

一个基于辫群的公钥密码算法

左黎明

(华东交通大学 基础科学学院, 江西 南昌 330013)

摘 要: 辫群是构造对抗量子公钥密码系统的新工具. 已知的基于辫群共轭问题的公钥密码系统都受到不同程度的攻击. 提出了一个基于辫群求根问题的公钥密码算法, 随后对算法的正确性、安全性、参数选择和效率进行分析. 新的公钥密码算法可以抵抗各种已知攻击.

关键词: 辫群; 求根问题; 公钥密码

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2012)01-0124-03

A Public Key Encryption Algorithm on Braid Group

ZUO Li-ming

(School of Natural Science, East China Jiaotong University, Nanchang 330013, China)

Abstract: The braid group is a new tool for constructing quantum attack-resistant public key encryption algorithm. A public key encryption algorithm base on root finding problem over braid group is put forward, the analysis of its correctness, security, efficiency and parameter choice are subsequently presented. The new algorithm can resist current known attacks.

Key words: braid group; root finding problem; public key cryptography

1 引言

目前已有的公钥密码系统及其相关密码协议主要建立在大整数分解问题, 离散对数问题和椭圆曲线上的离散对数问题的难解性之上. Shor 等人^[1]从理论上指出上述困难问题在量子计算模型框架内能够在量子多项式时间内解决. 这给当前的密码学应用带来了严重的挑战. 辫群是 Artin^[2]在 1925 年提出的一种非交换无限群. 文献[3]提出了基于不可解的共轭问题的辫群公钥加密体制. 文献[4]提出了一种基于 Diffie-Hellman 型共轭问题的辫群公钥加密体制. 汤学明等人^[5]提出了一个基于辫群上多重 P-BPKE 问题和 BFHP 问题的公钥加密体制. 本文提出了一个基于辫群求根问题的公钥加密机制.

2 辫群基础

辫群的详细定义、性质和相关算法见文献[6],

本文只给出必要的知识.

定义 1 辫群 B_n 是一种有限表示的无限群, B_n 的生成元是 $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$, 它具有如下性质: 当 $|i-j| \geq 2$ 时, $\sigma_i \sigma_j \sigma_i^{-1} \sigma_j^{-1} = e$, 当 $|i-j| = 1$ 时, $\sigma_i \sigma_j \sigma_i \sigma_j^{-1} \sigma_i^{-1} \sigma_j^{-1} = e$, 其中 e 为单位元. 因此, 辫群 B_n 可以表示为: $B_n = \langle \sigma_1, \sigma_2, \dots, \sigma_{n-1} \mid \begin{matrix} \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j, & |i-j|=1 \\ \sigma_i \sigma_j = \sigma_j \sigma_i, & |i-j| \geq 2 \end{matrix} \rangle$. n 称为辫群 B_n 的辫指数, 辫群 B_n 中的元素被称为辫子或辫元. $\Delta = (\sigma_1 \sigma_2 \dots \sigma_{n-1})(\sigma_1 \sigma_2 \dots \sigma_{n-2}) \dots (\sigma_1 \sigma_2) \sigma_1$ 称为辫群 B_n 的基本辫子.

定义 2 在辫群 B_n 中, 给定 $1 < l < r < n$, 其中 $r-l \geq 2$, 将生成元 $\sigma_1, \sigma_2, \dots, \sigma_l$ 生成的子群称为 B_n 的 l 左子群; 将生成元 $\sigma_{r+1}, \sigma_{r+2}, \dots, \sigma_n$ 称为 B_n 的 r 右子群.

定义 3 若 $x, y \in B_n$, 存在 $a \in B_n$ 使得 $y = a^{-1}xa$, 则称 x, y 共轭, 记为: $x \sim y$. 给定 $x, y \in B_n$, 判断

收稿日期: 2011-05-08; 修回日期: 2011-06-20

基金项目: 国家自然科学基金项目(11061014); 江西省教育厅青年科学基金项目(GJJ10129); 江西省教育厅科研项目(GJJ10708)

$x \sim y$ 是否成立称为共轭判断问题(CDP),寻找合适的 $a \in B_n$ 称为共轭搜索问题(CSP).

