基于辫群的代理盲签名方案

李 锋[1], 郭艾侠[2], 赵秀凤[3]
(1. 广东工业大学, 应用数学学院, 广州 510006; 2. 华南农业大学 信息学院, 广州 510642; 3. 解放军信息工程大学 电子技术学院, 郑州 450004)

摘 要: 由 Shor 等人构造的量子算法可以在多项式时间内解决传统三大难解问题而利用辫群构造的很多数学困难问题,在量子计算机条件下均无有效的解法,辫群是一种适合构造抵抗量子密码分析的计算平台。利用左右子群元素的可交换性,基于 CSP 问题、SCSP 问题和 p 次方根问题的难解性,提出了一个新的代理盲签名方案,并通过方案分析验证了该方案的有效性和可行性。

关键词: 辫群; 盲签名; 共轭搜索问题; 量子算法; 代理签名
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)07-2641-02
doi:10.3969/j.issn.1001-3695.2010.07.068

Proxy blind signature scheme based on braid group

LI Feng[1], GUO Ai-xia[2], ZHAO Xiu-feng[3]
(1. *College of Applied Mathematics, Guangdong University of Technology, Guangzhou* 510006, *China*; 2. *College of Information, South China Agricultural University, Guangzhou* 510642, *China*; 3. *Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou* 450004, *China*)

Abstract: Three types of traditional hard problem could be resolved by Shor, Boneh and Lipton's quantum algorithms in polynomial time. By the braid group constructed a lot of mathematics difficulties were not an effective solution under the conditions of the quantum computer. It seemed that braid group was a kind of considerable considerable cryptography platform in the future. This paper proposed a new proxy blind signature scheme based on 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. Through program analysis shows that the new scheme is effective and feasible.

Key words: braid group; blind signature; conjugacy search problem; quantum algorithms; proxy signature

Chaum[1] 在 1982 年首次提出了盲签名的概念,在该方案中,用户能够在不让签名人知道被签消息内容的前提下得到签名人的签名,签名人不可能把最终签名和签名过程对应起来。盲签名方案一般是通过用户与签名人之间的交互协议来实现。Chaum 同时提出了基于 RSA 的盲签名技术,Camenisch 等人[2] 提出了基于离散对数问题的盲签名方法, Mohammed 等人[3] 也提出了基于 ElGamal 签名算法的盲签名体制,能增加盲签名技术的匿名性,同时其所需要的计算复杂度较 Chaum 方法低且运算速度较快。Mambo 等人[4] 在 1996 年首次提出代理签名,是一个被指定的代理签名者可以代表原始签名者生成有效的签名。验证者能够验证并区分原始签名人的签名和代理签名人的签名。

由 Shor 等人提出的量子算法表明,基于有限域特性的某些难解问题都有量子的多项式时间算法,2001 年,Vandersypen 等人[5] 在一台量子比特的量子计算设备上实现了 Shor 的量子分解算法,可以在多项式时间内分解大整数,同时有效解决离散对数和椭圆曲线上的离散对数问题,传统的基于这三类难题的公钥密码系统在量子计算时代变得不再安全。一些学者开始研究基于具有特殊性质的非交换群、非交换半群、非交换环等的密码体制,而基于辫群(braid group)的公钥密码体制[6] 便是其中最有代表性的一类。目前,基于辫群的密码体制的研究是公钥密码体制研究的热点,在国内外的各类期刊发表了一些关于辫群密码体制的论文,朱萍等人[7] 综述了基于辫群的密码体制的研究成果和发展状况,从基于辫群的密码体制及分析得出,目前很多人构造的密码体制似乎不安全,但从攻击方法来看,攻击都是针对最基本的问题困难性假设的,还没有用到选择消息攻击、中间人攻击和已知密钥攻击等密码学分析方法。因此,基于辫群的密码体制还有很多值得研究的问题。本文在张利利等人[8] 提出基于辫群的代理签名方案的基础上,基于辫群的几个难解问题构造了新的代理盲签名方案,并对本方案作了安全性分析。

1 辫群及辫群上的难解问题

为了后文叙述方便,这里首先回顾辫群的理论及难解问题[9],并结合目前的研究进展给出辫群的研究方向。

1.1 辫群

定义 1 辫群 B_n($n\geq 3$,由单个初等辫子生成的辫群 B_2 是无限循环群,本文不考虑)是无限非交换群,但可以由有限的

收稿日期: 2009-12-23; **修回日期**: 2010-01-28

作者简介:李锋(1977-),男,山东济宁人,讲师,硕士,主要研究方向为信息安全与密码学(lfgdutnews@126.com);郭艾侠(1974-),女,安徽宿州人,讲师,博士研究生,主要研究方向为信息安全及虚拟现实;赵秀凤(1977-),女,山东梁山人,讲师,博士研究生,主要研究方向为信息安全与密码学.

