辫群上的不经意传输协议 *

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

摘 要: 量子计算的快速发展给基于整数分解或离散对数问题的密码协议带来严重威胁。为了研究抵抗量子分析的密码协议,基于非交换的辫群提出了一个 2 取 1 不经意传输协议,并将其扩展为 N 取 1 不经意传输协议。在共轭搜索问题和多重共轭搜索问题难解的前提下协议能同时保证发送方和接收方的隐私性。

关键词: 辫群; 不经意传输; 共轭搜索; 多重共轭搜索
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)08-3042-03
doi:10.3969/j.issn.1001-3695.2010.08.061

Oblivious transfer protocols over braid groups

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

Abstract: The rapid development of quantum computing brings great challenge to cryptographic protocols based on the integer factorization or the discrete logarithm problem. In order to research quantum cryptanalysis-resistant cryptographic protocols, this paper proposed a 1-out-of-2 oblivious transfer protocol based on non-commutative braid group, which was extended to a 1-out-of-*N* oblivious transfer protocol. The protocols could provide privacy for both the sender and the receiver on base of the difficulty of the conjugacy search problem and the multiple conjugacy search problem.

Key words: braid group; oblivious transfer; conjugacy search; multiple conjugacy search

0 引言

众所周知,目前公钥密码体制最典型的两类安全性假设为整数分解和离散对数的难解性。量子计算[1,2]的快速发展使得目前的公钥密码体制面临严重威胁。为了抵抗已知量子算法的攻击,大量学者开始设计非基于数论的、基于非交换代数的公钥密码体制,如基于一般非交换群的密码[3]、基于有限非交换群的 MOR 密码[4]等。辫群的概念由 Artin[5]于 1947 年首次提出,由于其复杂的非交换结构、运算所需的时间和空间很小的特点,也被用于构造公钥密码系统[6],基于辫群的密钥交换协议[7,8]、认证方案[9,10]、加密方案[11]及签名方案[12~17]相继被提出。

不经意传输协议使得协议双方以不经意的方式传送消息。不经意传输这一概念最早由 Rabin[18]提出:发送方发送一个消息给接收方,接收方得到该消息的概率为 0.5,而发送方不知道接收方是否得到该消息。在后来的研究中,不经意传输协议有多种形式,如 2 取 1 不经意传输[19,20]和 N 取 1 不经意传输[21,22]。在 2 取 1 不经意传输协议中,发送方向接收方发送两个消息,但接收方只能得到其中一个,且发送方不知道接收方得到了哪个消息。N 取 1 不经意传输是对 2 取 1 不经意传输的扩展,发送方发送了 N 个消息,但接收方只能得到其中一个,且发送方不知道接收方得到了哪个消息。不经意传输的应用非常广泛,如 2 取 1 不经意传输可用于构造安全计算协议[23]、公开盲签名[24]及电子拍卖协议[25]等,N 取 1 不经意传输则可用于数字版权的保护[26]。

目前尚未有公开文献对辫群上的不经意传输协议进行研究。本文基于辫群上共轭搜索问题和多重共轭搜索问题的难解性提出了一个 2 取 1 不经意传输协议,并将其扩展到 N 取 1 的情况。

1 预备知识

1.1 辫群

定义 1[6] 辫群 B_n($n \geq 2$ 为自然数)是由生成元 $\sigma_1, \sigma_2, \cdots, \sigma_{n-1}$ 生成的有限表示的无限群。其生成元满足:

$$\sigma_i\sigma_j = \sigma_j\sigma_i \quad (|i-j| \geq 2)$$

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \quad (1 \leq i \leq n-2)$$

辫群中的元素称为一个 n 辫或辫元。当 $n=2$ 时,B_n 为无限循环群,本文不予考虑。

定义 2[6] 在辫群 B_n 中,对 $l \leq n$,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,记做 LB_n;由 $\sigma_{l+1}, \cdots, \sigma_{n-1}$ 生成的群叫 B_n 的右子群,记做 RB_n。

显然,对任意 $(a,b) \in LB_n \times RB_n$,均有 $ab=ba$。

定义 3[6] 对于辫元 $x, y \in B_n$,若存在一个辫元 $a \in B_n$ 使

收稿日期: 2010-01-09; **修回日期**: 2010-02-23 **基金项目**: 国家自然科学基金资助项目(10501053)

作者简介:隗云(1982-),博士研究生,主要研究方向为密码协议的设计与分析(weiyun456@sohu.com);熊国华(1963-),高级工程师,博导,博士后,主要研究方向为密码与编码;张兴凯(1981-),硕士,主要研究方向为密码协议的设计与分析;鲍皖苏(1966-),教授,博导,博士,主要研究方向为密码学与网络安全.