定义4 给定 $x_1, x_2, \dots, x_n \in B_n$ 和 $a \in B_n$, 寻找合适 $b \in B_n$, 使得 $b^{-1}x_i b = a^{-1}x_i a$, 其中 $i=1, 2, \dots, n$, 称此问题为多重共轭搜索问题(SCSP).

定义5 给定 $y \in B_n$ 及正整数 r , 寻找满足 $y = x^r$ 的 $x \in B_n$, 称此问题为求根问题(RFP).

定义6 已知 $x, axa^{-1}, bxb^{-1} \in B_n$, 其中 a, b 属于 B_n 的不同子群, 且满足 $ab=ba$, 求 $abxa^{-1}b^{-1}$. 称此问题为 Diffie-Helman 型共轭问题(DHCP).

辫群 B_n 中任何辫子 w 都可以表示成 $w = \Delta^{l'} \alpha_1 \alpha_2 \dots \alpha_{l'}$, 其中 α_i 为一般标准因子, l' 称为辫子 w 的标准长度, 当 $n=2$ 时, 辫群 B_n 退化为一般无限交换循环群, 在密码学上无实用价值, 只有当 $n \geq 3$ 时, 辫群 B_n 是无限非交换群, 故一般要求 $n \geq 3$. 为了应用方便, 给定 $l < n-1$, 本文将辫群 B_n 中生成元 $\sigma_1, \sigma_2, \dots, \sigma_{l-1}$ 生成的左子群记为 LB_n , 将 $\sigma_{l+1}, \sigma_{l+2}, \dots, \sigma_{n-1}$ 生成的右子群记为 RB_n . 显然, 对任意 $(a, b) \in LB_n \times RB_n$, 都有 $ab=ba$, 即 $a=bab^{-1}$ 或者 $b=aba^{-1}$.

3 已有方案的分析

3.1 已有的公钥密码算法

假定 Bob 需要通过非安全的公开信道给 Alice 发送一条秘密信息, 他使用 Alice 的公钥对这条秘密信息进行加密并将密文发送给 Alice, Alice 收到密文后用自己的私钥进行解密. 以下是 Ko 等人提出的一个基于辫群 Diffie-Helman 型共轭问题的公钥密码算法:

(1) 密钥生成: Alice 选择一个 $s \in LB_n$ 作为私钥, 选择 $a \in B_n$ 计算 $a' = sas^{-1}$, 则将共轭辫子对 (a, a') 作为公钥.

(2) 加密过程: 假设消息明文为 $m \in \{0, 1\}^k$, $H: B_n \rightarrow \{0, 1\}^k$ 为抗碰撞的散列函数, Bob 随机选取一个辫子 $t \in RB_n$, 计算 $b = tat^{-1}$, 密文 $c = m \oplus H(ta't^{-1})$, 将 b, c 发送给 Alice.

(3) 解密过程: Alice 计算 $m' = c \oplus H(sbs^{-1})$, 从而得到明文 $m = m'$.

事实上, $s \in LB_n, t \in RB_n, s$ 与 t 是可交换的, 所以 $sbs^{-1} = stat^{-1}s^{-1} = tsas^{-1}t^{-1} = ta't^{-1}$, 从而 $m' = c \oplus H(sbs^{-1}) = m \oplus H(ta't^{-1}) \oplus H(sa's^{-1}) = m$.

文献[5]中汤学明等人提出了一个基于辫群上多重 P-BPKE 问题和 BFHP 问题(因子隐藏问题)的公钥加密算法. 具体方案如下:

(1) 密钥生成: 系统选择正整数 l, n, k 满足 $n -$

$2 > l > (2kn + 2k + 2)/(2k + 1)$. Alice 随机选取 $k + 1$ 个辫子 $x_i (0 \leq i \leq k) \in RB_n$ 作为私钥, 随机选取 k 个 $v_i (0 \leq i \leq k) \in B_n$, 并公开 $v_i (0 \leq i \leq k)$ 和 $w = x_0 v_1 x_1 v_2 \dots v_k x_k$ 作为公钥.

(2) 加密过程: 假设消息明文为 $m \in \{0, 1\}^k$, $H: B_n \rightarrow \{0, 1\}^k$ 为抗碰撞的散列函数, Bob 随机选择 $y_i (0 \leq i \leq k) \in LB_n$, 计算 $w_i = y_{i-1} v_i y_i^{-1} (1 \leq i \leq k), c = H(y_0 w y_k^{-1}) \oplus m$, 将 $(w_1, w_2, \dots, w_k, c)$ 发送给 Alice.

