

文章编号:1001-9081(2006)07-1634-03

Feng-Yuan 不可否认门限代理签名方案的改进

谢 琪

(杭州师范学院 信息工程学院, 浙江 杭州 310036)

(qixie68@yahoo.com.cn; qixie@hztc.edu.cn)

摘 要: Feng-Yuan 指出 Hsu 等的门限代理签名方案不具有不可否认性, 同时给出了具有不可否认性的改进方案。指出 Feng-Yuan 的改进方案无法抵抗内部成员的合谋攻击, 从而无法实现可识别性和不可否认性。进一步, 给出了改进方案以弥补该方案的安全性缺陷。

关键词: 代理签名; 门限代理签名; 合谋攻击

中图分类号: TP309 **文献标识码:** A

Improvement of Feng-Yuan nonrepudiable threshold proxy signature scheme

XIE Qi

(School of Information and Engineering, Hangzhou Teachers College, Hangzhou Zhejiang 310036, China)

Abstract: Feng-Yuan pointed out that Hsu et al.'s threshold proxy signature scheme lacks of undeniability, and proposed an improvement scheme with nonrepudiation. A conspiracy attack on Feng-Yuan's improvement scheme shows that their scheme suffered from forgeability, unidentifiability and deniability. Furthermore, an improved scheme was presented to remedy the security weakness of Feng-Yuan's scheme.

Key words: proxy signature; threshold proxy signature; conspiracy attack

0 引言

1996 年, 文献[1]首次提出了代理签名的概念, 一个代理签名方案允许原始签名人把自己的签名权交给指定的代理人(称为代理签名人), 代理签名人能够代表原始签人生成有效的代理签名。为防止滥用代理签名权, 1997 年文献[2]和文献[3]提出了 (t, n) 门限代理签名方案, 原始签名人把代理签名密钥分割成 n 份并分发给 n 个代理签名人, 它要求 n 个代理签名人中至少 t 个人的合作才能生成代表原始签名人的代理签名, 但是 $t-1$ 个以下的代理签名人则不行。

考虑到当代理签名发生争议时, 仲裁者必须知道谁是代理签名的真正签名者, 所以代理签名具有不可否认性是个十分重要的性质。1999 年, 文献[4]提出了具有已知签名人的不可否认门限代理签名方案, 文献[5]指出文献[4]的方案无法抵抗合谋攻击并给出了一个改进方案。2004 年, 文献[6]提出了一个效率优于文献[5]的不可否认门限代理签名方案。文献[7]指出文献[5]和文献[6]的方案都无法抵抗伪造攻击, 并给出了改进方案。2000 年, 基于文献[2]的方案文献[8]提出了一个不可否认门限代理签名方案, 然而文献[9]给出了原始签名人与一个代理签名人的合谋攻击方案表明他们的方案是不安全的, 文献[10]给出了一个更有效的攻击方案——原始签名人的假冒攻击, 指出了文献[8]的缺陷, 并给出了改进方案。文献[11]指出文献[10]的方案无法抵抗伪造攻击, 并给出了改进方案。

1999 年, 文献[12]提出了一个门限代理签名方案, 文献[13]指出文献[12]的方案违背了门限代理的原则, 他们的方案中代理签名的产生不一定完全遵守规定门限值, 并给出了

一个改进方案。2005 年, 文献[14]指出文献[5]的门限代理签名方案不具有不可否认性, 同时给出了具有不可否认性的改进方案。本文指出, 文献[14]的方案无法抵抗合谋攻击, 同时给出了改进方案, 克服了该方案的安全性缺陷。

1 Feng-Yuan 方案简介

设 p 和 q 是两个大素数, 满足 $q \mid (p-1)$, 随机选取 q 阶生成元 $g \in Z_p^*$ 。设 P_0 是原始签名人, $G = \{P_1, P_2, \dots, P_n\}$ 是 n 个代理签名人, 每个用户 P_i 的私钥为 $x_i \in Z_q^*$, 公钥为 $y_i = g^{x_i} \bmod p$, 并得到 CA 的认证。PGID = {EM, Time, Group} 记录代理人的身份, 其中 EM 表示代理密钥产生的标记包括参数 t 和 n , Time 表示代理签名的有效期限, Group 表示原始签名人和代理签名人的身份信息。ASID 表示实际签名群中的身份信息, $h(\cdot)$ 是单向抗碰撞 Hash 函数。Feng-Yuan 的方案由代理密钥产生阶段、代理签名产生与验证 3 个阶段组成。

