ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.3, March 2007, pp.722−729
DOI: 10.1360/jos180722

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

辫子群上的公钥加密算法*

汤学明+, 洪 帆, 崔国华

(华中科技大学 计算机科学与技术学院 信息安全系,湖北 武汉 430074)

A Public Key Encryption Algorithm on Braid Groups

TANG Xue-Ming+, HONG Fan, CUI Guo-Hua

(Department of Information Security, School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

+ Corresponding author: Phn: +86-27-87543986, Fax: +86-27-87561031, E-mail: pipilu126@126.com, http://www.hust.edu.cn

Tang XM, Hong F, Cui GH. A public key encryption algorithm on braid groups. *Journal of Software*, 2007, 18(3):722−729. http://www.jos.org.cn/1000-9825/18/722.htm

Abstract: Braid group is a new considerable public key cryptography platform for the quantum computer ages, but almost all current intractable braid problems used for public key cryptosystems are flawy. The security of a braid public key cryptosystem can't depend only on the hardness of conjugacy problems. By taking advantage of the non-conjugate transformation and multiple variant equations on braid groups, two intractable problems are proposed, and the hardness of these problems comes from the enlarged amount of variants. A new related public key algorithm and the analysis of its correctness, security, efficiency and parameter choice are subsequently presented. The new algorithm can resist current known attacks, and the ideal to combine some simple problems to a multiple variant difficult one is constructive for designing new public key algorithms.

Key words: public key encryption; braid group; conjugate; multiple variant equation; Burau representation

摘 要: 辫子群是一种新兴的适用于量子计算机时代的公钥密码平台,辫子群上已知的用于公钥密码系统的一些难解问题和基于这些难解问题的公钥加密算法都受到不同程度的攻击.辫子群上公钥密码系统的安全性不能仅仅依靠共轭问题的难解性.结合辫子群上非共轭变换和多变量方程组的特点所构造的难解问题,通过增加变量数量来增加问题的难解程度.新的公钥加密算法的安全性建立在新的难解问题之上,随后对其正确性、安全性、效率以及参数选择进行了分析.辫子群上新的公钥加密算法可以抵抗已知的各种攻击,将简单问题复合成多变量难解问题的思路,对公钥密码算法的设计起到一定的启发作用.

关键词: 公钥加密;辫子群;共轭;多变量方程组;Burau 表示
中图法分类号: TP309 文献标识码: A

1994 年,Shor 利用量子纠缠性和叠加性提出了著名的大数因子分解的量子算法——Shor 算法[1].利用该算法的思想并借助量子计算机,不仅可以在多项式时间内分解大整数,而且还可以有效地解决离散对数和椭圆曲线上的离散对数问题.Shor 算法使得目前广泛使用的基于以上 3 类"难解"问题的公钥密码系统受到了巨大挑

* Supported by the National Natural Science Foundation of China under Grant No.60403027 (国家自然科学基金)
Received 2005-08-08; Accepted 2006-04-03

战,一旦量子计算机制造出来,这些公钥密码系统将不能继续使用.因此,研究既能抵抗传统密码分析,又能抵抗量子密码分析的公钥密码平台是公钥密码学发展中的重要问题.

辫子群早在 1947 年由 Artin 提出,并在数学、物理和计算机等领域得到广泛的应用,其运算所需要的时间和空间要求很小,结构比较复杂.辫子群上的很多"难解"问题,即使利用量子计算机,目前也没有可行的解法,因此,辫子群是一种比较适合于用来构造未来公钥密码系统的平台.

本文第 1 节介绍辫子群的基本结构和辫子群上的难解问题.第 2 节介绍已有的辫子群上的公钥加密算法及已知的攻击方法.第 3 节提出辫子群上的两类新的难解问题.第 4 节设计一种新的公钥加密算法并对其正确性、安全性和效率进行分析.第 5 节对全文作一个简单的回顾.

1 辫子群和辫子群上的难解问题

关于辫子群的基本概念、性质和算法的详细情况可以参考文献[2].

定义 **1**(辫子群). 辫子群是一类特殊的 Artin 群,一个由 $n-1(n\geq 3$,由单个初等辫子生成的辫子群是无限循环群,本文不予考虑)个初等辫子生成的辫子群 B_n 表示为

$$B_n=\langle \sigma_1,\sigma_2,\ldots,\sigma_{n-1}|\sigma_i\sigma_{i+1}\sigma_i=\sigma_{i+1}\sigma_i\sigma_{i+1},i=1,2,\ldots,n-2;$$
$$\sigma_i\sigma_j=\sigma_j\sigma_i,i,j=1,2,\ldots,n-1,|i-j|\geq 2\rangle.$$

辫子群是一类无限、非交换的无纽群.一根辫子,如果其表达式中不出现初等辫子的负次幂,这样的辫子叫做正辫子,单位元ε也属于正辫子,所有的正辫子形成一个独异点(monoid),记作 B_n^+ .