(3) 解密过程: Alice 计算 $m' = H(x_0 w_1 x_1 w_2 \dots w_k x_k) \oplus c$, 从而得到明文 $m = m'$.

3.2 已有攻击方法

目前除求根问题之外, 大部分以前辫群上的“困难”共轭问题均存在启发式算法或者概率多项式算法. 主要方法有长度攻击方法^[7]、线性表示攻击方法^[8-9]、极端顶点级方法^[10]等. 基于辫子长度攻击^[7]是一种基于概率的攻击方法, 其基本思想是在辫群 B_n 中定义一种长度测度, 对于给定的一个辫子 x 和它的共轭 axa^{-1} , 尝试随机地用短辫子 b 作用 axa^{-1} , 使得 $baxa^{-1}b^{-1}$ 比 axa^{-1} 的长度短. 这种攻击对基于 SCSP 问题的密码协议攻击比较有效, 具体方法可参考文献[7]. 线性表示攻击的基本原理是通过建立一个从辫群 B_n 到一般线性群(例如可逆矩阵组成的线性群)的同态映射, 将辫子群中的问题转化成一般线性群中的同类问题, 由于一般线性群中的共轭问题是易解的, 最后通过群表示方法将结果提升回辫群中来. 这类方法比较著名的有 Burau 表示方法^[8]和 Lawrence-Krammer 表示方法^[9], 能够很好的解决一些 CSP 问题和 Diffie-Helman 型 CSP 问题. 超级顶点集方法和极端顶点集方法比较类似, 后者是前者的改进, 其主要思想是先定义超级顶点集 SSS 和极端顶点集 USS, 通过周期循环操作寻找一个特定的“碰撞”, 来得到使得共轭辫子对 $x \sim y$ 满足 $x = b^{-1}yb$ 的辫子 b , 该方法对于一定条件下辫群共轭问题都有效. 具体方法见文献[12]. 以上攻击方法在一定条件下对于基于辫群共轭问题的公钥密码系统和密码协议均有效, 对于辫群求根问题失效.

4 一种基于辫群求根问题的公钥密码算法

4.1 算法描述

设 B_n 为 $n > 3$ 的辫群, LB_n 为 B_n 的左子群, RB_n 为 B_n 的右子群. $H: B_n \rightarrow \{0, 1\}^k$ 为抗碰撞的散列函数, $\oplus$ 表示二进制异或运算. 明文 m 为长度为 k

的二进制串. 根据辫群求根问题(RFP)的难解性, 文中提出了如下新的公钥密码算法:

(1) 密钥生成: Alice 秘密选择一个 $u \in RB_n$ 作为私钥, 选择一个 $x \in B_n$, 计算 $y = (uxu)^r$, (x, y) 作为公钥公开.

(2) 加密过程: Bob 秘密选择 $t_1, t_2, \dots, t_{r+1} \in LB_n$, 计算 $p = t_1 y t_{r+1}^{-1}$, $q_1 = t_1 x t_2^{-1}$, $q_2 = t_2 x t_3^{-1}$, $\dots$, $q_r = t_r x t_{r+1}^{-1}$, 对于消息明文 $m \in \{0, 1\}^k$, 计算密文 $c = H(p) \oplus m$, 发送 $q_1, q_2, \dots, q_r$ 和 c 给 Alice.

(3) 解密过程: Alice 计算 $p = \prod_{i=1}^r u q_i u = (u q_1 u)(u q_2 u) \dots (u q_r u)$, 明文消息 $m' = H(p) \oplus c$.

