A New Anonymous Proxy Multi-Signature Scheme

Yin Xin-chun, Ou Fu-na

School of Information and Engineering, Yangzhou University, Yangzhou, China, 225009

E-mail address: lyofn@163.com

Abstract: A new proxy multi-signature scheme with anonymity is proposed. In this scheme, several original signers can delegate their signing authority to one proxy signer. Original signers conceal the identity of proxy signer in proxy signature. Verifier can not recognize the identity of proxy signer from proxy signature. But verifier can reveal the identity of proxy signer only with the help of an original signer when disputation happens. The new scheme has qualities of strong unforgeability and high security.

Keywords: proxy signature; anonymous proxy signature; proxy multi-signature; anonymity

一种新的匿名代理多签名方案

殷新春，欧付娜

扬州大学信息工程学院，扬州，中国，225009

E-mail address: lyofn@163.com

【摘要】提出了一种新的具有匿名性的代理多签名方案。在该方案中，单个代理签名人同时代表多个原始签名人生成有效的代理签名。原始签名人在代理签名中隐藏代理签名人的身份，验证人无法从代理签名中识别代理签名人身份。在签名出现争议时，验证人只需借助原始签名人中的一人即能揭示代理签名人的身份。分析表明，新方案具有强不可伪造性，安全性较高。

【关键词】代理签名；匿名代理签名；代理多签名；匿名性

1 Introduction

Proxy signature was first introduced by Mambo, Usuda and Okamoto [1] in 1996. It allowed an entity called original signer to delegate its signing power to another entity called proxy signer, and proxy signer signs message on behalf of original signer. Once the signature verifier receives the proxy signature, he can check the validity of the signature and identify proxy signer, and also original's agreement on the signed message. Many various extensions of the basic proxy signature have been put forwarded because of different applications situations [2,3,4,5].

Yi Lijiang et al. proposed the concept of proxy multi-signature [6,7] in 2000.In this scheme, several original signers can delegate their signing authority to one proxy signer, that is to say, the proxy multi-signature for a message is created by a proxy signer and some original signers.

In 2005, Gu Lize et al. put forward the concept of anonymous proxy signature and further classified proxy signature schemes into anonymous proxy [8,9,10] and proxy-overt proxy signatures according that whether proxy signer's identity was been protected or not. They also constructed an anonymous proxy signature scheme [11] which not only satisfied basic security properties of normal proxy signature, but also had anonymity and traceability.

By the security analysis of Gu Lize's scheme recently, Guo Gang et al. [12] found that the scheme was easy to suffer interior attack and original signer could forge proxy signature instead of proxy signer. They also put forward four different forgery methods and gave the improved scheme with anti-forgeability.

To be enlightened by the scheme [12], we propose a new anonymous proxy multi-signature scheme by the combination of anonymous proxy signature and proxy multi-signature. The new scheme has special requirement in practical application. For example, a company will issue a file about financial department, engineering department and administration department. To make the file valid, it must be signed by the three departments together. So these departments can delegate a proxy signer to sign the file instead of them. But they maybe need protect the identity of proxy signer because of the

978-1-935068-01-3

actual application. Original signers can reveal the identity of proxy signer when the disputation happens. Our new scheme can satisfy this requirement. The scheme has anonymity, traceability and strong unforgeability. It also has high security and a practical application.

The organization of our paper is as follows: the preliminary model of anonymous proxy multi-signature will be given in the following section. In Section 3, we describe our new anonymous proxy multi-signature scheme. Then we discuss the security of our scheme in Section 4 and we conclude the paper in the last section.

2 Security Model

We define a new type of anonymous proxy multi-signature as follows:

Definition 1 : An anonymous proxy multi-signature scheme is a digital signature scheme comprised of the following six procedures:

Setup: On input a security parameter λ, this algorithm outputs the initial system parameters, a warrant certificate m_w which all original signers establish together and include the valid time of the delegation of the signing power and the identities of original signers, etc. At the same time, it also outputs key pairs of participants.

Delegate: A protocol between all the original signers and a proxy signer.

Proxy Key Gen: The output is the proxy key pairs for proxy signer.

Proxy Si gn: An algorithm for which the input is original signers' public keys, proxy signer's proxy private key, the warrant certificate m_w and a message m. The output is the proxy signature on m.

Proxy Ver: An algorithm for establishing the validity of an alleged proxy signature of a message with respect to original signer's warrant. Anyone can use this algorithm to check whether a signature is a valid proxy signature.

Anonymous Revel ation Phase: An algorithm that given a valid proxy signature on a message, original signers' public and private key pairs, determines the actual identity of proxy signer who generated the proxy signature.

Besides the basic security properties of proxy signature, it also satisfies anonymity and traceability.

Anonymity: verifier can not recognize the identity of proxy signer from the proxy signature.

Traceability: original signers can reveal the identity of proxy signer by some methods.

3 Our Scheme

The participants of the scheme include original signers A_i(i=1,…,n), proxy signer B and anonymous proxy multi-signature verifier V.

