

基于身份来自辫群的指定验证人的代理签名

杨爱梅¹, 彭维平^{2,3}

(1 河南工业大学 信息科学与工程学院, 河南 郑州 450001;

2 北京邮电大学 网络与信息攻防技术教育部重点实验室, 北京 100876;

3 河南理工大学 计算机学院, 河南 焦作 454003)

摘 要: 针对辫群中的许多困难问题, 如字问题、共轭问题和根问题等, 介绍了辫群的基本概念、重要性质和辫群中的困难问题, 在此基础上, 利用辫群上的左右子群的可交换性、辫群上的共轭查找问题和 p 次根问题的难解性, 构造了一个基于身份的指定验证者的代理签名. 安全性分析表明, 该方案是安全有效的, 具有不可伪造性.

关键词: 身份; 辫群; 指定验证者代理签名; 共轭问题; p 次根问题

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2011)09-0035-04

Designated Verifier Proxy Signature Based on Identity from Braid Group

YANG Ai-mei¹, PENG Wei-ping^{2,3}

(1 School of Information Science and Engineering, Henan University of Technology, Zhengzhou 450001 China;

2 Key Laboratory of Network and Information Attack & Defence Technology of MOE,
Beijing University of Posts and Telecommunications, Beijing 100876, China;

3 School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003, China)

Abstract: For many hard problems such as the word problem, conjugacy problem and root problem in the braid group, the paper introduced the basic concept of nature and important properties and difficult problems of the braid group. Based on of that, the designated verifier proxy signature scheme is proposed based on identity using conjugate search problem and the p -th root finding problem, and the exchangeable of the group operation between the elements in the left subgroup and the right subgroup of a braid group. Its security is analyzed and the result shows that this scheme is secure and effective, and has the nature of unforgeability.

Key words: identity; braid group; designated verifier proxy signature; conjugacy problem; p -th root problem

1 引言

为了简化传统数字签名中证书的管理问题, 1984 年 shamir 提出了基于身份的密码系统, 用户的公钥可以通过用户的身份来标识, 如身份证号码、电子邮件地址、IP 地址、电话号码等. Mambo 等人于 1996 年提出了代理签名的概念^[1]. 利用代理签名, 一个被称为原始签名人的用户或个人, 可以将

他的数字签名权利委托给一个被称为代理签名人的用户, 代理签名人代表原始签名人产生的数字签名, 称为代理签名. 然而代理签名人代表原始人行使代理签名权时, 其签名可被任何第三方验证, 在一些情况下, 例如电子商务中的电子投票、电子投标等, 只希望指定的验证人才可以验证代理签名. 一个指定验证人的代理签名方案应当满足以下基本性质:

(1) 基本不可伪造性: 除了原始签名人外, 任何

人包括代理签名人都不能生成原始签名人的普通数字签名。

(2) 代理签名的不可伪造性:除了代理签名人外,任何人包括原始签名人都不能生成有效的代理签名。

(3) 代理签名的可区分性:任何一个代理签名都与原始签名人的普通数字签名有明显的区别;不同的代理签名人生成的代理签名之间也有明显的区别。

(4) 验证的指定性:只有被指定的验证人才能验证代理签名的有效性。

(5) 密钥依赖性:代理签名密钥依赖于原始签名人的秘密密钥。

(6) 不可否认性:任何签名人(不论是原始签名人还是代理签名人)在生成一个数字签名后,不能再对它加以否认。

1947 年 Arin 首次提出了辫群的概念。辫群内元素的乘法和求逆运算都存在着快速算法,可以用计算机编程来计算。辫群的某些性质特别适合密码学的要求,可以用来构造密码算法。2000 年韩国学者 Ki Hyoung Ko、Doo Ho Choi、Mi Sung Cho 和 Jang Won Lee 在文献[2]中提出了基于辫群共轭问题困难性的密钥交换协议和公钥密码体制,自此,辫群公钥密码体制得到了广泛的研究,取得了一定的成果。

