辫群上的非平衡比特承诺协议 *

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

摘 要: 为构造抗量子攻击的密码协议,以非交换的辫群为平台,基于求根问题的难解性提出了一个非平衡比特承诺协议。分析表明,协议具有绑定性和隐藏性,且协议执行过程不涉及共轭判断运算,在计算上比基于共轭搜索问题的比特承诺协议更有效。

关键词: 辫群; 比特承诺; 求根问题; 共轭搜索问题
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)03-1076-02
doi:10.3969/j.issn.1001-3695.2012.03.076

Biased bit commitment protocol over braid groups

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

Abstract: In order to construct quantum attack-resistant cryptographic protocols, non-commutative braid group is used as a new platform. This paper proposed a biased bit commitment protocol on base of the difficulty of root extraction problem over braid groups. Analysis shows that the proposed protocol is binding and hiding. And it is much more efficient in computation than the protocol based on since it needs no conjugacy decision operation.

Key words: braid group; bit commitment; root extraction problem(REP); conjugacy search problem(CSP)

0 引言

量子计算[1,2]的快速发展使得基于整数分解或离散对数问题难解性的公钥密码体制面临严重威胁。为了研究抗量子攻击的密码协议,很多学者开始以非交换代数为平台来设计公钥密码协议,如基于一般非交换环的签名协议[3,4]等。辫群的概念由 Artin[5] 于 1947 年提出,由于其复杂的非交换结构成为了构造密码协议的新平台。2000 年,辫群被首次用于构造密钥协商协议及加密方案[6]。此后,基于辫群的密钥交换协议[7,8]、认证协议[9,10]、加密方案[11]及签名协议[1218]相继被提出。

比特承诺协议是最基础的密码协议之一,常用于构造其他密码协议,如电子彩票[19]、盲签名[20]及合同签订等[21]。2008 年,王励成等人[22]基于辫群上共轭搜索问题的难解性构造了比特承诺协议,并对一般的比特承诺进行扩展提出了非平衡比特承诺的概念。他们构造的第一个非平衡比特承诺方案的安全性基础同样是共轭搜索问题的难解性。

本文基于辫群上求根问题的难解性构造了一个非平衡比特承诺协议,并对其安全性和计算效率进行了详细分析。

1 预备知识

本章简单介绍辫群、辫群上的难解问题及比特承诺协议的安全需求。

1.1 辫群

本节的定义参考文献[6]。

定义 1 辫群 B_n($n\geqslant 2$ 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:

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

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

因此辫群 B_n 可表示为

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

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,本文考虑 $n>2$。对于辫元 $x,y\in B_n$,若存在一个辫元 $a\in B_n$ 使得 $y=a^{-1}xa$,则称辫元 x,y 共轭,记做 xy。辫群上与共轭相关的数字难题可用于构造各种密码协议。

定义 2 共轭判断问题(conjugacy decision problem,CDP)。

问题实例:给定 $(x,y)\in B_n\times B_n$。

求解目标:判断 xy 是否成立。

定义 3 共轭搜索问题(CSP)。

问题实例:给定 $(\alpha,\beta)\in B_n\times B_n$,存在 $s\in B_n$ 使得 $\beta=s^{-1}\alpha s$。

求解目标:找到一个 $t\in B_n$ 满足 $\beta=t^{-1}\alpha t$。

定义 4 求根问题(REP)。

问题实例:给定正整数 $c(c>1)$ 及辫元 $\beta\in B_n$,存在 $\alpha\in B_n$ 使得 $\beta=\alpha^c$。

收稿日期: 2011-08-15; **修回日期**: 2011-09-30 **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,硕士研究生,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;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;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).

