无可信中心的可验证门限代理签名方案

闫德勤 赵洪波
(辽宁师范大学计算机与信息技术学院 大连 116029)

摘 要 提出了一个安全的门限代理签名方案。合谋攻击是指在不知道任何有效的门限代理签名的情况下,恶意代理成员人数大于或等于门限值时,他们能合谋重新构造代理群的秘密多项式函数,得到代理群的秘密参数,从而可以伪造其他代理成员的代理签名。以往方案大部分都是需要可信中心的,这样可信中心往往就会成为被攻击对象。提出的新方案能抵抗合谋攻击,任意 t 个人合作仍然无法知道其他代理人的秘密参数,也就无法伪造其他代理签名人的签名。还能满足门限代理签名的性质,且针对 t 个成员可能的恶意代理原始签名人签名的问题,由原始签名人两次授权来解决,这只需要维护签名生成者和原始签名人之间的一条安全信道。根据代理签名不能辨认代理签名人身份。每个参与者的公、私钥以及群公钥由参与者共同协商,无须可信中心参与,避免了对可信中心的攻击和成员之间的欺骗,使得安全性级别更高。

关键词 密码学,数字签名,门限代理签名,无可信中心,合谋攻击
中图法分类号 TP309 **文献标识码** A

Secure(t,n) Threshold Proxy Signature Scheme Without a Trusted Party

YAN De-qin ZHAO Hong-bo
(Department of Computer Science, Liaoning Normal University, Dalian 116029, China)

Abstract A secure threshold proxy signature scheme was proposed. Conspiracy attack, that is, any t(t is threshold value) or more malicious proxy signatures may work together to reconstruct the secret polynomial of the proxy group and derive the secret keys of other members in the proxy group, consequently they can impersonate some other proxy signers to generate a valid threshold proxy signature. A large number of the schemes which were proposed require trusted party. So the trusted party becomes the attacked part. The proposed scheme can withstand the conspiracy attack, arbitrarily signers of t still can't know the secure keys of other members in the proxy group, so they can't impersonate some other proxy signers to generate a valid threshold proxy signature. Furthermore, with regard to t of malicious signers impersonate the original signer, the original signer uses the second empower to solve, which only needs one secret channel between the original signer and the generation signer. It cannot distinguish the proxy signers by proxy signatures. In the scheme each participant's public key and private key and the group public key are negotiated among all participants with no trusted party required. We shall try to avoid attacking the trusted party and the cheating between proxy signers, the security of this scheme is more efficient than other schemes.

Keywords Cryptography, Digital signature, Threshold proxy signature, Without a trusted party, Conspiracy attack

1 引言

数字签名的概念首先是由 Diffie 和 Hellman 于 1976 年提出的。随着计算机和网络通信技术的发展,数字签名这种用于保证信息完整性、不可否认性、不可伪造性的技术得到了广泛的应用。数字签名根据其不同的应用可分为盲签名、多重签名,以及门限签名、代理签名等。门限签名主要应用于将签名权力通过门限的方式分配给群组的各成员的场合中。门限签名方案的安全性要求即便是破坏了 t 个成员的敌手也不能获得私有密钥的任何信息,不能伪造新消息的有效签名[1]。代理签名主要应用于将签名权力委托给其他人,使其代表自己签名的场合中。但是,人们将签名权力委托给代理人时,通常存在代理人是否可靠、是否会滥用代理签名权,以及代理人的代理密钥是否保存妥当、是否会被其他人窃取并进行恶意签名等问题。为了解决这些问题,将门限签名引入代理签名体制中,形成了门限代理签名。

门限代理签名是一个很重要的数字签名,近年来人们对它进行了广泛的研究。目前,已经提出了许多门限代理签名方案[2-10,13]。但这些方案都存在以下问题:(1)合谋攻击。文献[2-8]的方案中存在合谋攻击,即在不知道任何有效的门限

到稿日期:2008-09-23 返修日期:2008-12-11 本课题得到国家自然科学基金(No. 60372071),辽宁省教育厅高等学校科学研究基金(2004C031),辽宁师范大学校基金资助。
闫德勤(1962—),男,博士,教授,主要研究方向为信息安全、密码学、数据挖掘,E-mail: yandeqin@163.com;赵洪波(1983—),女,硕士研究生,主要研究方向为信息安全与密码学。

