A New Proxy Multi-Signature Scheme

Jiang Guan Xiong
Department of Computer Science
ShaoXing University
Shao Xing,Zhe Jiang,China(312000)
zscasjgx@foxmail.com

Abstract—**The proxy multi-signature is a very useful tool, which allows multiple signers to generate in a collaborative and simultaneous, and if a signer needs to delegate his signing capability to other signer, then the proxy signers can sign on behalf of an original signer. The paper proposed a new proxy multi-signature scheme, which the computation complicacy of the signature algorithm and the verification algorithm is independent of the number of signers. By verifying public-key, the new scheme can resist the forgery attack and the signing sequence of the proposed sequential scheme is fixed which unable to be changed freely by the signers. With the security analysis, it is a secure signature scheme.**

Keywords-proxy mlti-signatue;forgery attack;original signer; proxy signer;discrete logarithm;public-key verify

I. Introduction

The concept of proxy signature was first proposed by M.ambo, et al in 1996[1]. In a proxy signature scheme, an original signer is allowed to delegate his signing power to a designed person or group, who is called the proxy signer. During the past years, many proxy signature schemes and various types of proxy signature schemes were proposed [2,3,4,5]. Now proxy signatures have numerous applications, particularly in distribution computing and electronic commerce, etc.

In some cases, many original signers delegate the same proxy to sign the messages for all original ones. If an original signer could authorize a proxy group as his proxy agent, then only the cooperation of all of signers in the proxy group can generate the proxy signature on be half of an original signer, this proxy signature scheme that achieves such purpose is called the proxy multi-signature scheme. The proxy multi-signature scheme is a special case of the proxy signature schemes, which was first proposed by S.J.Hwang, et al.[6]

In 2000． Yi, et a1 proposed another type of proxy signature scheme: Proxy multi-signature schemes [7]. In this proxy multi-signature scheme, an original signer group can authorize one person as his proxy signer. In 2004, Hwang and Chen introduced the proxy multi-signature scheme [8]. Later, Lyuu and Wu pointed out Hwang et al.'s schemes were not secure and then proposed a modified scheme[9], but the improved scheme was not security and vulnerable to this insider attack [10].

In 2004, another proxy multi-signature scheme was proposed by Tzeng, et al[11]. Their scheme allows the group of original signers to delegate the signing capability to a designated group of proxy signers, and a set of verifiers in the designated verifier group to authenticate the proxy signature. But the scheme was insecure, then proposed an improved scheme with no Share Distribution Center (SDC)[12,13]. In 2006, Kang, et al proposed a new threshold proxy multi-signature scheme, but their scheme has serious security flaws due to the fact that an adversary can forge valid proxy signatures, which can be authenticated as if they were generated by the subset of the proxy, and there are two attack ways[14]. In 2007, Xie, et al shows that Bao, et al.'s scheme suffers from the proxy relationship inversion attack and forgery attack [15].

This paper proposed a new proxy multi-signature scheme based on the difficulty of the discrete logarithm problem. Compare with other scheme, this scheme can resist the forgery attack and can resist the allay attack by checking of pubic key. It also can ensure sequential scheme is fixed. And, the computation cost and the size of the proxy multi-signature are fixed too.

II. A new proxy multi-signature scheme

The new scheme is divided into four phases: system initialization phase, proxy share generation phase, proxy multi-signature generation phase and proxy multi-signature verification phase. In this paper, W is proxy certificate, which include the detail information of the original signers and the proxy signers, range of the proxy, period of the proxy, etc. M is the message which to be sign.

A. System initialization

The system randomly selects two large primes p and q, where p=2q+1. Let g is the primitive-root of the cyclic group GF(p), h() denotes a one-way collision resistant cryptographic hash function, Let s_0 =0.

All of the signers randomly choose their private keys $x_i \in$ [1,p-2] ,computes their public keys y_i =g^{x_i} mod p.