文中首先介绍了辫群的基本概念、重要性质和辫群中的几个困难问题,在此基础之上,利用辫群中的左右子群的可交换性,利用 CSP 问题和 p 次根问题,基于文献[3-7]中的指定验证者的签名和基于身份的代理签名方案,提出一个基于身份的指定验证人的代理签名方案,通过分析该方案是安全的,可行的。

2 辫群简介

2.1 辫群的基本概念

定义 1 辫群 B_n ($n \in N$) 是由生成元 $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$ 生成的有限表示的非交换无限群,并且当 $n \geq 2$ 时它的生成元满足如下关系:当 $1 \leq i \leq n-2$ 时, $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$; 当 $|i-j| \geq 2$ 时, $\sigma_i \sigma_j = \sigma_j \sigma_i$, 因此 B_n 辫群可以表示为^[2]:

$$B_n = \{ \sigma_1, \sigma_2, \dots, \sigma_{n-1} \mid \begin{cases} \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, & 1 \leq i \leq n-2 \\ \sigma_i \sigma_j = \sigma_j \sigma_i, & |i-j| \geq 2 \end{cases} \}$$

辫群中的元素称为一个 n 辫或辫元。

定义 2 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 共轭是指:存在 G 中元素 w , 使得 $y = w^{-1} x w$ 成立,通常记作 $\alpha \in B_n, w$ 称为 x, y 的共轭元。

定义 3 称 $LB_n = \langle \sigma_1, \dots, \sigma_{\lfloor n/2 \rfloor} \rangle$ 和 $RB_n = \langle \sigma_{\lfloor n/2 \rfloor + 1}, \dots, \sigma_{n-1} \rangle$ 分别为 B_n 的左右子群。关于左右子群有一个非常重要的性质:元素的可交换性,即对任意的 $\alpha \in LB_n$, 任意的 $\beta \in RB_n$, 有 $\alpha \beta = \beta \alpha$ 成立。

2.2 辫群的重要性质

辫群与一般的组合群不同,它有很多良好的性质,这些良好的性质也就使得辫群在密码学上扮演重要角色成为可能,两个比较重要的性质。

(1) 辫群中的元素都可以通过标准形式来统一表示,即由 $p+1$ 个参量 $(u, \pi_1, \pi_2, \dots, \pi_p)$ 表示,其中 u 是整数, π_1 是一个 n 阶置换,该表示是唯一的。标准型可以解决用字来表示群中元素的困难性。

(2) 对于辫群中元素的相乘和求逆运算都存在着快速算法。两个字 u 和 v 的乘积只是将 u 和 v 连接,即 uv , 在群运算中实际上是隐藏 u 和 v , 这可通过将 uv 变为标准型来得到。设 u 和 v 是两个辫元,其标准型中分别由 p 和 q 个置换表示,乘积 uv 的标准型可在 $O(pq \log n)$ 时间内计算出来,而 u 的逆的标准型可在 $O(pn)$ 时间内计算出来。

2.3 辫群中的困难问题

(1) 共轭判定问题(CDP)

条件: $(x, y) \in B_n \times B_n$, 满足 $y = \alpha^{-1} x \alpha, \alpha \in \beta_n$ (或 B_n 的子群)。

找到:判定 x, y 是否共轭。

(2) 共轭查找问题(CSP)

条件: x, y 共轭, 即 $(x, y) \in B_n \times B_n$, 满足 $y = \alpha^{-1} x \alpha, \alpha \in B_n$ (或 B_n 的子群)。

找到: $b \in B_n$, 使得 $y = b^{-1} x b$

(3) 一般共轭查找问题(GCSP)

条件: $(x, y) \in B_n \times B_m$, 满足 $y = \alpha^{-1} x \alpha, \alpha \in B_n, m < n$ 。

找到: $b \in B_m$, 使得 $y = b^{-1} x b$ 。

(4) 共轭分解问题(QCDP)

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

找到: $b_1, b_2 \in B_m$, 使得 $y = b_1 x b_2$ 。

(5) p 次根问题(RP)

条件: $(x, y) \in B_n \times B_n$, 满足 $y = x^p, p \in N$ 。

找到: $b \in B_n$, 使得 $y = b^p$ 。

3 基于身份来自辩群的指定验证者的代理签名方案

3.1 系统设置过程

假设用户 A 是原始签名人,用户 B 是代理签名人.用户 C 是指定的验证人.

