一种改进的辫子群上的密钥协商协议*)

汤学明　洪　帆　崔国华　王小非
(华中科技大学计算机学院　武汉 430074)

摘　要　由 Shor,Boneh 和 Liptonon 等人发现的、可在量子多项式时间内解决大整数分解、离散对数和椭圆曲线上的离散对数问题的量子算法使得当前以这些"难解"问题为基础的传统公钥密码体制受到挑战。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,但是目前基于辫子群的密钥协商协议 AAG、AAFG 和 BDH 等都有不同程度的安全弱点。本文利用随机化辫子和非共轭变换技术,在 AAG 和 AAFG 密钥协商协议的基础上,提出了一种改进的辫子群上的密钥协商协议,用于在非保密信道上安全协商共享密钥。该协议可以抵抗目前已知的长度攻击、线性表示攻击和各种基于共轭搜索方法的攻击。

关键词　辫子群,密钥协商协议,共轭,公钥密码

An Improved Key Agreement Protocol on Braid Groups

TANG Xue-Ming　HONG Fan　CUI Cuo-Hua　WANG Xiao-Fei
(College of Computer Science, Huazhong University of Science and Technology, Wuhan 430074)

Abstract　Shor, Boneh, Liptonon et al. present some remarkable quantum algorithms which can solve integer factoring problem, discrete logarithm problem and discrete logarithm problem on elliptic curves in quantum polynomial time. These quantum algorithms are great challenges to classical public key cryptographies based on the above-described hard problems. It seems that braid group is a kind of considerable public key cryptography platform, but current key agreement protocols, such as AAG, AAFG and BDH, all have different degrees of security weaknesses. This paper takes advantage of random braids and non-conjugate transformations to present an improved braid key agreement protocol related to AAG and AAFG, which can make the two communication parties securely share a common key over any insecure channel. This protocol can resists current length-based attacks, linear representation attacks and other conjugacy search attacks.

Keywords　Braid group, Key agreement protocol, Conjugate, Public key cryptography

1　引言

自 1976 年 Diffie-Hellman 发表了论文"New Directions in Cryptography"以来,公钥密码学作为密码学的一个分支得到了长足的发展。目前,实用的公钥密码系统主要基于三类数学上的"难解"问题,即大整数分解、离散对数和椭圆曲线上的离散对数。

在上个世纪中期, Shor[1] 和 Boneh, Liptonon[2] 等人指出,在未来的量子计算机上,不仅可以在量子多项式时间内分解大整数,而且可以解决离散对数和椭圆曲线上的离散对数等问题。这些量子算法使得基于以上三类"难解"问题的公钥密码系统受到了巨大挑战。科学家们预言,用于实现以上算法的量子计算机可能在未来的 15～20 年内被制造出来,到那时,目前的一些公钥密码系统将不能继续使用。

鉴于以上原因,公钥密码学当前需要解决的一个重要问题是:能否设计既能抵抗传统密码分析,又能抵抗量子密码分析的新型公钥密码系统?

从当前的一些研究结果来看,以下 5 类问题比较适合于构造新型的公钥密码系统:

1)多变量二次系统问题;2)格上的难解问题;3)基于组合群论中的难解问题;4)基于编码理论中的难解问题;5)利用散列函数和传统对称密码算法构造的难解问题。

辫子群早在 1947 年由 Artin 提出[3],并在数学、物理和计算机等领域得到广泛的应用,其运算所需的时间和空间要求很小,结构比较复杂。辫子群上有很多"难解"的问题可以用作构造公钥密码系统的基本元素。

1999 年, Anshel, Anshel 和 Goldfeld 在文[4]中提出了 AAG 密钥协商协议,可用于通信双方在非保密的信道上建立共享密钥。该协议可以在一般的独异点(monoid)上实现,辫子群只是其中的一种特例。由于一类称为"长度攻击"的攻击方法[5,6]的出现,AAG 密钥协商协议暴露出了脆弱性。AAG 密钥协商协议后来在文[7]中修改为 AAFG 密钥协商协议,但 AAFG 带来了新的安全弱点,即易受 Burau 等线性表示攻击[6,8]。基于辫子群的 SSS[9](super summit set)和 USS(ultra summit set)集合的有效计算,降低了辫子群上的共轭问题的计算难度,它们和长度攻击等攻击方法结合起来,会对辫子群上的 AAG 和 AAFG 密钥协商协议造成更大的威胁。特别是 USS 集合相对 SSS 集合较容易计算,可以以非常高的效率

*)国家自然科学基金(60403027)、湖北省自然科学基金(2005ABA243)资助项目。**汤学明**　博士研究生,主要研究方向为数论、密码学和计算机安全;**洪　帆**　教授,博士生导师,主要研究方向为密码学、信息安全、访问控制、网络安全等;**崔国华**　教授,博士生导师,主要研究方向为公钥密码学、数据库加密、信息安全;**王小非**　博士研究生,主要研究方向为密码学和计算机安全。

解决辫子群上的共轭判断问题和共轭搜索问题，详情可参考文[10]。文[11]描述了一种辫子群上的 Diffe-Hellman 协议 BDH，而 Cheon 和 Jun[12] 利用辫子群的 Lawrence-Krammer 表示，可以在多项式时间内破解 BDH 协议。由此可见，变子群上的密钥协商协议 AAG、AAFG 和 BDH 都有不同程度的安全弱点，不能抵抗目前的一些攻击方法。