3.1 Initial Setup Phase

In the proposed scheme, the following notations are used:

h: a collision-resistant cryptographic hash function;

m_w: warrant certificate ;

x_{A_i} : private key of original signer A_i;

y_{A_i} : public key of original signer A_i, where $y_{A_i} = g^{x_{A_i}} \bmod p$;

x_B: private key of proxy signer;

y_B: public key of proxy signer, where $y_B = g^{x_B} \bmod p$;

x_P: proxy private key of proxy signer;

y_P: proxy public key of proxy signer.

3.2 Proxy Delegation Phase

1)Firstly, all the original signers make a warrant certificate m_w together, which contains the identity of original signers, the valid period of delegation as well as possible other restrictions on the signing capability delegated to proxy signer. Then, A_i sends warrant certificate m_w to proxy signer B in a secret channel.

On receiving the warrant certificate m_w, proxy signer B computes s_B, r_{B_1} , s_{B_1} if he wants to accept the warrant. The computing process is as following:

B randomly selects an integer k_B, computing

$$r_B = g^{k_B} \bmod p$$

$$s_B = x_B + k_B r_B \bmod q$$

Then, B randomly selects an integer k computing

$$r_{B_1} = g^{k} \bmod p$$

$$s_{B_1} = x_B h(r_B, ID_B, r_{B_1}) + k \bmod q$$

B returns the parameter (r_B, ID_B, r_{B_1} , s_{B_1}) to A_i, A_i verifies the equation

$$g^{s_{B_1}} = y_B^{h(r_B, ID_B, r_{B_1}) r_{B_1}} \bmod p$$

Foundation Item：Supported by National High Technology Research and Development Program of China（2007AA012448）;The National Natural Science Foundation of China (NSF 60473012); The Fastigium for the Six Talents of Jiangsu Province of China (06-E-025).

If it holds, A_i preserves the parameter (r_B,y_B,ID_B) to reveal proxy signer's identity in the future and computes Y_p which is written in the m_w:

$$Y_p = y_B r_B^{r_B} \bmod p$$

2) Original signer A_i makes a digital signature for m_w which is added Y_P.The computing process is as following:

A_i randomly selects an integer k_i, computing

$$r_i = g^{k_i} \bmod p$$

$$s_i = x_{A_i} h(m_w, r_i) + k_i r_i \bmod p$$

Then, A_i sends delegation parameter (r_i,s_i,m_w) to proxy signer B in a secret channel.

3.3 Proxy key generation phase

On receiving the delegation parameter (r_i,s_i,m_w),proxy signer B verifies the equation

$$g^{s_i} = y_{A_i}^{h(m_w, r_i)} r_i^{r_i} \bmod p$$

If the equation is unequivalent, proxy signer B demands A_i to deliver it again, else accepts the delegation and produces proxy key pairs:

$$x_p = s_1 + s_2 + \cdots + s_n + s_B \bmod q$$

$$y_p = y_{A_1}^{h(m_w, r_1)} r_1^{r_1} y_{A_2}^{h(m_w, r_2)} r_2^{r_2} \cdots y_{A_n}^{h(m_w, r_n)} r_n^{r_n} Y_p \bmod p$$

3.4 Signing Phase

If the message m is appropriate in warrant certificate m_w, proxy signer B signs the message m by proxy private key x_p and generates proxy signature σ_p=sig(x_p,m).The valid anonymous proxy multi-signature is $\{m, \sigma_p, m_w, r_1, r_2, \ldots, r_n, y_{A_1}, y_{A_2}, \ldots, y_{A_n}\}$.

Then B sends it to the verifier V.

3.5 Verification Phase

V verifies wether m accords to warrant certificate m_w firstly, then computes proxy public key of anonymous proxy multi-signature:

$$y_p = y_{A_1}^{h(m_w, r_1)} r_1^{r_1} y_{A_2}^{h(m_w, r_2)} r_2^{r_2} \cdots y_{A_n}^{h(m_w, r_n)} r_n^{r_n} Y_p \bmod p$$

(where Y_p gets from m_w.).V confirms the signature validity by checking $Ver(y_p, \sigma_p, m)=true$.If it is true,the signature is valid.

3.6 Anonymous Revelation Phase

The verifier V provides proxy signature to any original signer A_i. A_i firstly verifies its validness and then gets Y_p from m_w.A_i gets the parameter (r_B,y_B,ID_B) which is preserved in the delegation phase and checks up the following equation:

$$Y_p = y_B r_B^{r_B} \bmod p$$

If the parameter (r_B,y_B,) can make it hold, the ID_B is the proxy signer of the anonymous proxy multi-signature $\{m, \sigma_p, m_w, r_1, r_2, \ldots, r_n, y_{A_1}, y_{A_2}, \ldots, y_{A_n}\}$.

