具有已知代理人的不可否认门限代理签密方案*

李继国[1+], 李建中[1], 曹珍富[2], 张亦辰[3]

[1](哈尔滨工业大学 计算机科学与技术学院,黑龙江 哈尔滨 150001)

[2](上海交通大学 计算机科学与工程系,上海 200030)

[3](齐齐哈尔大学 计算机科学与工程系,黑龙江 齐齐哈尔 161005)

A Nonrepudiable Threshold Proxy Signcryption Scheme with Known Proxy Agent

LI Ji-Guo[1+], LI Jian-Zhong[1], CAO Zhen-Fu[2], ZHANG Yi-Chen[3]

[1](School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China)

[2](Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200030, China)

[3](Department of Computer Science and Engineering, Qiqihar University, Qiqihar 161005, China)

+ Corresponding author: Phn: 86-451-86410291, E-mail: ljg1688@163.com

http://www.hit.edu.cn

Received 2002-09-18; Accepted 2003-07-02

Li JG, Li JZ, Cao ZF, Zhang YC. A nonrepudiable threshold proxy signcryption scheme with known proxy agent. *Journal of Software*, 2003,14(12):2021~2027.

http://www.jos.org.cn/1000-9825/14/2021.htm

Abstract: In 1996, Mambo *et al*. introduced the concept of proxy signature. However, a proxy signature only provides the delegated authenticity and doesn't provide the confidentiality. Chan and Wei proposed a threshold proxy signcryption scheme (denoted as Chan-Wei scheme), which extended the concept of proxy signature. In this paper, the authors demonstrate Chan-Wei scheme does not satisfy strong unforgeablity, strong nonrepudiation and strong identifiability. Based on Chan-Wei scheme, a nonrepudiable threshold proxy signcryption scheme with known proxy agents is proposed. The proposed scheme overcomes the weaknesses of Chan-Wei scheme. Completeness proof and security analysis of the proposed scheme are presented. In addition, compared with

* Supported by the National Natural Science Foundation of China under Grant Nos.60072018, 60273082 (国家自然科学基金); the National Natural Science Foundation of China for Distinguished Young Scholars under Grant No.60225007 (国家杰出青年科学基金); the National Research Foundation for the Doctoral Program of Higher Education of China under Grant No.20020248024 (国家教育部博士点基金); the National High-Tech Research and Development Plan of China under Grant No.2001AA41541 (国家高技术研究发展计划(863)); the National Grand Fundamental Research 973 Program of China under Grant No.G1999032704 (国家重点基础研究发展规划(973))

LI Ji-Guo was born in 1970. He is a Ph.D. candidate at the School of Computer Science and Technology, Harbin Institute of Technology. His current research interests include cryptography and its application. **LI Jian-Zhong** was born in 1950. He is a professor and doctoral supervisor at the School of Computer Science and Technology, Harbin Institute of Technology. His research interests include are database system technology and parallel computation technology. **CAO Zhen-Fu** was born in 1962. He is a professor and doctoral supervisor at the Department of Computer Science and Engineering, Shanghai Jiao Tong University. His research interests include number theory, cryptography and its application. **ZHANG Yi-Chen** was born in 1971. He is a lecturer at the Department of Computer Science and Engineering, Qiqihar University. His research interests include cryptography and its application.

Chan-Wei scheme, the proposed scheme exactly finds out which proxy agents present bogus secret shadow or tamper secret shadow.

Key words: proxy signcryption; proxy signature; threshold cryptography; discrete logarithm; nonrepudiation

摘 要: 1996 年,Mambo 等人提出了代理签名概念.但是,代理签名仅能提供授权的认证而不能提供保密性.Chan 和 Wei 提出一个门限代理签密方案(记为 Chan-Wei 方案),扩展了代理签名的概念.指出他们的方案不满足强不可伪造性、强不可否认性和强识别性.基于 Chan-Wei 方案,提出一个能够克服 Chan-Wei 方案缺点的不可否认门限代理签密方案.给出方案的完备性证明和安全性分析.此外,与 Chan-Wei 方案相比,所提出的方案能够确切地发现哪些代理人提供假子密钥或篡改子密钥.