本文设计了一种新的密钥协商协议，利用随机辫子和非共轭变换的优点，克服了当前协议中共轭变换易受攻击的弱点。经过安全性分析，我们认为新协议对当前已知的攻击方法是具有免疫能力的。

文章第 2 节介绍辫子群的基本结构和辫子群上的难解问题；第 3 节介绍已有的基于辫子群的密钥协商协议及其脆弱性分析和常用的攻击方法；第 4 节介绍改进的密钥协商协议；第 5 节分析改进的密钥协商协议的安全性；最后对全文的主要结论做简单的回顾。

2 辫子群和辫子群上的难解问题

定义 1 辫子群。辫子群是一类特殊的 Artin 群，一个由 $n-1(n\geqslant 3)$，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：

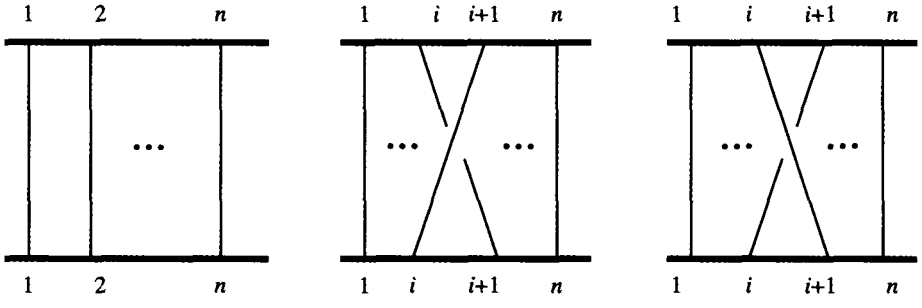
$$B_n=\{s_1,s_2,\cdots,s_{n-1}\mid s_is_{i+1}s_i=s_{i+1}s_is_{i+1},i=1,2,\cdots,n-2;$$

$$s_is_j=s_js_i,i,j=1,2,\cdots,n-1,\ |i-j|\geqslant 2\}$$

辫子群是一类无限、非交换的无纽群，B_n 的每一个元素称为一根辫子。从几何的角度来看，B_n 的单位元可以看成是一上一下两根平行的横梁，分别依次标上 1 到 n 的标记，n 根绳子头朝下依次连接相同标记，并且互不交叉；一个初等辫子 s_i 是将第 i 根绳子和第 $i+1$ 根绳子的头交换，并且第 i 根绳子在第 $i+1$ 根绳子的下面；s_i^{-1} 是将第 i 根绳子和第 $i+1$ 根绳子的头交换，并且第 i 根绳子在第 $i+1$ 根绳子的上面，如图 1 所示。

两根辫子 a 和 b 的乘积 ab 是指将 a 的下横梁和 b 的上横梁上标记相同的绳头连接起来，并以 a 的上横梁为乘积的上横梁，b 的下横梁为乘积的下横梁组成的新辫子。

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范式的形式[11]，两根辫子相等是指它们有相同的范式表示。



(a) B_n 的单位元　(b) B_n 的辫子 s_i　(c) B_n 的辫子 s_i^{-1}

图 1　辫子群 B_n 上元素的几何表示

辫子群之间有一些显而易见的关系。对于正整数 $m\leqslant n$，B_m 是 B_n 的子群；如果 l 和 r 是正整数，B_{l+r} 是由 $s_1,s_2,\cdots,s_{l+r-1}$ 这 $l+r-1$ 个元生成的辫子群。由 $s_1,s_2,\cdots,s_{l-1}$ 生成的群，我们记作 LB_l，由 $s_{l+1},\cdots,s_{l+r-1}$ 生成的群，我们记作 RB_r。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，这些问题有的可用于构造新的密码系统，下面仅列举和共轭相关的 5 个问题。

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 $a\in B_n$，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）共轭分解问题：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 $(a_1,a_2)\in B_m\times B_m$，满足 $y=a_1xa_2$。

5）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，问题 1、2、3 不仅在目前的计算机上，就是在未来的量子计算机上都还没有多项式时间内的确定性解法。问题 4、5 由于最近 Cheon、Jun 等人的工作，已经可以解决。

3 辫子群上已有的密钥协商协议

3.1 BDH 密钥协商协议

一个最直接的辫子群上的密钥协商协议是利用共轭搜索问题的难解性实现 Diffie-Hellman 协议（简称 BDH 密钥协商协议）。我们假设通信的双方为 Alice 和 Bob，在密钥协商开始之前，他们选定一对正整数 (l,r) 和 B_{l+r} 中的一个元 x，并将其公开。

协议 1 BDH 密钥协商协议[11]

BDH 密钥协商协议的过程为：

1）Alice 选择一个随机的秘密辫子 $a\in LB_l$，计算并发送 $y_1=a^{-1}xa$ 给 Bob；

2）Bob 选择一个随机的秘密辫子 $b\in RB_r$，计算并发送 $y_2=b^{-1}xb$ 给 Alice；

3）Alice 收到 y_2，计算共享的密钥 $K=a^{-1}y_2a$；

4）Bob 收到 y_1，计算共享的密钥 $K=b^{-1}y_1b$。

由于 $(a,b)\in LB_l\times RB_r$，满足 $ab=ba$，因而 $a^{-1}y_2a=a^{-1}b^{-1}xba=b^{-1}a^{-1}xab=b^{-1}y_1b=K$。

