基于辫子群的不经意传输协议*

朱 丹[1]，鲍皖苏[1]，隗 云[2]，张兴凯[3]
（1. 信息工程大学 电子技术学院，郑州 450004；2. 电子技术研究所，北京 100195；3. 96610 部队，北京 102208）

摘 要：分析指出现有辫子群上的不经意传输协议通过辫元的指数形式隐藏接收者的选择信息进而保证其隐私性，辫元指数形式的存在导致该协议计算效率较低。基于辫子群上同时共轭搜索问题和分解问题的难解性，提出了一个 N 取 M 不经意传输协议，当 $M=1$ 时对应协议比现有协议的计算效率更高。

关键词：辫子群；不经意传输；同时共轭搜索问题；分解问题
中图分类号：TP309 **文献标志码**：A **文章编号**：1001-3695(2012)06-2265-03
doi:10.3969/j.issn.1001-3695.2012.06.070

Oblivious transfer protocol based on braid groups

ZHU Dan[1], BAO Wan-su[1], WEI Yun[2], ZHANG Xing-kai[3]
(1. *Institute of Electronic Technology, Information Engineering University, Zhengzhou* 450004, *China*; 2. *Institute of Electronic Technology, Beijing* 100195, *China*; 3. *Unit* 96610, *Beijing* 102208, *China*)

Abstract: It is shown that the existing oblivious transfer protocols hided the choice of the receiver using exponential braids, which made the protocols have low efficiency. This paper proposed an M-out-of-N oblivious transfer protocol based on the difficulty of the simultaneous conjugacy search problem and the decomposition problem over the braid groups. When $M=1$ the proposed protocol is much more efficient in computation than existing protocol.

Key words: braid group; oblivious transfer; simultaneous conjugacy search problem; decomposition problem

20 世纪 90 年代中期，Shor[1] 和 Boneh 等人[2] 提出了能在多项式时间内求解整数分解和离散对数问题的量子算法，给目前广泛使用的公钥密码体制带来了严重威胁。为了构造抗量子攻击的密码体制，大量学者开始寻找新的数学难题作为构造密码体制的基础，如格上的难解问题[3]、组合群论中的难解问题[4] 等。

辫群[5] 是组合群论中具有代表性的一类群，当生成元个数不少于两个时，辫群是无限非交换群，其结构复杂，群上的乘法、求逆等运算所需的时间和空间都很小。辫群上的数学问题，如共轭搜索、Diffie-Hellman 共轭、共轭分解及求根问题等都是难解问题。辫群所具有的以上特点使得其一经提出就在公钥密码领域引起了广泛关注[6~18]。

不经意传输协议是密码学中一种重要的基础协议，其思想最早由 Rabin[19] 提出。随后，在该思想基础之上学者们分别提出 2 取 1 不经意传输[20,21]、N 取 1 不经意传输[22]、N 取 M 不经意传输协议[23]，不仅很好地解决了电子商务中保护用户隐私的问题，还为构造安全计算协议[24]、电子拍卖协议[25] 等提供了一种重要工具。

2010 年，辫子群首次被用于构造不经意传输协议[26]，该文献中协议通过辫元的指数形式隐藏接收者的选择信息进而保证其隐私性，辫元指数形式的存在导致该协议计算效率较低。本文基于辫子群上同时共轭搜索问题和分解问题的难解性，提出了一个 N 取 M 不经意传输协议，当 $M=1$ 时对应的 N 取 2 不经意传输协议、N 取 1 不经意传输协议都比现有协议的计算效率高。

记文献[26]中 N 取 1 不经意传输协议为 WXZB 协议。

1 预备知识

本章介绍辫子群、辫子群上的难解问题及不经意传输协议的安全性质。

1.1 辫子群

定义 1[6] 对于不小于 2 的自然数 n，由 $n-1$ 个初等辫子 $\sigma_1,\sigma_2,\cdots,\sigma_{n-1}$ 生成的辫子群 B_n 表示为

$$B_n=\left(\sigma_1,\sigma_2,\cdots,\sigma_{n-1}\left|\begin{array}{ll}\sigma_i\sigma_{i+1}\sigma_i=\sigma_{i+1}\sigma_i\sigma_{i+1} & 1\leqslant i\leqslant n-2\\ \sigma_i\sigma_j=\sigma_j\sigma_i & |i-j|\geqslant 2\end{array}\right.\right)$$