1.1 代理密钥产生阶段

- 1) P_0 随机选取 $\tilde{k} \in_R Z_q$, 计算并广播 $\tilde{r} = g^{\tilde{k}} \bmod p$ 。
- 2) 每个 $P_i \in G$, 随机选取 $\alpha_i \in_R Z_q$, 计算 $r_i = g^{\alpha_i} \tilde{r} \bmod p$, 使得 $r_i \in Z_p^*$ 成立, 然后广播 r_i 。
- 3) P_0 计算 $r = \prod_{i=1}^n r_i$, $\tilde{s} = x_0 h(r, PGID) + n\tilde{k} \pmod{q}$, 然后选择一个 $t-1$ 阶的秘密多项式 $f''(x) = \tilde{s} + \sum_{i=1}^{t-1} \alpha_i'' x^i \bmod q$, 计算 $\tilde{s}_i = f''(i)$, 并通过安全的通道把 \tilde{s}_i 发送给 P_i , 同时公布 $c_i'' = g^{\alpha_i''} \bmod p$ 。
- 4) 每个 $P_i \in G$, 计算 $r = \prod_{i=1}^n r_i$, 并通过下式检查 \tilde{s}_i 的正确性:

收稿日期: 2006-01-15; 修订日期: 2006-03-02

基金项目: 浙江省自然科学基金资助项目(Y105067); 浙江省教育厅科技计划项目(0561XP49)

作者简介: 谢琪(1968-), 男, 浙江上虞人, 副教授, 博士, 主要研究方向: 密码学、信息安全。

$$g^{x_i} = y_0^{h(r, PGID)} \tilde{r}^n \prod_{j=1}^{t-1} (c_j^n)^j \bmod p \quad (1)$$

5) 每个 $P_i \in G$, 产生一个 $t-1$ 阶的秘密多项式:

$$f_i(x) = \alpha_i + x_i h(r, PGID) + \sum_{k=1}^{t-1} a_{(i,k)} x^k \bmod q \quad (2)$$

然后计算 $f_j(i) (1 \leq i, j \leq n, i \neq j)$ 给其他成员, 计算并广播 $g^{a(u,v)} (1 \leq u \leq n, 1 \leq v \leq t-1)$ 。每个 P_i 收到来自 P_j 的 $f_j(i) (1 \leq i, j \leq n, i \neq j)$ 后, 通过下式验证 $f_j(i)$ 的正确性:

$$g^{f_j(i)} = r_j y_j^{h(r, PGID)} \tilde{r}^{n-1} \prod_{k=1}^{t-1} (g^{a(j,k)})^{i^k} \bmod p \quad (3)$$

如果成立, 记 $f(x) = \sum_{j=1}^n f_j(x) \bmod q$, 计算 $x_i' = f(i)$, 则:

$$f(0) = \sum_{i=1}^n (\alpha_i + x_i h(r, PGID)) \bmod q \quad (4)$$

1.2 代理签名的产生阶段

设 $D = \{P_1, P_2, \dots, P_t\}$ 是 t 个代理签名人, 他们想对消息 m 生成代表原始签名人的代理签名。他们共同合作执行以下步骤:

1) 每个 $P_i \in D$, 随机地选择一个数 $a_{i,0}' \in_R Z_q$, 计算并向其他成员广播 $c_{i,0}' = g^{a_{i,0}'} \bmod p$ 。

2) 每个 $P_i \in D$, 计算 $Y = \prod_{i=1}^t c_{i,0}' \bmod p$, 并产生一个 $t-1$ 阶的秘密多项式 $f_i'(x)$:

$$f_i'(x) = x_i h(Y, ASID) + \sum_{k=0}^{t-1} (a_{(i,k)}') x^k \bmod q \quad (5)$$

然后计算并广播 $f_j'(1 \leq i, j \leq n, i \neq j)$ 和 $c_{u,v}' = g^{a(u,v)'} (1 \leq u \leq n, 1 \leq v \leq t-1)$ 给其他成员。每个 P_i 收到来自 P_j 的 $f_j'(i) (1 \leq i, j \leq n, i \neq j)$ 后, 通过下式验证 $f_j'(i)$ 的正确性:

$$g^{f_j'(i)} = y_j^{h(Y, ASID)} \prod_{k=0}^{t-1} (c_{j,k}')^{i^k} \bmod p \quad (6)$$

如果成立, 则计算 $x_i'' = f'(i) \bmod q$, 显然 $f'(0) = \sum_{i=0}^t (x_i h(Y, ASID) + a_{(i,0)}') \bmod q$ 。

