一种门限代理签名方案的分析与改进

鲁荣波[1,2], 何大可[2], 王常吉[3]
(1. 吉首大学数学与计算机科学学院, 湖南吉首 416000; 2. 西南交通大学信息安全与国家计算网格实验室, 四川成都 610031; 3. 中山大学计算机科学系, 广东广州 510275)

摘 要: 通过对 Qian-cao-xue 的基于双线性映射的的门限代理签名方案分析, 发现该方案并不满足强不可伪造性, 任何人包括原始签名人可以伪造一个有效的代理签名, 同时该方案也不能抵抗原始签名人改变攻击. 在此基础上提出了改进的门限代理签名方案(方案 1), 改进的方案克服了原方案的安全缺陷. 并把矢量空间秘密共享和多重代理签名结合起来, 构建了一种更为广泛的基于访问结构的多重代理签名(方案 2). 门限代理签名方案(方案 1) 成为方案 2 的特殊情形. 方案 2 中任何参与者的授权子集能产生多重代理签名, 而非参与者不可能产生有效的多重代理签名, 接收者可以通过验证方法验证个体代理签名和多重代理签名的合法性, 而且能保证任何参与者都能检测出错误的子秘密. 能抵御各种可能的攻击.

关键词: 门限代理签名; 双线性映射; 强不可伪造性; 原始签名人改变攻击; 矢量空间秘密共享
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2007) 01-0145-05

Cryptanalysis and Improvement of a Threshold Proxy Signature Scheme from Bilinear Pairings

LU Rong-bo[1,2], HE Da-ke[2], WANG Chang-ji[3]
(1. *College of Math and Computer Science, Jishou University, Jishou, Hunan 416000, China;*
2. *Laboratory of Information Security and National Computing Gird, Southwest Jiaotong University, Chengdu, Sichuan 610031, China;*
3. *Department of Computer Science, Sun Yat-Sen University, Guangzhou, Guangdong 510275, China*)

Abstract: Present a security analysis of the Qian-cao-xue's new threshold proxy signature scheme from bilinear pairings, which does not posses the strong unforgeability property, anyone including original signer can forge a valid threshold proxy signature for any message, at the same time, this scheme can't resist original signer changing attack. An improved threshold proxy signature scheme (denoted as scheme one) is proposed, which can resolve the security problem existing in the Qian-cao-xue's new threshold proxy signature scheme. Based on scheme one, by combining vector space secret sharing with multi-proxy signature, a new and wider multi-proxy signature (denoted as scheme two) is constructed. Then scheme one becomes the typical representative of scheme two. In scheme two, the multi-proxy signature can be easily produced if an authorized subset of participants pool their secret shares, and it is impossible for them to generate a multi-proxy signature if an unauthorized subset of participants pool their secret shares. The validity of the partial signature and the multi-proxy signature can be verified by means of verification equations. Moreover the suspected forgery can be traced and the malicious participants can be caught. None of the possible attacks can successfully break this scheme.

Key words: threshold proxy signature; bilinear pairing; strong unforgeability; original signer changing attack; vector space secret sharing

1 引言

自从 2001 年 Boneh 等提出了基于双线性对的短签名[1]之后, 双线性对成了构造签名的重要工具. 由双线性对构造的签名方案具有签字短、安全、高效等特点, 所以, 一经提出就引起了广泛的关注. 此后, 又有不少学者在这方面进行了研究[2,6].

代理签名[4]是指某人授权其他人替自己行使签名权的一种签名. 目前, 人们已经提出了若干不同类型的代理签名方案[6]. 在代理签名的应用中, 有时需要多个授权参与者共同签署一个代理签名, 这就是多重代理签名[3]. 为了解决代理签名的可跟踪性及确认代理签名确实来自一个参与者授权子集这两个问题, 有时必须把秘密共享签名方案和多重代理签名方

收稿日期: 2005-12-12; 修回日期: 2006-08-14
基金项目: 国家自然科学基金(No. 60503005)

案结合起来,即构造秘密共享多重代理签名方案[5].但到目前为止,所构造的秘密共享多重代理签名方案[5,9]大都是基于Shamir(t, n)门限签名的,其中 n 为参与者的个数,t 为门限值.对于实际应用而言,基于访问结构[7,8]的密码体制具有更广的应用范围.