令$\Delta_1=\sigma_1$,递归地定义$\Delta_i=\sigma_1\sigma_2\ldots\sigma_i\Delta_{i-1}(2\leq i\leq n-1)$,则$\Delta=\Delta_{n-1}$ 称为辫子群 B_n 的基本辫子.

在 B_n 上可以定义一种偏序关系"$\leq$",任何$(x,y)\in B_n\times B_n,x\leq y$ 当且仅当存在$(\alpha,\beta)\in B_n^+\times B_n^+$,使得 $y=\alpha x\beta$.任何满足$\varepsilon\leq\alpha\leq\Delta$的辫子$\alpha$称作标准因子.

如果 $w,\alpha,\beta\in B_n^+$,$w=\alpha\beta$,则称β是 w 的一个尾部.进一步地,如果α是标准因子,则称 w 的这种分解是"左加权"的是指α在所有的分解中根据偏序关系"$\leq$",长度最长.根据这种"左加权"分解,任何辫子 w 可以唯一地表示成 Garside 范式[2]:

$$w=\Delta^r\alpha_1\alpha_2\ldots\alpha_s,$$

其中,$\alpha_i(1\leq i\leq s)$均为不等于ε和Δ的标准因子,且$\alpha_i\alpha_{i+1}$是左加权的.

我们将 s 称作辫子 w 的标准长度,$r=inf(w)$称作 w 的下确界,$r+s=sup(w)$称作 w 的上确界.

辫子群中的任何辫子都可以在多项式时间内有效地表示成 Garside 范式的形式,两根辫子相等,是指它们有相同的 Garside 范式表示.

辫子群之间有一些显而易见的关系,对于正整数 $m\leq n$,B_m 是 B_n 的子群;如果 l 和 r 是正整数,B_{l+r} 是由 $\sigma_1,\sigma_2,\ldots,\sigma_{l+r-1}$ 这 $l+r-1$ 个元生成的辫子群,由 $\sigma_1,\sigma_2,\ldots,\sigma_{l-1}$ 生成的群,记作 LB_l,由 $\sigma_{l+1},\ldots,\sigma_{l+r-1}$ 生成的群记作 RB_r,则它们都是 B_{l+r} 的子群,而且满足关系:任意$(a,b)\in LB_l\times RB_r$,均有 $ab=ba$.

定义 **2**(共轭). 辫子群 B_n 中的两个元素 x 和 y 共轭是指存在 $a\in B_n$,使得 $y=a^{-1}xa$.

辫子群上有很多数学上"难解"的问题,这些问题均可被用作构造公钥密码系统,下面仅列举与共轭相关的 4 个问题,其他问题可以参考文献[3].

1) 共轭判断问题:给定$(x,y)\in B_n\times B_n$,判断 x 和 y 是否共轭.

2) 共轭搜索问题:给定$(x,y)\in B_n\times B_n$,x 和 y 共轭,求解一个 $a\in B_n$,使得 $y=a^{-1}xa$.

3) 一般化共轭搜索问题(问题 2)的一般情况):给定$(x,y)\in B_n\times B_n$ 和 $m<n$,若存在 $b\in B_m$,使得 $y=b^{-1}xb$,求解一 $a\in B_m$,使得 $y=a^{-1}xa$.

4) Diffie-Hellman 共轭问题:给定 $p\in B_n$,对任意$(a,b)\in LB_l\times RB_r$,若已知 $a^{-1}pa$ 和 $b^{-1}pb$,求 $a^{-1}b^{-1}pab$.

就目前的研究状况来看,这些问题都遭到不同程度的攻击,依赖于这些"难解"问题所构造的公钥加密算法,其安全性是不够的.

2 辫子群上的公钥加密算法

2.1 已有公钥加密算法

一个实用的辫子群上的公钥加密算法 BPKE1 是由 Ko 和 Lee 等人在文献[3]中提出来的,其安全性是基于上述的 Diffie-Hellman 共轭问题,该公钥加密算法的一个更一般的版本是由 Cha 和 Cheon 等人在文献[2]中提出来的,下面我们描述这个更一般的算法.

算法 **1**. 辫子群上的公钥加密算法 BPKE2[2].

私钥:辫子对$(x_1,x_2)\in LB_l\times LB_l$.

公钥:辫子对(a,b),其中:$a\in B_n$;$b=x_1ax_2$.

加密过程:

假设消息为 $M\in\{0,1\}^k$,加密算法所使用的散列函数为 $H:B_n\to\{0,1\}^k$,

1) 随机选择$(y_1,y_2)\in RB_r\times RB_r$.