3) 每个 $P_i \in D$, 计算 $T_i = (x_i' + \hat{s}_i) h(m) + x_i'' \bmod q$, 然后把 T_i 广播给 D 中的其他代理签名人。当收到所有的 $T_j (j \neq i)$ 后, 每个 P_i 通过下列方程来验证 $T_j (j \neq i)$ 的有效性:

$$g^{T_j} = \left[r \left(y_0 \prod_{k=1}^n y_k \right)^{h(r, PGID)} \left(\prod_{i=1}^{t-1} (c_{i,0}' \prod_{k=1}^n c_{k,i}') \right)^{j^i} \right]^{h(m)} \times \left(\prod_{k=1}^t y_k \right)^{h(Y, ASID)} Y \prod_{i=1}^{t-1} \prod_{k=1}^t (c_{k,i}')^{j^i} \bmod p \quad (7)$$

4) 每个 $P_i \in D$ 能对 T_i 应用 Lagrange 插值多项式计算:

$$T = (f(0) + \hat{s}) h(m) + f'(0) \bmod q \quad (8)$$

则 $(r, PGID, ASID, Y, T)$ 为消息 m 的代理签名。

1.3 代理签名的验证阶段

验证者收到消息 m 的代理签名 $(r, PGID, ASID, Y, T)$ 后, 利用下式来验证代理签名的正确性:

$$g^T = \left((y_0 \prod_{i=1}^n y_i)^{h(r, PGID)} r \right)^{h(m)} \left(\prod_{i=1}^t y_i \right)^{h(Y, ASID)} Y \bmod p \quad (9)$$

2 对 Feng-Yuan 方案的安全性分析

任意其他 t 个成员, 不妨设为 $D_f = \{P_{t+1}, P_{t+2}, \dots, P_{2t}\}$, 一旦获得由 t 个成员 $D = \{P_1, P_2, \dots, P_t\}$ 关于消息 m 的代

理签名 $(r, PGID, ASID, Y, T)$ 后, 则他们可以按下面的方法、对任取的消息 m' 、假冒 $D = \{P_1, P_2, \dots, P_t\}$ 生成有效的代理签名 $(r, PGID, ASID, Y, T')$, 而 $D = \{P_1, P_2, \dots, P_t\}$ 中的 t 个成员成员却无法否认。

1) $D_f = \{P_{t+1}, P_{t+2}, \dots, P_{2t}\}$ 中的成员任取消息 m' , 计算 $d = (h(m))^{-1} h(m') \bmod q$ 。

2) $D_f = \{P_{t+1}, P_{t+2}, \dots, P_{2t}\}$ 中的成员合作, 从 $f(x) = \sum_{j=1}^n f_j(x) \bmod q$ 和 $f'(x) = \sum_{i=1}^{t-1} a_i'' x^i \bmod q$ 中得到 $f(0) = \sum_{i=1}^n (\alpha_i + x_i h(r, PGID)) \bmod q$ 和 $\hat{s} = x_0 h(r, PGID) + n\hat{k} \bmod q$ 。

3) 计算 $T' = T + (f(0) + \hat{s}) h(m) (d-1) \bmod q$ 。

则 $(r, PGID, ASID, Y, T')$ 就是关于消息 m' 的签名, 因为:

$$\begin{aligned} g^{T'} &= g^T g^{(f(0)+\hat{s})h(m)(d-1)} = \\ &= \left((y_0 \prod_{i=1}^n y_i)^{h(r, PGID)} r \right)^{h(m)} \left(\prod_{i=1}^t y_i \right)^{h(Y, ASID)} Y \times \\ &= \left(g^{\sum_{i=1}^n (\alpha_i + x_i h(r, PGID)) + x_0 h(r, PGID) + n\hat{k}} \right)^{h(m)(d-1)} = \\ &= \left((y_0 \prod_{i=1}^n y_i)^{h(r, PGID)} r \right)^{dh(m)} \left(\prod_{i=1}^t y_i \right)^{h(Y, ASID)} Y = \\ &= \left((y_0 \prod_{i=1}^n y_i)^{h(r, PGID)} r \right)^{h(m')} \left(\prod_{i=1}^t y_i \right)^{h(Y, ASID)} Y \bmod p \end{aligned}$$

虽然关于消息 m' 的签名 $(r, PGID, ASID, Y, T')$ 是由 $D_f = \{P_{t+1}, P_{t+2}, \dots, P_{2t}\}$ 产生的, 但在 $ASID$ 中包含的却是 $D = \{P_1, P_2, \dots, P_t\}$ 的身份信息, 从而使得被假冒的成员无法否认该签名, 这就是说, 方案的可识别性和不可否认性遭遇挑战。