4.2 算法分析

4.2.1 加解密过程的正确性

假定密文为密文 $c = H(p) \oplus m$, 由于 $u \in RB_n$, $t_i \in LB_n, i = 1, 2, \dots, r+1$, 所以 $ut_i = t_i u$, $t_{i+1}^{-1} u = ut_{i+1}^{-1}$, $u q_i u = u(t_i x t_{i+1}^{-1}) u = t_i (uxu) t_{i+1}^{-1}$. 因此:

$$\begin{aligned} p &= (u q_1 u)(u q_2 u) \dots (u q_r u) \\ &= t_1 (uxu)^r t_{r+1}^{-1} = t_1 y t_{r+1}^{-1} \\ c \oplus H(p) &= m \oplus H(p) \oplus H(p) = m. \end{aligned}$$

4.2.2 安全性分析

新公钥密码算法的安全基础建立在求解辫群求根问题(RFP)和多重 P-PBKE 问题的困难性之上的. 若攻击者试图通过公钥 (x, y) 和公开参数来推导私钥 u , 由于 $u \in RB_n, x \in B_n, y = (uxu)^r$ 为辫群求根问题, 因此已知 (x, y) 计算 u 是困难的. 同样攻击者试图通过公开参数来推导秘密参数 $t_i, i = 1, 2, \dots, r+1$, 根据文献[5], 计算 t_i 相当于求解多重 P-PBKE 问题. 若攻击者试图通过密文来推导明文, 其困难性等价于求解辫群求根问题(RFP). 目前, 辫群求根问题(RFP)对线性表示攻击, 长度攻击, 共轭搜索等已知攻击方法免疫. 所以算法是安全的.

4.2.3 参数选择与效率分析

根据文献[5-12], 为保证算法的安全, 算法中要求辫群 B_n 的辫指数 $n \geq 50$, 辫子最小标准长度 $l_{\min} \geq 50$, 初等辫子及其逆元总数 $\delta \geq 2000$, 辫群求根问题 $y = x^r$ 中指数 $r \geq 90$. 若辫子最大标准长度为 λ , 则辫群上的乘法、求逆和随机辫子生成的时间复杂度为 $O(\lambda n)$, 将辫子表示成标准 Garside 范式的时间复杂度为 $O(\lambda^2 n \log n)$, 加密算法和加密算法都至少需要完成一次表示成标准范式的运算, 时间复杂度为 $O(3\lambda^2 n \log n)$. 加密运算至少需要进行 $2r+2$ 次辫子群上的乘法运算, 解密运算至少需要进行 $2r$ 次辫子群上的乘法运算. 不考虑其他运算, 因此加密运

算和解密运算的时间复杂度都为 $O(r\lambda n)$. 表示一个辫子的空间复杂度为 $O(\lambda n \log n)$, 所以私钥的空间复杂度为 $O(\lambda n \log n)$, 而公钥的空间复杂度为 $O(r\lambda n \log n)$.

5 结束语

辫群中的困难问题是构造辫群公钥系统的基础, 目前已有的辫群公钥系统所依赖的困难问题(如 CSP 或者 SCSP)受到一些新的算法攻击(例如 Bureau 表示攻击和线性表示攻击)显得不够安全. 求根问题(RFP)目前没有启发式或者概率多项式算法, 其难解性大于 CSP 问题, 利用此问题可以将许多基于 DLP 和 ECDLP 的数字签名算法(例如代理多重盲签名方案^[13,14])思想推广到辫群上.

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] Artin E. Theory of braids [J]. The Annals of Mathematics, 1947, 48(1): 101-126.
- [3] Anshel I, Anshel M. From the post-markov decision problems to public-key cryptography [J]. American Mathematical Monthly, 1993, 100(9): 835-845.
- [4] Ko KH, Lee SJ, Cheon JH, et al. New public-key cryptosystem using braid groups [C] // Proceedings of the 10th Advances in Cryptology-CRYPTO 2000. LNCS 1880, Berlin: Springer-Verlag, 2000: 166-183.
- [5] Tang X M, Hong F, Cui G H. A public key encryption algorithm on braid groups [J]. J Software, 2007, 18(3): 722-729.
- [6] Cha JC, Cheon JH, Han JW, et al. An efficient implementation of braid groups [C] // Boyd C, ed. Advances in Cryptology-ASIACRYPT 2001. LNCS 2048, Berlin: Springer-Verlag, 2001: 144-156.
- [7] Lee S J, Lee E K. Potential weakness of the commutator key agreement protocol based on braid groups [C] // Proc EUROCRYPT 2002. Berlin: Springer-Verlag, 2002: 14-28.
- [8] Hofheinz D, Steinwand R. A practical attack on some braid group based cryptographic primitives [C] // Proc PKC 2003. Berlin: Springer-Verlag, 2002: 187-198.
- [9] Lee E K, Park J H. Cryptanalysis of the public-key encryption based on braid groups [C] // Proc EUROCRYPT 2003. Berlin: Springer-Verlag, 2003: 477-490.