所以，通过以上的 BDH 密钥协商协议，Alice 和 Bob 可以得到一个共享的密钥 K。

但破解 BDH 比解决共轭搜索问题要容易得多。事实上，BDH 是基于 Diffie-Hellman 共轭问题的难解性，可以更一

般化为共轭分解问题[13]。Cheon 和 Jun[11] 利用辫子群的 Lawrence-Krammer 表示，可以在多项式时间内破解 BDH 协议。

3.2 AAG 密钥协商协议

仍然假设通信的双方为 Alice 和 Bob，AAG 密钥协商协议可描述如下：

协议 2 辫子群上的 AAG 密钥协商协议

密钥协商双方 Alice 和 Bob 首先选定一个辫子群 B_n，并分别选择 B_n 的一个子群

$S=\langle s_1, s_2, \cdots, s_m\rangle$，$T=\langle t_1, t_2, \cdots, t_p\rangle$

其中，$s_i(1\leqslant i\leqslant m)$，$t_j(1\leqslant j\leqslant p)$均是 B_n 中的辫子，n，S 和 T 都公开，密钥协商过程如下：

1)Alice 选择 S 中的一个随机的秘密的辫子 $a=u(s_1, s_2, \cdots, s_m)$，其中 u 表示 Alice 由生成元 $s_1, s_2, \cdots, s_m$ 生成 a 的方法，计算并发送$(at_1a^{-1}, at_2a^{-1}, \cdots, at_pa^{-1})$给 Bob；

2)Bob 选择 T 中的一个随机的秘密的辫子 $b=v(t_1, t_2, \cdots, t_p)$，其中 v 表示 Bob 由生成元 $t_1, t_2, \cdots, t_p$ 生成 b 的方法，计算并发送$(bs_1b^{-1}, bs_2b^{-1}, \cdots, bs_mb^{-1})$给 Alice；

3)Alice 计算共享的密钥 $K=a(u(bsb_1^{-1}, bs_2b^{-1}, \cdots, bs_mb^{-1}))^{-1}=a(bu(s_1, s_2, \cdots, s_m)b^{-1})^{-1}=aba^{-1}b^{-1}$；

4)Bob 计算共享的密钥 $K=v(at_1a^{-1}, at_2a^{-1}, \cdots, at_pa^{-1})b^{-1}=av(t_1, t_2, \cdots, t_p)a^{-1}b^{-1}=aba^{-1}b^{-1}$。

辫子群上的 AAG 密钥协商协议的安全性主要基于两点：

一是共轭搜索问题的难解性(AAG 中依赖的实际是多重共轭搜索问题)。即攻击者利用$(at_1a^{-1}, at_2a^{-1}, \cdots, at_pa^{-1})$不能恢复出秘密的辫子 a，利用$(bs_1b^{-1}, bs_2b^{-1}, \cdots, bs_mb^{-1})$不能恢复出秘密的辫子 b。

二是辫子群中元素的表示问题。即攻击者利用 S 和 T 的生成元 $s_i(1\leqslant i\leqslant m)$和 $t_j(1\leqslant j\leqslant p)$，不能在有效的时间内猜测出 a 和 b 来。

3.3 辫子群上的密码攻击

由于一类称为“长度攻击”的方法的出现和近年来在辫子群共轭问题上的研究进展，辫子群上的 AAG 密钥协商协议暴露出了脆弱性。为了抵抗“长度攻击”，基于辫子群的 AAG 密钥协商协议后来修改为 AAFG 密钥协商协议[7]。修改的内容主要有两点：一是对 S 和 T 的生成元 $s_i(1\leqslant i\leqslant m)$，$t_j(1\leqslant j\leqslant p)$的选取做了一些限制，要求这些生成元的长度要足够小，一般要求由 5 或 10 个初等辫子或它们的逆组成；二是在计算共享密钥 K 的时候，利用辫子群的着色 Burau 表示来表示共享的密钥 K，并最终用散列函数来生成密钥。AAFG 密钥协商协议对 AAG 的修改也带来了一些新的问题。下面，我们对辫子群上的 AAG 和 AAFG 密钥协商协议的一些攻击方法进行简单的描述和分析。

3.3.1 长度攻击

长度攻击最早是由 Hughes 和 Tannenbaum 提出来的，后来由 Hofheinz 和 Steinwandt[5] 以及 Lee S J 和 Lee E[6] 等给出了一些比较好的实现。长度攻击是一种概率攻击方法，其基本思想是在辫子群 B_n 上定义一种长度函数 $len(x)$，使得对于随机选择的辫子 a 和 b 几乎都满足 $len(ab)=len(a)+len(b)$。那么一般而言，设 $a=g_1g_2\cdots g_i$，$y=axa^{-1}$，其中 g_1，$g_2, \cdots, g_i$ 是已知的生成元，则对于生成元 g_1，不等式 $len(g_1^{-1}yg_1)\langle len(y)$成立的概率较大；而对于其它生成元 g_j，$j=2,3,\cdots,i$，$len(g_j^{-1}yg_j)\rangle len(y)$成立的概率较大。而且当生成元 $g_j(j=1,2,\cdots,i)$的长度越长的时候，这种差异越大。根据这一概率事件，如果提供的共轭辫子对(x, axa^{-1})足够多，而生成元的长度较长的时候，攻击者可以以较大的概率逐步从 a 中去掉生成元 $g_1, g_2, \cdots, g_i$，从而恢复 a。具体到 AAG 协议而言，如果长度攻击成功，攻击者就可以恢复 Alice 和 Bob 所选择的秘密辫子，求出共享密钥。一般来讲，如果共轭辫子对很少，而生成元的长度较小或者生成元仅仅为初等辫子，那么长度攻击是很难奏效的。

