Attack and Improvement of a Proxy Multi-Signature Scheme

WEI Hong-ru，HU Jia-yuan*
School of Mathematics and Physics
University of Science and Technology Beijing
Beijing 100083, China
e-mail：837659172@qq.com

***Abstract*—Proxy multi-signature system is based on digital signature scheme for a class of special signature scheme, which requires the signer to own certain powers were delegated to each proxy signer to make these proxy signer to use these powers on behalf of himself. In this paper, a class before the enhanced proxy multi-signature scheme carry out the attack and improvement, three forgery attacks has been implemented,one for the any original signer,one for the any proxy signer,and one for the proxy signer modify the proxy deadline. While the original proposals put forward an improved model, to prevent a proxy signer rights transfer, the ability to prevent abuse of the signature to ensure that the proxy signature security.**

Keywords—digital signature; proxy signature; proxy multi-signature; forgery attack

I. INTRODUCTION

In recent years, with growing social networking technologies developed in the field of e-commerce, people often need to delegate some of their powers to give a reliable agent, agent on behalf of themselves and let them to exercise these powers. These can be delegated powers to include people in the right signature in 1996,Mambo, Usuda and Okamoto[1], who proposed the concept of proxy signature, digital signature gives a solution to this problem proxy a solution method. Because proxy signature plays an important role in practical applications, so it was put forth proxy signature has been widespread concern, its scholars have also conducted in-depth discussion and research[2,3]. Since then, Elly river[4,5], who proposed the idea of proxy multi-signature, which allows multiple users to use proxy signature on the file signature process, in many areas of e-commerce, elections, protocol exchange has played an important role[6].

By studying Zhou Hongsheng, iron Ling, Li Jianhua, Niyou Sheng et al[7] article, the second proxy multi-signature scheme given its paper analyzed, and any one of the original signers, any proxy signer, proxy signer modify the proxy deadline forgery attack, he explained the existence of security issues. After its signing process given signature generation process and the commission process has been improved. And described in the program to improve the complexity of its calculation has reached the security requirements can withstand before the attacks.

II. ZHOU HONGSHENG ET AL [7] PROXY MULTI-SIGNATURE SCHEME

A. Parameter Description

p is a large prime number, q of $p-1$ or $p-1$'s large prime factor, $g \in Z_q^*$ and $g^q \equiv 1 (\bmod p)$; A_i is L user digital signature scheme, x_{A_i} is a secret key of the user A_i, $x_{A_i} \in Z_q^*$, y_{A_i} for the user's public key A_i, $y_{A_i} = g^{x_{A_i}} (\bmod p)$; B_i is a digital signature scheme another L users; secret key all proxy signers B_i is, $x_{B_i} \in Z_q^*$ the public key is $y_{B_i} = g^{x_{B_i}} (\bmod p)$; $h()$ is a hash function; w_i commission is to delegate authority A_i to B_i a signature file.

B. commissioning process

1) A_i randomly selected for each user a number $k_i \in Z_q^*$, Calculate: $K_i = g^{k_i} (\bmod p), e_i = x_{A_i} h(w_i, K_i) + k_i (\bmod q)$; .

2) $g^{e_i} = y_{A_i}{}^{\mathrm{h}(\mathrm{w}_i, \mathrm{K}_i)} \mathrm{K}_i (\bmod p)$ verification is established.

C. Signature generation

1)Each agent signer B_i randomly picks a number $r \in Z_q^*$, calculation: $R_i = g^{r_i} (\bmod p)$;

2)calculation:

$$R = \prod_{i=1}^{L} R_i (\bmod p), s_i = (e_i - xB_i)m - nR (\bmod q);$$

3)calculation: $R = \prod_{i=1}^{L} R_i (\bmod p)$,

test equation is established:

$$(y_{A_i}{}^{h(w_i, K_i)} K_i)^m = g^{s_i} R_i^R y_{B_i}{}^m (\bmod p),$$

calculation: $s = \sum_{i=1}^{L} s_i (\bmod q)$,

The message of the proxy multi-signature is : $(R; K_1, K_2, ..., K_L; w_1, w_2, ...w_L; s; y_{A_1}, y_{A_2}, ...y_{A_L}; y_{B_1}, y_{B_2}, ..., y_{B_L})$.

