

基于辫群的代理签名方案的分析与改进

黄文平¹, 宁菊红²

(1. 南昌陆军学院 科文教研室, 南昌 330103; 2. 江西师范大学 数学与信息科学学院, 南昌 330022)

(jxnuhwp1@163.com)

摘要:对两个基于辫群的代理签名方案进行了分析,发现它们并不满足不可伪造性。第一个方案中不能抵抗原始签名人改变攻击,在第二个方案中任何攻击者可以伪造一个有效的代理签名,在该签名中,代理签名者以及消息可以任意指定。根据上述缺陷,提出一个改进的强代理签名方案,新方案在不增加计算复杂性的前提下,保证了签名的安全性,同时代理授权过程中还增加了不需要安全通道的性质。

关键词:辫群;代理签名;伪造攻击;安全分析;共轭查找问题

中图分类号: TP309.2 **文献标志码:** A

Analysis and improvement of proxy signature schemes over braid group

HUANG Wen-ping¹, NING Ju-hong²

(1. Department of Science and Arts, Nanchang Military Academy, Nanchang Jiangxi 330103, China;

2. College of Mathematics and Information Science, Jiangxi Normal University, Nanchang Jiangxi 330022, China)

Abstract: Analysis shows that two proxy signature schemes based on braid groups are insecure: the first scheme cannot resist the original signer's change attack; in the scheme of second, any antagonist can successfully forge a valid proxy signature scheme, which the antagonist can designate any proxy signer and messages. Later, a new proxy signature scheme was proposed. Analysis shows that the proposed scheme satisfies all security requirements; what's more, no security channel is in need in the communication of the original signer and the proxy signer.

Key words: braid group; proxy signature; forgery attack; security analysis; conjugacy search problem

随着量子技术的研究发展不断深入,对于许多基于数论难题假设的公钥密码系统形成了潜在威胁。于是,人们开始研究可以抵抗已知量子分析的公钥密码系统。基于辫群的公钥密码系统正是其中之一。自从文献[1]的作者提出基于辫群的公钥密码系统以来,辫群公钥密码体制得到了广泛研究。基于辫群的签名体制在2003年首次被提出^[2],随后有一系列的研究和分析。文献[3-4]提出一个基于辫群的代理签名方案。本文对文献[3-4]的方案进行安全性分析,指出它们都不能满足代理签名的安全性要求。同时,提出了一个改进的基于辫群的代理签名方案,最后证明其是安全的。

1 预备知识

1.1 辫群

辫群的定义有两种形式:一类是文献[5]给出的定义,一类是文献[6]给出的定义。由于这两类表示是等价的,因此仅介绍文献[5]给出的定义。

定义1 辫群 B_n (n 为群参数)是由生成元 $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$ 生成的有限表示的无限群,并且它的生成元 $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$ 满足如下关系:

- 1) $\sigma_i \sigma_j = \sigma_j \sigma_i (i - j > 1, 0 < i < j < n)$;
- 2) $\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j (i - j = 1, 0 < i < j < n)$ 。

定义2 由生成元 $\sigma_1, \sigma_2, \dots, \sigma_{i-1}$ 生成的子群称为 B_n 的左子群 LB_n ;而由 $\sigma_{i+1}, \sigma_{i+2}, \dots, \sigma_{n-1}$ 生成的子群称为 B_n 的右

子群,记作 RB_n 。

定义3 共轭问题。是否存在算法来判断群 G 中给定的任意两个元素是共轭元素。所谓两个元素 $x, y \in G$ 共轭是指:存在 G 中元素 ω ,使得 $y = \omega^{-1}x\omega$ 成立,通常记作 $x \sim y$, ω 称为 x, y 的共轭元。

辫群中的困难:

1) 共轭查找问题(Conjugacy Search Problem, CSP)

条件: x, y 共轭,即 $(x, y) \in (B_n, B_n)$ 满足 $y = a^{-1}xa$, $a \in B_n$,找到 $b \in B_n$,使得 $y = b^{-1}xb$ 。