2) 密文为$(y_1ay_2,H(y_1by_2)\oplus M)$.

解密过程:

给定密文(c,d),明文为 $M=H(x_1cx_2)\oplus d$.

文献[3]中的版本 BPKE1 规定 $x_2=x_1^{-1}$,$y_2=y_1^{-1}$.

显然,由于$(x_1,x_2)\in LB_l\times LB_l$,$(y_1,y_2)\in RB_r\times RB_r$,所以,$x_1y_1=y_1x_1$,$x_2y_2=y_2x_2$,因此,

$$H(x_1y_1ay_2x_2)\oplus H(y_1by_2)\oplus M=H(y_1x_1ax_2y_2)\oplus H(y_1by_2)\oplus M=H(y_1by_2)\oplus H(y_1by_2)\oplus M=M,$$

所以,解密是正确的.

2.2 已知攻击

定义 **3**(**P-BPKE** 问题)[4]. 给定$(x,y)\in B_n^+\times B_n^+$,如果存在$(a,b)\in LB_l^+\times LB_l^+$使得 $y=axb$,求出至少一对这样的(a,b).

显然,如果 P-BPKE 问题可解,那么 BPKE2 公钥加密算法就可以破译.

文献[4]给出了两种 P-BPKE 问题的概率解法.这些解法用辫子群的 Burau 表示,对 Hughes[5]算法进行了改进.实验结果表明:随着 n 以及 a 和 b 的标准长度的增加,线性表示攻击成功的概率会显著减小.

Cheon 和 Jun[6]利用辫子群的 Lawrence-Krammer 表示,可以在多项式时间内解决 Diffie-Hellman 共轭问题,因而也可以用来攻击 BPKE1.

BPKE2 公钥加密算法已经回避了利用共轭问题来构造加密算法,因此,一些基于辫子群共轭性的攻击方法,如 Hofheinz-Steinwandt 共轭搜索攻击[7]、SSS(super summit set)和 USS(ultra summit set)[8]集合攻击等,是不能奏效的.

此外,由 Hughes 等人提出的长度攻击,后来经 Garber 等人一般化[9],可以用来求解辫子群上的一般性方程.这种方法是一种概率攻击方法,成功的前提是同一变量必须提供足够的概率累积,不能用于 BPKE2.

3 新的难解问题

本节我们提出两种新的辫子群上的难解问题,它们均通过增加问题中变量的个数来增加难解性.

3.1 多重**P-BPKE**问题

定义 **4**(多重 **P-BPKE** 问题). 给定 w_i 和 $v_i\in B_n$,$1\le i\le k$,如果存在 $x_i(0\le i\le k)\in LB_l$,使得 $w_i=x_{i-1}v_i\,x_i^{-1}$ $(1\le i\le k)$,求出至少一组这样的 $x_i(0\le i\le k)$.

当所有 $x_i(0\le i\le k)$相等时,多重 P-BPKE 问题就是 MSCP(multiple simultaneous conjugacy problem)问题[10].MSCP 问题首先被应用在 AAG 密钥协商协议[11]之中,文献[5,10]对这一问题的解法进行了探讨.下面我们来分析多重 P-BPKE 问题的安全性.

首先,由于 $x_i(0\le i\le k)$的生成元为初等辫子,而且每个 $x_i(0\le i\le k)$和它的逆仅在最多两个等式中出现,所以不能提供概率累积,因而,长度攻击不能解决多重 P-BPKE 问题.

此外,多重 P-BPKE 问题不涉及明显的共轭变换,通过等式 $w_i=x_{i-1}v_i\,x_i^{-1}$ $(1\le i\le k)$唯一能够构造出的非平凡的一类共轭关系为 $w_{i+1}w_i=x_i(v_{i+1}\,x_{i+1}^{-1}x_{i-1}v_i)\,x_i^{-1}$,但是 $v_{i+1}\,x_{i+1}^{-1}x_{i-1}v_i$ 未知,共轭搜索攻击和基于 Diffie-Hellman 共轭问题的攻击都不能用于求解此类问题.

设ρ为 B_n 上的任一线性表示,E 为多重 P-BPKE 问题在ρ表示下的矩阵方程组,如果没有有效的算法可以判断某一矩阵是否为像集$\rho(B_n)$中的元素,那么,当 E 没有唯一确定解的时候,基于ρ表示的攻击不能解决多重 P-BPKE 问题,因为我们无法从 E 的无数个矩阵解中判断哪一个解才是像集$\rho(B_n)$中的元素,“提升”回辫子群的过程就会失效.Burau 表示、着色 Burau 表示和 Lawrence-Krammer 表示都属于此类线性表示.