III. PAIRS OF 2 PROXY MULTI-SIGNATURE ATTACKS

A. pairs of any original signer forgery attack

For any who want to forge the original signature of the signer, may wish to set A_0 , want to take any message m' to generate a valid proxy multi-signature:

$$(R,S',K'_1,K_2,...,K_L,w_i,y_{A_i},y_{B_i})(i=1,2,...,L),$$

then perform the following steps:

1)Calculation: $d = \mathrm{m}\bullet(\mathrm{m}')^{-1}(\mathrm{mod}\,q)$.

2)Calculation:

$$K_1' = (\prod_{i=1}^{L}(y_{A_i}{}^{h(W_i,K_i)}K_i))^{d-1}\, y_{A_0}{}^{h(W_1,K_1)}\bullet K_1(\prod_{i=1}^{l}y_{B_i})^{1-d}(\mathrm{mod}\,p).$$

3)Calculation: $S' = S + x_{A_1}\mathrm{h}(\mathrm{w}_1,\mathrm{k}_1')\mathrm{m}'(\mathrm{mod}\,q)$.

The proxy multi-signature:

$$(R,S',K'_1,K_2,...,K_L,w_i,y_{A_i},y_{B_i})(i=1,2,...,L)$$

can verify the person's verification,Proof:

$$\left\{(\mathrm{y}_{A_0}{}^{\mathrm{h}(w_1,k_1')}K_1')K_1')\prod_{i=2}^{L}(y_{A_i}{}^{h(w_i,K_i)}K_i)\right\}^{m'}$$

$$=\left\{y_{A_0}h(w_1,k_1')\prod_{i=1}^{L}(y_{A_i}{}^{h(w_i,K_i)})\right\}^{d-1}$$

$$=y_{A_0}{}^{h(w_1,k_1)}\bullet K_1[\prod_{i=1}^{L}y_{B_i}]^{1-d}\prod_{i=2}^{L}(y_{A_i}{}^{h(w_i,K_i)})^{m'}$$

$$=(g^x A_0{}^{h(w_1,K_1')})m'\bullet[\prod_{i=1}^{L}(y_{A_i}{}^{h(w_i,K_i)}K_i)]^{m}\bullet[(\prod_{\mathrm{i}=1}^{L}y_{B_i})^{1-d}]^{m'}$$

$$=(g^x A_0{}^{h(w_1,K_1')})^{\mathrm{m}'+s}R^R[(\prod_{i=1}^{L}y_{B_i})^{dm'}$$

$$=[(\prod_{i=1}^{L}y_{B_i})^{1-d}]^{m'}=\mathrm{g}^{\mathrm{S}'}R^R(\prod_{i=1}^{l}y_{B_i})^{m'}(\mathrm{mod}\,p).$$

B. pairs of any proxy signer forgery attack

Any one want to forge proxy signer signer may wish to want to take any message to generate a valid proxy multi-signature:

$$(R,S,y'_{B_1},y_{B_2},...,y_{B_L},K_i,w_i,y_{A_i})(i=1,2,...,L);$$

after performing the following steps:

1)Calculation: $d = \mathrm{m}\bullet(\mathrm{m}')^{-1}(\mathrm{mod}\,q)$.

2)Calculation:

$$y_{B_0}' = (\prod_{\mathrm{i}=1}^{L}(y_{A_i}{}^{h(W_i,K_i)}K_i))^{d-1}y_{B_0}\bullet(\prod_{i=1}^{l}y_{B_i})^{\mathrm{d}-1}(\mathrm{mod}\,p).$$

After B_0 can own private key is revealed by his own public key to y_{B_0}', the proxy multi-signature:

$$(R,S,y'_{B_1},y_{B_2},...,y_{B_L},K_i,w_i,y_{A_i})(i=1,2,...,L)$$

can verify the person's verification,proof:

$$g^S R^R(y_{B_0}'\prod_{i=2}^{L}y_{B_i})^{\mathrm{m}'}$$

$$=g^S R^R\left\{[(\prod_{i=1}^{L}(y_{A_i}{}^{h(w_i,K_i)}K_i))^{\mathrm{l-d}}\mathrm{y}_{B0}(\prod_{i=1}^{L}y_{B_i})^{d-1}]\prod_{i=2}^{L}y_{B_i}\right\}^{m'}$$

$$=g^S R^R(\prod_{i=1}^{L}y_{B_i})^{dm'}\left\{[\prod_{i=1}^{L}(y_{A_i}{}^{h(w_i,K_i)}K_i)]^{\mathrm{l-d}}\right\}^{m'}$$