其中：$\sigma_1,\sigma_2,\cdots,\sigma_{n-1}$ 又称为辫子群的生成子，辫子群 B_n 中的元素称为 n 辫子或辫元，n 称为辫指数。

显然，由一个初等辫子生成的辫子群 B_2 是无限阶的循环群，当 $n>2$ 时，B_n 是无限非交换群，本文不考虑 B_2。

定义 2[6] 在辫子群 B_n 中，对 $l\leqslant n$，其生成元的左边 $l-1$ 个生成元 $\sigma_1,\sigma_2,\cdots,\sigma_{l-1}$ 生成的群叫 B_n 的左子群，记作 LB_n；由 $\sigma_{l+1},\cdots,\sigma_{n-1}$ 生成的群叫 B_n 的右子群，记作 RB_n。

显然，对任意 $(\alpha,\beta)\in LB_n\times RB_n$，均有 $\alpha\beta=\beta\alpha$。

定义 3[6] 对于辫元 $\alpha,\beta\in B_n$，若存在一个辫元 $s\in B_n$ 使得 $\beta=s^{-1}\alpha s$，则称辫元 α,β 共轭，记作 $\alpha\sim\beta$。

定义 4[6] 给定 $(\alpha,\beta)\in B_n\times B_n$，判断 $\alpha\sim\beta$ 是否成立，称共轭判断问题(conjugacy decision problem)。

收稿日期：2011-10-15；**修回日期**：2011-12-09 **基金项目**：国家自然科学基金资助项目(10501053)

作者简介：朱丹(1978-)，男，硕士，主要研究方向为密码协议的设计与分析；鲍皖苏(1966-)，男，教授，博导，博士，主要研究方向为密码学；隗云(1982-)，女，博士，主要研究方向为密码协议的设计与分析(weiyun456@sohu.com)；张兴凯(1981-)，男，工程师，硕士，主要研究方向为密码协议的设计与分析.

2001 年,Cha 等人提出了一种多项式时间算法,能对辫子群上的共轭判断问题进行成功求解[6]。

定义 5[6] 给定辫元对$(\alpha,\beta)\in B_n\times B_n,\alpha\sim\beta$,找到满足$\beta=s^{-1}\alpha s$ 的辫元 $s\in B_n$,称共轭搜索问题(conjugacy search problem,CSP)。

定义 6[6] 给定 $\alpha_1,\cdots,\alpha_N\in B_n$ 及 $s^{-1}\alpha_1 s,\cdots,s^{-1}\alpha_N s\in B_n$,求辫元 $t\in B_n$,满足 $t^{-1}\alpha_1 t=s^{-1}\alpha_1 s,\cdots,t^{-1}\alpha_N t=s^{-1}x_N s$,称同时共轭搜索问题(simutaneous conjugacy search problem)。

定义 7[6] 给定$(\alpha,\beta)\in B_n\times B_n$,满足存在$s,s'\in B_{n'}(n'<n)$,使得$\beta=s\alpha s'$,找到 $t,t'\in B_{n'}$,使得$\beta=t\alpha t'$,称分解问题(decomposition problem)。

但是,尚未有算法能证明可在多项式时间内有效求解共轭搜索问题、同时共轭搜索问题或分解问题。

1.2 不经意传输

在一个 N 取 M 不经意传输协议中,发送者 Alice 的输入为消息 $m_1,\cdots,m_N\in\{0,1\}^k$,接收者 Bob 的输入为 $\tau_1,\cdots,\tau_M\in\{0,1\}$。在执行完协议后,Bob 能得到自己选择的消息$m_{\tau_1},\cdots,m_{\tau_M}$,而 Alice 则不知道 Bob 选择了哪几个消息。显然,2 取 1 不经意传输和 N 取 1 不经意传输都是 N 取 M 不经意传输的特例。