(下转第 130 页)

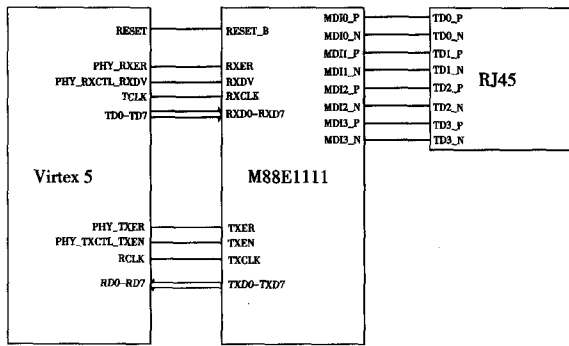


图 7 通信电路原理图

4 结束语

本文设计了可实时远程监测电能质量的光伏并网发电试验系统,完成了系统的总体结构和的主要功能模块的设计。该试验系统将太阳光辐照强度和温度的短期预测模型的预测值作为最大功率点跟踪算法的先验信息,实现对最大功率点的快速准确跟踪;实时计算系统输出电能指标,并实现系统与电能调度中心的远程通信,为电力调度提供参考,增强光伏发电的可调度性;以 FPGA 作为核心控制芯片,可以实现部分程序的重配置,方便不同最大功率点跟踪算法的验证。

本文所设计的试验系统调试和运行情况表明,设计方案合理,实际应用效果良好,保证了系统工作在最大功率点附近,提高了系统的发电效率,减少了电能损耗,增强了光伏发电系统的可调度性,并满足

对光伏发电最大功率点控制技术的研究需要。

参考文献:

- [1] 杨金焕,于化从,葛亮. 太阳能光伏发电应用技术 [M]. 北京:电子工业出版社,2009.
- [2] 卢静,翟海青. 光伏发电功率预测统计方法研究 [J]. 华东电力,2010,(38)4:563-567.
- [3] 何薇薇,杨金明. 太阳能光伏发电最大功率跟踪系统研究 [J]. 电力电子技术,2008,42(8):30-32.
- [4] 王兆安,黄俊. 电力电子技术 [M]. 北京:机械工业出版社,2000.
- [5] 田亚菲,何继爱,黄智武. 电压空间矢量脉宽调制 (SVPWM) 算法仿真实现及分析 [J]. 电力系统及其自动化学报,2004,(4):68-71.
- [6] 张超,王章权,将燕君. 无差拍控制在光伏并网发电系统中的应用 [J]. 电力电子技术,2007(41):3-5.
- [7] 董密,罗安. 光伏并网发电系统中逆变器的设计与控制方法 [J]. 电力系统自动化,2006,30(20):97-102.
- [8] 梁雪峰. 5kW 光伏并网逆变器的研究 [D]. 北京:北京交通大学,2008.

作者简介:

杨清宇 男,(1974—),副教授,硕士生导师.研究方向为电力系统控制与诊断、智能控制理论及应用.

张子光 男,(1984—),硕士研究生.研究方向为光伏发电技术.

邢志勤 男,(1985—),硕士研究生.研究方向为嵌入式系统.

马训鸣 男,(1963—),教授,硕士生导师.研究方向为机电控制及自动化.

(上接第 126 页)

- [10] Cheon J H, Jun B. A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem [C]//Proc CRYPTO 2003. Berlin: Springer-Verlag, 2003: 212-225.
- [11] El-Rifai E A, Morton H R. Algorithms for positive braids [J]. Quart J Math Oxford Ser, 1994, 45(2): 479-497.
- [12] Gebhardt V. A new approach to the conjugacy problem in Garside groups [J]. J Algebra, 2005, 292(1): 282-302.
- [13] 左黎明,刘二根,汤鹏志. 一种基于椭圆曲线的代理多重盲签名方案 [J]. 微电子学与计算机,2010,27(9): 69-72.
- [14] 秦艳琳,吴晓平. 对一种代理盲多重签名的分析与改进 [J]. 微电子学与计算机,2010,27(10):37-40.

作者简介:

左黎明 男,(1981—),硕士,讲师,CCF 会员 (E20-0013632M).研究方向为网络信息安全、非线性系统.