从文献[4,5]我们可以看出:Burau 线性表示攻击成功的必要条件是通过矩阵方程能够求得所求解对象的一个唯一确定的 Burau 表示,然后才能“提升”回辫子群.在文献[5]中,AAFG 密钥交换协议提供了足够多的共轭辫子对,使得方程的个数超过了变元的个数,因而矩阵方程可解;在文献[4]中,由于 BPKE2 加密算法的特殊性,使得矩阵方程(在系数为满秩的情况下)可以利用矩阵变换直接求解.

对于 Burau 线性表示,我们可以估算多重 P-BPKE 问题抵抗线性表示攻击的参数取值.首先,我们证明关于 Burau 线性表示的一个性质:

定理 **1**. 如果 $x\in LB_l$,那么,x 的 Burau 表示是一个分块对角矩阵:

$$\begin{pmatrix}\boldsymbol{x}_l & 0\\ 0 & \boldsymbol{I}_{n-l}\end{pmatrix}.$$

如果 $x\in RB_r$,那么,x 的 Burau 表示是一个分块对角矩阵:

$$\begin{pmatrix}\boldsymbol{I}_{n-r} & 0\\ 0 & \boldsymbol{x}_r\end{pmatrix},$$

其中:$\boldsymbol{x}_l,\boldsymbol{x}_r$ 是 l 阶和 r 阶方阵;$\boldsymbol{I}_{n-1},\boldsymbol{I}_{n-r}$ 是 $n-l$ 阶和 $n-r$ 阶单位矩阵.

证明:由 Burau 表示的定义,初等辫子σ_i 的 Burau 表示为

$$\rho(\sigma_i)(t)=\begin{pmatrix}\boldsymbol{I}_{i-1} & & & 0\\ & 1-t & t & \\ & 1 & 0 & \\ 0 & & & \boldsymbol{I}_{n-i-1}\end{pmatrix},$$

其中:$\boldsymbol{I}_{i-1},\boldsymbol{I}_{n-i-1}$ 分别为 $i-1$ 和 $n-i-1$ 阶单位矩阵;元素 $1-t$ 出现在主对角线上第 i 行和 i 列的位置.当 $i<l$ 时,$\sigma_i\in LB_l$;而当 $i>n-r$ 时,$\sigma_i\in RB_r$.两种情况下,$\rho(\sigma_i)(t)$显然均为定理中所述的分块对角矩阵.根据矩阵乘法的性质,分块对角矩阵对于矩阵乘法是封闭的,再由 Burau 表示的线性性质,即可得到结论. □

定理 **2**. 如果 $l>(2kn+2k+2)/(2k+1)$,则在多重 P-BPKE 问题的 Burau 线性表示中,变元的个数多于方程的个数.

证明:假设利用 Burau 表示形成的关于多重 P-BPKE 问题的 k 个矩阵方程为

$$\boldsymbol{W}_1=\boldsymbol{X}_0\boldsymbol{V}_1\,\boldsymbol{X}_1^{-1},\boldsymbol{W}_2=\boldsymbol{X}_1\boldsymbol{V}_2\,\boldsymbol{X}_2^{-1},\ldots,\boldsymbol{W}_k=\boldsymbol{X}_{k-1}\boldsymbol{V}_k\,\boldsymbol{X}_k^{-1} \tag{1}$$

其中:所有矩阵均是 n 阶方阵;$\boldsymbol{W}_i,\boldsymbol{V}_i$ 分别是 w_i 和 $v_i(1\le i\le k)$的 Burau 表示;$\boldsymbol{X}_i$ 是 $x_i(0\le i\le k)$的 Burau 表示.为了便于分析,我们对方程组(1)进行化简,变形为

$$\boldsymbol{W}_1\boldsymbol{X}_1=\boldsymbol{X}_0\boldsymbol{V}_1,\boldsymbol{W}_2\boldsymbol{X}_2=\boldsymbol{X}_1\boldsymbol{V}_2,\ldots,\boldsymbol{W}_k\boldsymbol{X}_k=\boldsymbol{X}_{k-1}\boldsymbol{V}_k \tag{2}$$