Then system publish p, g, h(). All of the signers respectively publish their public keys y_i and save their private keys x_i

B. Proxy share generation

a) Supposed the original signer is U_i , he delegate his signing power to proxy signer U_j

978-0-7695-3635-4/09 $25.00 © 2009 IEEE
DOI 10.1109/ICNDS.2009.85

b) U_i choose a randomly integer $l_i \in$[1,p-2]，compute $L_i = g^{l_i}$ mod p, $\delta_i = x_i$ h(W, l_i)+ l_i mod p-1.

c) U_i send（L_i , δ_i ）to U_j secretly, at the same time broadcasts L_i to the other signers.

d) U_j verify, if $g^{\delta_i} = y_i^{h(W,l_i)}$ L_i mod p then shows U_i delegate his signing power to U_j, and U_j's proxy key is δ_i , else show U_i don't delegate his signing power to U_j ,and U_j have no right to replace U_i's signature.

C. Proxy multi-signature generation

1) The first signer

If the signer is original signer U_1.

a) U_1 choose random two integers k_1 , l_1 ∈ [1,p-2], compute r_1 =g ^{k_1} mod p, $L_1 = g^{l_1}$ mod p. s_1 =(x_1 - $x_1 h(w,l_1)$ - l_1)h(M)- r_1 k_1 mod(p-1).

b) U_1 send (s_0 , s_1 ,M) to the next signer, and broadcasts r_1 , L_1 to all of the signers.

If the first signer is proxy signer, and supposed U_t is the proxy signer.

a) U_t choose a random integer $k_1 \in$[1,p-2] , compute r_1=g^{k_1} mod p, s_1 =(x_k - δ_1)h(M)- r_1 k_1 mod(p-1).

b) U_t sends (s_0 , s_1 ,M) to the next signer, and broadcasts r_1 , L_1 to all of the signers.

2) The second signer

a) Let S= g ^{s_1} * $r_1^{r_1}$ *($y_1^{h(W,l_1)}$ * L_1) $^{\text{h(M)}}$ mod p.

b) If the first signer is original signer then verify S $\overset{?}{=}$ (y_1)$^{\text{h(M)}}$ mod p, else if the first signer is proxy signer, supposed the signer is U_t , verify S $\overset{?}{=}$ (y_t)$^{\text{h(M)}}$ mod p. If the equation establish, it shows that the first signer's public key is valid and the first signer's signature is valid too, so the signature continued, else reject signature.

If the signer is original signer U_2 .

c) U_2 choose two random integers k_2 , l_2 ∈ [1,p-2], compute r_2 =g ^{k_2} mod p, $L_2 = g^{l_2}$ mod p, $s_2 = s_1$ +(x_2 - $x_2 h(W,l_2)$ - l_2)h(M)- r_2 k_2 mod(p-1).

d) U_i sends (s_1 , s_2 ,M) to the next signer, and broadcasts r_2 , L_2 to all of the signers.

If the second signer is proxy signer, supposed the proxy signer is U_t .

c) U_t choose a random integers $k_2 \in$ [1,p-2], compute r_2 =g^{k_2} mod p, $s_2 = s_1 + (x_t - \delta_2$)h(M)- r_2 k_2 mod(p-1).

d) U_t sends (s_1 , s_2 ,M) to the next signer, and broadcasts r_2 , L_2 to all of the signers.

3) Other signers (the No. i signer) (2<i≤n)

Supposed there are A original signers from the first signer to the No. (i-2) signer sign the message M. Their public keys, for the convenience of writing $y_1^{'} , y_2^{'} \ldots y_A^{'}$. And there are B proxy signers from the first signer to the No. (i-2) signer sign the message M, for the convenience of writing $y_1^{''}$, $y_2^{''}$ … $y_B^{''}$, it can draw the conclusion that A+B=i-2. The proxy multi-signature takes the following steps:

a) Let S=g$^{(s_{i-1} - s_{i-2})}$* $r_{i-1}^{r_{i-1}}$ *($y_{i-1}^{h(W,l_{i-1})}$ * L_{i-1}) $^{\text{h(M)}}$ mod p.