$$=[\prod_{i=1}^{L}y_{A_i}{}^{h(w_i,K_i)}K_i)]^{\mathrm{m}}\left\{[\prod_{i=1}^{L}(y_{A_i}{}^{h(w_i,K_i)}K_i)]^{\mathrm{l-d}}\right\}^{m'}$$

$$=[\prod_{i=1}^{L}y_{A_i}{}^{h(w_i,K_i)}K_i)]^{\mathrm{m}}(\mathrm{mod}\,p).$$

C. pairs proxy signer modify the proxy deadline forgery attack

For any who want to forge a signature by modifying the term of agency, it may be set to C_0 , you want to generate a valid proxy for any period by modifying agents take the message m' multi-signature:

$$(R,S,y'_{C1},y_{C_2},...,y_{C_L},K_i,w_i',y_{A_i})(i=1,2,...,L),$$

he can perform the following steps:

1)Calculation: $d = \mathrm{m}\bullet(\mathrm{m}')^{-1}(\mathrm{mod}\,q)$.

2)Calculation: $d_i = h(w_i,K_i)h(w_i',K_i)(\mathrm{mod}\,q)$,

where w_i' is the agent deadline modified value.

3)Calculation:

$$y_{C_0}' = [\prod_{\mathrm{i}=1}^{L}(y_{A_i}{}^{h(W_i',K_i)}K_i)]^{d-1}\bullet$$

$$\prod_{i=1}^{l}(y_{A_i}{}^{(d_i-1)h(w_i',K_i)})^{-d}y^{c_0}(\prod_{i=1}^{L}y_{c_i})^{d-1}(\mathrm{mod}\,p).$$

After C_0 can be your own private key is revealed by his own public key to y_{C_0}', then the proxy multi-signature:

$$(R,S,y'_{C_1},y_{C_2},...,y_{C_L},K_i,w_i',y_{A_i})(i=1,2,...,L)\ ,$$

person can be verified by the verification,prove:

$$g^S R^R (y_{C_0}' \prod_{i=2}^{L} y_{c_i})^{m'} = g^S R^R \bullet \left\{ \begin{array}{l} [(\prod_{i=1}^{L} (y_{A_i}{}^{h(w_i', K_i)} K_i))^{1-d} \bullet \\ \prod_{i=1}^{L} (y_{A_i}{}^{(d_i - 1) h(w_i', K_i)})^{-d} \bullet \\ y_{C_0} (\prod_{i=1}^{L} y_{c_i})^{d-1}] \prod_{i=2}^{L} y_{C_i} \end{array} \right\}^{m'}$$

$$= g^S R^R (\prod_{i=1}^{L} y_{C_i})^{dm'} \bullet \left\{ \begin{array}{l} [\prod_{i=1}^{L} (y_{A_i}{}^{h(w_i', K_i)} K_i)]^{1-d} \bullet \\ \prod_{i=1}^{L} (y_{A_i}{}^{(d_i - 1) h(w_i', K_i)})^{-d} \end{array} \right\}^{m'}$$

$$= [\prod_{i=1}^{L} y_{A_i}{}^{h(w_i, K_i)} K_i)]^{m} \bullet \left\{ \begin{array}{l} [\prod_{i=1}^{L} (y_{A_i}{}^{h(w_i', K_i)} K_i)]^{1-d} \bullet \\ \prod_{i=1}^{L} (y_{Ai}{}^{(d_i - 1) h(w_i', K_i)})^{-d} \end{array} \right\}^{m'}$$

$$= [\prod_{i=1}^{L} y_{A_i}{}^{d_i h(w_i', K_i)} K_i)]^{dm'} \bullet \left\{ \begin{array}{l} [\prod_{i=1}^{L} (y_{A_i}{}^{h(w_i', K_i)} K_i)]^{1-d} \bullet \\ \prod_{i=1}^{L} (y_{A_i}{}^{(d_i - 1) h(w_i', K_i)})^{-d} \end{array} \right\}^{m'}$$

$$= [\prod_{i=1}^{L} y_{A_i}{}^{h(w_i', K_i)} K_i)]^{m} (\bmod p).$$

IV. IMPROVEMENT AND PROXY MULTI-SIGNATURE ATTACK IN 2

We conducted three types of attack in 3, found 2 Zhou Hongsheng et al proxy multi-signature scheme is not safe, we will improve its programs:

1) delegate process

Each user A_i randomly selected a number $k_i \in Z_q^*$, calculated:

$$K_i = g^{k_i} (\bmod p), e_i = x_{A_i} h(w_i, K_i, y_{A_i}) + k_i K_i (\bmod q);$$

Verify: $g^{e_i} = y_{A_i}{}^{h(w_i, K_i, y_{A_i})} K_i{}^{K_i} (\bmod p)$ is established.