由于 $x_i\in LB_l$,所以,根据定理 1,可以将 $\boldsymbol{X}_i$ 看成是具有 l^2 个简单变量的未知元,这样,方程组(2)总共有$(k+1)l^2$ 个简单变量.将方程组(2)中的所有矩阵方程分块表示为

$$\begin{pmatrix}\boldsymbol{W}_{i,1} & \boldsymbol{W}_{i,2}\\ \boldsymbol{W}_{i,3} & \boldsymbol{W}_{i,4}\end{pmatrix}\begin{pmatrix}\boldsymbol{X}_{i,1} & 0\\ 0 & \boldsymbol{I}_{n-l}\end{pmatrix}=\begin{pmatrix}\boldsymbol{X}_{i-1,1} & 0\\ 0 & \boldsymbol{I}_{n-l}\end{pmatrix}\begin{pmatrix}\boldsymbol{V}_{i,1} & \boldsymbol{V}_{i,2}\\ \boldsymbol{V}_{i,3} & \boldsymbol{V}_{i,4}\end{pmatrix},i=1,2,\ldots,k,$$

也就是

$$\begin{pmatrix} \boldsymbol{W}_{i,1}\boldsymbol{X}_{i,1} & \boldsymbol{W}_{i,2} \\ \boldsymbol{W}_{i,3}\boldsymbol{X}_{i,1} & \boldsymbol{W}_{i,4} \end{pmatrix} = \begin{pmatrix} \boldsymbol{X}_{i-1,1}\boldsymbol{V}_{i,1} & \boldsymbol{X}_{i-1,1}\boldsymbol{V}_{i,2} \\ \boldsymbol{V}_{i,3} & \boldsymbol{V}_{i,4} \end{pmatrix}, i=1,2,\ldots,k.$$

对比矩阵中的各个元素,每个矩阵方程可以得到 $l^2+2l(n-l)$个关于简单变量的方程,k 个矩阵方程总共有 $k(l^2+2l(n-l))$个方程.由文献[5]还得知:Burau 表示的每个行向量和列向量均满足一个线性约束条件,这些约束条件的总个数为 $2l(k+1)$.将它们加上之后,我们共可以得到 $k(l^2+2l(n-l))+2l(k+1)$个关于变元的方程.如果要求 $k(l^2+2l(n-l))+2l(k+1)<(k+1)l^2$,即有 $l>(2kn+2k+2)/(2k+1)$. □

3.2 因子隐藏问题(BFHP)

定义 5(因子隐藏问题 **BFHP**). 给定 w 和 $v_i\in B_n, 1\le i\le k$,如果存在 $x_i(0\le i\le k)\in RB_r$ 使得 $w=x_0v_1x_1v_2\ldots v_kx_k$,求出至少一组这样的 $x_i(0\le i\le k)$.

首先,与多重 P-BPKE 问题一样,我们有下面的结论:长度攻击、共轭搜索攻击和基于 Diffie-Hellman 共轭问题的攻击不能解决 BFHP 问题.

利用 Burau 表示,我们计算 BFHP 问题抵抗 Burau 表示攻击的能力.

定理 **3**. 如果$(r-1)^2>n^2/(k+1)+1$,则在 BFHP 问题的 Burau 线性表示中,变元的个数多于方程的个数.

证明:利用 Burau 表示,我们将方程 $w=x_0v_1x_1v_2\ldots v_kx_k$ 映射成矩阵方程.由于 $x_i(0\le i\le k)\in RB_r$,其 Burau 表示中变元的个数为 r^2,所以,矩阵方程中总共有$(k+1)r^2$ 个变元.矩阵方程再加上 Burau 表示的约束条件,方程的总个数为 $n^2+2r(k+1)$.为了使变元的个数多于方程的个数,只需$(k+1)r^2>n^2+2r(k+1)$,即

$$(r-1)^2>n^2/(k+1)+1.$$ □

实事上,如果 $n=l+r$,定理 2 和定理 3 的条件是不可能同时满足的.因为由$(r-1)^2>n^2/(k+1)+1$ 和 $n=l+r$,我们有

$$l<n-1-\sqrt{n^2/(k+1)+1},$$

结合定理 2,我们可以得到

$$(2kn+2k+2)/(2k+1)<l<n-1-\sqrt{n^2/(k+1)+1}.$$

但是

$$(2kn+2k+2)/(2k+1)-(n-1-\sqrt{n^2/(k+1)+1})=\sqrt{n^2/(k+1)+1}-(n-1)/(2k+1)+2$$
$$>\sqrt{(n-1)^2/(k+1)}-(n-1)/(2k+1)+2>0,$$

这要求$(2kn+2k+2)/(2k+1)>n-1-\sqrt{n^2/(k+1)+1}$,矛盾. □

但是,BFHP 问题中的方程是 $Z[t,t^{-1}]$上的高次多变量方程,即使方程的个数多于变元的个数(overdefined),求解这样的系统也是一个 NP 困难的问题.

4 新的公钥加密算法

4.1 新加密算法描述

根据第 3 节所描述的两个辫子群上的难解问题,我们提出如下新的公钥加密算法.

算法 **2**. 辫子群上新的公钥加密算法 NBPKE.