生成元生成，B_n 的生成元为 $\sigma_1,\sigma_2,\cdots,\sigma_{n-1}$。其中 σ_i 为 Artin 生成元，且满足：$\sigma_i\sigma_j=\sigma_j\sigma_i,|i-j|>1;\sigma_i\sigma_j\sigma_i=\sigma_j\sigma_i\sigma_j,|i-j|=1$。

定义 2 称 $LB_m=(\sigma_1,\sigma_2,\cdots,\sigma_{m-1})$ 为 B_n 的左辫群，$RB_{n-1-m}=(\sigma_{m+1},\sigma_{m+2},\cdots,\sigma_{n-1})$ 为右辫群，且均有 $\alpha\beta=\beta\alpha$，$(\alpha,\beta)\in LB_m\times RB_{n-1-m}$。

定义 3 共轭。称辫群 B_n 中的两个元素 x 和 y 共轭，如果满足 $y=a^{-1}xa,a\in B_n$，记做 $x\sim y$，辫元 a 称做共轭对 (x,y) 的共轭元。

1.2 辫群上的难解问题

1）共轭问题（CSP）（又称共轭搜索问题）

$$(x,y)\in B_n\times B_n,y=a^{-1}xa$$

其中：$a\in B_n$。问题：寻找 $b\in B_n$，使得 $y=b^{-1}xb$。

2）多共轭问题（SCSP）（又称同时共轭搜索问题）

$$(x_1,a^{-1}x_1a),(x_2,a^{-1}x_2a),\cdots,(x_r,a^{-1}x_ra)\in B_n\times B_n$$

其中：$a\in B_n$。问题：寻找 $b\in B_n,b^{-1}x_1b=a^{-1}x_1a,b^{-1}x_2b=a^{-1}x_2a,\cdots,b^{-1}x_rb=a^{-1}x_ra$。

3）求根问题（RP）

$$(x,y)\in B_n\times B_n$$

其中：$y=x^p,p\in\boldsymbol{N}$。问题：寻找 $b\in B_n$，使得 $y=b^p$。

4）移位共轭搜索问题

对任意 $x,y\in B_\infty$，定义运算 $x\circ y=xf(y)\sigma_1f(x)^{-1}$。其中 $f(x)$ 是 x 在 B_∞ 的移位，即 f 是 B_∞ 上将 σ_i 映射为 σ_{i+1} 的单射。已知 $x,y\in B_\infty$，发现辫子 $x^*\in B_\infty$，使得 $x^*\circ y=x\circ y$。

从目前的研究来看，除了后面两个问题外，其他的都有一些理论上的启发式概率解法，但仍然没有给出真正意义上的解法。而对于 p 次方根问题，Styshnev 等人用不同的方法证明了可以判定 B_n 中元素的 p 次方根的存在性问题，Gonzalez-Meneses 证明了 p 次方根在共轭的意义下是惟一的，从 p 次方根的应用来看，该难解性还没有被应用到公钥密码上来。而基于移位共轭搜索问题困难性假设的密码体制的研究才刚开始，还有待于进一步深入研究应用。