关键词: 代理签密;代理签名;门限密码学;离散对数;不可否认性

中图法分类号: TP309 **文献标识码**: A

The concept of proxy signature introduced by Mambo, Usuda, and Okamoto[1] in 1996 allows a designated person, called a proxy signer, to sign on behalf of an original signer. Mambo *et al*. showed proxy signature should have the properties of proxy signer's deviation, unforgeability, verifiability, distinguishability, identifiablity, and undeniability. The proxy signature plays an important role in many applications[2,3] and has received great attention since it was proposed. So far, three types of delegation: full delegation, partial delegation and delegation with warrant have been proposed. Kim *et al*.[4] proposed a threshold proxy signature in 1997, which is a variant of the proxy signature. Sun *et al*.[5] showed that their threshold proxy signatures suffered from some weaknesses and gave a modified scheme. Latter, Sun[6] proposed an efficient nonrepudiable threshold proxy signature. However Hwang *et al*.[7] showed that Sun's scheme had two disadvantages and proposed a modified scheme which remedies the weakness of Sun's scheme. Sun[8] proposed a time-stamped proxy signature scheme with traceable receivers which can ascertain whether a proxy signature is created at a certain time and trace the receivers who receive the proxy signature from the proxy signer.

To avoid the abuse of signing power, a threshold proxy signature scheme should have the nonrepudiation property that provides the ability to identify the actual proxy signers of the proxy signature. Based on Kim *et al*.'s scheme, Sun[6] proposed an efficient nonrepudiable threshold proxy signature scheme with known signers to achieve the above goal. However, Hsu *et al*.[9] showed Sun's scheme was vulnerable against the conspiracy attack and gave an improved scheme. In 2000, Yi *et al*.[10] proposed a new type of proxy scheme: proxy multi-signature scheme. Recently, Li *et al*.[11~14] proposed some proxy signature schemes which analyzed and improved proxy schemes in Ref. [1,4,5,10], respectively. In Ref.[3], Lee *et al*. showed that a strong proxy signature scheme should satisfy the following five properties:

(1) Strong unforgeability: Anyone except the proxy signer cannot generate a valid proxy key pair. Only the legitimate proxy signer can create a valid proxy signature.

(2) Verifiability: The original signer's delegation on the signed message is verifiable using publicly available parameters.

(3) Strong identifiability: Anyone can determine the identity of the corresponding proxy signer from a proxy signature.

(4) Strong undeniability: Once a proxy signer creates a valid proxy signature for an original signer, he cannot repudiate his signature creation against anyone else.

(5) Prevention of misuse: It should be confident that a proxy key pair should be used only for creating a proxy signature which conforms to delegation information. In case of any misuse of the proxy key pair, the responsibility of a proxy signer should be determined explicitly.

However, a proxy signature only provides the delegated authenticity and doesn't provide the confidentiality. In 1999, Gamage *et al*.[15] extended the proxy signature and introduced a proxy signcryption scheme by combining proxy signature and encryption technology. It enables a principal to delegate its authority in producing authenticated and encrypted message (i.e. signcryption) to a trusted proxy agent. Recently, Chan and Wei[16] proposed a threshold proxy signcryption scheme. In a threshold proxy signcryption scheme, at leas t proxy agents in the entrusted group of n proxy agents are required to produce a valid authenticated and encrypted message on behalf of the original rights owner, the principal. In this paper, the authors demonstrate Chan-Wei scheme doesn't satisfy the strong unforgeablity, strong nonrepudiation and strong identifiablity. Furthermore, a nonrepudiable threshold proxy signcryption scheme with known proxy agents is proposed.

The paper is organized as follows: In Section 1, Chan-Wei scheme is reviewed and analyzed. In Section 2, on basis of Chan-Wei scheme, a nonrepudiable threshold proxy signcryption scheme with known proxy agents is presented. In Section 3, completeness proof and security analysis of the proposed scheme are presented. Finally, we draw our conclusions in Section 4.