b) If the previous signer is an original signer then verify S $\overset{?}{=}$ (y_{i-1})$^{\text{h(M)}}$ mod p, else if the previous signer is proxy signer, supposed the signer is U_t , verify S $\overset{?}{=}$ (y_t)$^{\text{h(M)}}$ mod p. If the equation establish, it is mean that the previous signer's public key is valid, and the pervious signer's signature is also valid, so the signature continued, else reject signature.

c) Let $Y_{i-2} = \prod_{j=1}^{A} (y_j^{'}) \prod_{j=1}^{B} (y_j^{''})$ mod p.

d) Verify $g^{s_{i-2}} * \prod_{j=1}^{i-2} r_j^{r_j} *(\prod_{j=1}^{i-2} y_j^{h(W,l_j)} * \prod_{j=1}^{i-2} L_j)^{\text{h(M)}} \overset{?}{=}$ (Y_{i-2})$^{\text{h(M)}}$ mod p, if the equation establish, it is mean that before the previous signer's signature is valid, and the signature continued, else reject the signature, and judge the signature invalid.

If the signer is original signer U_i .

e) U_i choose two integers k_i , l_i $\in$[1,p-2] randomly, compute r_i =g ^{k_i} mod p, $L_i = g^{l_i}$ mod p, $s_i = s_{i-1}$ +(x_i - $x_i h(W,l_i)$ - l_i)h(M)- r_i k_i mod(p-1).

f) U_i sends (s_{i-1} , s_i ,m) to the next signer, and broadcasts r_i , L_i to all of the signers.

If the signer is proxy signer, supposed the signer is U_t .

e) U_t choose a integer k_i $\in$[1,p-2] randomly, compute r_i =g^{k_1} mod p, $s_i = s_{i-1} + (x_t - \delta_i$)h(M)- r_i k_i mod(p-1).

f) U_t sends (s_{i-1} , s_i ,m) to the next signer, and broadcasts r_i , L_i to all of the signers.

D. Proxy multi-signature verification

When all the signers finishing signing the message M, the last signer send the（ s_{n-1} , s_n ,M）to the signature verifier U_v , U_v let S= g$^{(s_n - s_{n-1})}$* $r_n^{r_n}$ *($y_n^{h(W,\text{l}_n)}$ * L_n)$^{\text{h(m)}}$ mod p. If the last signer is original signer U_n , then verify S $\overset{?}{=}$ (y_n)$^{\text{h(M)}}$ mod p, else if the last signer is proxy signer supposed the signer is U_t , verify S $\overset{?}{=}$ (y_t)$^{\text{h(M)}}$ mod p.

Then compute $Y_{n-1}=\prod_{j=1}^{A}(y_j^{'})\ \prod_{j=1}^{B}(y_j^{"})$ mod p(with A+B=n-1). Then verify the equation that $g^{s_{n-1}}$ * $\prod_{j=1}^{n-1}$ $r_{n-1}^{r_{n-1}}$ * $(\prod_{j=1}^{n-1} y_j{}^{h(W,l_j)} * \prod_{j=1}^{n-1} L_j)^{\text{h(M)}} \overset{?}{=} (Y_{n-1})^{\text{h(M)}}$ mod p.

If both the two equations establish, it is means that all the signature is valid, else reject the signature, and judge the signature invalid.

III. THE NEW SCHEME CORRECTNESS TESTIFY

A. public key validity

$$\begin{cases} g^{s_i-s_{i-1}} *(y_i^{h(w.l_i)} * L_i)^{\text{h(m)}} * r_i^{r_i} \overset{?}{=} y_i^{h(m)} \text{ mod p} \\ \text{(the NO.i signer is original signer } U_i\text{)} \\ g^{s_i-s_{i-1}} *(y_i^{h(w.l_i)} * L_i)^{\text{h(m)}} * r_i^{r_i} \overset{?}{=} y_t^{h(m)} \text{ mod p} \\ \text{(the NO.i signer is proxy signer } U_t\text{)} \end{cases}$$

If the NO.i signer is original signer U_i

$s_i = s_{i-1}$ +(x_i - $x_i h(w,l_i)$ - l_i)h(m)- r_i k_i mod(p-1)=> $g^{s_i-s_{i-1}}$ =g$^{((}$ x_i - $x_i h(w,l_i)$ - l_i $^{)\text{h(m)-}}$ r_i k_i $^{)}$ mod p= $y_i^{h(m)}$ /($r_i^{r_i}$ *($y_i^{h(w,l_i)}$ * L_i)$^{\text{h(m)}}$) mod p=> $g^{s_i-s_{i-1}}$ *($y_i^{h(w.l_i)} * L_i)^{\text{h(m)}} * r_i^{r_i} \overset{?}{=} y_i^{h(m)}$ mod p.