辩群 $B_n(l) = \{b \in B_n \mid 0 \leq \inf(b) \leq \sup(b) \leq l\}$,其中 n 和 l 是两个足够大的整数,两个整数 s, t ,左右子半群 LB_s, RB_t ; ID 是一个表示用户身份的 $\{0, 1\}$ 字符串,两个抗碰撞的密码学单向散列函数:

$$H_1: B_n(l) \rightarrow \{0, 1\}^*; H_2: \{0, 1\}^* \rightarrow B_n(l).$$

3.2 产生密钥过程

A 建立一个授权许可信息 m_w 来明确说明包含 A, B, C 的身份信息的授权关系, A, B, C 的公钥,授权关系的使用限制包括使用期限 T_A, T_B, T_C 等内容, A 的身份是 ID_A , B 的身份是 ID_B , C 的身份是 ID_C ;

A, B, C 将各自的身份信息 ID_A, ID_B, ID_C 提交给可信机构 TA , TA 计算 $x_1 = H_1(ID_A \parallel T_A)$, $x_2 = H_1(ID_B \parallel T_B)$, $x_3 = H_1(ID_C \parallel T_C)$ 选择 $p \in \mathbb{Z}^+$, $p \geq 2$, $a_{TA} \in {}_R LB_s$, 计算 $y = a_{TA} x_2 a_{TA}^{-1}$, 公开 (x_1, x_2, x_3, p) , 保存 $a_{TA} \in {}_R LB_s$, 并将 y 公开.

A 选择 $a_A \in {}_R RB_t$, 计算 $P_A = a_A x_1 a_A^{-1}$, a_A 为私钥, (x_1, P_A) 为公钥.

B 选择 $a_B \in {}_R LB_s$, 计算 $P'_B = a_B x_2 a_B^{-1}$, $k = a_B y a_B^{-1}$, $\gamma_B = k^p$, a_B 为私钥, (x_2, γ_B) 为公钥.

C 选择 $a_C \in {}_R RB_t$, 计算 $P_C = a_C x_3 a_C^{-1}$, a_C 为私钥, (x_3, P_C) 为公钥.

3.3 委托过程

A 用自己的私钥 a_A 和代理人的身份信息, 在 T_A, T_B 有效期内计算 $\sigma = a_A H_2(ID_B \parallel m_w) a_A^{-1}$, 然后把 σ 发给 B .

B 收到后, 必须对 σ 进行验证. 如果 $\sigma \sim H_2(ID_B \parallel m_w)$, 并且 $P_A \sigma \sim x_1 H_2(ID_B \parallel m_w)$ 成立, 则是合法的授权.

3.4 代理签名过程

若 T_C 在有效期内, 代理人 B 对消息 $m \in \{0, 1\}^*$ 进行签名, 于是指定 C 作为验证者.

选择 $b_2 \in {}_R B_n(l)$, 计算 $h = H_1(H_2(P_A \sigma \parallel m \parallel T_C))$, $Y = b_2 h b_2^{-1}$, $s = a_B x_3 a_B^{-1}$, $n = a_B P_C a_B^{-1}$, $\lambda = H_1(n) \oplus m$, $\delta = H_2(m_w) k$, 则在消息 m 上指定验证人 C 的签名为 $SIG = (Y, \sigma, P'_B, s, \lambda, \delta, m_w)$.