文献[9]基于GDH签名(短签名方案)首次构造了一种基于双线性对的门限代理签名(以下简称Qian-cao-xue方案).本文分析了Qian-cao-xue方案的安全性,指出该方案并不满足强不可伪造性,同时该方案不能抵抗原始签名人改变攻击.对此,文章提出了改进的方案(方案1).在方案1的基础上进一步构建了一种新的基于访问结构的秘密共享多重代理签名体制(方案2).门限代理方案(方案1)是方案2的特殊情形.

2 预备知识

2.1 双线性映射

设 G_1, G_2 分别是同为 q 阶的加群和乘群,P 为 G_1 的生成元.在群 G_1, G_2 中,离散对数问题是难解的.可定义双线性映射为 $e: G_1 \times G_1 \rightarrow G_2$,并满足双线性性、非退化性和可计算性三种特性.对于这样定义的 G_1,我们可以定义离散对数问题(DLP)、可计算Diffie-Hellman问题(CDHP)、可判定Diffie-Hellman问题(DDHP)、Gap Diffe-Hellman(GDH)问题等难解问题,并称具有CDH问题难解而DDH问题易解特征的群为GDH群.有关详细内容可参看文献[1].

2.2 矢量空间秘密共享

矢量空间构造是一种针对访问结构构造某些理想方案的方法,有关矢量空间秘密共享构造方法可参看文献[7].Shamir方案即(t, n)门限方案是矢量空间秘密共享的一个特例[8].

3 Qian-cao-xue方案及分析

3.1 初始阶段

群 G_0 和 G_1 的阶数为素数 q,P 为GDH群 G_0 的生成元,$e: G_0 \times G_1 \rightarrow G_1$ 为一个安全的双线性对.两个hash函数 $H_1: \{0,1\}^* \times G_0 \rightarrow Z_q^*$, $H_2: \{0,1\}^* \rightarrow G_0 \setminus \{1\}$.原始签名人 O 任选 $x_0 \in Z_q^*$, $pk_0 = Y_0 = x_0 P$ 为其公钥,代理签名人 p_i($i = 1, \cdots, n$)任选 $x_i \in Z_q^*$, $pk_i = Y_i = x_i P$ 为相应的公钥.

3.2 代理密钥生成

(1) O 任选 $r \in Z_q^*$,计算 $U = rP$, $h = H_1(m_w, U)$, $Q = H_2(m_w)$, $V = (r + hx_A)Q$, $s = n^{-1}(hr + x_0)$,其中 m_w 为代理授权证书.O 将(σ, s)和 m_w 发送给每个 p_i.

(2) 每个 p_i 验证: $e(P, V) = e(U + hY_0, H_2(m_w))$

$$nsP = hU + Y_0$$

若成立,接受(σ, s).并任选 $k_i \in Z_q^*$,公开 $k_i P$,计算 $s_i = s + x_i + k_i$ 为自己的代理秘密.

(3) p_i 任选系数在 Z_q 中、次数为 $t-1$ 的多项式 $f_i(z)$ 并使 $f_i(0) = s_i = a_{i,0}$ 即 $f_i(z) = s_i + a_{i,1}z + a_{i,2}z + \cdots + a_{i,t-1}z^{t-1}$,广播 $a_{i,j}P$ ($j = 1, 2, \cdots, t-1$).将 $f_i(j)$ 秘密发送给 p_j ($j = 1, \cdots, n$, $j \neq i$).

(4) p_i 从 p_j 那里收到 $f_j(i)$ ($j = 1, 2, 3, \cdots, n$, $j \neq i$),验证 $f_j(i)P = \sum_{k=0}^{t-1} i^k a_{j,k} P$ 是否成立,若成立,p_i 计算 $x_i' = \sum_{k=1}^{n} f_k(i)$,公开 $Y_i' = x_i' P$.若令 $f(z) = \sum_{i=1}^{n} f_i(z)$,则 $x_i' = f(i)$.

3.3 代理签名生成

设 m 为要签名的消息,p_i($i = 1, 2, \cdots, t$)为 t 个代表原始签名人对消息 m 进行代理签名.

(1) p_i($i = 1, 2, \cdots, t$)计算 $w_i = \prod_{j=1, j\neq i}^{t} j/(j-i)$,得到部分签名 $\sigma_i = x_i' w_i H_2(m)$.