代理签名的情况下，恶意代理成员人数大于或等于门限值时，他们能合谋重新构造代理群的秘密多项式函数，得到代理群的秘密参数，从而可以伪造其他代理成员的代理签名。在Hsu等人提出的门限代理签名方案[7]中，产生代理签名时需要代理签名人的私钥，因此恶意代理签名人因没有其他代理签名人的私钥不能伪造其他代理签名人的代理签名。但仍然存在着恶意代理签名人的人数大于或等于门限值时，他们能合谋重新构造代理群的秘密多项式函数，从而得到代理群的秘密参数的不安全因素。另外，在Hsu等人的方案中，原始签名人能根据代理签名辨认出代理签名人的身份，这对原始签名人是非常有用的，因为原始签名人能对代理签名人的代理签名进行监督，防止代理签名人滥用自己的代理签名权。但是，在有些实际情况下，尽管代理签名人忠实地行使着原始签名人委托给自己的代理签名权利，代理签名人仍然不愿意原始签名人能根据代理签名确定代理签名人的身份，例如电子选举、电子支付等。(2)在文献[2-8]的方案中，一旦原始签名人将签名权委托给代理签名人，那么代理签名人就具有对这个签名权的永久代理，这对原始签名人是很不利的。原始签名人希望代理签名人在某一段时间内具有代理签名权，当这段有效期过后，就收回代理签名权。(3)到目前为止所提出的代理门限签名方案几乎都是需要可信中心的，王斌等提出了无可信中心的门限签名方案[11]，然而其安全性被证明并不可行[12]。由可信中心来负责参与者的密钥协商，而维护一个可信中心会增加系统的实现代价和复杂度。而且在很多特定的应用环境下，一个可被所有小组成员信任的可信中心是不存在的。针对以上问题，本文提出了一个安全的无可信中心的门限代理签名方案。方案能满足门限代理签名的性质，能抵抗文献[2-8]提到的合谋攻击，针对 t 个成员可能的恶意代理原始签名人签名的问题，由原始签名人两次授权来解决，这只需要维护签名生成者和原始签名人之间的一条安全信道；根据代理签名不能辨认代理签名人身份；方案中参与者的公、私钥以及群公钥由参与者共同协商，无须可信中心参与。

2 安全的无可信中心的(t,n)门限代理签名方案

2.1 系统参数

令 $N=p_1p_2$，$q|(p_1-1)$，其中 p_1，p_2 和 q 都为大素数。阶为 q 的元素 g(即 $g^q=1 \bmod N$)。$ID_0\in Z_q$ 为原始签名人 p_0 的身份标志，x_0 和 $y_0=g^{x_0} \bmod N$ 分别为 p_0 的私钥和公钥。设两个整数(e,d) 满足 $\gcd(e,\phi(N))=1$，$ed=1 \bmod \phi(N)$，其中 $\phi(N)=(p_1-1)(p_2-1)$。代理群 $G_p=(P_1,P_2,\cdots,P_n)$，$ID_0\in Z_q(i=1,2,\cdots,n)$为每个代理签名人的身份标志。$h(\cdot)$为安全的单向Hash函数。$m_{w1}$和 m_{w2}是授权消息，主要包含原始签名人和代理签名人的身份、代理签名的范围等。

2.2 密钥生成阶段

首先，每个成员 P_i 对外公开自己唯一的身份标示号 ID_i，每个组成员 P_i 选定一个 $n-1$ 次多项式，$f_i(x)=a_{i0}+a_{i1}x+\cdots+a_{in-1}x^{n-1}$。$P_i$ 为其余 $n-1$ 个成员计算 $\lambda_{ij}=f_i(x_j) \bmod q$，并通过广播方式将其发送给其他成员 P_j。在每个成员都完成上面的步骤后，组成员 P_i 可以计算 $\lambda_i=\sum_{j=1}^{n}\lambda_{ji} \bmod q$，即 $\lambda_i=\sum_{j=1}^{n}f_j(x_i) \bmod q$。

