辫群上新的签名体制

隗　云[①]　　熊国华[②]　　鲍皖苏[①]　　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：辫群是构造抗量子攻击密码协议的新平台。该文基于辫群上求根问题的难解性提出了新的签名体制，并证明其在随机预言模型下能抵抗适应性选择消息的存在性伪造攻击。新体制在签名验证阶段不需要判断辫元是否存在共轭关系，计算效率比共轭签名体制、改进共轭签名体制更高；签名由一个整数和一个辫元组成，与共轭签名体制相比长度更短，与改进共轭签名体制长度相当。

关键词：数字签名；辫群；求根问题；随机预言模型
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2010)12-2930-05
DOI: 10.3724/SP.J.1146.2010.00167

New Signature Scheme over the Braid Groups

Wei Yun[①]　　Xiong Guo-hua[②]　　Bao Wan-su[①]　　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: The braid group is a new candidate platform for constructing quantum attack-resistant cryptographic protocols. A new signature scheme is proposed based on the difficulty of the root extraction problem over braid groups, which can resist existential forgery against the adaptively chosen-message attack under the random oracle model. Compared with the Conjugacy Signature Scheme (CSS) and the Enhanced Conjugacy Signature Scheme (ECSS), the verification phase of the proposed scheme desires less computation because it does not have to determine whether two braids are conjugate. The signature is composed of an integer and a braid, which is much shorter than that of CSS and almost same as that of ECSS.

Key words: Digital signature; Braid group; Root Extraction Problem (REP); Random oracle model

1　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，如基于非交换环的签名体制[3,4]等。

1947 年，Artin[5]首次提出辫群的概念。辫群上的运算所需时间和空间很小，且当辫指数大于 2 时，辫群具有复杂的非交换结构，是构造抗量子攻击密码体制的新平台。2000 年，文献[6]首次提出了基于辫群的公钥密码体制。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]相继被提出。2002 年，文献[12]提出了基于辫群的签名体制，其理论基础是辫群上共轭判断问题的可解性和共轭搜索问题的难解性，签名验证通过判断元素是否共轭来实现，因此被称为共轭签名体制。后来提出的改进共轭签名体制[13]及各种特性签名体制[14−23]都是基于共轭问题进行设计，均属于共轭签名体制。

长度攻击[24]和线性表示攻击[25]的研究使得人们对共轭搜索问题的难解性产生了质疑，目前的研究表明辫群上的求根问题比其它问题都难解，但是除了文献[9]提出的认证协议外，尚无其它协议充分利用该问题的难解性。本文基于辫群上求根问题的难解性提出了新的签名体制，签名及验证过程只涉及乘法和求逆运算而不需要判断元素是否共轭，提高了计算效率。此外，与共轭签名体制相比签名长度更短。本文第 2 节主要介绍辫群的相关概念及签名

2010-03-01 收到，2010-06-15 改回
国家自然科学基金(10501053)资助课题
通信作者：隗云　weiyun456@sohu.com

的安全模型；第 3 节给出辫群上新的签名体制；第 4 节对签名体制的安全性质和效率进行分析；第 5 节总结全文。

2　相关知识

2.1 辫群及辫群上的难解问题

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：

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

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

因此辫群 B_n 可表示为

$$B_n = \left\langle \sigma_1,\sigma_2,\cdots,\sigma_{n-1} \,\middle|\, \begin{matrix} \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, & 1 \leq i \leq n-2 \\ \sigma_i\sigma_j = \sigma_j\sigma_i, & |\, i-j \,| \geq 2 \end{matrix} \right\rangle$$

$\sigma_1,\sigma_2,\cdots,\sigma_{n-1}$ 称为辫群的生成子或 Artin 生成子，还称为初等辫子。辫群中的元素称为一个 n 辫子或辫元，n 称为辫指数。B_2 是无限阶的循环群，本文不予考虑，当 $n>2$ 时 B_n 是无限非交换群。表达式中不出现初等辫子的负次幂的辫子称为正辫子，单位元 $\varepsilon \in B_n$ 也是正辫子，所有正辫子集合记作 B_n^+。$\Delta = (\sigma_1\sigma_2\cdots\sigma_{n-1})(\sigma_1\sigma_2\cdots\sigma_{n-2})\cdots(\sigma_1\sigma_2)\sigma_1$ 称为 B_n 的基本辫子。