(2) t 个代理签名人一起验证: $e(P, \sigma_i) = e(w_i Y_i', H_2(m))$若通过,则合作产生 $\sigma' = \sum_{i=1}^{t} \sigma_i$, $K = \sum_{m=1}^{n} k_m P$.得到代理签名(m, U, m_w, σ', K).

3.4 代理签名验证

代理签名的接收人可以用下面的等式进行验证:

$$e(P, \sigma') = e(H_1(m_w, U)U + Y_0 + K + \sum_{i=1}^{n} Y_i, H_2(m))$$

3.5 强不可伪造性分析

任何人(包括原始签名人)可以按照下面步骤伪造一个 p_i ($i = 1, \cdots, m$)代表 O 对消息 m' 的代理签名(m', U', m_w, σ'', K').

① 伪造者 C 任选 $r' \in Z_q^*$,计算 $U' = r'P$, $h = H_1(m_w, U')$,其中 m_w 可从公开渠道获得.

② C 任选 $\alpha \in Z_q^*$,令 $K' = \alpha P - \sum_{i=0}^{n} Y_i - H_1(m_w, U')U'$,计算 $\sigma'' = \alpha H_2(m')$.则($m'$, U', m_w, σ'', K')为有效的代理签名.这是因为:

$$e(P, \sigma'') = e(P, \alpha H_2(m')) = e(\alpha P, H_2(m'))$$

$$= e(K' + \sum_{i=0}^{n} Y_i + H_1(m_w, U')U', H_2(m'))$$

$$= e(K' + Y_0 + \sum_{i=1}^{n} Y_i + H_1(m_w, U')U', H_2(m'))$$

即: $e(P, \sigma'') = e((Y_0 + H_1(m_w, U')U' + K' + \sum_{i=1}^{n} Y_i, H_2(m)))$成立.

3.6 原始签名人改变攻击分析

如果 p_i($i = 1, \cdots, n$)独立地获得了两个原始签名人 O 和 O' 的代理授权(这种情况在现实应用中是很常见的),并且代理签名人已经生成了一个代表 O 的有效的代理签名(m, U, m_w, σ', K).那么 O' 可以按照以下方法伪造一个原始签名人为自己的代理签名.

(1) 初始化: O' 的私钥为 $x_o' \in Z_q^*$, $pk_o' = Y_o' = x_o' P$ 为相应的公钥.代理签名人为 p_i($i = 1, \cdots, n$),对应有授权证书 m_w',授权参数与 m_w 相同(更进一步,O' 甚至可以按照 m_w 的格式伪造这样的授权证书 m_w').O' 从公开渠道获得代理签名人生成的代表 O 的代理签名(m, U, m_w, σ', K)以及(σ, s).

(2) O' 随机选择 $r' \in Z_q^*$,计算 $U' = r'P$, $h' = H_1(m_w', U')$,

(3) 令 $\sigma'' = \sigma' + (x'_o + h'r' - ns)H_2(m)$, 则 $(m, U', m'_w, \sigma'', K)$ 为一个有效的代理签名. 因为:

$$\begin{aligned} e(P, \sigma'') &= e(P, \sigma' + (x'_o + h'r' - ns)H_2(m)) \\ &= e(P, \sum_{i=1}^{t} \sigma_i + (x'_o + h'r' - ns)H_2(m)) \\ &= e(P, \sum_{i=1}^{t} x'_i w_i H_2(m) + (x'_o + h'r' - ns)H_2(m)) \\ &= e(P, f(0)H_2(m) + (x'_o + h'r' - ns)H_2(m)) \\ &= e(P, \sum_{i=1}^{n} f_i(0)H_2(m) + (x'_o + h'r' - ns)H_2(m)) \\ &= e(P, (ns + \sum_{i=1}^{n}(x_i + k_i))H_2(m) + (x'_o + h'r' - ns) \\ &\quad \cdot H_2(m)) \\ &= e(P, (x'_o + h'r' + \sum_{i=1}^{n}(x_i + k_i))H_2(m)) \\ &= e((x'_o + H_1(m'_w, U')r')P + \sum_{i=1}^{n}(x_i + k_i)P, H_2(m)) \\ &= e((Y'_o) + H_1(m'_w, U')U' + K + \sum_{i=1}^{n} Y_i, H_2(m)) \end{aligned}$$

这样, O' 就成功地伪造了一个原始签名人为自己, 代理签名人为 $p_i (i = 1, \cdots, n)$ 的对消息 m 的门限代理签名 $(m, U', m'_w, \sigma'', K)$.