求解目标:找到一个 $t \in B_n$ 满足 $\beta = t^c$。

对辫群上的共轭判断问题,Ko 等人[6]提出了一种多项式时间算法,其他学者还提出了求解共轭判断问题、共轭搜索问题的变形以及求根问题的算法[2326]。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或求根问题,且求根问题比共轭搜索问题更难解。因此,这些数字难题仍可用于构造密码协议。

1.2　比特承诺

在一般的比特承诺协议中,承诺方向另一方承诺一个随机比特 $\tau \in \{0,1\}$。在承诺打开之前,被承诺方无法得知承诺到底是 0 还是 1,而承诺方也不能打开一个与最初承诺相反的比特。

如果一个比特承诺协议具备以下性质,则称其是正确的[22]:

a)如果承诺方打开的确实是其最初承诺的比特,则该承诺应该被接受。

b)如果承诺方打开的不是其最初承诺的比特,则该承诺应该被拒绝。

一个安全的比特承诺协议还应具备以下性质[22]:

a)绑定性。承诺方不能成功地欺骗被承诺方不被发觉,即他不能打开一个与其最初承诺相反的承诺。

b)隐藏性。被承诺方不能作弊,即不能在承诺方打开承诺之前获取所承诺的信息。

非平衡比特承诺是一般比特承诺的推广。在非平衡比特承诺中,承诺可以是集合 $\{1,\cdots,k\}$ 中的任意值,其中 $k \geq 2$ 为整数。与一般的比特承诺协议相比,非平衡比特承诺协议的优势在于,其可直接用于构造非平衡投币协议、抽签协议等。

2　辫群上的非平衡比特承诺协议

本章给出辫群上的非平衡比特承诺协议,协议分承诺阶段和打开阶段。

假设承诺方和被承诺方分别为 Alice 和 Bob,承诺 $\tau \in \{1,\cdots,k\}$,承诺过程如下:

a)Bob 随机选择 k 个两两不同的辫元 $y_1,\cdots,y_k \in B_n$,并将其发送给 Alice;

b)Alice 随机选择辫元 $t \in B_n$,计算 $T = t^2 y_\tau$,将其发送给 Bob,并秘密保存 t;

c)收到 T 后,Bob 宣布承诺结束。

在打开阶段,Alice 将 τ 和 t 发送给 Bob,Bob 验证等式 $T = t^2 y_\tau$ 是否成立,若成立,接受承诺;否则,认为 Alice 有欺骗。

3　协议分析

3.1　正确性分析

性质 1　提出的协议是正确的。

证明　非平衡承诺协议的正确性意味着如果协议双方都诚实地执行协议,被承诺方将接受承诺。

如果 Alice 诚实地向 Bob 承诺 $\tau \in \{1,\cdots,k\}$,她必然计算 $T = t^2 y_\tau$ 并发送给 Bob。而在打开阶段,Alice 向 Bob 发送的 τ 和 t 必然满足等式 $T = t^2 y_\tau$,Bob 验证其成立后会接受承诺。

3.2　安全性分析

性质 2　提出的协议是绑定的。

证明　如果 Alice 想打开一个与原始承诺不同的承诺 $\tau' \in \{1,\cdots,k\}$,$\tau' \neq \tau$ 且不被发现,需要向 Bob 发送 t' 和 τ',使得 $T = (t')^2 y_{\tau'} = t^2 y_\tau$,即 $(t')^2 = t^2 y_\tau y_{\tau'}^{-1}$,这意味着 Alice 将面临求解 $t^2 y_\tau y_{\tau'}^{-1}$ 的平方根。因此,在求根问题的难解性前提下,该协议是绑定的。

性质 3　提出的协议是隐藏的。

证明　在承诺打开之前,Bob 只知道 $y_1,\cdots,y_k$ 和 T。对任意 y_i 都可能存在某个 $t \in B_n$,使得 $T = t^2 y_i$。因此,Bob 只能以 $1/k$ 的概率猜测承诺的值,即协议是隐藏的。

3.3　性能比较

本节将在计算效率上对提出的非平衡比特承诺协议与王励成等人的协议进行比较,主要考虑辫元的乘法、求逆及共轭判断运算。表 1 列出了两种协议所需进行的各种运算的数量。

表 1　两协议所需各种运算数量

协议	承诺阶段	打开阶段
王励成等人的协议	乘法:2	乘法:2
	求逆:1	求逆:1
	共轭判断:$k-1$	共轭判断:0
新协议	乘法:3	乘法:3
	求逆:0	求逆:0
	共轭判断:0	共轭判断:0