在 B_n 上定义整除关系“$\leq$”如下：对 $(v,w) \in B_n \times B_n$，$v \leq w$ 当且仅当存在 $\alpha,\beta \in B_n^+$ 使得 $w = \alpha v \beta$。满足 $\varepsilon \leq \alpha \leq \Delta$ 的辫子 $\alpha \in B_n$ 称为正规因子。对满足 $\gamma = \alpha\beta$ 的正辫子 α,β,γ，称 β 为 γ 的一个尾部，若 α 为正规因子，且 α 在所有的分解中根据整除关系“$\leq$”长度最长，则称这种分解是左加权的。根据这种左加权分解，任意辫子 $w \in B_n$ 都可以唯一表示成 $w = \Delta^r\alpha_1\cdots\alpha_q$，其中 $\alpha_1,\cdots,\alpha_q$ 为正规因子，$\alpha_i\alpha_{i+1}(1 \leq i < q)$ 是左加权的。$w = \Delta^r\alpha_1\cdots\alpha_q$ 称为辫子 $w \in B_n$ 的左规范型，简称为规范型。q 称为 w 的正规长度，r 称为 w 的下确界，记作 $\inf(w)$。$r+q$ 称为 w 的上确界，记作 $\sup(w)$。根据规范型，每个辫元可以唯一表示成一个二进制数。

对辫群 B_n，由生成子 $\sigma_1,\sigma_2,\cdots,\sigma_{\lfloor n/2 \rfloor -1}$ 生成的子群记为 LB_n，称为左子群；由生成子 $\sigma_{\lfloor n/2 \rfloor +1}$, $\sigma_{\lfloor n/2 \rfloor +2},\cdots,\sigma_{n-1}$ 生成的子群记为 RB_n，称为右子群。显然，对任意 $\alpha \in \mathrm{LB}_n$，$\beta \in \mathrm{RB}_n$，有 $\alpha\beta = \beta\alpha$。

定义 2[6]　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，记作 $x \sim y$。

定义 3[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(Conjugacy Decision Problem，CDP)。

定义 4[6]　给定共轭辫元对 $(x,y) \in B_n \times B_n$，$x \sim y$，找到满足 $y = a^{-1}xa$ 的辫元 $a \in B_n$，称共轭搜索问题(Conjugacy Search Problem, CSP)。

定义 5[6]　给定整数 $c(c>1)$ 及 $\beta \in B_n$，满足存在 $\alpha \in B_n$ 使 $\beta = \alpha^c$，找到 $\gamma \in B_n$ 使 $\beta = \gamma^c$，称求根问题(Root Extraction Problem，REP)。

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，文献[12]提出了一种多项式时间算法。但是，尚未有算法能证明可在多项式时间内求解 CSP 或 REP，且解 REP 比 CSP 更难。

2.2 安全模型

针对签名体制的安全性，Pointcheva 和 Stern[26] 将对签名体制的攻击方法分为唯密钥攻击、一般的选择消息攻击、定向选择消息攻击和适应性选择消息攻击，攻击者攻击成功的强度分为完全攻破、一般性伪造和存在性伪造。他们首次提出了一般签名体制的概念，并针对适应性选择消息攻击下的存在性伪造给出了证明一般签名体制安全性的 Forking 引理。

定义6[26]　输入消息 m，一般签名体制输出的签名为三元组 (s_1,h,s_2)，其中 s_1 是随机选择于一个大集合的元素，h 是 $(m \,||\, s_1)$ 的哈希函数值，s_2 由 s_1 和 h 决定，s_1 在签名中出现的概率不大于 $2/2^k$ (k 为安全参数)，“||”表示二进制串的级联。

Forking引理　考虑安全参数为 k 的一般签名体制。设 $\mathcal{F}$ 是输入为公开参数的多项式时间算法，可以分别向随机预言、签名预言询问 q_h 和 q_s 次。如果 $\mathcal{F}$ 能在时间 t 内，以概率 $\varepsilon \geq 10(q_h+1)(q_h+q_s)/2^k$ 成功地产生关于消息 m 的有效签名 (s_1,h,s_2)，且未向签名预言询问过 m 的签名，则通过算法 $\mathcal{F}$ 可以在时间 $t' \leq 120686q_h t/\varepsilon$ 内得到关于消息 m 的两个有效签名 (s_1,h,s_2) 和 (s_1,h',s_2') 满足 $h \neq h'$。

