} l'_j)^d \bmod n$ where $l'_j = K - l_j$ and sends to clerk C.

Now clerk C verifies for v_i and w_j such that they check the relation $s = H(m_w \| \prod_{i=1}^{n} g^{v_i^e} \prod_{j=1}^{m} g^{w_j^e} \prod_{i=1}^{n} y_{u_i}^K \prod_{j=1}^{m} y_{p_j}^K K^{-s})$ if this relation is hold then clerk C computes $A = \sum_{i=1}^{n} v_i \sum_{j=1}^{m} w_j$ sends to proxy signers.

4.3 The multi-proxy multi-signature generation phase

Now proxy signers wants to sign the messages M on behalf of the original signer group, the following steps are performed below:

For $j = 1,2,3,.....m$, all proxy signers agree on two numbers $\alpha, \beta \in z_n^*$. Now proxy signers randomly select

$t_j \in z_n^*$ and computes $T_j = g^{t_j} \bmod p$ and broadcasts to all (m-1) proxy signers and clerk C.

Now the clerk C computes

$R = \prod_{j=1}^{m} T_j \bmod p$

$R' = R^{\alpha} \prod_{j=1}^{m} y_{p_j}^{\beta} \bmod p$

$h = H(M \| A \| R')$. Now clerk C send h to all proxy signers.

For $j = 1,2,3,.....,m$ proxy signer computes $B_j = (x_{p_j} \beta d + h t_j) \bmod n$, $(C_j = t_j \alpha - x_{p_j} e) \bmod n$ Thus proxy signers sends $(h, \{B_j\}_{j=1}^{m}, \{C_j\}_{j=1}^{m})$ to the clerk C.

Now clerk C computes $B = \sum_{j=1}^{m} B_j$ and $C = \sum_{j=1}^{m} C_j$ Thus the multi-proxy multi-signature of the message M is (h, R, A, B, C)

4.4 The multi-proxy multi-signature verification phase

The verifier check the relation $h \equiv H(M \| A \| g^{Be+C} R^{-he} \prod_{j=1}^{m} y_{p_j}^{-e})$ if it holds, it is ensured that (h, R, A, B, C) is a valid multi-proxy multi-signature scheme of message M

5. Security Analysis

In this section, we analyze the security of our scheme. Our scheme is based on factoring and DLP. We will show that our scheme satisfies all the security requirements of a proxy signatures mentioned in section 2

Any verifier can verify the multi-proxy multi-signature scheme. The verifier can be convinced of the original signer's agreement on the signed message. Verification of correctness is described as above.

In our scheme, proxy signers used his own private key $\{x_{p_j}\}_{j=1}^{m}$ and creates $R', \{B_j\}_{j=1}^{m}, \{C_j\}_{j=1}^{m}$. Therefore proxy signer can't denied the proxy signature creation.

The multi-proxy multi-signatures are distinguishability. Since in multi-proxy multi-signature scheme, proxy signers used his own private key and it is different from normal signature.

In our scheme, Original signer and proxy signer both are creates s and A. Thus proxy signers can't sign messages with the proxy key that have not been authorized by the original signer.

In our scheme, any other parties can't forge a multi-proxy multi- signature scheme. Since proxy signers creates $\{B_j\}_{j=1}^{m}, \{C_j\}_{j=1}^{m}$ in which used his own private key. Proxy signers and original signers both are also create h. Thus designated proxy signers create a valid proxy signatures.

First Verifier computes R'' such that

$$R'' = g^{Be+C} R^{he} \prod_{j=1}^{m} y_{p_j}^{-e}$$

$$= g^{\sum_{j=1}^{m} B_j e + \sum_{j=1}^{m} C_j} \prod_{j=1}^{m} y_{p_j}^{-e}$$

$$= g^{\sum \{x_{p_j} \beta d e + h e t_j + t_j \alpha - x_{p_j} e\}} (\prod_{j=1}^{m} g^{t_j \alpha})^{-he} (\prod_{j=1}^{m} y_{p_j}^{-e})$$

$$= g^{\sum \{x_{p_j} \beta d e + h e t_j + t_j \alpha - x_{p_j} e - t_j h e + x_{p_j} e\}}$$

$$= g^{\sum t_j \alpha + x_{p_j} \beta}$$

$$= (\prod_{j=1}^{m} T_j)^{\alpha} \prod_{j=1}^{m} y_{p_j}^{\beta}$$

then check the relation

$h = H(M \| A \| R'')$,

if it is true then accept the signature (h, R, A, B, C).

6. Conclusion

In this paper, we have proposed a secure multi-proxy multi-signature schemes based on factoring and discrete logarithm problem. Our scheme is more secure than Hwang and Chen's multi-proxy multi-signature schemes since in our scheme we have used two hard problem factoring and and discrete logarithm problem. Our schemes offers a higher level of security than the scheme based on a single hard problem. 50

References

[1] Feng Cao, Zhenfu Cao. A secure identity-based proxy multi-signature scheme. Information science's 2009, 179(01) : 292 – 302

[2] M. Mambo, K. Usuda and E. Okamoto, Proxy signatures: delegation of the power to sign message, IEICE Transactions on Fundamentals, vol. E 79 -A(9), 1996, PP. 1338 – 1354.

[3] S. J. Hwang and C.H. Shi, A simple multi-proxy signature scheme, Proceedings of the 10*th* National Conference on Information Security, Hualien, Taiwan 2000, PP. 134 – 138

[4] C. L. Hsu, T.S. Wu, and T. C. Wu, "New nonrepudiable threshold proxy signature scheme with known signers ", The Journal of systems and software, Vol. 48, 2001, PP. 119 – 124

[5] M. S. Hwang, I. C. Lin, and J. L. Lu, "A secure

nonrepudiable threshold proxy signature scheme with known signers", Informatica, vol. 11, No. 2, 2000, PP. 137 – 144

[6] K. Zhang, Threshold proxy signature schemes, Proceedings of 1997 Information Security Workshop, Japan, September 1997 PP. 191 – 197

[7] H. M. Sun, An efficient nonrepudiable threshold proxy signature scheme with known signers, Computer Communications, Vol. 22, 1999, PP. 717 – 722

[8] L. Yi, G. Bai and G. Xiao, Proxy multi-signature schemes: a new type of proxy signature scheme, IEE Electronics Letters, Vol. 36(6), 2000, PP. 527 – 528.

[9] S. Hwang and C. Chen, New multi-proxy multi-signature schemes, Appl. Math Comput. 147, 2004, PP. 57 – 67

[10] B. Lee, H. Kim, and K. Kim, Secure mobile agent using strong non-designated proxy signature, Proc. of ACISP01 LNCS 2119, Springer-Verlag, PP. 474 – 486, 2001

[11] J. G. Li, and Z. F. Cao, "Improvement of a Threshold Proxy Signature Scheme," Journal of computer research and development, 39(11), 2002, PP. 515-518.

[12] J. G. Li, Z. F. Cao and Y. C. Zhang, "Non-repudiable proxy multi-signature scheme, " Journal of computer science and technology, 18(3), 2003, PP. 399-402, doi: 10.1007/ BF02948911