4 Security Analysis of Our Scheme

4.1 Verifiability

The verifier V computes proxy public key by signature and verifies the corresponding signature by proxy public key. Because of

x_p=s_1+s_2+⋯+s_n+s_B mod q

then

$$y_p = g^{x_p} = g^{s_1+s_2+\ldots+s_n+s_B} \bmod p = g^{x_{A_1} h(m_w, r_1)} g^{k_1 r_1} g^{x_{A_2} h(m_w, r_2)} g^{k_2 r_2} \ldots g^{x_n h(m_w, r_n)} g^{k_n r_n} g^{x_B} g^{k_B r_B} \bmod p = y_{A_1}^{h(m_w, r_1)} r_1^{r_1} y_{A_2}^{h(m_w, r_2)} r_2^{r_2} \ldots y_n^{h(m_w, r_n)} r_n^{r_n} Y_p \bmod p$$

From the above equation, we can find that $y_p = g^{x_p} \bmod p$ holds.

Anyone can convince the original signer's agreement on the signed message by the signature $\{m, \sigma_p, m_w, r_1, r_2, \ldots, r_n, y_{A_1}, y_{A_2}, \ldots, y_{A_n}\}$, it is because that the public keys of the original signer are included in the signature.

4.2 Strong Unforgeability

The forgeability attack aims at the structure of proxy private key x_p. However, private key comes from two parts: one is got from original signers A_i(i=1,2,⋯,n),another is from proxy signer B. If the original signer A_i wants to forge it, he must compute the parameters r_i (i=1,2,⋯n) from the following equation:

$$r_1^{r_1} r_2^{r_2} \ldots r_n^{r_n} = g^r (Y_p)^{-1} \bmod p$$

Unfortunately, it is as difficult as solving the discrete logarithm problem (DLP). This is infeasible. So the original signer A_i can not forge a valid proxy signature by wiping off the Y_P to get proxy private key x_p.

4.3 Anonymity and Traceability

The verifier V checks up the signature by computing

978-1-935068-01-3 © 2009 SciRes.

proxy public key from proxy signature, but it doesn't include the identity of proxy signer. V can't get proxy signer's public key y_B although he gets the parameter Y_P .So V only can verify the validness of proxy signature, but he can't reveal the identity of proxy signer. The verifier can reveal the identity of proxy signer with the help of original signers when the disputation happens.

5 Conclusions

We propose a new anonymous proxy multi-signature scheme by the combination of anonymous proxy and proxy multi-signature. The new scheme not only satisfies the basic security characters, but also has anonymity and traceability. To important, verifier can reveal the identity of proxy signer only with the help of an original signer when disputation happens. It has qualities of strong unforgeability and high security in application.

References

[1] Mambo M, Usuda K, Okamoto E. Proxy signature: delegation of the power to sign messages [J]. EICE Trans. Fundamentals, 1996, E79-A: 9: 1338−1353.

[2] K. Wei Victor K. A proxy signer privacy strong proxy signature scheme with protection. http:// www.computer.org/proceedings/ wetice/1748/17480055.pdf,2002.

[3] Wang S H, Wang G L, Bap F, et al. Cryptanalysis of a proxy-protected proxy signature scheme based on elliptic curve cryptosystem [A]. Vehicular Technology Conference[C], USA, IEEE 60th2004: 3240−3243.

[4] Eric JuiLin Lu, Min-Shiang HWang, Cheng-Jian Huang. A new proxy signature scheme with revocation [J].In Applied Mathematics and Computation, 2005, 161(3): 799−806.

[5] Zhuojun Lin, Zuowen Tan. A New Type of Collusion Attacks against Threshold Proxy Signature Schemes [A]. 2007 International Conference on Convergence Information Technology [C], 2007, 279−283.

[6] Yi Li-jiang, Bai Guo-qiang, Xiao Zhen-guo. Proxy multi-signature: A new type of proxy signature schemes [J].Acta Electronica Sinica, 2001, 29(4): 569−570.

[7] Yi Li-jiang, Bai Guo-qiang, Xiao Zhen-guo. Proxy multi-signature [J]. Journal of Computer Research and Development, 2001, 38 (2): 204−206.

[8] Wu Ting, Yu Xiuyuan, Chen Qin, et al. An Ideal Proxy Signature Scheme with Proxy Signer Privacy Protection [J].Journal of Computer Research and Development, 2004, 41 (4): 710−714.

[9] Zhao Jianjun, Liu Jingsen. Pairing-Based Proxy Signature Scheme with Proxy Signer's Privacy Protection [A].2007 International Conference on Computational Intelligence and Security[C], 2007, 627−631.

[10] Aimei Yang, Yuxun Liu. A Modified Strong Proxy Signature with Proxy Signer Privacy Protection [A]. Proceedings of 2008 IEEE International Symposium on IT in Medicine and Education[C], 872−875.

[11] Gu Lize, Zhang Sheng, Yang Yi-xian. A New Proxy Signature Scheme [J].Journal of Electronics & Information Technology, 2005, 27 (9): 1463−1466.

[12] Guo Gang, Zeng Guo-ping. Improvement of a New Proxy Signature Scheme [J]. Journal of Electronics & Information Technology, 2008, 30 (1): 245−248.