本文考虑适应性选择消息攻击下的存在性伪造(existential forgery under adaptively chosen-message attack)。在这种攻击中，攻击算法 $\mathcal{F}$ 可以：(1)向随机预言询问不超过 q_h 个消息的哈希值；(2)向签名预言询问不超过 q_s 个消息的有效签名，其中询问的消息由 $\mathcal{F}$ 自主选择。

q_h 和 q_s 应是关于安全参数 k 的多项式，若 $\mathcal{F}$ 能在多项式时间内以不可忽略的概率 $Adv_{\mathcal{F}}^{\text{EFU-CMA}}(k)$ 产生关于消息 m 的签名，且满足：$\mathcal{F}$ 未向签名预言询问关于消息 m 的签名，则称 $\mathcal{F}$ 攻击成功。

3　基于求根问题的签名体制(REP-SS)

签名体制由系统初始化、密钥生成、签名及验

证 4 部分组成。

初始化 选择足够大的正整数 n 和 l，辫群 B_n 及奇素数 p。令

$$B_n(l)=\{b\in B_n \mid 0\le \inf(b)\le \sup(b)\le l\}$$

$$\mathrm{LB}_n(l)=\{b\in \mathrm{LB}_n \mid 0\le \inf(b)\le \sup(b)\le l\}$$

$$\mathrm{RB}_n(l)=\{b\in \mathrm{RB}_n \mid 0\le \inf(b)\le \sup(b)\le l\}$$

则 $|B_n(l)|\le l(n!)^l$，$B_n(l)$，$\mathrm{LB}_n(l)$ 和 $\mathrm{RB}_n(l)$ 都是有限集合[12]。$H:\{0,1\}^*\to\{1,\cdots,p-1\}$ 是抗碰撞的哈希函数。

密钥生成 用户随机选择 $x\in \mathrm{LB}_n(l)$ 作为私钥，计算 $y=x^p$ 作为公钥。

签名 给定消息 m，签名用户随机选择 $t\in \mathrm{RB}_n(l)$，计算 $T=t^p$，$c=H(m\,||\,T)$ 及 $s=tx^{-c}$，其中辫元 T 在作为哈希函数的输入时为二进制表示。则关于消息 m 的签名为 $\sigma=(c,s)$。

验证 给定消息 m 的签名 $\sigma=(c,s)$，验证者验证等式 $c=H(m||\,|\,s^py^c)$ 是否成立，若成立，接受签名；否则，拒绝签名。

4 签名体制分析

4.1 正确性

由 $x\in \mathrm{LB}_n$，$t\in \mathrm{RB}_n$ 知 $xt=tx$，则有 $s^py^c=(tx^{-c})^py^c=t^px^{-cp}y^c=t^py^{-c}y^c=T$，则 $c=H(m\,||\,T)=H(m\,||\,s^py^c)$。

4.2 不可伪造性

定理 在随机预言模型下，如果存在适应性选择消息攻击算法 $\mathcal{F}$ 能在多项式时间 t 内以不小于 $\varepsilon\ge 10(q_h+1)(q_h+q_s)/2^n$（$n$ 为辫指数)的概率成功伪造关于消息 m 的签名 σ，$m\notin\{m_i(i=1,\cdots,q_s)\}$，其中 q_h，q_s 分别为 $\mathcal{F}$ 向随机预言和签名预言提出询问的次数，$m_i(i=1,\cdots,q_s)$ 为 $\mathcal{F}$ 向签名预言提出的询问，则存在一个多项式时间算法 $\mathcal{A}$，能通过调用算法 $\mathcal{F}$ 在时间 t' 内以不小于 ε' 的概率解辫群上的求根问题，其中 $t'\le 120686q_ht/\varepsilon$，$\varepsilon'\ge 7q_h/2^n$。

证明 由签名过程可知，若给定有效签名 $\sigma=(c,s)$，可计算 $T=s^py^c=t^p$，t 随机选择于集合 $\mathrm{RB}_n(l)$，因此 T 也可视为集合 $\mathrm{RB}_n(l)$ 中的随机元素。c 是 $m\,||\,T$ 的哈希值，$s=tx^{-c}=T^{1/p}x^{-c}$ 由 T 和 c 决定。因此当辫指数 n 和 l 选择适当时，上述签名体制是一般签名体制。下面证明存在算法 $\mathcal{A}$，可以调用算法 $\mathcal{F}$ 解求根问题。