4 改进的方案(方案 1)

4.1 初始阶段

在 Qian cao xue 方案的基础上增加 $H_3: \{0, 1\}^* \times G_0 \rightarrow G_0 \setminus \{1\}$.

4.2 代理密钥生成

(1) 同 3.2 节(1).

(2) 同 3.2 节(2)一样, 首先每个 p_i 验证 m_w 的合法性后, 然后 p_i 随机选择 $k_i \in Z_q^*$, 公开 k_iP, 计算 $K = \sum_{m=1}^{n} k_m P$, 计算 $s_i = s + x_i + k_i H_1(K)$ 作为自己的代理秘密.

(3) p_i 任选系数在 Z_q 中、$t-1$ 次多项式 $f_i(z)$, 使 $f_i(0) = s_i = a_{i,0}$ 即 $f_i(z) = s_i + a_{i,1}z + a_{i,2}z + \cdots + a_{i,t-1}z^{t-1}$, 广播 $a_{i,j}P (j = 1, 2, \cdots, t-1)$, 将 $f_i(j)$ 秘密发送给 $p_j (j = 1, \cdots, n, j \neq i)$.

(4) p_i 从 p_j 那里收到 $f_j(i) (j = 1, 2, \cdots, n, j \neq i)$ 验证等式: $f_j(i)P = \sum_{k=0}^{t-1} i^k a_{j,k} P$, 若成立, p_i 计算 $x'_i = \sum_{k=1}^{n} f_k(i)$, 和广播 $Y'_i = x'_i P$. 令 $f(z) = \sum_{i=1}^{n} f_i(z)$, 则 $x'_i = f(i)$, $Y'_i = x'_i P$.

4.3 代理签名生成

设 m 为要签名的消息, $p_i (i = 1, 2, \cdots, t)$ 为 t 个实际参与签名的代理签名人.

(1) $p_i (i = 1, 2, \cdots, t)$ 计算 $w_i = \prod_{j=1, j\neq i}^{t} j/(j - i)$ 得到消息的部分签名 $\sigma_i = x'_i w_i H_3(m, U)$.

(2) $p_i (i = 1, 2, \cdots, t)$ 验证: $e(P, \sigma_i) = e(w_i Y'_i, H_3(m, U))$ 若通过, 则计算 $\sigma' = \sum_{i=1}^{t} \sigma_i$, 得到代理签名 (m, U, m_w, σ', K)

4.4 代理签名验证

代理签名的接收人可用下面的等式验证代理签名的有效性:

$$\begin{aligned} e(P, \sigma') = e(&H_1(m_w, U)U + Y_0 + H_1(K)K \\ &+ \sum_{i=1}^{n} Y_i, H_3(m, U)) \end{aligned}$$

4.5 新方案分析

4.5.1 可验证性

签名验证过程的正确性可由如下方程给出:

$$\begin{aligned} e(P, \sigma') &= e(P, \sum_{i=1}^{t} \sigma_i) = e(P, \sum_{i=1}^{t} x'_i w_i H_3(m, U)) \\ &= e(P, f(0)H_3(m, U)) = e(P, \sum_{i=1}^{n} f_i(0)H_3(m, U)) \\ &= e(P, (ns + \sum_{i=1}^{n}(x_i + k_i H_1(K))H_3(m, U)) \\ &= e(P, (H_1(m_w, U)r + x_0 + \sum_{i=1}^{n}(x_i + k_i H_1(K))H_3(m, U)) \\ &= e((H_1(m_w, U)r + x_0 + \sum_{i=1}^{n}(x_i + k_i H_1(K))P, H_3(m, U)) \\ &= e(H_1(m_w, U)U + Y_0 + H_1(K)K + \sum_{i=1}^{n} Y_i, H_3(m, U)) \end{aligned}$$