正是由于长度攻击的威胁，AAFG 密钥协商协议在 AAG 的基础上进行了修改，其主要目的是为了减小生成元的长度。

3.3.2 线性表示攻击

BigeLow 等人证明辫子群是线性的，辫子群有多种不同的线性表示，例如 Burau 表示、着色 Burau 表示和 Lawrence-Krammer 表示等。AAFG 由于减小了生成元的长度，为了避免辫子群在小生成元情况下的一些计算上的弱点，在生成共享密钥的时候使用了着色 Burau 表示。Huges[8] 给出了一个基于线性代数的攻击方法。Lee S J 和 Lee E[6] 也指出，AAFG 协议在小生成元情况下是极易受线性攻击的，而且着色 Burau 表示增加了该协议受线性攻击的可能性。

3.3.3 其它攻击

Dehornoy[10] 指出，如果不随机选择辫子，特别是当 a 和 b 的长度很小的时候，乘积 ab 中将显而易见地包含 a 和 b 的很多信息，这也给攻击者带来方便。

基于辫子群的 SSS[9] 和 USS 集合的有效计算，降低了辫子群上的共轭问题的计算难度，它们和长度攻击等攻击方法结合起来，会对辫子群上的 AAG 和 AAFG 密钥协商协议造成更大的威胁。

从以上分析我们可以看出，基于辫子群的 AAG 和 AAFG 密钥协商协议陷入矛盾的局面：长度攻击要求协议必须使用较短的生成元；而较短的生成元降低了共轭问题的难度，不能抵抗诸如线性表示攻击等一类攻击方法；SSS 和 USS 方法的出现使得 AAG 和 AAFG 等利用辫子群共轭搜索问题构造的公钥密码系统可信度大为降低。

4 改进的密钥协商协议

自 BDH、AAG 和 AAFG 密钥协商协议发布以来，由于人们对于辫子群理论的认识不断深入和一些新的攻击方法的不断出现，基于辫子群的密钥协商协议一直处于停滞状态。

本文受 AAG 和 AAFG 密钥协商协议的启发，对其进行改进，提出了一种新的密钥协商协议。新协议对于目前已知的一些攻击方法具有免疫能力，同时可以抵抗一些未知的攻击手段。

首先，我们详细描述改进的密钥协商协议的密钥协商过程。

协议 3 改进的密钥协商协议

协议准备阶段：

密钥协商双方 Alice 和 Bob 首先选定一个辫子群 B_n，并分别秘密选择 B_n 中的 4 个随机的辫子 x_A，y_A，s_A，t_A 和 x_B，y_B，s_B，t_B。

Alice 计算 $R_A=x_A^{-1}t_Ay_A$，并将 R_A 表示成初等辫子相乘的形式，不妨设 $R_A=s_{i_1}s_{i_2}\cdots s_{i_t}$（$R_A$ 的这种表示不需要是范式）。Alice 将所有这 t 个初等辫子从左到右分成 m 组，如果这 m 组初等辫子的乘积分别为 $a_1, a_2, \cdots, a_m$，则有 $R_A=a_1a_2\cdots a_m$。

Alice 又秘密选取 $2m-1$ 个随机的辫子 $a'_1, a'_2, \cdots, a'_m$，$x_{A_1}, x_{A_2}, \cdots, x_{A_{m-1}}$。如果我们用$(x, y)$表示辫子对$(x, y)$或$(y, x)$，即 x 和 y 的任意一个排列，用 $x(a, b)y$ 表示辫子对(xay, xby)，Alice 公开的 m 个辫子对表示如下：

$x_A\pi(a_1,a'_1)xA_1^{-1}, x_{A_1}\pi(a_2,a'_2)x_{A_2}^{-1}, x_{A_2}\pi(a_3,a'_3)x_{A_3}^{-1}$ $\cdots, x_{A_{m-2}}\pi(a_{m-1},a'_{m-1})x_{A_{m-1}}^{-1}, x_{A_{m-1}}\pi(a_m,a'_m)y_A^{-1}$

Bob 计算 $R_B=x_B^{-1}s_By_B$。接下来,用和 Alice 一样的方法将 R_B 的初等辫子进行分组,设结果为 $R_B=b_1b_2\cdots b_k$。

Bob 秘密选取 $2k-1$ 个随机的辫子 $b'_1,b'_2,\cdots,b'_k,x_{B_1},x_{B_2},\cdots,x_{B_{k-1}}$,通过计算,公开如下 k 个辫子对:

$x_B\pi(b_1,b'_1)x_{B_1}^{-1}, x_{B_1}\pi(b_2,b'_2)x_{B_2}^{-1}, x_{B_2}\pi(b_3,b'_3)x_{B_3}^{-1},\cdots,$ $x_{B_{k-2}}\pi(b_{k-1},b'_{k-1})x_{B_{k-1}}^{-1}, x_{B_{k-1}}\pi(b_k,b'_k)y_B^{-1}$