If the NO.i signer is proxy signer, supposed the signer is U_t :

$s_i = s_{i-1}$ +(x_t - δ_i)h(m)- r_i k_i mod(p-1)= s_{i-1} +(x_t - x_i h(w, l_i)+ l_i)h(m) - r_i k_i mod(p-1)=> $g^{s_i-s_{i-1}}$ = g$^{((}$ x_t - $x_i h(w,l_i)$ - l_i $^{)\text{h(m)-}}$ r_i k_i $^{)}$ mod p=> $g^{s_i-s_{i-1}}$ * $r_i^{r_i}$ * $(y_i^{h(w.l_i)} * L_i)^{\text{h(m)}} \overset{?}{=} y_t^{h(m)}$ mod p.

B. Signature validity

$g^{s_{i-2}} * \prod_{j=1}^{i-2} r_j^{r_j} *(\prod_{j=1}^{i-2} y_j{}^{h(w,l_j)} * \prod_{j=1}^{i-2} L_j)^{\text{ h(m)}} \overset{?}{=} (Y_{i-2})^{\text{h(m)}}$

verify, from (1), it can know that $g^{s_{i-2}-s_{i-3}} * g^{s_{i-3}-s_{i-4}}$ *… * $g^{s_1-s_0}$ ($\prod_{j=1}^{i-2} y_j{}^{h(w,l_j)}$ * $\prod_{j=1}^{i-2} L_j$)$^{\text{h(m)}}$ * $r_i^{r_i}$ $\prod_{j=1}^{i-2} r_j^{r_j}$ = $\prod_{j=1}^{A}(y_j^{'})$ $\prod_{j=1}^{B}(y_j^{"})$ mod p=> $g^{s_{i-2}}$ * $\prod_{j=1}^{i-2}$ $r_j^{r_j}$ * $(\prod_{j=1}^{i-2} y_j{}^{h(w,j)} * \prod_{j=1}^{i-2} L_j)^{\text{h(m)}}$ =$(Y_{i-2})^{\text{h(m)}}$ mod p.

IV. SECURITY ANALYSIS OF THE NEW SCHEME

A. Public key checking

Because computing s_{n-1} , s_n with the equations $g^{s_{n-1}}$ = (Y)$^{\text{h(M)}}$/($\prod_{j=1}^{n-1}$ $r_{n-1}^{r_{n-1}}$ * ($\prod_{j=1}^{n-1}$ $y_j{}^{h(w,l_j)}$ * $\prod_{j=1}^{n-1}$ L_j)$^{\text{h(M)}}$) mod p, g($^{s_n - s_{n-1}}$)* $r_n^{r_n}$ *($y_n^{h(w,\text{l}_n)}$ * L_n)$^{\text{ h(m)}}$=(y_k)$^{\text{ h(m}}$ mod p, which is very difficult, because computing s_{n-1} , s_n is the difficulty in solving the discrete logarithm problem (DLP). By checking of the signer’s public key with the equation of ($^{s_n - s_{n-1}}$)* $r_n^{r_n}$ *($y_n^{h(w,\text{l}_n)}$ * L_n)$^{\text{ h(m)}}$=(y_k)$^{\text{ h(M)}}$ mod p , which can avoid forgery attack by the attacker fabricate public key. And by this way, it also can resist attacker fabricate public key to sign part of signature with his authority.