选择正整数 l,n,k 满足 $n-2>l>(2kn+2k+2)/(2k+1)$.

私钥:随机选取的 $k+1$ 个辫子 $x_i(0\le i\le k)\in RB_r$.

公钥:随机选取 k 个辫子 $v_i(1\le i\le k)\in B_n$,并公开 $v_i(1\le i\le k)$和 $w=x_0v_1x_1v_2\ldots v_kx_k$.

加密过程:

假设消息为 $M\in\{0,1\}^m$,加密算法所使用的散列函数为 $H:B_n\to\{0,1\}^m$,

1) 随机选择 $y_i(0\le i\le k)\in LB_l$,计算 $w_i=y_{i-1}v_i\,y_i^{-1}(1\le i\le k)$.

2) 密文为$(w_1,w_2,\ldots,w_k,H(y_0w\,y_k^{-1})\oplus M)$.

解密过程:

若给定密文为($w'_1, w'_2, \ldots, w'_k, c$),则对应的明文为 $H(x_0\, w'_1\, x_1\, w'_2 \ldots w'_k\, x_k)\oplus c$.

4.2 算法分析

4.2.1 l 的存在性

从算法参数的选择可知,l 必须满足 $n-2>l>(2kn+2k+2)/(2k+1)$.适当地选择 n 和 k,在 $n-2$ 和 $(2kn+2k+2)/(2k+1)$ 之间必然有这样的整数 l 存在,这是因为 $n-2-(2kn+2k+2)/(2k+1)=(n-1)/(2k+1)-3$,当 $n-1>5(2k+1)$ 时,$(n-1)/(2k+1)-3>5-3=2$.即 $n-2$ 和 $(2kn+2k+2)/(2k+1)$ 的差比 2 大,它们之间至少存在一个整数.

例如,当 $n=150$ 时,k 取 10,l 可以取从 143~147 的所有整数,相应地,r 的取值为 7~3.

4.2.2 加解密过程的正确性

假设密文为

$$(w_1,w_2,\ldots,w_k,H(y_0w\ y_k^{-1})\oplus M),$$

则

$$x_0w_1x_1w_2\ldots w_kx_k=x_0(y_0v_1\ y_1^{-1})x_1(y_1v_2\ y_2^{-1})\ldots(y_{k-1}v_k\ y_k^{-1})x_k.$$

由于 $x_i(0\le i\le k)\in RB_r, y_i(0\le i\le k)\in LB_l$,所以,$x_i$ 和 y_i 是可以交换的,因此,

$$x_0(y_0v_1\ y_1^{-1})x_1(y_1v_2\ y_2^{-1})\ldots(y_{k-1}v_k\ y_k^{-1})x_k= y_0x_0v_1x_1v_2\ldots v_kx_k\ y_k^{-1}=y_0w\ y_k^{-1},$$

所以,$H(x_0w_1x_1w_2\ldots w_kx_k)\oplus H(y_0w\ y_k^{-1})\oplus M=M$,解密成功.

4.2.3 算法的安全性

NBPKE 公钥加密算法的安全基础恰好是第 3 节中描述的两个辫子群上的难解问题.攻击者企图从公钥恢复私钥,也就是从 $v_i(1\le i\le k)$和 w 恢复 $x_i(0\le i\le k)$,等价于要解决 BFHP 问题;而企图从密文恢复随机辫子或者明文,也就是从 $w_i=y_{i-1}v_i\ y_i^{-1}\ (1\le i\le k)$或者 $H(y_0w\ y_k^{-1})\oplus M$ 中恢复 $y_i(0\le i\le k)$或者 M,只要散列函数足够安全,就等价于要解决多重 P-BPKE 问题.

从第 3 节的讨论可知:多重 P-BPKE 问题和 BFHP 问题可以抵抗长度攻击、共轭搜索攻击和基于 Diffie-Hellman 共轭问题的攻击,而且通过 Burau 表示来求解 BFHP 问题是一个 NP 难的问题.

在方程组(2)中,当所有方程的个数不少于变元的个数时,由于这些方程均为线性方程,可以以非零的概率通过线性方程组求解的方法求得所有变元.而当所有方程的个数少于变元的个数时,方程组(2)就没有确定的解.此时,若选择方程组(1)的任意一个特解,由于我们不能判断它是否属于 Burau 表示的像集,因此,Burau 表示攻击将失效.这说明适当地选择参数,多重 P-BPKE 问题可以抵抗基于 Burau 表示的线性攻击.从算法 2 的描述中我们可以知道:由于 $n-2>l>(2kn+2k+2)/(2k+1)$,算法满足定理 2 的条件.

综上所述,NBPKE 对于目前已知的这些攻击方法都具有免疫能力.