一个安全的 N 取 M 不经意传输协议应满足以下性质:

正确性:若发送者与接收者正确执行协议,协议完成后接收者得到其所选择的消息,即 P[Bob 得到 $m_{\tau_1},\cdots,m_{\tau_M}$ | Alice 和 Bob 都是诚实的]=1。

接收者的隐私性(不经意性):接收者的不同选择所对应的传输副本对于发送者是不可区分的,即 P[Alice 得到 τ | Bob 是诚实的]$=M/N(\tau\in\{\tau_1,\cdots,\tau_M\})$。

发送者的隐私性:接收者不能得到他没有选择的消息。除他所选择的消息所对应密文外,其余密文与随机数据对于接收者是不可区分的,即 P[Bob 得到 m_j | Alice 是诚实的]$=1/2^k$ $(1\leqslant j\leqslant N,j\notin\{\tau_1,\cdots,\tau_M\})$。

2 WXZB 协议

2.1 WXZB 协议

由于文献[26]中 2 取 1 不经意传输协议是 N 取 1 不经意传输协议的特例,本节只介绍其 N 取 1 不经意传输协议,即 WXZB 协议。

假设协议参与者为 Alice 和 Bob,其中 Alice 为发送方,Bob 为接收方。Alice 拥有的消息为 $m_1,\cdots,m_N$,Bob 选择的消息为 m_τ。

系统参数:Alice 和 Bob 共同选择辫子群 B_n,其左右子群 LB_n、RB_n 及抗碰撞的单向函数 $H:B_n\to\{0,1\}^*$。Bob 选择 $x\in B_n$,$h\in RB_n$ 及足够大的正整数 r,计算 $y=x^r$,公开 y 和 h。

协议过程如下:

a) Bob 随机选择 $a\in LB_n$,计算 $t=a^{-1}xah^\tau$;

b) Alice 随机选择 $b\in RB_n$,计算

$$A=b^{-1}yb$$
$$k_i=b^{-1}th^{-i}b\quad i=1,\cdots,N$$
$$C_i=H(k_i^r)\oplus m_i$$

并将$(A,C_1,\cdots,C_N)$发送给 Bob;

c) Bob 收到$(A,C_1,\cdots,C_N)$后,计算 $m_\tau=H(a^{-1}Aa)\oplus C_\tau$。

2.2 协议分析

由 2.1 节协议过程可知

$$(th^{-r})^r=(a^{-1}xah^\tau h^{-\tau})^r=(a^{-1}xa)^r=a^{-1}ya;y$$

不管 τ 的取值如何,$(th^{-\tau})^r$ 总是与 y 共轭。为了防止 Alice 猜测 r 的值进而通过$(th^{-\tau})^r$ 与 y 的共轭关系判断 Bob 的选择,r 需要取较大的值。由于 $C_i=H(k_i^r)\oplus m_i$,随着 r 的增大,协议复杂度也大大增加。

3 新的不经意传输协议

3.1 N 取 M 不经意传输协议

系统参数:Alice 和 Bob 共同选择辫子群 B_n,其左右子群 LB_n、RB_n 及抗碰撞的单向函数 $H:B_n\to\{0,1\}^*$。

协议过程如下:

a) Alice 随机选择 $x_1,\cdots,x_N\in B_n$,$a\in LB_n$,对 $i=1,\cdots,N$ 计算

$$A_i=a^{-1}x_i a$$
$$L_i=H(A_i)\oplus m_i$$

并将(x_i,L_i)发送给 Bob;

b) Bob 选择 $\tau_1,\cdots,\tau_M\in\{1,\cdots,N\}$ 后,随机选择 $b_0,b_1\in RB_n$,$b_0\neq b_1^{-1}$,计算