得 $y=a^{-1}xa$,则称辫元 x,y 共轭,记做 $x\sim y$。

定义 4[6]　给定$(x,y)\in B_n\times B_n$,判断 $x\sim y$ 是否成立,称共轭判断问题。

定义 5[6]　给定共轭辫元对$(x,y)\in B_n\times B_n$,找到满足 $y=a^{-1}xa$的辫元 $a\in B_n$,称共轭搜索问题。

定义 6[6]　给定

$$(x_1,a^{-1}x_1a),\cdots,(x_N,a^{-1}x_Na)\in B_n\times B_n$$

求辫元 $b\in B_n$,满足

$$b^{-1}x_1b=a^{-1}x_1\ a,\cdots,b^{-1}x_Nb=a^{-1}x_Na$$

称多重共轭搜索问题。

定义 7[6]　给定辫元 $y=x^r\in B_n$ 及正整数 r,找到满足 $y=z^r$ 的辫元 z,称根问题。

辫群内元素的乘法和求逆运算都存在快速算法,可以用计算机编程来实现。对辫群上的共轭判断问题,Ko 等人[6]提出了一种多项式算法。但是,尚未有算法能证明可在多项式时间内求解共轭搜索问题、多重共轭搜索问题或根问题。

1.2　不经意传输

不经意传输协议应满足以下基本性质:

a)正确性。若发送方与接收方正确执行协议,协议完成后接收方得到其所选择的消息。

b)不经意性(接收方的隐私性)。接收方的不同选择所对应的传输副本对于发送方是不可区分的。

c)发送方的隐私性。接收方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方是不可区分的。

2　辫群上的 2 取 1 不经意传输协议

2.1　2 取 1 不经意传输协议

假设协议参与者为 Alice 和 Bob,其中 Alice 为发送方,Bob 为接收方。

系统参数:Alice 和 Bob 共同选择辫群 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 $c\in\{0,1\}$,$a\in LB_n$,计算 $t=a^{-1}xah^c$,并将其发送给 Alice;

b)Alice 随机选择 $b\in RB_n$,计算

$$A=b^{-1}yb,k_0=b^{-1}tb,k_1=b^{-1}\mathrm{th}^{-1}b$$

$$C_0=H(k_0{}^r)\oplus m_0,C_1=\mathrm{H}(k_1{}^r)\oplus m_1$$

并将(A,C_0,C_1)发送给 Bob;

c)Bob 收到(A,C_0,C_1)后,计算 $m_c=H(a^{-1}Aa)\oplus C_c$。

2.2　协议分析

1)正确性

由 $a\in LB_n$ 及 $b\in RB_n$ 知

$$a^{-1}Aa=a^{-1}b^{-1}yba=b^{-1}a^{-1}yab$$

若 $c=0$,有 $t=a^{-1}xa$ 及

$$k_0{}^r=(b^{-1}tb)^r=(b^{-1}a^{-1}xab)^r=a^{-1}Aa$$

若 $c=1$,有 $t=a^{-1}xah,th^{-1}=a^{-1}xa$ 及

$$k_1{}^r=(b^{-1}th^{-1}b)^r=(b^{-1}a^{-1}xab)^r=a^{-1}Aa$$

因此,如果 Alice 和 Bob 都遵守协议,则 Bob 总可以得到 $k_c{}^r$,进而得到 $m_c=H(a^{-1}Aa)\oplus C_c$。

2)不经意性(Bob 的隐私性)

由正确性可知,若 $c=0,t=a^{-1}xa\sim x,th^{-1}=a^{-1}xah^{-1}\sim xh^{-1},t^r=a^{-1}x^ra\sim y$;若 $c=1,t=a^{-1}xah\sim xh,th^{-1}=a^{-1}xa\sim x,(th^{-1})^r=a^{-1}x^ra\sim y$。