2 基于辫群的代理盲签名方案

本方案中，由原始签名人 OS、代理签名人 PS 和用户 U 三方参与。三方分别选取自己的公钥对 (x_o,y_o)、(x_p,y_p)、(x_u,y_u)，满足 $y_o=a_o^{-1}x_oa_o$、$y_p=a_p^{-1}x_pa_p$、$y_u=a_u^{-1}x_ua_u$，这里 $a_o\in B_n,a_u\in LB_m,a_p\in RB_{n-1-m}$ 为三方各自的私钥。ID_p，ID_u 分别表示 PS 和 U 的身份标志，包括各自的足够多的信息，如姓名、性别、生日、电话号码、指纹信息等。由文献[10]构造两个安全的哈希函数 $h_1:\{0,1\}^*\to B_n,h_2:\{0,1\}^*\to B_n$，假定所有代理签名人的身份 ID_p 均保存在原始签名人的数据库中。

a）PS 计算。$y_1=h_1(ID_p)$ 发给 OS。

b）OS 先验证 PS 的身份，即计算 $h_1(ID_p)$ 与收到的 y_1 是否相等。通过验证后，计算 $y_2=h_2(ID_p),\sigma_0=a_o^{-1}y_2a_o$，并将 y_2、σ_0 发给 PS。

c）PS 验证。$\sigma_0\sim y_2,\sigma_0y_o\sim y_2x_o$，计算 $\sigma_1=\sigma_0^c$，将 σ_1、c、y_2 发给用户 U。

d）用户 U 要把消息 m 让 PS 盲签名。首先验证 $\sigma_1\sim y_2^c$，$\sigma_1y_o\sim y_2{}^cx_o,\sigma_1y_p\sim y_2{}^cx_p$，随机选择辫元 $k\in LB_m$ 作为盲因子，首先将信息 m 编码为 B_n 中的一个辫元 m_1（保密），计算 $y_2=k^{-1}m_1k,y_3=h_1(ID_u\parallel y_2),\sigma(M')=k^{-1}y_3k$，将 y_2、y_3 和 $\sigma(M')$ 发给 PS。

e）如果代理签名人拥有用户 U 的身份标志 ID_u 的权限，利用收到的 y_2 计算 $h_1(ID_u\parallel y_2)$，与收到的 y_3 作比较确认用户身份的真实性；如果不拥有用户 U 的身份标志 ID_u 的权限，PS 直接验证 $\sigma(M')\sim y_3,\sigma(M')y_u\sim y_3x_u$，然后再对消息 $\sigma(M')$ 进行签名，计算 $\sigma_2=a_p^{-1}\sigma(M')a_p$，将 σ_2 发给用户 U。

f）用户 U 去盲因子 k，验证 $\sigma_2\sim\sigma(M'),\sigma_2y_u\sim\sigma(M')x_u$，计算 $s=k\sigma_2k^{-1}$。其中 s、σ_1、σ_2 为盲代理签名结果。

3 方案分析

1）正确性 用户 U 验证了 PS 的信息的真实性后，去除盲因子 k，即 $s=k\sigma_2k^{-1}=ka_p^{-1}\sigma(M')a_pk^{-1}=ka_p^{-1}k^{-1}y_3ka_pk^{-1}$，利用左右辫群元素的可交换性，可得到 $s=a_p^{-1}y_3a_p$ 为签名结果，其中加入了代理签名人 PS 的私钥。

2）不可伪造性 在签名中，参与人的公钥 (x_o,y_o)、(x_p,y_p)、(x_u,y_u) 满足 $y_o=a_o^{-1}x_oa_o$、$y_p=a_p^{-1}x_pa_p$、$y_u=a_u^{-1}x_ua_u$ 共轭关系，三个私钥是基于 CSP 困难性；同样，相互之间不能推导出对方的私钥，基于 MSCSP 困难问题，由 $\sigma_1=\sigma_0^c,\sigma_0=a_o^{-1}y_2a_o$ 可知，别人没有 a_o，无法伪造 σ_0，而去求解 $\sigma_1=\sigma_0^c$ 是求根问题的困难性，故不能伪造合法的签名。

3）盲性 对于代理人来说，知道 y_2 及 $\sigma(M')$ 但得不到任何原始消息 m，即签名时只能知道 y_2。

4）不可否认性 由安全性分析可知，代理签名是不可伪造的。一个代理签名只能由代理人生成，因为只有他拥有 $y_p=a_p^{-1}x_pa_p$，而在验证 $s=a_p^{-1}y_2a_p$ 时用到 a_p，所以他不能否认没签名。

5）可注销性 本方案中，原始签名人可以注销代理签名人的权限，与用户达成一个协议，即用户在让代理签名人签名前，先验证代理签名人的身份是否处在有效期内。具体方案借鉴文献[11]：$t=(h_2(ID_p))^r,\sigma=a_o^{-1}ta_o$，原始签名人将 (t,σ) 发给用户，用户先验证 $t\sim\sigma,ty_o\sim\sigma x_o$，确定是否为原始签名人的撤销，然后验证 $t^c\sim\sigma_1^r$，如果成立则确认代理签名人资格已被取消。