1 Review and Cryptanalysis of Chan-Wei Scheme

Assume p,q are large primes and $q|p-1$, g is an element of order q in the multiplicative group Z^*_p, $E_e(\cdot)$ is the symmetric encryption algorithms with the private key e, $D_e(\cdot)$ is the decryption algorithms with the private key e, $H_e(\cdot)$ is a secure keyed hash function with the private key e. ($x_a \in_R Z^*_q$, $y_a=g^{x_a} \bmod p$) and ($x_b \in_R Z^*_q$, $y_b=g^{x_b} \bmod p$) are the discrete logarithm key pairs of the principal and the receiver, respectively.

In this section, a brief review of Chan-Wei scheme is given and the readers can refer to the original paper[16] for more details. Chan and Wei presented two schemes: a (n,n) threshold proxy signcryption scheme and a (t,n) threshold proxy signcryption scheme. The schemes involve n+2 parties, which are the principal, Alice, the receiver, Bob, and n entrusted proxy agents P_i, where i is its unique ID number. Assume that Alice, with the (x_a,y_a) key pair, wants to delegate her signcryption rights to the proxy agents and let them signcrypt the message m, on behalf of her to Bob, with the (x_b,y_b) key pair. Because of space limitation, we only review the (t,n) threshold proxy signcryption scheme.

1.1 (t,n) threshold proxy signcryption scheme

The (t,n) threshold proxy signcryption scheme consists of the following three phases:

Group key and proxy key generation:

Input: Defined public parameters p, q, g, and Alice's key pair (x_a,y_a).

Output: Proxy ID u_i, proxy signcryption key x_{u_i}, and parameter K.

(1) Generation of group secret: The principal, Alice, randomly chooses x, where $1 \le x \le q-1$ and computes $K=g^x \bmod p$. Then Alice computes group's private key $x_G=x_a+x \cdot K \bmod p-1$ and group's public key $y_G=g^{x_G} \bmod p$.

(2) Generation of proxy shares: The principal, Alice, randomly chooses a polynomial over Z_q of degree $t-1$, $f(z)=x_G+a_1 z+\ldots+a_{t-1}z^{t-1} \bmod q$. Then Alice generates $U=\{u_i,u_j \in Z_q \,\&\, i,j \in Z_{n-1} \,\&\, u_i \neq u_j \,\&\, i \neq j\}$ which are ID of the proxy agents and generates n key pair of proxy agent P_{u_i}, (x_{u_i},y_{u_i}), where $x_{u_i}=f(u_i) \bmod q$. Finally, Alice sends (u_i,x_{u_i},K) securely to proxy agent P_{u_i} and broadcasts $y_G,g^{a_1},g^{a_2},\ldots,g^{a_{t-1}}$ to all proxy agents in the group.

(3) Verification of proxy share: Each $P_i,i \in U$, checks whether the equation $g^{x_i}=y_G \times \prod_{n=1}^{t-1}(g^{a_n})^{i^n} \bmod p$ holds. If $P_i,i \in U$, finds out that the equation is not justified, P_i rejects and broadcasts (i,x_i). If $P_i,i \in U$, receives (j,x_j), where $j \neq i$, P_i rejects (i,x_i). If any proxy agent rejects, the protocol terminates.

(4) Verification of group public key: Each $P_i,i \in U$, checks whether the equation $y_G=y_a \cdot K^K \bmod p$ holds. If

the equation is not justified, the protocol is rejected and terminated.

(t,n) threshold proxy signcryption: Let $\tilde{U}$ be a set containing all the ID of t proxy agents participating in the proxy signcryption.

Input: Defined public parameters p,q,g, participating proxy agents' proxy share (u_i,x_{u_i},K) and receiver's key pair (x_b,y_b).

Output: A proxy signcrypted text (c,r,s,K).

(1) Each $P_i,i\in\tilde{U}$, with the key pair (x_i,y_i) computes $t_i=c_ix_i$, where $c_i=\prod_{l\in\tilde{U},\ l\neq i}\frac{l}{l-i}$.

(2) Each $P_i,i\in\tilde{U}$, randomly chooses $n_i\in Z_q^*$, computes $e_i=y_b^{n_i} \bmod p$ and broadcasts e_i to all $p_j,j\in\tilde{U}\setminus\{i\}$.