不管 c 的取值如何,t 和 th^{-1}都分别与两个未知元素共轭,且 t^r 和$(th^{-1})^r$ 中总有一个与 y 共轭。Alice 若想通过共轭关系判断 Bob 的选择,必须先求出 x 或 r。而在 r 未知的情况下,由 $y=x^r$ 求 x 比求解根问题难。又因为辫群是无限群,Alice 无法通过穷举方式找到 x。同时,在 x 未知,r 足够大的情况下 Alice 也无法求出 r。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,当 $c=0$ 时,有

$$k_0{}^r=(b^{-1}tb)^r=b^{-1}t^rb=a^{-1}Aa$$

$$k_1{}^r=(b^{-1}th^{-1}b)^r=b^{-1}(th^{-1})^rb$$

由 $x\in B_n$,$h\in RB_n$,$t=a^{-1}xa$ 及 $b\in RB_n$ 知,h 与 b,t 都不满足交换性,因此 Bob 不能由 $k_0{}^r$ 得到 $k_0{}^r$。若 Bob 想通过求解 b 来求 k_1^r 将面临解共轭搜索问题或多重共轭搜索问题,因为由 A、k_0 和 k_1 中之一求解 b 是共轭搜索问题;而由 A、k_0 和 k_1 求解 b 是多重共轭搜索问题。故 Bob 选择 $c=0$ 后只能得到消息 m_0,无法得到 m_1;同理,Bob 选择 $c=1$ 后只能得到消息 m_1,无法得到 m_0。因此,协议保证了 Alice 的隐私性。

3　N 取 1 不经意传输协议

3.1　N 取 1 不经意传输协议

系统参数同 2.1 节。协议过程如下:

a)Bob 随机选择 $c\in\{1,\cdots,N\}$,$a\in LB_n$,计算 $t=a^{-1}xah^c$,并将其发送给 Alice;

b)Alice 随机选择 $b\in RB_n$,计算 $A=b^{-1}yb,k_i=b^{-1}th^{-i}b$ $(i=1,\cdots,N)$及 $C_i=H(k_i{}^r)\oplus m_i$,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 $m_c=H(a^{-1}Aa)\oplus C_c$。

3.2　协议分析

正确性:由 $a\in LB_n$ 及 $b\in RB_n$ 知 $a^{-1}Aa=b^{-1}a^{-1}yab$,而 $k_c{}^r=(b^{-1}th^{-c}b)^r=(b^{-1}a^{-1}xah^ch^{-c}b)^r=b^{-1}a^{-1}yab$,因此,如果 Alice 和 Bob 都遵守协议,则 Bob 总可以得到 $k_c{}^r$,进而得到 $m_c=H(a^{-1}Aa)\oplus C_c$。

协议的不经意性(Bob 的隐私性)和 Alice 的隐私性类似 2 取 1 的协议,因此不再赘述。

4　结束语

本文对辫群上的不经意传输协议进行了研究,提出了一个基于共轭搜索问题和多重共轭搜索问题难解性的 2 取 1 不经意传输协议及其扩展协议。提出的协议既可直接用于电子商务中保护用户隐私或数字版权,也可用于构造辫群上的其他密码协议,如比特承诺协议、电子拍卖协议等。

参考文献:

[1] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM J Comput,

1997,26(5):1484-1509.

[2] KITAEV A. Quantum measurements and the abelian stabilizer problem [EB/OL]. [2010-01-11]. http://arxiv.org/quant-ph/9511026.

[3] ANSHEL I, ANSHEL M, GOLDFELD D. An algebraic method for public key cryptography[J]. Math Research Letters, 1999, 6: 287-291.

[4] PAENG S H, KWON D, HA K C, *et al*. Improved public key cryptosystem using finite non-abelian groups[EB/OL]. [2010-01-11]. http://eprint.iacr.org/2001/066.

[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 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. London: Springer-Verlag, 2001:144-156.