密钥协商过程:

1)Alice 随机秘密选取 $k-1$ 个辫子 $c_1,c_2,\cdots,c_{k-1}$,对 Bob 公开的 k 个辫子对计算

$s_Ax_B\pi(b_1,b'_1)x_{B_1}^{-1}c_1, c_1^{-1}x_{B_1}\pi(b_2,b'_2)x_{B_2}^{-1}c_2, c_2^{-1}x_{B_2}\pi(b_3,$ $b'_3)x_{B_2}^{-1}c_3,\cdots, c_{k-2}^{-1}x_{B_{k-2}}\pi(b_{k-1},b'_{k-1})x_{B_{k-1}}^{-1}c_{k-1}, c_{k-1}^{-1}$ $x_{B_{k-1}}\pi(b_k,b'_k)y_B^{-1}t_A$

并发送给 Bob;

2)Bob 随机秘密选取 $m-1$ 个辫子 $d_1,d_2,\cdots,d_{m-1}$,对 Alice 公开的 m 个辫子对计算

$s_Bx_A\pi(a_1,a'_1)x_{A_1}^{-1}d_1, d_1^{-1}x_{A_1}\pi(a_2,a'_2)x_{A_2}^{-1}d_2, d_2^{-1}x_{A_2}\pi$ $(a_3,a'_3)x_{A_3}^{-1}d_3,\cdots, d_{m-2}^{-1}x_{A_{m-2}}\pi(a_{m-1},a'_{m-1})x_{A_{m-1}}^{-1}d_{m-1},$ $d_{m-1}^{-1}x_{A_{m-1}}\pi(a_m,a'_m)y_A^{-1}t_B$

并发送给 Alice;

3)Alice 接收 Bob 发送的 m 个辫子对,由于只有她才知道她所公布的每个辫子对中哪一个辫子是有效的,因此她可以计算如下的共享密钥:

$$\begin{aligned}K&=s_A(s_Bx_Aa_1x_{A1}{}^{-1}d_1)(d_1{}^{-1}x_{A1}a_2x_{A_2}{}^{-1}d_2)\cdots(d_{m-2}{}^{-1}\\&\quad x_{A_{m-2}}a_{m-1}x_{A_{m-1}}{}^{-1}d_{m-1})(d_{m-1}{}^{-1}x_{A_{m-1}}a_my_A{}^{-1}t_B)\\&=s_As_Bx_Aa_1a_2\cdots a^{m-1}a_my_A^{-1}t_B=s_As_Bx_AR_Ay_A^{-1}t_B\\&=s_As_Bx_Ax_A^{-1}t_Ay_Ay_A^{-1}t_B\\&=s_As_Bt_At_B\end{aligned}$$

4) Bob 接收 Alice 发送的 k 个辫子对,类似地计算共享的密钥

$$\begin{aligned}K&=(s_Ax_Bb_1x_{B_1}^{-1}c_1)(c_1^{-1}x_{B_1}b_2x_{B_2}^{-1}c_2)\cdots(c_{k-2}^{-1}x_{B_{k-2}}b_{k-1}\\&\quad x_{B_{k-1}}^{-1}c_{k-1})(c_{k-1}^{-1}x_{B_{k-1}}b_ky_B^{-1}t_A)t_B\\&=s_Ax_Bb_1b_2\cdots b_{k-1}b_ky_B^{-1}t_At_B=s_Ax_BR_By_B^{-1}t_At_B\\&=s_Ax_Bx_B^{-1}s_By_By_B^{-1}t_At_B\\&=s_As_Bt_At_B\end{aligned}$$

至此,Alice 和 Bob 就完成了密钥协商过程,他们的共享密钥为 $s_As_Bt_At_B$。

5 新协议的安全性分析

5.1 改进协议的安全基础

5.1.1 密钥组合

AAG 和 AAFG 密钥协商协议的秘密辫子可以由生成元的任意组合生成,不仅可以包含生成元的逆,还可以重复多次使用同一个生成元。根据新协议的需要,我们仅使用多个辫子对的二选一的组合问题,Alice 共公开了 m 个辫子对,每个辫子对中只有一个辫子是有效的,密钥的可能性只有 2^m 种。虽然密钥组合的可能性减少了,但是穷举 2^m 个可能的密钥还是具有指数时间的复杂度。

通常,公开辫子对的数量要取得足够大。以 Alice 为例,如果攻击者能够以某种方法知道辫子对中的哪个辫子是用来生成 R_A 的,那么攻击者就可以将它们相乘,计算出 t_A。因为,

$$\begin{aligned}&(x_Aa_1x_{A_1}^{-1})(x^{A_1}a_2x_{A_2}^{-1})\cdots(x_{A_{m-2}}a_{m-1}x_{A_{m-1}}^{-1})(x_{A_{m-1}}\\&\quad a_my_A^{-1})=x_Aa_1a_2\cdots a_{m-1}a_my_A^{-1}=x_AR_Ay_A^{-1}=t_A\end{aligned}$$

假设攻击者能够以同样的方法计算出协议中的 s_B,那么利用 Alice 发送给 Bob 的 k 个辫子对,攻击者可以计算:

$(s_Ax_Bb_1x_{B1}^{-1}c_1)(c_1^{-1}x_{B_1}b_2x_{B_2}^{-1}c_2)\cdots(c_{k-2}^{-1}x_{B_{k-2}}b_{k-1}x_{B_{k-1}}^{-1}$ $c_{k-1})(c_{k-1}^{-1}x_{B_{k-1}}b_ky_B^{-1}t_A)t_A^{-1}s_B^{-1}=(s_As_Bt_A)t_A^{-1}s_B^{-1}=s_A$

利用 Bob 发送给 Alice 的 m 个辫子对,攻击者可以计算:

$t_A^{-1}s_B^{-1}(s_Bx_Aa_1x_{A_1}^{-1}d_1)(d_1^{-1}x_{A_1}a_2x_{A_2}^{-1}d_2)\cdots(d_{m-2}^{-1}x_{A_{m-2}}a_{m-1}$ $x_{A_{m-1}}^{-1}d_{m-1})(d_{m-1}^{-1}x_{A_{m-1}}a_my_A^{-1}t_B)=t_A^{-1}s_B^{-1}(s_Bt_At_B)=t_B$

也就是说,如果公开的辫子对的数目太小,攻击者就有可能恢复出共享的密钥 $s_As_Bt_At_B$。建议选择 64 个辫子对或者更多。

5.1.2 方程组求解问题

共轭搜索问题是一类一元方程求解问题。一般而言,辫子群上关于 x 的方程 $x^{-1}ax=b$ 的解不唯一,共轭搜索问题是求出其中的一个特解。我们用 Z_a 表示群$\langle a\rangle$的中心化子,即 $Z_a=\{z\in B_n\mid za=az\}$。如果 x 是方程 $x^{-1}ax=b$ 的一个解,那么集合 $C_{a,b}=\{zx\mid z\in Z_a\}$恰好是方程 $x^{-1}ax=b$ 的所有解。破解辫子群上的 AAG 密钥协商协议中的共享密钥 K 并不需要精确地恢复 Alice 和 Bob 秘密选择的辫子 a 和 b。事实上,若令 $C_A=C_{t_1,a_1a^{-1}}\cap C_{t_2,a_2a^{-1}}\cap\cdots\cap C_{t_p,a_pa^{-1}}$, $C_B=C_{s_1,b_1b^{-1}}\cap C_{s_2,b_2b^{-1}}\cap\cdots\cap C_{s_m,b_mb^{-1}}$,则 $a\in C_A$,$b\in C_B$;反之,对于任意的 $a'\in C_A\cap S$,$b'\in C_B\cap T$,均有 $a'b'a'^{-1}b'^{-1}=ab'a^{-1}b'^{-1}=aba^{-1}b^{-1}=K$。也就是说,只要找到任意的 $a'\in C_A\cap S$ 和 $b'\in C_B\cap T$,都可以恢复共享密钥。

辫子群上循环群的中心化子可以在多项式时间内计算出来[14]。但是,目前还没有有效的算法可以计算 C_A 和 C_B,而且判断 a' 是否是 S 中的元素以及 b' 是否是 T 中的元素,也没有有效的算法,所以计算 $C_A\cap S$ 和 $C_B\cap T$ 都是难解的问题。从这一点上来讲,即使解决了共轭搜索问题,也并不意味着破译了一般的辫子群上的 AAG 密钥协商协议。

本文所提出的改进的密钥协商协议在这一点上做了进一步加强,增加了攻击难度。

以 Alice 对 Bob 的公开元素做变换为例。攻击者为了利用共轭搜索方法恢复 s_A,需要构造关于 s_A 的共轭方程,这一点可以做到。例如:

设 $s_A(x_Bb_1x_{B_1}^{-1})c_1=s_1$ 以及 $s_A(x_Bb'_1x_{B_1}^{-1})c_1=t_1$,则有 $c_1=(x_Bb_1x_{B_1}^{-1})^{-1}s_A^{-1}s_1$,从而,$s_A(x_Bb'_1x_{B_1}^{-1})(x_Bb_1x_{B_1}^{-1})^{-1}s_A^{-1}s_1=t_1$,这样就得到了关于 s_A 个共轭方程:

$s_A(x_Bb'_1x_{B_1}^{-1})(x_Bb_1x_{B_1}^{-1})^{-1}s_A^{-1}=t_1s_1^{-1}$

其中,$x_Bb'_1x_{B_1}^{-1}$、$x_Bb_1x_{B_1}^{-1}$ 以及 t_1 和 s_1 都假设攻击者可以获取。

类似地,若还设 $c_1^{-1}(x_{B_1}b_2x_{B_2}^{-1})c_2=s_2$ 和 $c_1^{-1}(x_{B_1}b'_2x_{B_2}^{-1})c_2=t_2$,我们通过方程变换还可以得到以下两个关于 s_A 的共轭方程:

$$\begin{aligned}&s_A(x_Bb_1x_{B_1}^{-1})(x_{B_1}b'_2x_{B_2}^{-1})(x_{B_1}b_2x_{B_2}^{-1})^{-1}(x_Bb_1x_{B_1}^{-1})^{-1}s_A^{-1}\\&\quad=s_1t_2s_2^{-1}s_1^{-1}\\&s_A(x_Bb'_1x_{B_1}^{-1})(x_{B_1}b'_2x_{B_2}^{-1})(x_{B_1}b_2x_{B_2}^{-1})^{-1}(x_Bb'_1x_{B_1}^{-1})^{-1}\\&\quad s_A^{-1}=t_1t_2s_2^{-1}t_1^{-1}\end{aligned}$$