B. Fix the sequential scheme

The paper shows how to fixed the sequential scheme with the example of the two adjacent original signers U_{i-1} , U_i , If U_{i-1} , U_i want to change the sign sequential:

U_i compute r_i =g ^{k_i} mod p, L_i = g^{l_i} mod p $s_i^{'}$ = s_{i-2} +(x_i - $x_i h(W,l_i)$ - l_i)h(M)- r_i k_i mod(p-1), then U_i sends (s_{i-2} , $s_i^{'}$,m) to the U_{i-1} , and broadcasts r_i , L_i to all of the signers.

U_{i-1} compute r_{i-1} =g $^{k_{i-1}}$ mod p, $s_{i-1}^{'}$ = $s_i^{'}$ +(x_{i-1} - $x_{i-1}h(W,l_{i-1})$ - l_{i-1})h(M)- r_{i-1} k_{i-1} mod(p-1), then send ($s_i^{'}$, s_{i-2} ,m) to the U_{i+1} .

U_{i+1} verify the equations g$^{(}$ $s_{i-1}^{'}$ - $s_i^{'}$ $^{)}$* ($y_i^{h(W,l_i)}$ * L_i)$^{\text{h(M)}}$* $r_i^{r_i} \overset{?}{=} y_i^{h(m)}$ mod p and g $^{s_{i-1}^{'}}$ * $\prod_{j=1}^{i-1}$ $r_j^{r_j}$ *($\prod_{j=1}^{i-1}$ $y_j{}^{h(w,l_j)}$ * $\prod_{j=1}^{i-1}$ L_j) $^{\text{h(M)}} \overset{?}{=}$ (Y_{i-1})$^{\text{h(M)}}$ isn’t establish. Prove as follows:

a) g$^{(\,s_{i-1}\,\text{-}\,s_i\,)}$*($y_i^{h(W,l_i)}$ * L_i)$^{\text{h(M)}}$* $r_i^{r_i}$ = ($y_i^{h(W,l_i)}$ * L_i)$^{\text{h(M)}}$ *(y_{i-1} $^{\text{h(M)}}$) * $r_i^{r_i}$ /(($y_{i-1}^{h(W,l_{i-1})}$ * L_{i-1})$^{\text{h(M)}}$* $r_{i-1}^{r_{i-1}}$) mod p≠ $y_i^{h(m)}$ mod p, so the equation don’t exist.

b) g $^{s_{i-1}^{'}}$ * $\prod_{j=1}^{i-1}$ $r_j^{r_j}$ *($\prod_{j=1}^{i-1}$ $y_j{}^{h(W,l_j)}$ * $\prod_{j=1}^{i-1}$ L_j) $^{\text{h(M)}}$mod p = g $^{s_{i-2}}$ $(y_{i-1}y_i)^{h(m)}$ / ($(y_i{}^{h(W,l_i)} y_{i-1}{}^{h(W,l_{i-1})} L_i L_{i-1})^{h(m)} r_i^{r_i} r_{i-1}{}^{r_{i-1}}$)* $\prod_{j=1}^{i-1}$ $r_j^{r_j}$ *($\prod_{j=1}^{i-1}$ $y_j{}^{h(W,l_j)}$ * $\prod_{j=1}^{i-1}$ L_j) mod p= ($(y_{i-1}y_i)^{h(m)}$ Y_{i-2})/ ($y_i{}^{h(W,l_i)}$ L_i $r_i^{r_i}$) mod p≠ $Y_{i-1}{}^{h(m)}$ mod p.

This shows it is very difficulty that the two adjacent signers collusion and change the sequence the proxy multi-signature. If they want to set the two equations all establish, they must obtain $s_{i-1}^{'}$ from the g $^{s_{i-1}}$ =($(y_{i-1}y_i)^{h(m)}$ Y_{i-2})

$/((L_i\ y_i^{h(W,l_i)}\ r_i^{r_i})\prod_{j=1}^{i-1} r_j^{r_j} *(\prod_{j=1}^{i-1} y_j^{h(W,l_j)} * \prod_{j=1}^{i-1} L_j)^{\mathrm{h(M)}})$mod p, then obtain $s_i^{'}$ from the $\mathrm{g}^{(s_{i-1}^{'} - s_i^{'})}=(y_{i-1}{}^{\mathrm{h(M)}})$ $/((y_{i-1}^{h(W,l_{i-1})} * L_{i-1})^{\mathrm{h(M)}} * r_{i-1}^{r_{i-1}})$ mod p. This way need to compute two discrete logarithm problems, so it is impossible to compute, and the new proxy-multi-signature can be unable to be changed freely by the signers. If the two adjacent signs are proxy signers or one is an original signer, the other is a proxy signer, the two equations aren't existence too, and sequential scheme is fixed.