[9] SIBERT H, DEHORNOY P, GIRAULT M. Entity authentication schemes using braid word reduction[EB/OL]. [2010-01-11]. http://eprint.iacr.org/2002/187.

[10] LAL S, CHATURVEDI A. Authentication schemes using braid groups [EB/OL]. [2010-01-11]. 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]. [2010-01-11]. http://eprint.iacr.org/2002/168.

[13] THOMAS T, LAL A K. Group signature scheme using braid groups [EB/OL]. [2010-01-11]. http://arXiv.org/cs.CR/0602063.

[14] VERMA G K. Blind signature schemes over braid groups[EB/OL]. [2010-01-11]. http://eprint.iacr.org/2008/027.

[15] VERMA G K. A proxy signature scheme over braid groups[EB/OL]. [2010-01-11]. http://eprint.iacr.org/2008/160.

[16] ZHANG L L, ZENG J W. Proxy signature based on braid group[J]. Journal of Mathematical Study, 2008, 41(1):56-64.

[17] LAL S, VERMA V. Some proxy signature and designated verifier signature schemes over braid groups[EB/OL]. [2010-01-11]. http://arXiv.org/cs.CR/09043422.

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

[19] MOROZOV K, SAVVIDES G. Computational oblivious transfer and interactive hashing[EB/OL]. [2010-01-11]. http://eprint.iacr.org/2009/074.

[20] GROHMANN B. A new protocol for 1-2 oblivious transfer [EB/OL]. [2010-01-11]. http://eprint.iacr.org/2009/172.

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

[22] 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.

[23] 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.

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

[25] JUELS A, SZYDLO M. A two-serve, sealed-bid auction protocol [C]//Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2002:72-86.

[26] 杨乐. 基于不经意传输协议的数字版权保护方案[D]. 西安:西安电子科技大学, 2008.

(上接第 3041 页)的协议及网络的安全策略约束建立起检测规范,当无线网络执行的协议发生变化时,只需将改变后的协议规范加入到检测规范当中即可,具有很强的可扩展性。同时该方法还可以根据对网络流量的在线监测自动调整检测阈值。通过仿真实验,证明了本文提出的方法在检测 DoS 攻击上的有效性。

参考文献:

[1] CHEN J C, JIANG M C, LIU Yi-wen. Wireless LAN security and IEEE 802.11i[J]. IEEE Wireless Communications, 2005, 12(1): 27-36.

[2] XING Xin-yu, SHAKSHUKI E, BENOIT D, *et al*. Security analysis and authentication improvement for IEEE 802.11i specification[C]//Proc of IEEE GLOBECOM. New Orleans, LD:[s.n], 2008:1-5.

[3] KO C, RUSCHITZKA M, LEVITT K. Execution monitoring of security critical programs in a distributed system: a specification-based approach[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 1997:175-187.

[4] SONG Tao, KO C, TSENG H T, *et al*. Formal reasoning about a specification-based intrusion detection for dynamic auto-configuration protocols in Ad hoc networks[C]//Proc of the 3rd International Workshop Formal Aspects in Security and Trust. 2005:16-33.

[5] GUO Fang-lu, CHIUEH T C. Sequence number-based MAC address spoof detection[C]//Proc of the 8th International Symposium on Recent Advances in Intrusion Detection. Berlin: Springer, 2005:309-329.

[6] GILL R, SMITH J, LOOI M, *et al*. Passive techniques for detecting session hijacking attacks in IEEE 802.11 wireless networks[C]//Proc of AusCERT. 2005:26-38.

[7] SHENG Yong, TAN K, CHEN Guan-ling, *et al*. Detecting 802.11 MAC layer spoofing using received signal strength[C]//Proc of IEEE INFOCOM. 2008:1768-1776.

[8] HSIEH W C, LO C C, LEE J C, *et al*. The implementation of a proactive wireless intrusion detection system[C]//Proc of the 4th International Conference on Computer and Information Technology. 2004: 581-586.

[9] Snort-wireless user's guide [EB/OL]. (2005). http://www.snort-wireless.org.

[10] WIDZ: the wireless intrusion detection system[EB/OL]. (2006). http://www.loud-fat-bloke.co.uk.

[11] Back track3 final[EB/OL]. (2008). http://remote-exploits.com.