2) signature generation process

Each agent signer B_i of a random number $r \in Z_q^*$, calculated:

$$R_i = g^{r_i} (\bmod p), R = \prod_{i=1}^{L} R_i (\bmod p),$$

$$s_i = e_i h(m) - x_{B_i} y_{B_i} h(m, R) - r_i R (\bmod q);$$

calculated: $R = \prod_{i=1}^{L} R_i (\bmod p);$

Inspection equation:

$$(y_{A_i}{}^{h(w_i, K_i, y_{A_i})} K_i{}^{K_i})^{h(m)} = g^{s_i} R_i^R y_{B_i}{}^{y_{B_i} h(m, R)} (\bmod p),$$

is established, calculate: $s = \sum_{i=1}^{L} s_i (\bmod q)$,

The message of the proxy multi-signature is:

$$(R; K_1, K_2, ..., K_L; w_1, w_2, ..., w_L;$$
$$s; y_{A_1}, y_{A_2}, ..., y_{A_L}; y_{B_1}, y_{B_2}, ..., y_{B_L}).$$

3) Signature Verification Process

Certifier V After receiving the message m and proxy multi-signature, verify the identity of m and all the proxy signer is within the set of all commission license signature $(w_1, w_2, ..., w_L)$ range,verify:

$$[\prod_{i=1}^{L} (y_{Ai}{}^{h(w_i, K_i, y_{A_i})} K_i{}^{K_i}]^{h(m)} = g^S R^R (\prod_{i=1}^{L} y_{B_i}{}^{y_{B_i}})^{h(m,R)} (\bmod p)$$

is satisfied.

4) To resist the attack process

We have 3.1 people for any signature forgery attack, for example, to attack the improved signature scheme, similar to the previous attacks, can be drawn:

$$r_1 = h(m,R) \bullet (h(m',R))^{-1} (\bmod q),$$
$$r_2 = (1 - r_1) h(m',R) \bullet (h(m'))^{-1} (\bmod q),$$
$$r_3 = h(m) \bullet (h(m'))^{-1} (\bmod q).$$

So you want a successful attack, the need to find such a (y_{A_1}', K_1'), satisfies:

$$\prod_{i=1}^{L} (y_{A_0}{}^{h(w_i, k_i, y_{A_i})} \bullet K_i^{K_i})^{r_3} (\prod_{i=1}^{L} y_{B_i}{}^{y_{B_i}})^{r_2} =$$
$$(y_{A_0}')^{h(w_1, K_1', y_{A_1}')} (K_1')^{K_1'} \bullet \prod_{i=2}^{L} (y_{A_i}{}^{h(w_i, K_i, y_{A_i})} K_i^{K_i}) \bmod p.$$

But it is theoretically impossible, because you want from the following equation where:

$$(K_1')^{K_1'} = y_{A_0}{}^{h(w_1, K_1, y_{A_0})} (K_1)^{K_1} \bullet$$
$$\prod_{i=1}^{L} (y_{A_0}{}^{h(w_i, k_i, y_{A_i})} \bullet K_i{}^{K_i})^{r_3 - 1} \bullet (\prod_{i=1}^{L} y_{B_i}{}^{y_{B_i}})^{r_2} \bmod p.$$

Solving the K_1' process than the theoretically calculated discrete logarithm is even more difficult (because K_1' in the equation itself acts as this element, its computational complexity is greater than $O(\log(n)^2)$), and public key y_{A_0} becomes $y_{A_0}'$is the formula established in the calculation of hash function (because $h(\bullet)$ is a one-way hash function collisions), so in the theory, the attack is failure.