(3) Each $P_i,i\in\tilde{U}$, computes $e=\prod_{j\in\tilde{U}}e_j \bmod p$, $r=H_e(m)$, $c=E_e(m)$, $s_i=t_ir+n_i-t^{-1}r \bmod q$ and broadcasts s_i to all proxy agents. Finally, $P_i,i\in\tilde{U}$, computes $s=\sum_{j\in\tilde{U}}s_j$.

(t,n) threshold proxy unsigncryption:

Input: p,q,g,c,r,s,K,y_a,x_b. Output: Plaintext m.

The receiver first computes $y_G=y_a\cdot K^K \bmod p$, $e=(g^{s+r}\cdot y_G^{-r})^{x_b} \bmod p$ and then decrypts cipher text $m=D_e(c)$. Finally, the receiver checks whether the equation $r=H_e(m)$ holds.

1.2 Cryptanalysis on Chan-Wei scheme

In this section, we give a brief remark on Chan-Wei scheme.

Attack1: Chan-Wei scheme has no strong unforgeablity because the principal himself also creates a valid proxy signcryption according to the step of Chan-Wei scheme.

Attack2: Chan-Wei scheme has no strong nonrepudiation. A proxy group can repudiate they are proxy agents because, on one hand, group public key $y_G=y_a\cdot K^K$ which is used to verify the validity of proxy signcryption does not contain any information of the proxy group, on the other hand, there is no private information of the proxy agent P_i in the proxy signcryption equation $s_i=t_ir+n_i-t^{-1}r \bmod q$. On the contrary, an illegal group can also claim that they are the owners of the threshold proxy signcryption.

Attack3: Chan-Wei scheme has no strong identifiability. The verifier doesn't know which proxy agents participate the proxy signcryption because there is no identity information of the proxy group in the (t,n) threshold proxy unsigncryption phase.

Remark1: The (n,n) threshold proxy signcryption scheme of Chan-Wei scheme also has similar weaknesses.

2 Nonrepudiable Threshold Proxy Signcryption Scheme

In this section, based on Chan-Wei scheme, a nonrepudiable threshold proxy signcryption scheme with known proxy agents is proposed. In the scheme, each proxy agent P_i randomly chooses $v_i\in Z_q^*,i=1,...,n$ as his private key and computes $ID_i=g^{v_i} \bmod p$ as his public key which is regarded as identity information of the proxy agent P_i, other parameters are the same as those in Chan-Wei scheme. The (t,n) nonrepudiable threshold proxy signcryption scheme consists of the following three phases:

Group key and proxy key generation:

Input: Defined public parameters p,q,g, and Alice's key pair (x_a,y_a).

Output: Proxy ID u_i, proxy signcryption key x_{u_i}, and parameter K.

(1) Generation of group secret: The principal, Alice, randomly chooses x, where $1\le x\le q-1$ and computes $K=g^x \bmod p$. Then Alice computes group's private key $x_G=x_a+x\cdot K \bmod p-1$ and group's public key $y_G=g^{x_G} \bmod p$.

(2) Generation of proxy shares: The principal, Alice, randomly chooses a polynomial of degree $t-1$ over Z_q, $f(z)=x_G+a_1z+...+a_{t-1}z^{t-1} \bmod q$. Then Alice generates $U=\{u_i,u_j \in Z_q \ \& \ i,j \in Z_{n-1} \ \& \ u_i \neq u_j \ \& \ i \neq j\}$ which are ID of the proxy agents and generates n proxy private key $x_{u_i}=f(u_i) \bmod q, i=1,...,n$. The key pair of proxy agent P_{u_i} is (x_{u_i},y_{u_i}), where $y_{u_i}=g^{x_{u_i}} \bmod p$. Finally, Alice sends (u_i,x_{u_i},K) securely to proxy agent P_{u_i} and broadcasts $y_G,g^{a_1},g^{a_2},...,g^{a_{t-1}}$ to all proxy agents in the group.

(3) Verification of proxy share: Each $P_i,i \in U$, checks whether the equation $g^{x_i}=y_G \times \prod_{n=1}^{t-1}(g^{a_n})^{i^n} \bmod p$ holds. If $P_i,i \in U$, finds out that the equation is not justified, P_i rejects and broadcasts (i,x_i). If $P_i,i \in U$, receives (j,x_j), where $j \neq i$, P_i rejects (i,x_i). If any proxy agent rejects, the protocol terminates.