现定义一个新函数 $F(x)=\sum_{j=1}^{n}f_j(x) \bmod q$，容易得知 $\lambda_i=F(x_i)$。P_i 在$[1,p_1-1]$上选取一个随机数 k_i，把 $x_i=\lambda_ik_i \bmod q$ 作为组成员 P_i 的密钥。令 $v_i=g^{k_i} \bmod p_1$。P_i 把 v_i 通过广播的方式发给其他成员。

每个成员可计算 $\omega=\prod_{i=1}^{n}v_i \bmod p_1$。$n$ 个成员可以通过利用多项式插值得 $F(0)=(\sum_{i=1}^{n}F(x_i)\prod_{j=1,j\neq i}^{n}\frac{-x_i}{x_i-x_j}) \bmod q$。然后把 $y_G=g^{F(0)}\times\omega \bmod q$ 作为组的公钥。相应的组密钥为 $D=F(0)+\sum_{i=1}^{n}k_i \bmod q$。同理，利用多项式插值可得 $F(x)=(\sum_{i=1}^{n}F(x_i)\prod_{j=1,j\neq i}^{n}\frac{x-x_i}{x_i-x_j}) \bmod q$。公共信息：$U_i=g^{F(k_i)L_ix_i} \bmod N$，$(j=1,2,\cdots,n)$；其中 $L_i=\prod_{l=1,l\neq j}^{n+1-t}\frac{-k_l}{k_i-k_l}$ $(k_1,k_2,\cdots,k_n$ 为密钥生成阶段各参与者所选定的随机数)将公共信息广播。

2.3 代理权的委托过程

当原始签名人 P_0 同意将签名权委托给代理群时，原始签名人和代理群中的每个代理签名人 $P_i\in G_p$ 一起完成以下步骤：

(1) P_0 选取随机数 $\varepsilon\in Z_q$，计算

$u=g^{\varepsilon} \bmod N$　$\sigma=\varepsilon+x_0h(m_{w1}||u||y_G||y_0) \bmod q$

然后随机选择一个秘密多项式：

$f'(x)=\sigma+c_1x+\cdots+c_nx^n \bmod q$

其中 $c_i\in Z_q(i=1,2,\cdots,m)$，并计算

$b_i=f'(ID_i) \bmod q,(i=1,2,\cdots,n)$

$C_k=g^{c_k} \bmod N,(k=1,2,\cdots,n)$

$B_j=g^{f'(k_j)L_j} \bmod N,(j=1,2,\cdots,n+1-t)$

最后，分别秘密送 b_i 给每个 $P_i\in G_p$，公布所有(C_k,B_j,u,m_{w1})。

(2) 收到 b_i 后，每个 $P_i\in G_p$ 验证 $g^{b_i}=uy_0^{h(m_{w1}||u||y_G||y_0)}\prod_{j=1}^{n}C_j^{ij} \bmod N$。如等式成立，$P_i$ 计算 $\gamma_i=eb_i+x_ih(m_{w1}||u||y_G||y_0) \bmod q$ 作为它的代理子密钥。

2.4 代理签名的产生过程

设 $G_p=(P_1,P_2,\cdots,P_n)$中 t 个代理签名人 $G_t=(P_1,P_2,\cdots,P_t)$为消息 m 签名。代理签名产生过程如下：

(1)每个 $P_i\in G_t$ 选择随机数 $\beta_i,\delta_i\in Z_q$，计算 $R_i=g^{\beta_i}\delta_i \bmod N$，送 R_i 给代理群的签名生成者(可以是任意一个成员)。

(2) 签名生成者收到所有的 R_i 后，计算

$R=\prod_{i=1}^{t}R_i \bmod N$，送 R 给每个 $P_i\in G_t$。

(3) 每个 $P_i\in G_t$ 选择随机数 $\alpha_i\in Z_q$，计算

$v=(\prod_{j=1}^{n+1-t}U_j^{L_j'})^{h(m_{w1}||u||y_G||y_0)}(\prod_{j=1}^{n+1-t}B_j^{L_j'}) \bmod N$