一般而言,依照上面的方法,理论上攻击者共可以得到

$1+2+2^2+\cdots+2^{k-1}=2^k-1$

个不同的关于 s_A 的共轭方程,而秘密辫子 s_A 必然包含在这 2^k-1 个方程的解集的交集之中。用同样的方法,攻击者还可以得到 2^k-1 个关于 t_A 的共轭方程。

当 k 充分大的时候,攻击者显然不可能求出所有关于 s_A 和 t_A 的共轭方程的解集,只能选择其中的一部分方程求解。我们仅以一种情况为例来说明即使求得了这些共轭方程的

解，攻击者攻击成功的概率仍然很小。

假设攻击者在构造共轭方程的过程中选择了两个关于 s_A 和 t_A 的方程 $s_A a t_A = s$ 和 $s_A a' t_A = t$，其中 a 和 a' 是从 $x_B \pi(b_1, b'_1) x_{B_1}^{-1}, x_{B_1} \pi(b_2, b'_2) x_{B_2}^{-1}, x_{B_2} \pi(b_3, b'_3) x_{B_3}^{-1}, \cdots, x_{B_{k-2}} \pi(b_{k-1}, b'_{k-1}) x_{B_{k-1}}^{-1}, x_{B_{k-1}} \pi(b_k, b'_k) y_B^{-1}$ 这 k 个辫子对中任选一个辫子，然后将 k 个辫子相乘得到的。由此形成的关于 s_A 的共轭方程为 $s_A a' a^{-1} s_A^{-1} = t s^{-1}$。如果 $a \neq a'$，该共轭方程的每一个解 s'_A 都唯一对应一个 t'_A，使得 $s'_A a t'_A = s$ 以及 $s'_A a' t'_A = t$。和共轭变换不同的是，$s'_A a t'_A$ 一般情况下不是同态变换，所以攻击者得到了 $s'_A a t'_A = s$ 和 $s'_A a' t'_A = t$，仅仅意味着他们知道了 s'_A 和 t'_A 对辫子 a 和 a' 的作用结果，而不能由此推导出 s'_A 和 t'_A 对 a 和 a' 的其它组合（例如 $a a'$）的作用结果。但为了寻找 s'_A、s'_B、t'_A 和 t'_B 使得 $s'_A s'_B t'_A t'_B = s'_A s_B t'_A t_B = s_A s_B t_A t_B$ 成立，必然有 $s'_A s_B t'_A = s_A s_B t_A$，说明攻击者必须要能够恰好获得 s'_A 和 t'_A 对 s_B 的作用结果，这要求攻击者必须了解 Bob 实际使用的是哪些生成元。

通过对其它的共轭方程进行类似的分析，我们可以知道，攻击者用共轭搜索的方法进行攻击，成功的概率很小。

5.1.3 随机辫子问题

改进的协议中包含两类随机辫子问题：

一是随机辫子的生成问题。新协议中多处使用了随机辫子，这些辫子都是临时生成的。假设 RNG 是一个取值范围为 $[1-n, -1] \cup [1, n-1]$ 的随机数发生器，当 RNG 取值为 i ($1 \leqslant i \leqslant n-1$) 时，我们就选择初等辫子 s_i；当 RNG 取值为 j ($1-n \leqslant j \leqslant -1$) 时，我们就选择初等辫子 s_{-j} 的逆 s_{-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形成的随机辫子。关于随机辫子的其它生成算法，可以参考文[7]。

第二个问题是如何将一个辫子表示成随机辫子的乘积。具体到 Alice 而言，她计算 $R_A = x_A^{-1} t_A y_A$，并将 R_A 分成 m 组。为了抵抗一些未知的可能的攻击，x_A^{-1} 和 y_A 应该尽可能均匀地分布在每个分组中，而不是仅分布在最前面或最后面的几个分组中。文[10]介绍了两种方法，可以将辫子进行不规则化处理。

5.2 协议的抗攻击能力分析

5.2.1 长度攻击

改进的协议对长度攻击具有免疫能力。一方面，我们采用随机化的方法隐藏了秘密参数的长度较长的生成元。以 Alice 为例，虽然

$$t_A = (x_A a_1 x_{A_1}^{-1})(x_{A_1} a_2 x_{A_2}^{-1})(x_{A_2} a_3 x_{A_3}^{-1}) \cdots (x_{A_{m-2}} a_{m-1} x_{A_{m-1}}^{-1})(x_{A_{m-1}} a_m y_A^{-1})$$

但是，与 AAG 和 AAFG 不同的是，$x_A, x_{A_1}, x_{A_2}, \cdots, y_A$ 都是随机选择与 t_A 毫无关联的辫子，乘积 $(x_A a_1 x_{A_1}^{-1})(x_{A_1} a_2 x_{A_2}^{-1})(x_{A_2} a_3 x_{A_3}^{-1}) \cdots (x_{A_{m-2}} a_{m-1} x_{A_{m-1}}^{-1})(x_{A_{m-1}} a_m y_A^{-1})$ 中的这些随机辫子实际上会完全抵消。因此，一般情况下，用 Alice 公布的辫子对中的任何一个辫子去消除 t_A 中的长度较长的辫子，企图降低 t_A 的复杂性，都是不可能的。