(4) Verification of group public key: Each $P_i,i \in U$, checks whether the equation $y_G=y_a \cdot K^K \bmod p$ holds. If the equation is not justified, the protocol is rejected and terminated.

(t,n) threshold proxy signcryption: Let $\tilde{U}$ be a set containing all the ID of t proxy agents participating in the proxy signcryption.

Input: Defined public parameters p,q,g, participating proxy agents' proxy share (u_i,x_{u_i},v_{u_i},K) and receiver's public key y_b.

Output: A proxy signcrypted text (c,r,s,K).

(1) Each $P_i,i \in \tilde{U}$, with key tuple (x_i,y_i,v_i,ID_i) computes $t_i=c_ix_i$, where $c_i=\prod_{l \in U,\ l \neq i} \frac{l}{l-i}$.

(2) Each $P_i,i \in \tilde{U}$, randomly chooses $n_i \in Z_q^*$, computes $e_i=y_b^{n_i} \bmod p$ and broadcasts e_i to the receiver and all $p_j,j \in \tilde{U} \setminus \{i\}$.

(3) Each $P_i,i \in \tilde{U}$, computes $e=\prod_{j \in \tilde{U}} e_j \bmod p$, $r=H_e(m)$, $c=E_e(m)$, $s_i=(t_i+v_i)r+n_i-t^{-1}r \bmod q$ and broadcasts s_i to the receiver and all agents. Finally, $P_i,i \in \tilde{U}$, computes $s=\sum_{j \in \tilde{U}} s_j$.

The tuple (c,r,s,K) is the proxy signcrypted text and it is sent to the receiver. When he receives (c,r,s,K), he executes the following (t,n) threshold proxy unsigncryption algorithm to authenticate and decrypt the plaintext m.

(t,n) threshold proxy unsigncryption:

Input: $p,q,g,c,r,s,K,y_a,x_b,ID_j,j \in \tilde{U}$. Output: Plaintext m.

The receiver first computes $y_V=y_a\prod_{j \in \tilde{U}} ID_j \cdot K^K \bmod p$, $e=(g^{s+r} \cdot y_V^{-r})^{x_b} \bmod p$ and then recovers the plaintext $m=D_e(c)$. Finally, the receiver checks whether the equation $r=H_e(m)$ holds. If the equation holds the receiver accepts m, otherwise he rejects m.

The completeness proof of the (t,n) nonrepudiable threshold proxy signcryption scheme can be confirmed through Theorem 1.

Theorem 1. If the proxy agents conform to the steps of the proposed (t,n) nonrepudiable threshold proxy signcryption scheme, the receiver with the proxy signcrypted text (c,r,s,K) can recover the plaintext m by using the equation $m=D_e(c)$ and verify the validity of the plaintext m by using the equation $r=H_e(m)$.

Proof. According to the proxy signcrypted text (c,r,s,K), the receiver computes

$$\left(g^{s+r} \cdot y_V^{-r}\right)^{x_b} \bmod p = \left(g^{r+\sum_{j \in \tilde{U}} s_j} \cdot \left(y_a \prod_{j \in \tilde{U}} ID_j \cdot K^K \right)^{-r} \right)^{x_b} \bmod p$$

$$= \left(g^{r+\sum_{j \in \tilde{U}} ((t_j+v_j)r+n_j-t^{-1}r)} \cdot \left(y_G \cdot g^{\sum_{j \in \tilde{U}} v_j} \right)^{-r} \right)^{x_b} \bmod p$$

$$= \left(g^{r+\sum_{j\in\tilde{U}} t_j r + \sum_{j\in\tilde{U}} v_j r + \sum_{j\in\tilde{U}} n_j + \sum_{j\in\tilde{U}} (-t^{-1}r)} \cdot \left(g^{x_G + \sum_{j\in\tilde{U}} v_j} \right)^{-r} \right)^{x_b} \bmod p$$

$$= \left(g^{r+x_G r + \sum_{j\in\tilde{U}} v_j r + \sum_{j\in\tilde{U}} n_j - r} \cdot g^{-r\left(x_G + \sum_{j\in\tilde{U}} v_j\right)} \right)^{x_b} \bmod p$$

$$= \left(g^{\sum_{j\in\tilde{U}} n_j} \right)^{x_b} \bmod p$$

$$= y_b^{\sum_{j\in\tilde{U}} n_j} \bmod p$$

$$= \prod_{j\in\tilde{U}} e_j \bmod p$$

$$= e .$$

Thus, the receiver with the proxy signcrypted text (c,r,s,K) can recover the plaintext m by using the equation $m = D_e(c)$ and verify the validity of the plaintext m by using the equation $r = H_e(m)$.