2) 一般共轭查找问题(Generalized Conjugacy Search Problem, GCSP)

条件: $(x, y) \in (B_n, B_m)$ 满足 $y = a^{-1}xa$, $a \in B_n, n < m$,找到 $b \in B_m$,使得 $y = b^{-1}xb$ 。

3) 共轭分解问题(Conjugacy Decomposition Problem, CDP)

条件: $(x, y) \in (B_n, B_m)$ 满足 $y = a^{-1}xa$, $a \in B_n, n < m$,找到 $b_1, b_2 \in B_m$,使得 $y = b_1xb_2$ 。

1.2 代理签名

代理签名^[7]的概念,即,经过原始签名者的授权,被指定的代理签名人可以代表原始签名人生成有效的代理签名。由于代理签名在电子货币、电子商务、网格计算等方面都有广泛的应用,所以代理签名一提出便受到广泛关注,国内外很多学者对其进行了深入的探讨与研究。一个安全的代理签名必

收稿日期:2009-10-30;修回日期:2009-12-14。

基金项目:江西省自然科学基金资助项目(2007GQS0159);江西省教育厅科研计划项目(GJJ08161)。

作者简介:黄文平(1974-),男,江西南丰人,副教授,硕士,主要研究方向:信息安全;宁菊红(1977-),女,河南三门峡人,副教授,博士,主要研究方向:函数论、信息安全。

须满足以下条件:

- 1) 不可伪造性: 任何人(包括原始签名人)无法伪造有效的代理签名;
- 2) 可验证性: 验证者能够从代理签名中确信原始签名人认同该签名;
- 3) 不可否认性: 代理人一旦生成有效的代理签名, 则他不可否认;
- 4) 可区分性: 任何人可以区分原始签名人与代理人产生的签名;
- 5) 阻止签名权力的滥用: 代理签名人不能为了其他的目使用代理密钥生成有效的签名, 就滥用而言, 签名者的责任是可以被明显确定的。

2 两个代理签名方案简介

在文献[3-4]中, 参数规定为:

$$B_n(l) = \{b \in B_n \mid 0 \leq \inf(b) \leq \sup(b) \leq l\}, LB_n(l) = \{b \in LB_n \mid 0 \leq \inf(b) \leq \sup(b) \leq l\}, RB_n(l) = \{b \in RB_n \mid 0 \leq \inf(b) \leq \sup(b) \leq l\} \\ H_0: \{0, 1\}^* \rightarrow B_n, H_1: B_n \rightarrow \{0, 1\}^*, H_2: \{0, 1\}^* \rightarrow B_n$$

原始签名人为 A , 代理签名人为 B , A 、 B 的公钥对分别为 $(x_A, y_A), (x_B, y_B)$, 私钥分别为 a_A, a_B , 其中 $y_A = a_A x_A a_A^{-1}$, $y_B = a_B x_B a_B^{-1}$, 在文献[3]中 $x_A, y_A, x_B, y_B, a_A, a_B \in B_n$ 。在文献[4]中 $a_A, a_B \in LB_n(l), x_A, y_A, x_B, y_B \in B_n(l)$ 。

2.1 代理签名方案^[3]

1) A 用私钥 a_A 和 B 的身份 ID_B 计算 $\sigma_0 = a_A H_0(ID_B) a_A^{-1}$, 将 σ_0 发送给 B 。

2) B 收到 σ_0 后, 检验是否有 $\sigma_0 \sim H_0(ID_B)$ 和 $\sigma_0 y_A \sim H_0(ID_B) x_A$ 。

3) 对于消息 m , B 随机选择大于 2 的素数 c 令 $\sigma_1 = \sigma_0^c$, $\sigma_2 = a_B H_0(m) a_B^{-1}$, 将 $(\sigma_1, \sigma_2, c, m)$ 作为代理签名发布。