In 3.2, we want to attack to be successful, you need to find such a (y_{B_1}', K_1'), satisfies:

$$\prod_{i=1}^{L}(y_{B_i}^{h(w_i,k_i,y_{B_i})} \bullet K_i^{K_i})^{r_3}(\prod_{i=1}^{L} y_{B_i}^{y_{B_i}})^{r_2} =$$

$$(y_{B_1}')^{h(w_1,K_1',y_{B_1}')}(K_1')^{K_1'} \bullet \prod_{i=2}^{L}(y_{A_i}^{h(w_i,K_i,y_{B_i})} K_i^{K_i}) \bmod p.$$

In 3.3, we want to attack to be successful, you need to find such a (y_{C_0}', K_1'), satisfies:

$$\prod_{i=1}^{L}(y_{C_0}^{h(w_i,k_i,y_{C_i})} \bullet K_i^{K_i})^{r_3}(\prod_{i=1}^{L} y_{C_i}^{y_{C_i}})^{r_2} =$$

$$(y_{C_0}')^{h(w_1,K_1',y_{C0}')}(K_1')^{K_1'} \bullet \prod_{i=2}^{L}(y_{A_i}^{h(w_i,K_i,y_{C_i})} K_i^{K_i}) \bmod p.$$

Therefore, similarly to 3.1, 3.2 and 3.3 for the attacks in the calculation of the time and complexity of computing discrete logarithms is over, so the model can be modified to resist a general attack.

5) Security Analysis and Discussion

Since the introduction of the new program as well as increased commission parameter, its security has been enhanced, specifically as follows:

(1) new programs, including a proxy signature proxy signer's information, as well as others such as authorization and so can not pretend to participate in proxy multi-signature process, nor can the legitimate proxy multi signature repudiation.

(2) The new program introduced a letter of appointment, and for each, can be limited by the ability for the signature power of attorney can be used are constrained proxy signature and a certain period of the valid range, it can not be beyond the competence of signature, to avoid the abuse of the rights of proxy signature.

(3) can be set through the development of a legal proxy predecessors, beyond the signature others designated muster areas such participation may reject to accept, therefore, even if sent to other people, if not within the scope of the previous formulation of the agent then, is not the representative to carry out multi-signature process.

Through the above analysis we can see, the new proxy multi-signature scheme can satisfy the following properties:

*(1)*Verifiability: any certifier can verify this since the proxy multi-signature is valid and can be confirmed whether or not all of the original signers recognize these documents have been signed in accordance with a valid signature.

*(2)*Can not be forged strong line: Because proxy multi-signature includes proxy signer's information, so in addition to anyone who thought the signature can not be substituted for forged signature, signature overcome denial.

*(3)*Proof of identity of the strong: because the proxy multi-signature includes a proxy signer's public key, so anyone can participate in the proxy signature confirmation process signer from the proxy signature inside.

*(4)*A strong non-repudiation: Once a proxy signer to participate and generate a valid proxy signature multi-after, we can not deny.

*(5)*To prevent the abuse Signature: Signature proxy multi-signature process ensures that if strictly followed all of the original signers of the commission information generation.

*(6)*Efficiency of the new signature program: the new program compared with the original program adds some parameters, but in contrast to the original scheme operation only increased the number of four operations, a new program on the operation efficiency and space utilization with the original plan remained unchanged.

V. CONCLUSION

Based on the basis of research and analysis of Zhou Hongsheng[7]et al paper, combining the characteristics of proxy multi-signature, the second proxy multi-signature scheme given in the original text is analyzed and attack, discovered its existence in security deficiencies. After the process of signature of the principal,the signature generation process and signature verification process of revision,the parameter is added on the basis of the original,and it is proved that the modified model in resisting attacks can be more complicated than computing discrete logarithm,so it can ensure the security of the signature.Proxy multi-signature and application affect people's production and life in the relevant fields have a positive role in promoting the same time, issues related to the efficiency of its processes and its signature and other security is the need for more in-depth study and discussion.

REFERENCES

[1] Mambo M, Usuda K, Okamoto E. Proxy signatures Delegation of the power to sign messages[J]. IEICE Trans Fundamentals, 1996.E79-A(9):1338-1353.

[2] Boyd C.Multi-Signatures Revisited[A]. Cryptography and Coding III[C]. Oxford:Clarendon Press 1993:21-30.

[3] Ham I.Digital Multi-Signature with Distinguished Signing Authorities[J]. Electronics Letters, 1999,35(4):294-295.

[4] Yi L,Bai G,Xiao G. Proxy multi-signature scheme A new type of proxy signature scheme[J]. Electronics Letters, 2000:527-528.

[5] 傅晓彤,伊丽江,肖国镇. 一类行的代理多重签名体制[J].西安电子科技大学学报,2001,28(6): 729-731.

[6] 程元元,毛志芹. 基于代理多重签名的电子公文交换系统研究[J]. . 中州大学学报, 2014,31(5).116-120.

[7] 周红生,铁玲，李建华，倪佑生. 一类增强的代理多重签名体制[J]. . 上海交通大学学报, 2004,38(1):83-86.