Compared with Chan-Wei scheme, once some proxy agents present bogus secret shadow or tamper secret shadow, the proposed scheme can exactly find out which proxy agents are dishonest. This can be confirmed through Theorem 2.

Theorem 2. In the (t,n) threshold proxy unsigncryption phase, if the receiver finds the plaintext text $m = D_e(c)$ doesn't satisfy the equation $r = H_e(m)$, he can find out which proxy agents are dishonest by checking whether the equation $y_b^{s_i + t^{-1}r} = y_i^{c_i x_b r} ID_i^{x_b r} e_i \bmod p$ holds.

Proof. This is due to the fact that the receiver knows the private key x_b. According to the proxy signcrypted text (c,r,s,K) and broadcasted messages e_i and s_i, if the proxy agents don't present bogus secret shadow or tampers secret shadow, the following equation must hold.

$$y_b^{s_i} = y_b^{(t_i+v_i)r+n_i-t^{-1}r} \bmod p = y_b^{c_i x_i r} ID_i^{x_b r} e_i y_b^{-t^{-1}r} \bmod p = y_i^{c_i x_b r} ID_i^{x_b r} e_i y_b^{-t^{-1}r} \bmod p .$$

Namely, $y_b^{s_i + t^{-1}r} = y_i^{c_i x_b r} ID_i^{x_b r} e_i \bmod p$, where $c_i = \prod_{l\in U,\ l\neq i} \frac{l}{l-i}$.

Remark 2: Similarly, a (n,n) threshold proxy signcryption scheme with known proxy agents can also be proposed.

3 Security Analysis

(1) The security of the proposed scheme is based on the discrete logarithm difficult problem and the verifiable secret sharing scheme proposed by Pedersen[17]. It is equal to the discrete logarithm difficult problem of solving the x_a, x_b, x_i, v_i from $y_a = g^{x_a} \bmod p$, $y_b = g^{x_b} \bmod p$, $y_i = g^{x_i} \bmod p$ and $ID_i = g^{v_i} \bmod p$.

(2) Strong unforgeability: Because $s_i = (t_i + v_i)r + n_i - t^{-1}r \bmod q$ contains private key information v_i of the proxy agent P_i in the threshold proxy signcryption phase, without private key information v_i of the proxy agent P_i, the principal cannot generate a valid threshold proxy signcryption scheme by himself.

(3) Strong identifiability: Because $y_V = y_a \prod_{j\in\tilde{U}} ID_j \cdot K^K \bmod p$ contains identity information $ID_j, j \in \tilde{U}$, of the proxy agents participating proxy signcryption in the proxy unsigncryption phase, any verifier can determine which proxy agents participate in the threshold proxy signcryption.

(4) Strong nonrepudiation: In the scheme, proxy agents don't repudiate their participation in threshold proxy signcryption while illegal groups don't claim that they are proxy agents, because $s_i = (t_i + v_i)r + n_i - t^{-1}r \bmod q$ contains private key information v_i of the proxy agent P_i in the threshold proxy signcryption phase, at the same time,

$y_V = y_a \prod_{j \in \tilde{U}} ID_j \cdot K^K \bmod p$ contains identity information $ID_j, j \in \tilde{U}$, of proxy agents P_j participating in proxy signcryption in the proxy unsigncryption phase.

(5) Obviously, the proposed scheme satisfies the properties of verifiability and the prevention of misuse.