6）可区分性 代理签名的验证过程中需要代理签名人的公钥，原始签名人和代理签名人使用了各自的私钥，其算法结构也不同，因此任何人都可区分代理签名人和原始签名人的签名。

7）不可追踪性 由于 $y_2=h_1(ID_u\parallel m)$，而 ID_u 和 m 都是保密的，h_1 是单向散列函数，同时由 $\sigma(M')=k^{-1}y_2k$ 算不出盲因子 k，无法追踪消息的拥有者，签名中算不出 ID_u，即满足了不可追踪性。

8）本方案与基于离散对数问题的代理盲签名的比较 在构造方式上，由 Shor 等人构造的量子算法就已经指出，量子计算机可以在多项式时间内分解大整数问题、解决离散对数问题和椭圆曲线上的离散对数问题，同时科学家预测实用的量子计算机在未来的 15～20 年内将被制造出来，这将导致目前的基于传统三类公钥算法的系统不能使用，而广泛使用的基于离散对数问题的代理盲签名方案也变得不再安全。

而在计算量上，本方案与基于离散对数的 T-L-T 方案[11]在每个阶段所需的计算量作了详细比较，从表 1 可以看出，由于

（下转第 2646 页）

可以看到在相同的最小支持度下,本文的加权移动窗口算法执行的时间最少。在图 5 中,最小支持度是 0.5%。可以看到随着事务平均大小的增加,各算法执行时间都会加长,但本文的加权移动窗口算法在该情况下仍然是相对较优的。

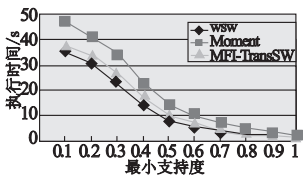

图4　不同最小支持度下各算法执行时间

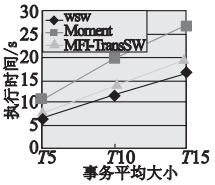

图5　事务平均大小增加情况下各算法执行时间

图 6 显示当数据集增大时,对最小支持度 0.1%,加权移动窗口算法平均性能还是超出其他算法的。图 7 显示最小支持度保持 0.5% 不变,窗口大小从 1 k ~ 20 k 变化时各算法的执行时间都会随之降低,但降幅不同。这是因为当窗口很小时,每个窗口包含频繁项集的事务数目比较少,因此将备选项集判断为非频繁项集的概率较高。总体上,加权移动窗口算法性能在算法比较中可以显现出优势。

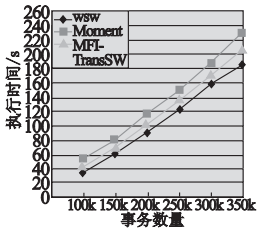

图6　数据集增大时各算法执行时间

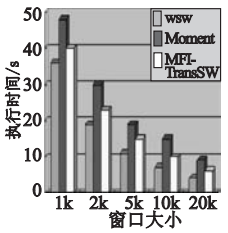

图7　不同窗口大小情况下各算法执行时间

7　结束语

由于将移动窗口算法应用于入侵检测的研究还处于发展阶段,成熟的算法不多。本文从数据流的角度介绍了现有的两个性能较优的移动窗口算法,即 MFI-TransSW 算法和 Moment 算法。针对现有算法存在的缺陷,本文考虑将加权移动窗口的概念引入,判断数据流中的频繁项集来检验异常的网络状况,获得攻击者的入侵信息,从而使得入侵检测能更好地处理大量的连续数据,通过实例检测和结果分析,加权移动窗口算法优于其他算法,并在此基础上建立了入侵检测系统模型。加权移动窗口是一种数据挖掘的方法,将其应用于入侵检测将对提高网络的可用性和可靠性具有非常重要的意义。

参考文献:

[1] LEE W, STOLFO S J, MOK K W. A data mining framework for building intrusion detection models[C]//Proc of IEEE Symposium on Security and Privacy. Berlin:Springer, 1999:120-132.