4.2.4 算法参数选择

BFHP 问题的 Burau 表示中共有 $(k+1)r^2$ 个变元和 $n^2+2r(k+1)$个方程,为了增加 BFHP 问题的难度,变元的个数应该尽可能地多,这就要求 k 和 r 要尽可能地大.但是,由 $r+l=n$ 和 $n-2>l>(2kn+2k+2)/(2k+1)$可知:当 k 增大时,n 必须取得足够大才能保证 l 的存在性;而当 r 增大时,l 又必须相应地减小.为此,我们建议 NBPKE 公钥加密算法中 n 的取值要充分大,而 l 只需取比 $(2kn+2k+2)/(2k+1)$稍大的整数即可.例如:对于以上 $n=150$ 的情况,k 取 10,l 和 r 的取值可分别为 143 和 7.

4.2.5 随机辫子的生成

定义 **6**(方阵的带宽). 一个方阵的带宽是指该方阵中与主对角线最远的非零元素的距离.

例如:任意 $\sigma_i(1\le i\le n-1)$及其逆的 Burau 表示的带宽为 1;任意 $\sigma_i^{\pm1}\ \sigma_j^{\pm1}\ (1\le i,j\le n-1)$,当 $|i-j|=1$ 时,其 Burau 表示的带宽为 2;否则为 0 或者 1.

Burau 表示的带宽是 Burau 线性表示攻击能否成功的一个非常重要的因素,因为如果带宽很小,那么 Burau 表示方阵中偏离对角线较远的未知元是可以事先预知的,这就降低了线性方程组中未知元的个数,从而增加了

求解唯一确定解的可能性.文献[5]正是利用了 Burau 表示的这一特点,简化了方程求解过程.

NBPKE 中的辫子都是随机产生的,假设 RNG 是一个取值范围为[1–n, –1]∪[1,n–1]的随机数发生器,一个直接的生成随机辫子的方法是:当 RNG 取值为 i(1≤i≤n–1)时,我们就选择初等辫子σ_i;当 RNG 取值为 j(1–n≤j≤–1)时,我们就选择初等辫子σ_{-j}的逆σ_{-j}^{-1},经过 k 次这样的处理,我们就可以得到一个由 k 个初等辫子或它们的逆的乘积所形成的随机的辫子.

根据以上对于 Burau 表示方阵的带宽的讨论,两个初等辫子相乘,只有当|i–j|=1 时,带宽才会增加,因此,我们得出了下面带宽增加较快的随机辫子生成算法.

算法 **3**. 随机辫子生成算法.

输入:正整数 n≥3.

输出:由 k 个初等辫子或它们的逆相乘生成的随机辫子 w.

1) 选择一个取值范围为[1,n–1]的随机数发生器 RNG,初始化 w=ε.
2) 调用 RNG 产生一个随机的正整数 i.
3) 调用 RNG 产生一个随机的正整数 j,令 j=j mod 5.
   如果 i=1:j 为 0 或者 1,则跳转到步骤 2);j 为 2,则 w=$w\sigma_i$;j 为 3,则 w=$w\sigma_{i+1}$,i=i+1;j 为 4,则 w=$w\sigma_{i+1}^{-1}$,i=i+1.
   如果 i=n–1:j 为 0,则 w=$w\sigma_{i-1}$,i=i–1;j 为 1,则 w=$w\sigma_{i-1}^{-1}$,i=i–1;j 为 2,则 w=$w\sigma_i$;j 为 3 或 4,则跳转到步骤 2).
   如果 1<i<n–1:j 为 0,则 w=$w\sigma_{i-1}$,i=i–1;j 为 1,则 w=$w\sigma_{i-1}^{-1}$,i=i–1;j 为 2,则 w=$w\sigma_i$;j 为 3,则 w=$w\sigma_{i+1}$,i=i+1;j 为 4,则 w=$w\sigma_{i+1}^{-1}$,i=i+1.
4) k=k–1:如果 k=0,w 即为所求;否则跳转到步骤 3).

利用此算法,由于相邻元素的序号多数仅相差 1,因此,其 Burau 表示的带宽增长更快.

值得注意的是:算法 3 虽然较快地增加了带宽,但是在随机性上是有所损失的,建议在生成随机辫子的过程中,对算法 3 的结果作进一步的混乱.