V. Conclusions

This paper proposed a new proxy multi-signature scheme based on the difficulty of the discrete logarithm problem. By verifying public-key, the security of the proposed scheme is confirmed. Some possible attacks are considered, which can't successfully break the proposed scheme. Furthermore, it also can ensure sequential scheme is fixed. Particularly, the computation cost and the size of the proxy multi-signature are independent on the number of the original signers and the proxy signature.

References

[1] M. Mambo, K.Usuda, and E.Okamoto. Proxy signatures: delegation of the power to sign messages. IEICE Trans. on Fundamentals. E79. A(1996)9,1338-1354.

[2] C.-L.Hsu, T.-S.Wu, T.-C.Wu, New nonrepudiable threshold proxy signature scheme with known signers. J. Syst. Softw. (58)(2)(2001) 119-124.

[3] M. S. Hwang, I.C. Lin, E.J.L. Lu, A secure nonrepudiable proxy signature scheme with known signers, Int. J. Inform.1l(2)(2000)1-8.

[4] S. Kim, S. Park, D.Won, proxy signature, revisited, In : Proceedings of the ICICS 7, Lecture Notes in Computer Science,vo1.1334, 1997, PP.223−232.

[5] H.M. Sun, An efficient nonrepudiable threshold proxy signature scheme with known signers, Comput. Commun 22(8) (1999)717-722.

[6] S.J.Hwang, C.h.-Shi, A simple multi-proxy signature scheme. Proceedings of the Tenth National Conference on Information Security, Hualien, Taiwan, ROC,2000. pp.134-138.

[7] L.Yi, G.Bai, G.Xiao. Proxy multi-signature scheme: a new type of proxy signature scheme, Electronics Letters 36(6)(2000)527-528.

[8] J.Hwang, C.H.Chen. A new multi-proxy multi-signature scheme.2001 National Computer Symposium: Information Security,Taiwan ,China, 2001,F019-F026.

[9] Lyuu, Y.D.,Wu, M.-L.Cryptanalysis of and improvement on the Hwang-Chen multi-proxy multi-signature schemes (2005)Applied Mathematics and Computation,167(1),pp. 729-739.doi: 10.1016/j.amc. 2004.06.117.

[10] Guo, L, Wang, G. Insider attacks on multi-proxy multi-signature schemes. Computers and Electrical Engineering 33 (2)(2007), pp. 88-93.

[11] S.F.Tzeng, C.Y.Yang, and M.S.Hwang. A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification. Future Generation Computer Systems, 20(2004)9, 887-893.

[12] Bao, H.,Cao, Z.,Wang, S. Improvement on Tzeng et al.'s nonrepudiable threshold multi-proxy multi-signature scheme with shared verification (2005)Applied Mathematics and Computation, 169(2),pp. 1419-1430.

[13] Hsu, C.-L., Tsai, K.-Y., Tsai, P.-L.. Cryptanalysis and improvement of nonrepudiable threshold multi-proxy multi-signature scheme with shared verification. Information Sciences 177 (2)(2007), pp. 543-549.

[14] Lu Rongbo, He Dake, Wang Changji. Security Analysis and Improvement of a New Threshold Multi-Proxy Multi-Signature Scheme. Journal of Electronics(China). 2008,vol25,372-377.

[15] Xie, Q, Wang, J., Yu, X.. Improvement of nonrepudiable threshold multi-proxy threshold multi-signature scheme with shared verification. Journal of Electronics. 2007(11). 806-811.