4) 当验证者收到 $(\sigma_1, \sigma_2, c, m)$ 后, 验证 $\sigma_1 \sim H_2(ID_B)^c$, $\sigma_1 y_A \sim H_0(ID_B)^c x_A$, $\sigma_2 \sim H_0(m)$, $\sigma_2 y_B \sim H_0(m) x_B$ 是否成立。如果均成立则接受签名, 否则拒绝接受。

2.2 代理签名方案^[4]

1) 原始签名人计算 $w = a_A^{-1} x_B' a_A, z_0 = H_2(m_\omega \parallel H_1(w)), t_0 = a_A z_0 a_A^{-1}$, 将 (m_ω, t_0) 通过安全通道传送给签名者。其中 m_ω 中包含了原始签名者、代理签名者、代理期限、代理消息的内容限制等。

2) 代理签名人计算 $z_0 = H_2(m_\omega \parallel H_1(w))$, 并且检查是否有 $t_0 y_A \sim z_0 x_A$, 若成立, 则随机选择 $b \in {}_R RB_n(l)$, 计算 $\alpha = b a_B b^{-1}, h = H_2(m \parallel H_1(\alpha)), \beta = t_0 a_B b t_0^{-1} h t_0 b^{-1} a_B^{-1} t_0^{-1}, \gamma = t_0 b y_B b^{-1} t_0^{-1}, \theta_1 b t_0^{-1} h t_0 b^{-1}, \theta_2 b w b^{-1}$, 将 $(m_\omega, \alpha, \beta, \gamma, \theta_1, \theta_2, m)$ 作为签名发表。

3) 当验证者收到 $(m_\omega, \alpha, \beta, \gamma, \theta_1, \theta_2, m)$, 验证者首先计算 $z_0 = H_2(m_\omega \parallel H_1(w)), h = H_2(m \parallel H_1(\alpha))$, 然后验证 $\alpha \sim x_B, \beta \sim h, \beta \gamma \sim \theta_1 \alpha, \gamma \sim y_B, \gamma y_A \sim z_0 \theta_2 z_0^{-1} x_A$ 是否均成立, 如果成立则接受, 否则拒绝接受签名。

3 两个代理签名方案的分析

3.1 文献[3]代理签名方案的分析

文献[4]指出, 在文献[3]中通过不同的两个签名, 任何人可以得到 σ_0 , 因此可以构造另一个有效的签名, 但是这个伪造的签名既没有改变原始签名者, 也没有改变代理签名者

和消息的内容。因此可以认为这个构造只是对签名的另一种表达形式。对该方案的安全性, 没有实质性的影响。

在文献[3]中消息的验证有四个共轭关系需要判别, 通过观察我们可以发现, 前面两个和后面两个是完全分离的。针对这个特点, 可以得到以下两种攻击方式。

1) 改变原始签名人。如果某个代理签名人分别为两个不同的原始签名人的代理签名 $(m, \sigma_1, \sigma_2, c), (\bar{m}, \bar{\sigma}_1, \bar{\sigma}_2, \bar{c})$, 则很简单只需要构造 $(m, \bar{\sigma}_1, \sigma_2, \bar{c})$, 很显然验证过程完全不变, 但是这时已经将原始代理签名人已经改变了。反之, 也同样成立。

2) 对于任何攻击者 C , 首先利用自己的密钥 a_c 计算, $\sigma_0 = a_c H_0(ID_B) a_c^{-1}$, 然后随机选择一个大于 2 的素数 C , 计算 $\sigma_1 = \sigma_0^c$, 很显然可以直接验证 $\sigma_1 \sim H_0(ID_B)^c, \sigma_1 y_c \sim H_0(ID_B)^c y_c$, 由于 σ_2, m, y_B, x_B 都不变化, 后两个要验证的表达式不变, 因此也显然会成立。这样, 就得到了一个 C 对 B 授权的关于消息 m 的有效代理签名。