4.2.6 效率分析

由文献[2]可知:如果用 s 表示辫子的最大标准长度(这里假设 s 为 NBPKE 中随机辫子的最大标准长度),用 n 表示辫子群的指标,而且 B_n 中的辫子采用 Artin 表示,那么,辫子群上的乘法、逆运算和随机辫子生成的复杂度均为 $O(sn)$,将辫子表示成范式的复杂度为 $O(s^2n\log n)$.在算法 2 中,由于要计算 $H(y_0w\ y_k^{-1})$,必须将 $y_0w\ y_k^{-1}$ 表示成范式,所以,加密和解密过程均涉及到一次表示成范式运算,复杂度为 $O(k^2s^2n\log n)$.此外,加密过程共用了 2k+2 次乘法和 k 次求逆运算,解密过程共用了 2k 次乘法,所以,除了表示成范式,其他运算的算法复杂度均为 $O(ksn)$.

根据文献[3]的结论,一个由 s 个标准因子相乘所形成的辫子可以用 $sn\log n$ 比特来表示.由于存储一根辫子的空间复杂度为 $O(sn\log n)$,所以,算法的总体空间复杂度为 $O(ksn\log n)$.经过简单计算可知:NBPKE 的私钥大小为(k+1)$sr\log r$;公钥大小最多为 $ksn\log n$+(2k+1)$sn\log n$=(3k+1)$sn\log n$.

当 n=150,s=20 时,在 Pentium III 866MHZ 机器上,BPKE2 的加密速度为 163.40KB/s,解密速度为 206.94KB/s;而 NBPKE 算法的加解密速度大致为 BPKE2 的 1/k.因此在实用过程中,参数 k 的选取应兼顾安全性和效率两方面的因素,综合加以考虑.

5 结束语

本文分析了当前针对辫子群公钥密码系统的各种攻击方法和攻击成功的原因,提出了两个辫子群上的难解问题:多重 P-BPKE 问题和 BFHP 问题,并在这两个问题的基础上设计了一个新的公钥加密算法 NBPKE.由分析可知,该算法可以抵抗目前各种已知的攻击方法.

本文将简单问题复合成多变量难解问题的研究思路,对于设计新型公钥密码系统有一定的启发作用.

致谢　我们向给予本文工作支持和建议的信息安全实验室的教师、博士生和讨论班的所有学生表示感谢.

References:

[1] Shor PW. Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1997,26(5):1484−1509.

[2] Cha JC, Cheon JH, Han JW, Ko KH, Lee SJ. An efficient implementation of braid groups. In: Boyd C, ed. Advances in Cryptology-ASIACRYPT 2001. LNCS 2048, Berlin: Springer-Verlag, 2001. 144−156.

[3] Ko KH, Lee SJ, Cheon JH, Han JW, Kang SJ, Park CS. New public-key cryptosystem using braid groups. In: Bellare M, ed. Advances in Cryptology- CRYPTO 2000. LNCS 1880, Berlin: Springer-Verlag, 2000. 166−183.

[4] Lee E, Park JH. Cryptanalysis of the public key encryption based on braid groups. In: Biham E, ed. Advances in Cryptology-EuroCrypt 2003. LNCS 2656, Berlin: Springer-Verlag, 2003. 477−490.

[5] Hughes J. A linear algebraic attack on the AAFG1 braid group cryptosystem. In: Batten L, Seberry J, eds. Information Security and Privacy—7th Australian Conf., ACISP 2002. LNCS 2384, Berlin: Springer−Verlag, 2002. 176−189.

[6] Cheon JH, Jun B. A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem. In: Boneh D, ed. Advances in Cryptology-CRYPTO 2003. LNCS 2729, New York: Springer-Verlag, 2003. 212−225.

[7] Hofheinz D, Steinwandt R. A practical attack on some braid group based cryptographic primitives. In: Desmedt YG, ed. Public Key Cryptography-PKC 2003. LNCS 2567, Berlin: Springer-Verlag, 2003. 187−198.

[8] Dehornoy P. Braid-Based Cryptography. In: Group Theory, Statistics, and Cryptography, Contemporary Mathematics 360. New York: ACM Press, 2004. 5−33.

[9] Garber D, Kaplan S, Teicher M, Tsaban B, Vishne U. Probabilistic solutions of equations in the braid group. Advances in Applied Mathematics, 2005,35(3):323−334.

[10] Lee SJ, Lee E. Potential weaknesses of the commutator key agreement protocol based on braid groups. In: Knudsen LR, ed. EUROCRYPT 2002. LNCS 2332, New York: Springer-Verlag, 2002. 14−28.

[11] Anshel I, Anshel M, Goldfeld D. An algebraic method for public-key cryptography. Mathematical Research Letters, 1999,6(3): 287−291.

汤学明(1974－),男,湖北武汉人,博士生,讲师,主要研究领域为密码学,数据库安全,网络安全.

洪帆(1942－),女,教授,博士生导师,主要研究领域为访问控制技术,数字水印技术,电子商务.

崔国华(1947－),男,教授,博士生导师,主要研究领域为密码学,计算方法.