$$B_j=b_0x_{\tau_j}b_1\quad j=1,\cdots,M$$

并将其发送给 Alice;

c) 对 $j=1,\cdots,M$,Alice 计算 $C_j=a^{-1}B_j a$,并将其发送给 Bob;

d) Bob 计算

$$A'_j=b_0^{-1}C_j b_1^{-1}$$
$$m_{\tau_j}=H(A'_j)\oplus L_{\tau_j}$$

即可得到消息 $m_{\tau_j}(j=1,\cdots,M)$。

3.2 协议分析

下面对协议的安全性及效率进行分析。

1)正确性

由 $a\in LB_n$,$b_0,b_1\in RB_n$,知

$$A'_j=b_0^{-1}C_j b_1^{-1}=b_0^{-1}a^{-1}B_j a b_1^{-1}=a^{-1}b_0^{-1}(b_0x_{\tau_j}b_1)b_1^{-1}a=a^{-1}x_{\tau_j}a=A_{\tau_j}$$
$$H(A'_j)\oplus L_{\tau_j}=H(A_{\tau_j})\oplus L_{\tau_j}=m_{\tau_j}$$

成立。因此,如果 Alice 和 Bob 都遵守协议,则 Bob 总可以得到 $m_{\tau_j}(j=1,\cdots,M)$。

2)不经意性(Bob 的隐私性)

由 $b_0,b_1\in RB_n$,$b_0\neq b_1^{-1}$,$B_j=b_0x_{\tau_j}b_1(j=1,\cdots,M)$ 可知,B_j 与 x_{τ_j}不存在共轭关系。由于分解问题的难解性以及 b_0、b_1 的随机性,Alice 无法判断 $B_j(j=1,\cdots,M)$是由 $x_1,\cdots,x_N$ 中哪个元素计算而来。因此,Alice 不能得到 Bob 的选择,即协议可以保证 Bob 的隐私性。

3)Alice 的隐私性

由正确性可知,Bob 可计算

$$A'_j=a^{-1}x_{\tau_j}a=A_{\tau_j}$$

而对于 $i\neq\tau_1,\cdots,\tau_M$,$A_i=a^{-1}x_i a$,要想求出 A_i 必须先求出 a,而从 A_{τ_j}及 $C_j=a^{-1}B_j a$ 求解 a 将面临求解同时共轭搜索问题。

因此,Bob 选择 $\tau_1,\cdots,\tau_M\in\{1,\cdots,N\}$ 后只能得到消息 m_{τ_j}

$(j=1,\cdots,M)$,无法得到 $m_i(i\neq\tau_1,\cdots,\tau_M)$。因此,协议保证了 Alice 的隐私性。

4)计算效率

从协议过程可以看出,当 $M=1$ 时,WXZB 协议需执行 $N(r-1)+\tau+N(N+1)/2+2N+6$ 次乘法运算,而新协议只需执行 $2N+6$ 次乘法运算,计算效率大大提高。

4　结束语

非交换的辫子群是构造抗量子攻击密码协议的新平台。在现有辫子群上的不经意传输协议中,为保护接收者的隐私性,协议通过辫元的指数形式隐藏接收者的选择信息。为保证协议的安全性,需要选择较大的指数,使得协议执行过程中存在大量乘法运算,计算效率较低。本文基于辫子群上同时共轭搜索问题和分解问题的难解性,提出了一个 N 取 M 不经意传输协议,当 $M=1$ 时对应协议比现有协议的计算效率更高。

参考文献:

[1] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer [J]. SIAM Journal on Computing,1997,26(5):1484-1509.

[2] BONEH R,LIPTON R. Quantum cryptanalysis of hidden linear functions[C]//Advances in Cryptology-Crypto'95. [S. l.]:Springer-Verlag,1995:424-437.

[3] BOYEN X. Lattice mixing and vanishing trapdoors:a framework for fully secure short signatures and more[C]//Lecture Notes in Computer Science. Berlin:Springer-Verlag,2010:499-517.