4.5.2 强不可伪造性

部分签名中 p_i 使用的是抗选择消息攻击下安全的 GDH 短签名, 代理签名私钥是保密的, 伪造者不知道代理签名人的代理私钥, 因此不可能伪造出部分签名; 伪造者 C 试图按照 3.1 节的方法对代理签名进行全局伪造: C 首先任选 $r' \in Z_q^*$, 计算 $U' = r'P$, $h = H_1(m_w, U')$, 任选 $\alpha \in Z_q^*$, 计算 $\sigma'' = \alpha H_3(m', U)$, 如果能寻找合适的 K' 满足: $H_1(K')K' = \alpha P - \sum_{i=0}^{n} Y_i - H_1(m_w, U')U'$, 那么 $(m', U, m_w, \sigma'', K')$ 为一个有效的代理签名, 但由哈希函数的性质知道, C 是无法计算出满足该等式的 K'. 由以上分析可以得出结论, 任何人包括原始签名人都不可能伪造一个有效的代理签名.

4.5.3 抗原始签名人改变攻击

由 $e(P, \sigma'') = e((Y'_o + H_1(m'_w, U')U' + K + \sum_{i=1}^{n} Y_i, H_2(m))$ 的证明过程可以看出, 原始签名人改变攻击成功的原因是在代理签名产生过程中并没有使用原始签名人合法产生并签名了的授权证书, 伪造者可以通过公开信道获得 (σ, s), 来选择适当的 σ'', 进而在验证过程中消去 ns (详见 3.2 节). 改进方案引入了一个新的哈希函数 H_3, 通过计算 $H_3(m, U)$ 来确保在代理签名生成阶段, 使用到原始签名人合法产生的签名了的授权证书 m_w, 这样就保证了原始签名人在签名产生过程中不会被更换, 而且无需使用安全信道发送 (σ, s).

其可区分性、强可识别性、强不可否认性以及抗滥用性等分析详见文献[9].

5 方案 1 的推广(方案 2)

5.1 系统初始化

设 $P = \{p_1, p_2, \cdots, p_n\}$ 是所有的代理签名者的集合, 有访

问结构 $\Omega=\{A_1, A_2, \cdots, A_\lambda\}$, 其中, $A_j\subset\Omega$ 是授权子集, $1\leqslant j\leqslant\lambda$. 其余的同 4.1 节.

5.2 代理密钥生成

(1)(2) 同方案 1(见 4.2(1)和 4.2(2)节)

(3) 每一个参与者 p_i, $p_i\in P$, 随机选择 $v_{2i}, v_{3i}, \cdots, v_{ri}\in K_0$. 令 $v_i=(v_{1i}, v_{2i}, \cdots, v_{ri})$, 其中, $v_{1i}=s_i$. 则 $v_i\bullet\varphi(D)=s_i$, 计算 $w_{ij}=v_i\bullet\varphi(p_i)$, 这里 φ 是公开的, v_i 以及 w_{ij} 均保密. 假设 $A=\{p_1, p_2, \cdots, p_t\}$ 是一个授权子集, 则有 $\varphi(D)=c_1\varphi(p_1)+c_2\varphi(p_2)+\cdots+c_t\varphi(p_t)$, 这里, $0<c_i<q$ 可被任何参与者计算, 此时当 $p_i\notin A$, 秘密 $s_i=c_1w_{i1}+c_2w_{i2}+\cdots+c_tw_{it}$, 并通过安全信道分配给 $p_j(p_j\in P, j\neq i)$ 子秘密 w_{ij}. p_i 公开 $z_i=s_iP=(s+x_i+k_i)P$ 与 $w_{ij}P(j: p_j\in P, j\neq i)$.

(4) p_i 计算 $x_i'=\sum_{j:p_j\in P, p_j\notin A}w_{ji}$, 公开 $Y_i'=x_i'P$.

5.3 代理签名的生成

(1) $p_i(i=1, 2, \cdots, l)$ 计算 $\sigma_i=(s_i+x_i'c_i)H_3(m, U)$.

(2) t 个代理签名人收集到 σ_i 后, 可用式 $e(P, \sigma_i)=e(c_iY_i'+z_i, H_3(m, U))$ 验证 σ_i 的有效性. 因为:

$$\begin{aligned}e(P, \sigma_i)&=e(P, s_i+x_i'c_iH_3(m, U))\\&=e((s_i+x_i'c_i)P, H_3(m, U))\\&=e(c_iY_i'+z_i, H_3(m, U))\end{aligned}$$

每个部分签名通过验证后, 则合作产生代理签名(m, U, m_w, σ', K), 其中: $\sigma'=\sum_{i=1}^{t}\sigma_i$.