3.5 指定验证者验证过程

指定验证人 C 收到签名 $SIG = (Y, \sigma, P'_B, s, \lambda, \delta, m_w)$ 若 T_A, T_B 都在有效期内, 将执行以下操作:

首先计算 $h = H_1(H_2(P_A \sigma \parallel m \parallel T_C))$, 验证 $Y \sim h$, 接着验证 $P'_B s \sim x_2 x_3$, 如果不成立, 拒绝接受签名; 否则, 继续计算;

计算 $n = a_C s a_C^{-1}$, $m = H_1(n) \oplus \lambda$, 验证人 C 接受 SIG 为有效的签名当且仅当 $[H_2^{-1}(m_w) \delta]^p = \gamma_B$.

4 安全性分析

该方案是基于辩群上的 CSP 和 RP 问题而提出的指定验证者的代理签名方案, 所以在安全性方面是可行的, 安全性分析具体如下:

(1) 代理签名的可验证性

指定验证人计算 $h = H_1(H_2(P_A \sigma \parallel m \parallel T_C))$, 因为 $Y = b_1 h b_1^{-1}$, 所以 $Y \sim h$ 由于 $P'_B s = a_B x_2 a_B^{-1} a_B x_3 a_B^{-1} = a_B x_2 x_3 a_B^{-1}$, 所以验证者 C 验证 $P'_B s \sim x_2 x_3$ 成立时, 他将继续计算 $n = a_B P_C a_B^{-1} = a_B a_C x_3 a_C^{-1} a_B^{-1} = a_C a_B x_3 a_B^{-1} a_C^{-1} = a_C s a_C^{-1}$, $m_w = H_1(n) \oplus \lambda$, $[H_2^{-1}(m_w) \delta]^p = [H_2^{-1}(m_w) H_2(m_w) k]^p = [k]^p = \gamma_B$, 当以上等式成立时, C 接受该签名是有效的签名.

(2) 代理签名的不可否认性

验证签名时使用了代理签名人 B 的公钥, 所以 B 不能否认是他指定了验证人 C . 当发生争执或 B 不承认自己指定 C 时, 除了验证人 C 可通过计算 $n = a_C s a_C^{-1}$, $m = H_1(n) \oplus \lambda$, TA 也可利用代理人的身份 ID_B 或私钥 a_{TA} 和 P'_B , 验证

$$\begin{aligned} \delta &= H_2(m_w) k = H_2(m_w) a_B y a_B^{-1} \\ &= H_2(m_w) a_B a_{TA} x_2 a_{TA}^{-1} a_B^{-1} \\ &= H_2(m_w) a_{TA} a_B x_2 a_B^{-1} a_{TA}^{-1} \\ &= H_2(m_w) a_{TA} P'_{BA} a_{TA}^{-1} \end{aligned}$$

(3) 代理签名的不可伪造性

基本不可伪造性: 从 A 发给 B 的授权委托书 σ 可以得出, 除了 A 之外, 任何人(包括 B) 都不能生成委托书. 即使伪造人得到了 A 的 σ , 但他要从 σ 中通过求解 CSP 问题而推出 A 的私钥 a_A , 是不可行的, 因为文献[8]中已经证明.

代理签名的不可伪造性: 对于消息 m 上的签名 $SIG = (Y, \sigma, P'_B, s, \lambda, \delta, m_w)$, 除了代理签名人 B 之外, 任何人都不能伪造签名. 攻击者要想伪造签名, 他必须从 $P'_B = a_B x_2 a_B^{-1}$, $s = a_B x_3 a_B^{-1}$, $n = a_B P_C a_B^{-1}$ 那里求出 a_B , 这也是 CSP 问题, 而该问题是不可行

的. 通过求解 CSP 问题而推断出 A 的私钥 a_B , 成功的概率最多为 $1/(n!)^t$, 这里在文献[8] 中已经得到证明.

(4) 验证人的指定性

在指定验证签名阶段会用到验证人 C 的私钥, 除了指定 C , 其他任何人都不能验证此签名的合法性.