3.2 文献[4]代理签名方案的分析

对于任意攻击者 C 来说, 对于任意消息 m 和任意委托书 m_w , 计算 $\alpha = b x_B b^{-1}, z_0 = H_2(m_w \parallel H_1(w)), h = H_2(m \parallel H_1(\alpha)), \beta = a_c h a_c^{-1}, \gamma = a_c x_B a_c^{-1}, \theta_1 = h x_B \alpha^{-1}, \theta_2 = z_0^{-1} x_B z_0$,

下面证明其正确性:

其中 $\alpha \sim x_B, \beta \sim h$ 显然成立:

$$\because \gamma \sim x_B, x_B \sim y_B$$

$$\therefore \gamma \sim y_B; \beta \gamma = (a_c h a_c^{-1})(a_c x_B a_c^{-1}) = a_c h x_B a_c^{-1}, \text{ 同时} \\ \theta_1 \alpha = (h x_B \alpha^{-1}) \alpha = h x_B$$

$$\therefore \beta \gamma \sim \theta_1 \alpha; \gamma y_c = a_c x_B a_c^{-1} a_c x_c a_c^{-1} = a_c x_B x_c a_c^{-1}, \\ z_0 \theta_2 z_0^{-1} x_A = z_0 (z_0^{-1} x_B z_0) z_0^{-1} x_A = x_B x_A$$

$$\therefore \gamma y_A \sim x_B x_A$$

所有的等式都成立。在这些参数的构造中没有任何参数利用了代理签名人的密钥 a_B , 也不需要用到左、右辩群中的任何元素。

通过上述构造, 对于任意攻击者 C , 可以获得关于任何代理签名者 B 代理的任何消息 m 的有效签名。

4 改进的方案及其安全性分析

4.1 改进的代理签名方案

通过对上述两个方案的安全分析, 本文提出一个新的代理签名方案。

首先将所有的私钥改为左辩群的元素, 即 $a_A, a_B \in LB_n(l)$, 其余参数不变。

1) Alice 随机选取 $t \in {}_R RB_n(l)$, 计算 $t_0 = a_A m_\omega a_A^{-1} \oplus h(t y_B t^{-1}), k = t x_B t^{-1}$, 并把 (k, t_0, m_ω) 发送给 Bob。

2) Bob 首先计算 $k' = a_B k a_B^{-1}, t_0' = t_0 \oplus H(k')$ 验证 $t_0' \sim m_\omega$ 是否成立, 如果成立, 则继续进行下一步; 否则, Bob 拒绝接受 Alice 的委托。

3) Bob 随机选择 $b \in {}_R B_n(l)$, 计算 $h = H(m_\omega \parallel m)$, 以及 $\alpha = b x_B b^{-1}, \beta = b h b^{-1}, \gamma = b a_B^{-1} h a_B b^{-1}$, 将 $(\alpha, \beta, \gamma, t_0', m_\omega, m)$ 作为一个有效的代理签名发布。

4) 验证者首先计算 $h = H(m_\omega \parallel m)$, 然后验证 $t_0' y_A \sim m_\omega x_A, \beta \sim h, \gamma \sim h, \alpha \beta \sim x_B h, \alpha \gamma \sim y_B h$ 是否成立。

下面证明其正确性:

在步骤 2) 中, $k' = a_B k a_B^{-1} = a_B t x_B t^{-1} a_B^{-1}$, 由于 a_B, t 可以交换, 有:

$$\begin{aligned}
k' &= ta_B x_B a_B^{-1} t^{-1} = t y_B t^{-1} \\
t_0' &= t_0 \oplus H(k') = t_0 \oplus H(t y_B t^{-1}) = \\
& a_A x_A a_A^{-1} \oplus h(t y_B t^{-1}) \oplus H(t y_B t^{-1}) = \\
& a_A m_\omega a_A^{-1}
\end{aligned}$$