5.4 代理签名的验证

代理签名的接收人可用下面的等式验证代理签名的有效性:

$$e(P, \sigma')=e(H_1(m_w, U)U+Y_0+H_1(K)K+\sum_{i=1}^{n}Y_i, H_3(m, U)).$$

实际上, (t, n) 门限代理签名方案(方案 1)是方案 2 的特殊情况, 因为只需令 $c_i=\prod_{j=1, j\neq i}^{t}j/(j-i)$, 即可, 此时 $|A|=t$.

5.5 方案 2 的安全性分析

方案 2 的安全性基于求解椭圆曲线上离散对数问题和矢量空间秘密共享方案的安全性之上, 是方案 1 的推广, 继承了方案 1 和 Qian-caor-xue 方案的优点. 其全局不可伪造分析和抗原始签名人改变攻击分析见方案 1, 其可区分性、强可识别性、强不可否认性以及抗滥用性等分析详见文献[9].

(1) 签名验证过程的正确性可由如下方程给出:

$$\begin{aligned}e(P, \sigma')&=e(P, \sum_{i=1}^{t}\sigma_i)=e(P, \sum_{i=1}^{t}(s_i+x_i'c_i)H_3(m, U)\\&=e(P, \sum_{i=1}^{t}(s_i+c_i\sum_{j:p_j\in P, p_j\notin A}w_{ji})H_3(m, U))\\&=e(\sum_{i=1}^{t}s_iP+\sum_{i=1}^{t}(c_i\sum_{j:p_j\in P, p_j\notin A}w_{ji})P, H_3(m, U))\\&=e(\sum_{i=1}^{t}s_iP+\sum_{j:p_j\in P, p_j\notin A}s_jP, H_3(m, U))\\&=e(\sum_{i=1}^{n}s_iP, H_3(m, U))\\&=e(\sum_{i=1}^{n}(s+x_i+kH_1(K))P, H_3(m, U))\\&=e(H_1(m_w, U)U+Y_0+H_1(K)K+\sum_{i=1}^{n}Y_i, H_3(m, U))\end{aligned}$$

(2) 伪造者通过求解 s_iP, $w_{ji}P$ 得到 s_i 和 w_{ji} 的难度等同于求解椭圆曲线上离散对数的难度, 由于无法得到 s_i 和 w_{ji}, 从式 $(s_i+c_i\sum_{j:p_j\in P, p_j\notin A}w_{ji})H_3(m, U)$ 中求 $(s_i+c_i\sum_{j:p_j\in P, p_j\notin A}w_{ji})$ 是解离散对数问题, 因此很难找到合适的值 s_i' 和 w_{ji}', 使它满足 $(s_i'+c_i\sum_{j:p_j\in P, p_j\notin A}w_{ji}')H_3(m, U)=(s_i+c_i\sum_{j:p_j\in P, p_j\notin A}w_{ji})\bullet H_3(m, U)$.

(3) 如果不诚实的参与者 p_j 发送给 p_i 一个伪子秘密 w_{ji}', 并公开 $w_{ji}'P$, 根据关系式 $s_j=\sum_{i=1}^{t}c_iw_{ji}$, 任意 p_i 能够根据等式 $\sum_{i:i\in A}c_iw_{ji}P=s_jP=$ 来验证 p_j 是否是欺诈者, 若等式不成立, 则 p_i 确定是 p_j 欺诈者.

(4) 为了检测 p_i 收到来自 p_j 的子秘密 w_{ji}' 是否因为通信传输而产生了错误, 可通过检测 $w_{ji}'P$ 与公开的值是不是相等. 若不等, 则 w_{ji}' 是一个因通信传输产生的错误子秘密.

(5) 由式 $\sigma_i=(s_i+x_i'c_i)H_3(m, U)$ 是不能求得 x_i' 的, 因为未知数的个数总比能得到的方程个数多; 同样的原因, 从 $\sigma'=\sum_{i=1}^{t}\sigma_i=\sum_{i=1}^{t}(s_i+c_i\sum_{j:p_j\in P, p_j\notin A}w_{ji})H_3(m, U)$ 中不能恢复出秘密 s_i. 由矢量空间秘密共享的安全性, 任何小于门限人数的参与者的联合不能重构代理秘密 s_i 和 $v_i=(v_{1i}, v_{2i}, \cdots, v_{ri})$, 只有授权子集内的成员可以生成有效的多重代理签名, 只有授权子集才能正确的重构秘密 s_i. 由秘密共享的性质可知, 它可以挫败任何来自授权子集外的假冒攻击. 这一点可由门限方案的性质保证[7, 8].