[4] SHPILRAIN V,ZAPATA G. Combinatorial group theory and public key cryptography[J]. Applicable Algebra in Engineering,communication and Computing,2006,17(4):291-302.

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

[6] KO K H,LEE S J,CHEON J H,*et al*. New public key cryptosystem using braid groups[C]// Lecture Notes in Computer Science. Berlin:Springer-Verlag,2000:166-183.

[7] ANSHEL I,ANSHEL M,FISHER B,*et al*. New key agreement protocol in braid group cryptography[C]//Lectures Notes in Computer Science. Berlin:Springer-Verlag,2001:1-15.

[8] CHA J C,KO K H,LEE S J,*et al*. An efficient implementation of braid groups[C]//Lecture Notes in Computer Science. [S. l.]:Springer-Verlag,2001:144-156.

[9] SIBERT H, DEHORNOY P, GIRAULT M. Entity authentication schemes using braid word reduction[EB/OL]. [2011-10-15]. http://eprint. iacr. org/2002/187.

[10] LAL S,CHATURVEDI A. Authentication schemes using braid groups [EB/OL]. [2011-10-15]. http://arXiv. org/cs. CR/0507066.

[11] 汤学明,洪帆,崔国华. 辫子群上的公钥加密算法[J]. 软件学报,2007,18(3):722-729.

[12] KO K H,CHOI D H,CHO M S,*et al*. New signature scheme using conjugacy problem[EB/OL]. [2011-10-15]. http://eprint. iacr. org/2002/168.

[13] THOMAS T,LAL A K. Group signature scheme using braid groups [EB/OL]. [2011-10-15]. http://arXiv. org/cs. CR/0602063.

[14] ZOU Shi-hua,ZENG Ji-wen,QUAN Jun-jie. Designated verifier signature scheme based on braid groups[EB/OL]. [2011-10-15]. http://eprint. iacr. org/2006/329.

[15] VERMA G K. Blind signature schemes over braid groups[EB/OL]. [2011-10-15]. http://eprint. iacr. org/2008/027.

[16] VERMA G K. A proxy signature scheme over braid groups[EB/OL]. [2011-10-15]. http://eprint. iacr. org/2008/160.

[17] ZHANG Li-li,ZENG Ji-wen. Proxy signature based on braid group [J]. Journal of Mathematical Study,2008,41(1):56-64.

[18] LAL S,VERMA V. Some proxy signature and designated verifier signature schemes over braid groups[EB/OL]. [2011-10-15]. http://arXiv. org/cs. CR/09043422.

[19] RABIN M O. How to exchange secrets by oblivious transfer,Technical Report TR281[R]. [S. l.]:Aiken Computation Laboratory,Harvard University,1981.

[20] MOROZOV K,SAVIDES G. Computational oblivious transfer and interactive hashing[EB/OL]. [2011-10-15]. http://eprint. iacr. org/2009/074.

[21] GROHMANN B. A new protocol for 1-2 oblivious transfer [EB/OL]. [2011-10-15]. http://eprint. iacr. org/2009/172.

[22] CAMENISCH J,NEVEN G,SHELAT A. Simulatable adaptive oblivious transfer[C]//Lecture Notes in Computer Science. Berlin:Springer-Verlag,2007:573-590.

[23] HUANG H F,CHANG C C. A new *t*-out-*n* oblivious transfer with low bandwidth[J]. Applied Mathematical Sciences,2007,1(7):311-320.

[24] CACHIN C,CAMENISCH J,KILIAN J,*et al*. One-round secure computation and secure autonomous mobile agents[C]//Lecture Notes in Computer Science. Berlin:Springer-Verlag,2000:512-523.

[25] STADLER M,PIVETEAU J M,CAMENISCH J. Fair blind signatures [C]//Lecture Notes in Computer Science. Berlin:Springer-Verlag,1995:209-219.

[26] 隗云,熊国华,张兴凯,等. 辫群上的不经意传输协议[J]. 计算机应用研究,2010,27(8):3042-3044.