在步骤4)中, $\beta \sim h, \gamma \sim h$, 显然成立:

$$\begin{aligned}
t_0' y_A &= a_A m_\omega a_A^{-1} a_A x_A a_A^{-1} = a_A m_\omega x_A a_A^{-1} \sim m_\omega x_A \\
\alpha\beta &= b x_B b^{-1} b h b^{-1} = b x_B h b^{-1} \sim x_B h \\
\alpha\gamma &= b x_B b^{-1} b a_B^{-1} h a_B b^{-1} = b x_B a_B^{-1} h a_B b^{-1} = \\
& b a_B^{-1} y_B h a_B b^{-1} \sim y_B h
\end{aligned}$$

4.2 改进方案的安全性分析

在本方案中, A 在传递证书给 B 时, 不需要通过安全通道。而是通过公开通道传递给 B , 对于任何攻击者 C 截获了证书 (k, t_0, m_ω) , 首先不能冒充代理签名者, 因为在计算 t_0' 时用到了 B 的私钥 a_B , 只有 B 才能正确地计算出。没有 t_0' , 除了原始签名者, 任何其他人都不能构造出 $t_0' y_A \sim m_\omega x_A$ 。同样地, 也不能假冒原始签名人 A , 如果假冒原始签名人 A , 即使能够通过代理签名人 B 的验证, 也不能满足 $t_0' y_A \sim m_\omega x_A$ 。

对于原始签名者也不能假冒代理签名者进行伪造, 因为除了代理签名者 B , 任何人都无法构造出 $\alpha\beta \sim x_B h, \alpha\gamma \sim y_B h$ 同时成立。

5 结语

本文在分析文献[3-4]两个方案安全缺陷的基础上, 提出了一个改进的方案, 同时分析了方案的安全性, 该方案满足代理签名方案的安全性要求, 能够抵抗原始签名者的伪造攻击和原始签名者的变换攻击, 不但保证了方案的安全性, 同时还增加了不需要安全信道的功能, 增强了方案的安全性。

参考文献:

- [1] KO K H, LEE S J, CHEON J H, *et al.* New public-key cryptosystem using braid groups[C] // Advances in Cryptology-Crypto2000, LNCS 1880. Berlin: Springer-Verlag, 2000: 166-184.
- [2] CHA J C, KO K H, LEE S J, *et al.* An efficient implementation of braid groups[C] // Proceedings of Asiacrypt 2001, LNCS 2448. Berlin: Springer-Verlag, 2003: 477-490.
- [3] 张利利, 曾吉文. 基于辫群的代理签名方案[J]. 数学研究, 2008, 41(3): 56-64.
- [4] WEI Y, XIONG G H. Security analysis and design of proxy signature schemes over braid groups [EB/OL]. [2009-10-29]. <http://eprint.iacr.org/2009/458.pdf>.
- [5] ARTIN E. Theory of braids [J]. Annals of Math, 1947, 48(2): 101-126.
- [6] BIRMAN J S, KO K H, LEE S J. A new approach to the word and conjugacy problems in the braid groups [J]. Advances in Mathematics, 1998, 139(2): 322-353.
- [7] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures for delegating signing operation [C] // Proceedings of the 3rd ACM Conference on Computer and Communications Security (CCS). New York: ACM, 1996: 48-57.
- [8] ANSHEL M, GOLDFELD D. An algebraic method for public-key cryptography [J]. Mathematical Research Letters, 1999, 6: 287-291.
- [9] LEE H Y, LEE H S, LEE Y R. Security analysis of a proxy blind signature scheme over braid groups [EB/OL]. [2009-10-29]. <http://eprint.iacr.org/2009/158.pdf>.
- [10] VERMA G K. A proxy blind signature schemes over braid groups [J]. International Journal of Network Security, 2009, 19(3): 214-217.
- [11] QI DONGXU, WANG DAOSHUN, YANG DILIAN. Matrix transformation of digital image and its periodicity [J]. Progress in Natural Science, 2001, 11(7): 542-549.
- [12] YANG YALI, CAI NA, NI GUOQIANG. Digital image scrambling technology based on the symmetry of Arnold transform [J]. Journal of Beijing Institute of Technology, 2006, 15(2): 216-220.
- [13] 赵亮, 廖晓峰, 向涛, 等. 对高维混沌系统的图像加密算法安全性和效率的改进[J]. 计算机应用, 2009, 27(7): 1775-1781.
- [14] 黄良永, 肖德贵. 二值图像 Arnold 变换的最佳置乱度[J]. 计算机应用, 2009, 29(2): 474-476.
- [15] 孙伟. 关于 Arnold 变换的周期性[J]. 北方工业大学学报, 1999, 11(1): 29-32.
- [16] 邹建成, 铁小匀. 数字图像的二维 Arnold 变换及其周期性[J]. 北方工业大学学报, 2000, 12(1): 1014-1032.
- [17] 吴发恩, 邹建成. 数字图像二维 Arnold 变换周期的一组必要条件[J]. 北方交通大学学报, 2001, 25(6): 66-69.
- [18] 李兵, 徐家伟. Arnold 变换的周期及其应用[J]. 中山大学学报: 自然科学版, 2004, 43(S2): 139-142.
- [19] 黎罗罗. Arnold 型置乱变换周期分析[J]. 中山大学学报: 自然科学版, 2005, 44(2): 1-4.
- [20] 袁明豪. Fibonacci 数列的模数列的周期性[J]. 数学的实践与认识, 2007, 37(3): 119-122.
- [21] 袁明豪. Fibonacci 数列的模数列的周期的一个性质[J]. 数学的实践与认识, 2008, 38(8): 207-210.
- [22] 李用江, 李昌利, 李司东, 等. Fibonacci 数列模 p^r 的周期性研究[J]. 数学的实践与认识, 2009, 39(17): 138-143.

(上接第1029页)

开辟了新的途径, 也为探讨高阶猫映射的周期性问题^[10]提供了新的方法。

参考文献:

- [1] 王朔中, 张新鹏, 张开文. 数字密写和密写分析[M]. 北京: 清华大学出版社, 2005: 5-7.
- [2] 王育民, 张彤, 黄继武. 信息隐藏-理论与技术[M]. 北京: 清华大学出版社, 2006: 30-33.
- [3] QI DONGXU, ZOU JIANCHENG, HAN XIAOYOU. A new class of scrambling transformation and its application in the image information covering [J]. Science in China: Series E, 2000, 43(3): 304-412.
- [4] 李昌利, 卢朝阳. 数字水印的去同步攻击及其对策[J]. 中国图象图形学报, 2005, 10(4): 403-409.
- [5] 张博, 李小斌, 侯彪. 基于 Hermit 矩阵扰动特性的图像数字水印[J]. 西安电子科技大学学报, 2008, 35(6): 1127-1130.
- [6] 谢静, 吴一全. 基于奇偶量化的 Contourlet 变换域指纹图像水印算法[J]. 计算机应用, 2007, 27(6): 1365-1367.
- [7] 刘芳, 贾成, 袁征. 一种基于 Arnold 变换的二值图像水印算法[J]. 计算机应用, 2008, 28(6): 1044-1046.
- [8] 孙圣和, 陆哲明, 牛夏牧. 数字水印技术与应用[M]. 北京: 科学出版社, 2004: 14-19, 74-79.
- [9] ARNOLD V I, AVEZ A. Ergodic problems of classical mechanics [C] // Mathematical Physics Monograph Series. New York: Addison-Wesley, 1968: 271-281.
- [10] 杨礼珍, 陈克非. 变换矩阵(modn)的阶及两种推广 Arnold 变换矩阵[J]. 中国科学, E 辑, 2004, 34(2): 151-161.