另一方面，在 AAG 和 AAFG 中，Alice 和 Bob 均仅采用一个秘密参数对所有的公开生成元做共轭变换，利于攻击者在攻击时进行概率累积，改进协议中用不同的辫子对公开元做变换，任何一个随机的辫子在公开元中最多出现 4 次。例如 c_1 仅在 $s_A x_B b x_{1B_1}^{-1} c_1$、$s_A x_B b'_1 x_{B_1}^{-1} c_1$、$c_1^{-1} x_{B_1} b_2 x_{B_2}^{-1} c_2$ 和 $c_1^{-1} x_{B_1} b'_2 x_{B_2}^{-1} c_2$ 中各出现一次，虽然攻击者可以采用一些方程变换的方法使得 c_1 在不同的方程中出现，但是紧靠 c_1 左右的辫子始终只有固定的几个，这些固定的辫子可以阻挡其它的随机辫子与 c_1 相乘。所以，攻击者即使能对所有的关于 c_1 的方程实施长度攻击，他们也不可能取到很多有意义的随机的样本点，这使得概率攻击成功的机会很小。

5.2.2 线性表示攻击和共轭搜索攻击

线性表示攻击和共轭搜索攻击都是基于可以以某种方式求共轭方程的特解。从 5.1.2 的分析中我们可以看出，这些攻击方法对改进的协议都不能奏效。

5.2.3 量子算法攻击

从目前量子算法的研究情况来看，量子计算机在隐藏子群和随机搜索问题上具有当前计算机无法比拟的快速算法，这些算法对本文所提出的新的密钥协商协议不构成本质上的威胁。

结论 本文基于 AAG 和 AAFG 提出了辫子群上的一个改进的密钥协商协议。改进的密钥协商协议主要采用了随机化方法和非共轭变换，克服了辫子群计算上的弱点，能有效抵抗当前辫子群上的长度攻击、线性表示攻击和共轭搜索攻击等攻击方法。本文的研究思路对于辫子群密钥协商协议的发展以及在组合群论中研究公钥密码系统具有重要意义。

致谢 作者所在的信息安全课题组的老师和博士研究生组织讨论班对辫子群的理论与密码学应用进行了深入的讨论，并在本文写作过程中提出了许多宝贵的意见和建议，在此一并表示感谢。

参 考 文 献

1 Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1997,26:1484～1509

2 Boneh R, Lipton R. Quantum cryptanalysis of hidden linear functions. Advances in Cryptology-Crypto'95. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1995, 963:424～437

3 Artin E. Theory of Braids. Ann of Math, 1974, 48:101～126

4 Anshel I, Anshel M, Goldfeld D. An Algebraic Method for Public-key Cryptography. Mathematical Research Letters, 1999, 6:1～5

5 Hofheinz D, Steinwandt R. A Practical Attack on Some Braid Group Based Cryptographic Primitives. In: Desmedt Y G, ed. Public Key Cryptography—PKC 2003, Lecture Notes in Computer Science 2567, Berlin: Springer-Verlag, 2003. 187～198

6 Lee S J, Lee E. Potential weakness of the commutator key agreement protocol based on braid groups. In: Knudsen L, ed. Advances in Cryptology-EUROCRYPT 2002, Lecture Notes in Computer Science 2332, Berlin: Springer-Verlag, 2002. 14～18

7 Anshel I, Anshel M, Fisher B, et al. New Key Agreement Protocols in Braid Group Cryptography. In: Naccache D, ed. Topics in Cryptology—CT-RSA 2001, Lecture Notes in Computer Science 2020, Berlin: Springer-Verlag, 2001. 13～27

8 Hughes J. A linear algebraic attack on the AAFG1 braid group cryptosystem. In: Batten L, Seberry J, eds. Information Security and Privacy -7th Australian Conference, ACISP 2002, Lecture Notes in Computer Science 2384, Berlin: Springer-Verlag, 2002. 176～189

9 El-Rifai E A, Morton HR. Algorithms for positive braids. Quart J Math Oxford Ser, 1994, 45(2):479～497

10 Dehornoy P. Braid-based cryptography. Contemporary Mathematics, 2004, 360:5～33

11 Ko K H, Lee S J, Cheon J H, et al. New public-key cryptosystem using braid groups. In: Bellare M, ed. Advances in Cryptology-CRYPTO 2000, Lecture Notes in Computer Science 1880, Berlin: Springer-Verlag, 2000. 166～183

12 Cheon JH, Jun B. A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem. In: Boneh D, ed. Advances in Cryptology-CRYPTO 2003, Lecture Notes in Computer Science 2729, New York: Springer-Verlag, 2003. 212～225

13 Cha J C, Cheon J H, Han J W, et al. An efficient implementation of braid groups. In: Boyd C. ed. Advances in Cryptology-ASIACRYPT 2001, Lecture Notes in Computer Science 2048, Berlin: Springer-Verlag, 2001. 144～156

14 Franco N, Gonzalez-Meneses J. Computation of centralizers in braid groups and Garside groups. Rev Mat Iberoamericana, 2003, 19(2):367～384