(5) 代理签名的密钥依赖性

在代理签名的生成过程中, 代理签名人 B 计算 $h = H_1(H_2(P_A\sigma \parallel m \parallel T_C))$, 因为 $\sigma = a_A H_2(ID_B \parallel m_w) a_A^{-1}$, 所以没有原始人的私钥, B 就不能生成有效的代理签名.

(6) 代理签名的可区分性

代理签名过程中, 代理签名人在接到原始签名的授权 σ 的基础上, 才能产生代理签名, 签名中用到 B 的私钥 a_B , 代理人的代理签名和正常签名是可区分的.

5 结束语

利用辫群中的 CSP 问题和 p 次根问题的难解性, 构造了一个基于身份的指定验证者的代理签名. 辫群理论是未来构造公钥密码体制的平台, 在组合群论应用于密码学中扮演了重要的角色, 基于辫群上的一些困难问题无论是在现代计算机上, 还是在量子计算机上目前都没有非常好的解法. 随着科学技术的发展, 辫群在密码学上将会有有一个广阔的应用前景.

参考文献:

- [1] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation[C]//Proceedings of the 3rd ACM Conference on Computer and Communication Security. Japan: Tokyo, 1996: 48-57.
- [2] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, et al. New public key cryptosystem using braid groups[C]//LNCS 1880: Proc of Crypto2000. Berlin: Springer-Verlag, 2000: 166-183.
- [3] 卓泽朋, 魏仕民. 基于辫群的指定验证者的签名方案[J]. 计算机应用, 2008, 28(12): 3197-3798.
- [4] Verma G K. A proxy signature scheme over braid groups [EB/OL]. [2011-01-05]. <http://eprint.iacr.org/2008/160.pdf>.
- [5] 卓泽朋, 魏仕民. 基于身份的代理签名方案[J]. 计算机工程与应用, 2009, 45(28): 112-114.
- [6] 唐忠宽, 殷新春, 赵荣. 基于身份的代理盲签名在电子现金中的应用[J]. 微电子学与计算机, 2009, 26(8): 71-73.
- [7] 秦艳琳, 吴晓平. 对一种代理盲多重签名的分析与改进[J]. 微电子学与计算机, 2010, 27(10): 37-40.
- [8] Ko K H, Cho ID H, Chom S, et al. New signature scheme using conjugacy problem [EB/OL]. [2008-05-18]. <http://eprint.ia2cr.org/2002/168.pdf>.

作者简介:

杨爱梅 女, (1979-), 硕士, 讲师. 研究方向为信息安全.
彭维平 男, (1979-), 博士研究生, 讲师. 研究方向为网络与信息安全.

(上接第 34 页)

Instruments, 2003.

- [5] Ivan W Selesnick Sidney Burrus C. Generalized digital butterworth filter design [J]. Signal Processing, 1998 (46): 1688-1694.
- [6] 李钟慎. 基于 MATLAB 设计巴特沃斯低通滤波器[J]. 信息技术, 2003, 27(3): 44-52.
- [7] Hui Li. Gear fault monitoring based on order tracking and Bi-spectrum under running-up condition[J]. Fuzzy Systems and Knowledge Discovery, 2007(4): 379-383.
- [8] 张韧, 杨世锡, 任达千, 等. 一种应用重采样技术的整周

期采样方法[J]. 机电工程, 2004, 21(3): 1-3.

作者简介:

杨舟 男, (1985-), 硕士研究生. 研究方向为数模混合电路的设计、检测技术.
王红 女, (1971-), 副教授. 研究方向为电子技术、检测技术、系统故障诊断理论和技术.
杨士元 男, (1949-), 教授, 博士生导师. 研究方向为电子技术、检测技术、系统故障诊断理论和技术、智能家居系统.
胡喜 男, (1973-), 高级研究员. 研究方向为电路设计、系统控制.