6 结束语

本文首先分析了 Qian-caor-xue 方案的安全性, 指出该方案并不满足强不可伪造性, 同时该方案不能抵抗原始签名人改变攻击, 并提出了改进的方案(方案 1). 改进方案克服了原方案的安全缺陷. 在此基础上, 构建了一种更为广泛的基于访问结构的多重代理签名(方案 2). 方案 1 是方案 2 的特殊情形. 方案 2 能保证参与者的授权子集能容易地产生多重代理签名, 而参与者的非授权子集不可能产生有效的多重代理签名, 验证者可通过验证方案验证个体签名和多重代理签名的合法性. 任何参与者都能检测出错误的子秘密, 可以跟踪被怀疑的伪造者. 由于基于访问结构, 所以比基于一般秘密共享机制的多重代理签名具有更广泛的应用前景.

参考文献:

[1] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[A]. Advances in Cryptology-Asiacrypt2001[C]. LNCS

2248. Springer-Verlag, 2001. 514- 532

[2] Boneh D, Boyen X, Shacham H. Short group signatures[A]. Advances in Cryptology-CRYPTO2004 [C]. LNCS 3152. Berlin: Springer-Verlag, 2004. 41- 59.

[3] Hwang S J, Shi Ch. A simple multi-proxy signature scheme [A]. In: Proceedings of the 10th National Conference on Information Security[C]. Taiwan, 2000. 134- 138.

[4] Mambo M, Usuda K, Okamoto E. Proxy signature: Delegation to sign messages[J]. IEICE Transactions on Fundatamentals, 1996, E79-A(9): 1338- 1354.

[5] K Zhang. Threshold proxy signature schemes[A]. In: Proc of the 1st Int l Information Security Workshop (ISW 97) [C]. LNCS 1396. Springer-Verlag, 1997. 191- 197.

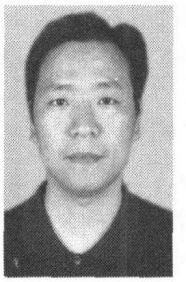
[6] Zhang F, Safavi-Naini R, Lin C Y. New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairing[OL]. http://eprint.iacr.org/2003/104.

[7] Padro C, Saez G. Detection of cheater s in vector space secret sharing schemes[J]. Journal of Designs, Codes and Cryptography, 1999, 16(1): 75- 85.

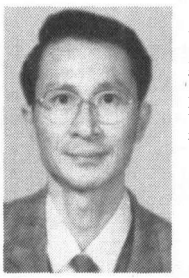
[8] 许春香, 董庆宽, 肖国镇. 矢量空秘密共享多重数字签名[J]. 电子学报, 2003, 31(1): 48- 50.
XU Chun-xiang, DONG Qing-kuan, XIAO Guo-zhen. A vector space secret sharing multisignature scheme[J]. Acta Electronica Sinica, 2003, 31(1): 48- 50. (in Chinese)

[9] QIAN Haifeng, CAO Zhenfu, XUE Qingshui. A new threshold proxy signature scheme from bilinear pairings[J]. Science in China Ser. F Information Sciences, 2004, 47(5): 612- 622.

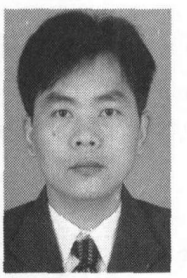
作者简介:



鲁荣波　男, 1970 年出生于湖南省慈利县, 湖南吉首大学副教授, 西南交通大学博士研究生. 主要研究方向信息安全、电子支付. E-mail: lurongbo8563@163.com



何大可　男, 1944 年 9 月出生于重庆, 西南交通大学教授, 博士生导师, 四川省重点实验室信息安全与国家计算网格实验室主任, 主要研究方向网络安全、信息安全、电子支付、并行计算.



王常吉　男, 1972 年 2 月出生于湖南省衡山, 博士后, 中山大学副教授, 主要研究方向电子支付和密码学理论与应用.