$c=h(R||m)$

$S_{1i}=\beta_i-\gamma_iL_ic+\alpha_ie \bmod q$

$S_{2i}=\delta_ig^{-\alpha_i}V^{-c} \bmod N$，送$(S_{1i},S_{2i},c)$给签名生成者，其中 $L_j'=\prod_{l=1,l\neq j}^{t}\frac{ID_l}{k_j-ID_l}$，$L_i=\prod_{l=1,l\neq i}^{t}\frac{ID_l}{ID_i-ID_l}\prod_{l=1}^{n+1-t}\frac{-k_l}{ID_i-k_l}$。

(4)收到所有(S_{1i},S_{2i},c)后，签名生成者首先计算

$V=(\prod_{j=1}^{n+1-t}U_j^{L_j'})^{h(m_{w1}||u||y_G||y_0)}(\prod_{j=1}^{n+1-t}B_j^{L_j'}) \bmod N$

然后验证

$$g^{S_{1i}} S_{2i}^{e} = R_i \times \{[(u y_0^{h(m_{w1}\|u\|y_G\|y_0)} \prod_{j=1}^{n} C_j^{ID_i^j})^e (y_G \prod_{j=1}^{n} A_j^{ID_i^j})^{h(m_{w1}\|u\|y_G\|y_0)}]^{L_i} V^e\}^{-c} \bmod N \quad (1)$$

如果式(1)成立,签名生成者计算

$$S_1 = \sum_{i=1}^{t} S_{1i} \bmod q$$

$$S_2 = (\prod_{i=1}^{t} S_{2i}) V^{c(t-1)} \bmod N$$

然后签名生成者将代理签名$(S_1, S_2, c, u, m_{w1}, m)$发送给原始签名人,原始签名人核实后将$(S_1, S_2, c, u, m_{w1}, m_{w2}, m)$作为代理签名。

2.5 代理签名的验证过程

当收到代理签名$(S_1, S_2, c, u, m_{w1}, m_{w2}, m)$时,签名接收者首先计算

$$R' = [(u y_0^{h(m_{w1}\|u\|y_G\|y_0)})^e y_G^{h(m_{w1}\|u\|y_G\|y_0)}]^c g^{S_1} S_2^e \bmod N$$

然后验证

$$c = h(R' \| m) \quad (2)$$

如式(2)成立,代理签名$(S_1, S_2, c, u, m_{w1}, m_{w2}, m)$有效。

2.6 安全性验证

(1)签名生成者通过验证式(1)是否成立来确认代理签名人的个人代理签名是否有效

$$\begin{aligned} g^{S_{1i}} S_{2i}^{e} &= g^{\beta_i} g^{-\gamma_i L_i c} g^{\alpha_i e} \delta_i^e g^{-\alpha_i e} V^{-\alpha e} \\ &= R_i (g^{\phi_i} g^{x_i h(m_{w1}\|u\|)})^{-L_i c} V^{-\alpha e} \\ &= R_i \{[(u y_0^{h(m_{w1}\|u\|y_G\|y_0)} \prod_{j=1}^{n} C_j^{ID_i^j})^e (y_G \prod_{j=1}^{n} A_j^{ID_i^j})^{h(m_{w1}\|u\|y_G\|y_0)}]^{L_i} V^e\}^{-c} \bmod N \end{aligned}$$

(2)签名验证者通过验证式(2)是否成立来确认门限代理签名是否有效

记 $h = h(m_{w1}\|u\|y_G\|y_0)$

$$\begin{aligned} R' &= [(u y_0^h)^e y_G^h]^c g^{\sum_{i=1}^{t} S_{1i}} (\prod_{i=1}^{t} S_{2i}) V^{c(t-1)e} \\ &= [(u y_0^h)^e y_G^h]^c (\prod_{i=1}^{t} g^{\beta_i} \delta_i^e) g^{-\sum_{i=1}^{t} \gamma_i L_i c} V^{-\alpha e} \\ &= [(u y_0^h)^e y_G^h]^c R g^{-\sum_{i=1}^{t} (\phi_i L_i c + x_i h L_i c)} V^{-\alpha e} \\ &= [(u y_0^h)^e y_G^h]^c R g^{-\sum_{i=1}^{t} f'(ID_i) L_i c e} g^{-\sum_{i=1}^{t} f'(ID_i) L_i c h} (\prod_{j=1}^{n+1-t} U_j^{L_j'})^{-hce} (\prod_{j=1}^{n+1-t} B_j^{L_j'})^{-\alpha e} \\ &= [(u y_0^h)^e y_G^h]^c R (g_i^{\sum_{i=1}^{t} f'(ID_i) L_i + \sum_{j=1}^{n+1-t} f'(k_j) L_j L_j'})^{-\alpha e} \times \\ &\quad (g_i^{\sum_{i=1}^{t} f'(ID_i) L_i + \sum_{j=1}^{n+1-t} f'(k_j) L_j L_j'})^{-ch} \\ &= [(u y_0^h)^e y_G^h]^c R [(u y_0^h)^e y_G^h]^{-c} \\ &= R \bmod N \end{aligned}$$