根据文献[8,12],辫元的乘法和求逆运算复杂性相当,均远小于共轭判断运算的复杂性。由表 1 可以看出,新协议在计算效率上优于王励成等人的协议。

4　结束语

作为构造抗量子攻击密码协议的新平台,辫群一经提出便成为研究热点。本文基于辫群上的求根问题构造了一个非平衡比特承诺协议,为构造基于非交换代数的密码协议提供了新思路。

参考文献:

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

[2] KITAEV A. Quantum measurements and the abelian stabilizer problem[EB/OL]. [2011-08-15]. http://arxiv.org/quant-ph/9511026.

[3] HASHIMOTO Y, SAKURAI K. On the construction of signature schemes based on birational permutations over noncommutative rings [EB/OL]. [2011-08-15]. http://eprint.iacr.org/2008/340.

[4] OGURA N, UCHIYAMA S. Cryptanalysis of the birational permutation signature scheme over a noncommutative ring[EB/OL]. [2011-08-15]. http://eprint.iacr.org/2009/066.

[5] ARTIN E. Theory of braids[J]. Annals of Math, 1947, 48(2): 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. Berlin: Springer-Verlag, 2001: 144-156.

(下转第 1083 页)

Computer Standards & Interfaces,2010,32(4):185-196.

[2] YAO Z Y,KIM D,DOH Y. PLUS:parameterized and localized trust management scheme for sensor networks security[C]//Proc of the IEEE International Conference on Mobile Ad hoc and Sensor Systems. Piscataway: IEEE Computer Society,2006:437-446.

[3] JI Wen,YANG Shou-bao,WEI Dong,*et al*. GARM:a group-anonymity reputation model in peer-to-peer system[C]//Proc of the 6th International Conference on Grid and Cooperative Computing. New York: ACM Press,2007:32-40.

[4] BOUKERCHEA,LI Xu. ATRM:an agent-based trust and reputation management scheme for wireless sensor networks[C]//Proc of Global Telecommunications Conference. New York:IEEE Press,2005:1857-1861.

[5] JONKER C M,SCHALKEN J J P,THEEUWES J,*et al*. Human experiments in trust dynamics[C]//Proc of the 2nd International Conference on Trust Management. 2004:206-220.

[6] BUCHEGGER S,BOUDEC J Y L. A robust reputation system for peer-to-peer and mobile Ad hoc networks[C]//Proc of P2PEcon'04. Cambridge MA:Harvard University,2004.

[7] CROSBY G V,PISSINOU N,GADZE J. A framework for trust-based cluster head election in wireless sensor networks[C]//Proc of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems. Washington DC:IEEE Computer Society,2006:13-22.

[8] HUNG K S,LUI K S,KWOK Y K. A trust-based geographical routing scheme in sensor networks[C]//Proc of IEEE Wireless Communications and Networking Conference. 2007:3123-3127.

[9] ZOURIDAKI C,MARK B L,HEJMO M,*et al*. A quantitative trust establishment framework for reliable data packet delivery in MANETs [C]//Proc of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks. New York:ACM Press,2005:1-10.

[10] CROSBY G V,PISSINOU N. Cluster-based reputation and trust for wireless sensor networks[C]//Proc of IEEE Consumer Communications and Networking Conference. 2007:604-618.

[11] BAOHUA H,HEPING H,ZHENGDING L. Identifying local trust value with neural network in P2P environment[C]//Proc of the 1st IEEE and IFIP International Conference in Central Asia on Internet. 2005.

[12] CHEN Jing, DU Rui-ying. A trust game method basing on probability model in networks[J]. Chinese Journal of Electronics,2010,38(2):427-433.