3 改进方案及其安全性分析

3.1 改进的方案

改进的方案除了下面的部分参数有变化, 其余同原方案。

设 $y_p = \prod_{i=1}^n y_i \bmod p$, 则:

在代理密钥产生阶段, \hat{s} 用 $\hat{s} = x_0 h(r, PGID, y_0, y_p) + n\hat{k} \bmod q$ 来代替, $f_i(x)$ 用 $f_i(x) = \alpha_i + x_i h(r, PGID, y_0, y_p) + \sum_{k=1}^{t-1} a_{(i,k)} x^k \bmod q$ 来代替, 其余的参数 $\hat{s}_i, x_i, f(0)$ 以及各验证方程作相应的调整。

在代理签名产生阶段, $f_i'(x)$ 用 $f_i'(x) = x_i y_i h(Y, ASID, m) + \sum_{k=0}^t (a_{(i,k)}') x^k \bmod q$ 来代替, T_i 用 $T_i = (x_i' + \hat{s}_i) h(m, Y) + x_i'' \bmod q$ 来代替, 其余的参数 $x_i'', f(0), T$ 以及各验证方程作相应的调整。 $(r, PGID, ASID, Y, T)$ 即为消息 m 的代理签名。

代理签名的验证方程为 $g^T = \left((y_0 y_p)^{h(r, PGID, y_0 y_p)} r \right)^{h(m, Y)} \left(\prod_{i=1}^t y_i \right)^{h(Y, ASID, m)} Y \bmod p$ 。

3.2 安全性分析

1) 秘密参数的保密性。改进的方案是在原方案基础上的加强, 所以, 在离散对数难解的假设下, 攻击者无法获得任何秘密参数。

2) 内部成员的合谋攻击。考虑到 $h(m)$ 出现在验证式右边的 $(y_0 y_p)^{h(r, PGID, y_0 y_p) r}$ 和 $(\prod_{i=1}^t y_i^{y_i})^{h(Y, ASID, m)}$ 中, 所以 $D_f = \{P_{t+1}, P_{t+2}, \dots, P_{2t}\}$ 想对任取的消息 m' 、假冒 $D = \{P_1, P_2, \dots, P_t\}$ 生成有效的代理签名, 虽然 $D_f = \{P_{t+1}, P_{t+2}, \dots, P_{2t}\}$ 能够合作获得 $f(0)$ 和 \hat{s} , 但要使伪造签名成功, 需要找到满足等式 $(\prod_{i=1}^t y_i^{y_i})^{h(Y', ASID, m)} Y' = g^{\beta} \bmod p$ 的 Y' 和 β , 也就是只有知道 D 中各成员的私钥或者能够解离散对数问题, 而这是不可能的, 所以攻击失败。

3) 伪造攻击。由 2) 的讨论可知, 给定 m' 和 Y' , 能够获得满足验证式的 T' 的前提是攻击者知道 D 中各成员的私钥或者能够解离散对数问题; 另一方面, 给定 m' , 由于 Y 受单向 Hash 函数的保护, 所以寻找满足验证式的 T' 和 Y' 也会面临同样的困难, 因此攻击无法成功。

4) 可识别性和不可否认性。既然改进的方案能够抵抗伪造攻击和合谋攻击, 所以验证者可以通过 ASID 找到真实的签名者, 他们是可识别的、不可否认的。

参考文献:

- [1] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures: delegation of the power to sign messages[J]. IEICE Transactions on Fundamentals, 1996, E79-A(9): 1338 - 1354.
- [2] KIM S, PARK S, WON D. Proxy signatures, revisited[A]. Proceedings of ICICS97[C]. Berlin: Springer-Verlag, 1997. 223 - 232.
- [3] ZHANG K. Threshold proxy signature schemes[A]. 1997 Information Security Workshop[C], 1997. 191 - 197.
- [4] SUM HM. An Efficient Nonrepudiable threshold proxy signature scheme with known signers[J]. Computer Communications, 1999, 22(8): 717 - 722.
- [5] HSU CL, WU TS, WU TC. New nonrepudiable threshold proxy signature scheme with known signers[J]. The Journal of Systems and Software, 2001, 58(5): 119 - 124.
- [6] YANG CY, TZENG SF, HWANG MS. On the efficiency of nonrepudiable threshold proxy signature scheme with known signers[J]. The Journal of Systems and Software, 2004, 73(3): 507 - 514.
- [7] XIE Q, YU X. Cryptanalysis of two nonrepudiable threshold proxy signature schemes[J]. International Journal of Network Security, 2006, 3(1): 21 - 25.
- [8] HWANG MS, LIN IC, LUE JL. A secure nonrepudiable threshold proxy signature scheme with known signers[J]. Informatica, 2000, 11(2): 137 - 144.
- [9] HWANG SJ, CHEN CC. Cryptanalysis of nonrepudiable threshold proxy signature schemes with known signers[J]. Informatica, 2003, 14(2): 205 - 212.
- [10] TZENG SF, HWANG MS, YANG CY. An Improvement of nonrepudiable threshold proxy signature scheme with known signers[J]. Computers & security, 2004, 23(2): 174 - 178.
- [11] XIE Q. Improvement of Tzeng et al.'s nonrepudiable threshold proxy signature scheme with known signers[J]. Applied Mathematics and Computation, 2005, 168(2): 776 - 782.
- [12] SUN HM, LEE NY, HWANG T. Threshold proxy signatures[J]. IEE Proceedings of Computers & Digital Techniques, 1999, 146(5): 259 - 263.
- [13] HSU CL, WU TS, WU TC. Improvement of threshold proxy signature scheme[J]. Applied Mathematics and Computation, 2003, 136(2/3): 315 - 321.
- [14] 冯朝胜, 袁丁. 一种不可否认门限代理签名方案的改进. 计算机应用, 2005, 25(11): 2530 - 2532.

(上接第 1625 页)

ms05-039 补丁) 的重要模块进行测试的结果如表 1 所示。表 2 显示了 ms05-025 补丁升级前后 pngfilt.dll 比较的不同之处, 有两个函数的签名发生了变化。通过人工对汇编码的分析, 这些函数的功能确实有所改变, 而改变就意味着前一个版本 pngfilt.dll 中这两个函数里可能存在安全漏洞。

原型系统对补丁进行分析时, 匹配的成功率同具体的补丁对原程序的改动有关, 有时候还会受编译器的影响。经过大量的试验测试, 平均的匹配率可以达到 80% 左右。

表 1 原型系统的测试结果

动态库名	正确匹配 函数个数	未匹配 函数个数	匹配成功 率(%)
ms05-025 补丁前 pngfilt.dll	123	2	98
ms05-025 补丁后 pngfilt.dll	123	2	98
ms05-039 补丁前 umpnmpmgr.dll	127	73	63
ms05-039 补丁后 umpnmpmgr.dll	127	71	64
ms05-049 补丁前 webvw.dll	315	73	81
ms05-049 补丁后 webvw.dll	315	72	81

表 2 pngfilt.dll 补丁前后没有能够正确匹配的函数

安装补丁前				安装补丁后			
地址	#nodes	#links	#calls	地址	#nodes	#links	#calls
70533925	10	21	4	1B063925	10	22	4
70533B33	7	13	4	1B063B3E	8	15	4

3 结语

控制流级结构化比较方法的优点是结构化签名与平台无关, 一般不受编译器优化的影响, 而指令级图形化比较方法不会漏掉非结构化的变动。通过对两个算法的研究和实现, 可以更好地发现相同软件不同版本之间的差异, 了解补丁对代码的修改。虽然结构化的比较方法有以上的优点, 但由于签名信息主要体现了函数结构化的信息, 对程序非结构的改动不敏感, 因此该算法会出现误判。改进的方法为首先利用结构化算法对所有的函数进行签名匹配, 对那些函数签名相同即匹配成功的函数对再利用指令相似性的图形化比较算法分析其非结构化的改变。

参考文献:

- [1] BUCKLEY F, LEWINTER M. 图论简明教程[M]. 李慧霸, 王凤芹, 译. 北京: 清华大学出版社, 2005.
- [2] 段刚. 加密与解密[M]. 北京: 电子工业出版社, 2003.
- [3] IA-32 Intel Architecture Software Developer's Manual, Vol 2: Instruction Set Reference[EB/OL]. <http://www.intel.com/>, 2004.
- [4] SABIN T. Comparing binaries with graph isomorphisms[EB/OL]. http://www.bindview.com/services/razor/paper/2004/comparing_binaries.cfm, 2004.
- [5] FLAKE H. Structural Comparison of Executable Objects[A]. Detection of Intrusions and Malware & Vulnerability Assessment[C]. Dortmund: GI SIG SIDAR Workshop, 2004. 161 - 173.
- [6] HOGLUND G. 软件剖析——代码攻防之道[M]. 邓劲生, 译. 北京: 清华大学出版社, 2005.