3 方案对比与结论

3.1 方案对比

方案实现功能对比如表1所列。

表1 方案实现功能对比

	The schemes of references[2-8]	Our scheme
Withstand the conspiracy	No	Yes
Without a trusted party	No	Yes

3.2 结论

本文提出了一个安全的无可信中心的门限代理签名方案。该方案满足如下性质:(1)原始签名人不能伪造门限代理签名。这是因为原始签名人不知道代理签名人的秘密参数x_i,要想从y_i中解出x_i,相当于解离散对数问题。(2)抗合谋攻击。即使G_p中t个恶意群成员合谋,他们也不可能知道其他代理签名人的代理密钥,因为他们无法知道其他代理人P_i的$f_i(x_i)$和随机数k_i,因此也就无法伪造其他代理人签名。其安全性基于离散对数问题。对于t个恶意群成员恶意代理原始签名人签名的情况,采用了原始签名人两授权的解决方案,只有经过两次授权的签名才有效,这只需要维护签名生成者和原始签名人之间的一条安全信道。(3)未被委托的群体不能假冒一个合法的代理群产生有效的门限代理签名,这是因为未被委托的群体不知道代理群的秘密参数。其安全性基于Shamir的(t,n)门限方案的安全性和大整数分解问题。

参考文献

[1] 徐静. 标准模型下可证安全的门限签名方案[J]. 计算机学报, 2006,29(9):1636-1640

[2] Kim S, Park S, Won D. Proxy signature[C]// ICICS'97, Lecture Notes in Computer Science. Berlin, Springer, 1997, 1334: 223-232

[3] Zhang K. Threshold proxy signature scheme[C]// 1997 Information Security Workshop. Tokyo, Japan, September 1997: 191-197

[4] Sun H M. An efficient nonrepudiable threshold proxy signature scheme with known signers[J]. Computer Communication, 1997,22(8):717-722

[5] Hwang M S, Lu J L, Lin L C. A practical(t,n) threshold proxy signature scheme based on the RSA cryptosystem[J]. IEEE Trans. on Knowledge and Data Engineering, 2003,15(6):1552-1560

[6] Sun H M, Lee N Y, Hwang T. Threshold proxy signatures[J]. IEE Proc-Computers and Digital Techniques, 1999,146(5):259-263

[7] Hsu C L, Wu T S, Wu T C. New nonrepudiable threshold proxy signature scheme with known signers[J]. Journal of Systems and Software, 2001,58(9):119-124

[8] Lee N Y, Hwang T, Wang C H. On Zhang's nonrepudiable proxy signatures[C]// ACISP'98, Lecture Notes in Computer Science. Berlin: Springer, 1998:414-422

[9] 蒋瀚,徐秋亮,周永彬. 基于RSA密码体制的门限代理签名[J]. 计算机学报,2007,30(2):241-247

[10] 鲁荣波,何大可,王长吉. 一种门限代理签名方案的分析与改进[J]. 电子学报,2007,35(1):145-149

[11] 王斌,李建华. 无可信中心的(t,n)门限签名方案[J]. 计算机学报,2003,26(11):1581-1584

[12] 郭丽峰,程相国. 一个无可信中心的(t,n)门限签名方案的安全性分析[J]. 计算机学报,2006,29(11):2013-2016

[13] 王晓明,张震,符方伟. 一个安全的门限代理签名方案[J]. 电子与信息学报,2006,28(7):1308-1311