[13] CASTELFRANCHI C,FALCONE R,PEZZULO G. Integrating trustfulness and decision using fuzzy cognitive maps[C]//Proc of the 1st International Conference on Trust Management. Berlin:Springer-Verlag,2003:195-210.

[14] KIM T K,SEO H S. A trust model using fuzzy logic in wireless sensor network[C]//Proc of World Academy of Science, Engineering and Technology. 2008:2070-3740.

[15] JIANG T,BARAS J S. Ant-based adaptive trust evidence distribution in MANET[C]//Proc of the 24th International Conference on Distributed Computing Systems Workshop. 2004:588-593.

[16] THEODORAKOPOULOS G,BARAS J S. On trust models and trust evaluation metrics for Ad hoc networks[J]IEEE Journal on Selected Areas in Communications,2006,2(24):318-328.

[17] GUAN Shang-yuan, WU Wei-guo, DONG Xiao-she,*et al*. Survey of trust management in open distributed environments[J]. Computer Science,2010,3(37): 22-28.

[18] BANDYOPADHYAY S,COYLE E J. An energy efficient hierarchical clustering algorithm for wireless sensor networks[C]//Proc of IEEE Wireless Communications and Networking Conference. [S. l.]:IEEE Press, 2003:1713-1723.

(上接第 1077 页)

[9] SIBERT H, DEHORNOY P, GIRAULT M. Entity authentication schemes using braid word reduction[EB/OL]. [2011-08-15]. http://eprint.iacr.org/2002/187.

[10] LAL S,CHATURVEDI A. Authentication schemes using braid groups [EB/OL]. [2011-08-15]. http://arXiv.org/cs.CR/0507066.

[11] 汤学明, 洪帆, 崔国华. 辫群上的公钥加密方案[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]. [2011-08-15]. http://eprint.iacr.org/2002/168.

[13] THOMAS T, LAL A K. Group signature scheme using braid groups [EB/OL]. [2011-08-15]. http://arXiv.org/cs.CR/0602063.

[14] VERMA G K. Blind signature schemes over braid groups[EB/OL]. [2011-08-15]. http://eprint.iacr.org/2008/027.

[15] VERMA G K. A proxy signature scheme over braid groups[EB/OL]. [2011-08-15]. http://eprint.iacr.org/2008/160.

[16] 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.

[17] LAL S,VERMA V. Some proxy signature and designated verifier signature schemes over braid groups[EB/OL]. [2011-08-15]. http://arXiv.org/cs.CR/09043422.

[18] VERMA G K. A proxy blind signature scheme over braid groups[J]. International Journal of Network Security,2009,9(3): 214-217.

[19] 郑东, 张彤, 陈克非, 等. 基于比特承诺的电子彩票方案[J]. 电子学报, 2000, 28(10): 141-142.

[20] 钟鸣, 杨义先. 一种基于比特承诺的部分盲签名方案[J]. 通信学报, 2001,22(9)1-6.

[21] 万武南, 索望, 陈运. 基于 Bit 承诺的合同网模型[J]. 计算机工程, 2009,35(19):1-3.

[22] WANG L C, CAO Z F, CAO F, *et al*. Biased bit commitment and applications[J]. Journal of Information Science and Engineering,2008,24:441-452.

[23] MYASNIKOV A, SHPILRAIN V,USHAKOV A. A practical attack on a braid group based cryptographic protocol[C]//Lecture Notes in Computer Science. Berlin: Springer-Verlag,2005:86-96.

[24] MYASNIKOV A, USHAKOV A. Length based attack and braid groups: cryptanalysis of Anshel-Anshel-Goldfeld key (AAGK) exchange protocol[C]//Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2007:76-88.

[25] GONZALEZ-MENESES J. Improving an algorithm to solve multiple simultaneous conjugacy problems in braid groups[J]. Contemporary Mathematics,2005,372:35-42.

[26] KALKA A G. Representation attacks on the braid Diffie-Hellman public key encryption[J]. Application of Algebra Engineering, Communication and Computer,2006,17:257-266.