[2] 钟玉峰,雷国华.一种基于滑动窗口技术的入侵检测方法[J].信息技术,2009(7):166-167.

[3] GOLAB L, OZSU M T. Issues in data stream management[J]. ACM SIGMOD Record, 2003, 32(2): 5-14.

[4] 方金和,冯雁,王瑞杰. 基于数据挖掘的自适应入侵检测研究[J].计算机工程与应用,2006, 42(18):152-154.

[5] 崇志宏.基于屏蔽/汇总技术的数据流处理算法[D].上海:复旦大学,2006.

[6] 潘立强,李建中,王伟平.数据流上加权共享滑动窗口的连接查询处理算法[J].计算机工程与应用,2005, 41(27):160-163.

[7] 邱剑.基于主动检测概念漂移的数据流多分类器方法[J].信息技术,2009(6):212-214.

[8] 陈照阳, 黄上腾.流数据分类中的概念漂移问题研究[J].计算机应用与软件, 2009, 26(2):254-256.

[9] 姜远,刘力平.数据流挖掘技术[J].江南大学学报:自然科学版, 2007, 6(6):654-657.

[10] 尹志武,黄上腾.一种自适应局部概念漂移的数据流分类算法[J].计算机科学,2008, 35(2):138-139.

(上接第 2642 页)共轭判定问题不再是难解问题,可以通过有效的算法解决。在运算时间和空间上要求很小,而模乘、模加、指数和求逆等运算量较大,安全性上本方案的困难性即使利用量子计算机也没有可行的解法。

表 1　两种盲签名方案的计算复杂性比较

签名体制	代理密钥生成阶段	签名生成阶段	签名验证阶段	安全性
T-L-T 方案	2 个模加运算 1 个模乘运算 2 个指数运算	3 个模加运算 6 个模乘运算 8 个指数运算 4 个求逆运算	3 个模乘运算 3 个指数运算 1 个求逆运算	离散对数难解问题
本文方案	3 次共轭计算	共轭判定 5 次 散列计算 3 次 辫群运算 5 次	共轭判定 2 次 散列计算 2 次 辫群运算 1 次	辫群中的 CSP 问题、SCSP 问题和 p 次方根问题的难解性

4　结束语

代理签名是随着计算机广泛普及的一种新的实用签名技术,研究安全高效的代理盲签名方案具有重要的实际意义。本文基于辫群的难解(CSP、SCSP 和 RP)问题,构造了满足七个特性的代理盲签名方案,这为辫群在密码学中的广泛应用提供了较高研究参考价值。

参考文献:

[1] CHAUM D. Blind signatures for untraceable payments[C]//Advances in Cryptology-Crypto. Berlin: Springer-Verlag, 1983: 199-203.

[2] CAMENISCH J, PIVETEAU M, STADLER M A. Blind signatures based on the discrete logarithm problem[C]//Advances in Cryptology-EUROCRYPT. Berlin: Springer-Verlag,1995:428-432.

[3] MOHAMMED E, EMARAH A E, SHENNAWY K E. A blind signatures scheme based on ElGamal signature[C]//Proc of the 17th National Radio Science Conference. 2000: 25-35.

[4] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures: delegation of the power to sign messages[J]. IEICE Trans on Fundam,1996, E79-A(9):1338-1354.

[5] VANDERSYPEN L M K, STEFFEN M, BRERYTA G, *et al*. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance[J]. Nature,2001,414(6866):883-887.

[6] KO K H,LEE S J,CHEON J H, *et al*. New public-key cryptosystem using braid groups [C]//Proc of the 20th Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag, 2000: 166-184.

[7] 朱萍,温巧燕. 基于辫群的密码体制研究及进展[J]. 通信学报,2009,30(5):105-113.

[8] 张利利,曾吉文. 基于辫群的代理签名方案[J]. 数学研究,2008, 41(1):56-64.

[9] ARTIN E. Theory of Braids[J]. Annals of Math,1947, 48(1): 101-126.

[10] KO K H, CHOI D H, CHO M S, *et al*. New signature scheme using conjugacy problem[EB/OL]. (2002-11). http:// eprint. Iacr. org/2002/168. pdf.

[11] 谭作文,刘卓军,唐春明. 基于离散对数的代理盲签名[J]. 软件学报,2003, 14(11):1931-1935.