4 Conclusions

In this paper, we show Chan-Wei scheme doesn't satisfy strong unforgeablity, strong nonrepudiation and strong identifiability. Based on Chan-Wei scheme, a nonrepudiable threshold proxy signcryption scheme with known proxy agents is proposed. The proposed scheme overcomes the weaknesses of Chan-Wei scheme. Completeness proof and security analysis of the proposed scheme are presented. In addition, compared with Chan-Wei scheme, the proposed scheme exactly finds out which proxy agents present bogus secret shadow or tamper secret shadow.

Acknowledgement The authors would like to thank Professor Victor K. Wei in the Department of Information Engineering, Chinese University of Hong Kong Shatin, NT, Hong Kong for his valuable references.

References:

[1] Mambo M, Usuda K, Okamoto E. Proxy signatures: Delegation of the power to sign messages. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1996,E79-A(9):1338~1353.

[2] Lee B, Kim H, Kim K. Secure mobile agent using strong non-designated proxy signature. In: Varadharajan V, Mu Y, eds. Proceedings of the ACISP2001. LNCS 2119, Berlin: Springer-Verlag, 2001. 474~486.

[3] Lee B, Kim H, Kim K. Strong proxy signature and its application. In: Proceedings of the SCIS2001. 11B-1, 2001. 603~608.

[4] Kim S, Park S, Won D. Proxy signatures, revisited. In: Han Y, *et al*. eds. Proceedings of the ICICS'97 International Conference on Information and Communications Security. LNCS 1334, Berlin: Springer-Verlag, 1997. 223~232.

[5] Sun HM, Lee NY, Hwang T. Threshold proxy signatures. IEE Proc.-Computers & Digital Techniques, 1999,146(5):259~263.

[6] Sun HM. An efficient nonrepudiable threshold proxy signature scheme with known signers. Computer Communications, 1999, 22(8):717~722.

[7] Hwang MS, Lin IC, Lu EJL. A secure nonrepudiable threshold proxy signature scheme with known signers. International Journal of Informatica, 2000,11(2):1~8.

[8] Sun HM. Design of time-stamped proxy signatures with traceable receivers. IEE Proc.-Computers & Digital Techniques, 2000, 147(6):462~466.

[9] Hsu CL, Wu TS, Wu TC. New nonrepudiable threshold proxy signature scheme with known signers. The Journal of Systems and Software, 2001,58(2):119~124.

[10] Yi LJ, Bai GQ, Xiao GZ. Proxy multi-signature scheme: A new type of proxy signature scheme. Electronics Letters, 2000,36(6): 527~528.

[11] Li JG, Cao ZF, Zhang YC. Improvement of M-U-O and K-P-W proxy signature schemes. Journal of Harbin Institute of Technology, 2002,9(2):145~148.

[12] Li JG, Cao ZF. Improvement of a threshold proxy signature scheme. Journal of Computer Research and Development, 2002, 39(11):1513~1518 (in Chinese with English abstract).

[13] Li JG, Cao ZF, Zhang YC, Li JZ. Cryptographic analysis and modification of proxy multi-signature scheme. High Technology Letters, 2003,13(4):1~5 (in Chinese with English abstract).

[14] Li JG, Cao ZF, Zhang YC. Nonrepudiable proxy multi-signature scheme. Journal of Computer Science and Technology, 2003,18(3): 399~402.

[15] Gamage C, Leiwo J, Zheng Y. An efficient scheme for secure message transmission using proxy-signcryption. In: Edwards J, ed. Proceedings of the 22th Australasian Computer Science. Auckland: Springer-Verlag, 1999. 420~431.

[16] Chan WK, Wei VK. A threshold proxy signcryption. In: Proceedings of the 2002 International Conference on Security and Management (SAM2002). Monte Carlo Resort, Las Vegas, Nevada, 2002.

[17] Pedersen TP. A threshold cryptosystem without a trusted party. In: Davies DW, ed. Proceedings of the Advances in Cryptology-Eurocrypt'91. LNCS 547, Brighton: Springer-Verlag, 1991. 552~526.

附中文参考文献:

[12] 李继国,曹珍富.一个门限代理签名方案的改进.计算机研究与发展,2002,39(11):1513~1518.

[13] 李继国,曹珍富,张亦辰,李建中.代理多重签名方案的密码分析与修改.高技术通讯,2003,13(4):1~5.