在求解过程中，$\mathcal{A}$ 必须对算法 $\mathcal{F}$ 可询问的随机预言和签名预言进行模拟，模拟过程中分别为各预言建立一个询问、回答相对应的关系列表 L_h 和 L_s。

对随机预言 H 的模拟：当 $\mathcal{F}$ 提出询问时，$\mathcal{A}$ 首先检查询问是否已经存在于列表 L_h 中，若是，则返回对应的值；否则，从 $\{1,\cdots,p-1\}$ 中随机选择一个值作为回答，并将该次询问及回答保存于关系列表 L_h 中。

对签名预言的模拟：当 $\mathcal{F}$ 向签名预言机询问关于消息 $m_i(1\le i\le q_s)$ 的签名时，$\mathcal{A}$ 按如下方式进行回答：

(1)随机选择 $c_i\in\{1,\cdots,p-1\}$；

(2)随机选择 $s_i\in B_n(l)$；

(3)计算 $T_i=s_i^py^{c_i}$，验证是否 $T_i\in \mathrm{RB}_n(l)$，若不是，返回至第(2)步；否则，继续下一步；

(4)检查 $m_i\,||\,T_i$ 是否已经存在于关系列表 L_h 中，若 $m_i\,||\,T_i$ 存在于 L_h 中，且对应回答为 c_i，则输出签名 $\sigma_i=(c_i,s_i)$；若 $m_i\,||\,T_i$ 存在于 L_h 中，而对应回答不为 c_i，返回至第(1)步；若 $m_i\,||\,T_i$ 不存在于 L_h 中，则将 c_i 作为与询问 $m_i\,||\,T_i$ 对应的回答保存到关系列表 L_h 中，并输出签名 $\sigma_i=(c_i,s_i)$。

由 Forking 引理可知，若 $\mathcal{F}$ 在时间 t 内以概率 $\varepsilon\ge 10(q_h+1)(q_h+q_s)/2^n$ 成功伪造出公钥为 y 的用户对消息 m 的签名 $\sigma=(c,s)$，则 $\mathcal{A}$ 可以在时间 $t'\le 120686q_ht/\varepsilon$ 内，以概率 $\varepsilon'\ge 7\varepsilon/10\ge 7q_h/2^n$ 得到两个有效的签名 $\sigma=(T,c,s)$ 和 $\sigma'=(T,c',s')$ 满足 $c\ne c'$，$s\ne s'$，$T=s^py^c$，$T=(s')^py^{c'}$，则有 $s^py^c=(s')^py^{c'}$。由 $T\in RB_n(l)$，$y=x^p\in LB_n(l)$ 知 $Ty=yT$，又由 $s=(Ty^{-c})^{1/p}$，$s'=(Ty^{-c'})^{1/p}$ 可得 $ss'=s's$。故有

$$s^{-p}(s')^p=(s^{-1}s')^p=y^cy^{-c'}=y^{c-c'}=x^{(c-c')p}$$

即有 $s^{-1}s'=x^{c-c'}$。

由 $c,c'\in\{1,\cdots,p-1\}$，$c\ne c'$ 可知 $0<|c-c'|<p$。p 是素数，则存在整数 a,b 满足 $a(c-c')+bp=1$。$\mathcal{A}$ 可以计算 $(s^{-1}s')^ay^b=(x)^{a(c-c')}x^{bp}=x^{a(c-c')+bp}=x$，即 $\mathcal{A}$ 求得了 y 的 p 次根。 证毕

4.3 参数选择

根据文献[9]，辫指数 n 应不小于 30，辫元正规长度不小于 15。若辫元表示成初等辫子及其逆的乘积，应保证初等辫子和逆的总数不小于 1000。素数 p 的大小可以权衡计算效率和安全性选择适当的值。

4.4 效率分析

本节分析签名体制 REP-SS 的效率，并将其与简单共轭签名体制 SCSS[12]、共轭签名体制 CSS[12] 及改进共轭签名体制 ECSS[13]相比较。

表 1 给出了 REP-SS，SCSS，CSS 和 ECSS 中签名及验证所需各种运算的次数。4 种签名体制每次签名都要用到签名密钥的逆，可进行预计算，因此表中的求逆运算不包括求签名密钥的逆。在 REP-SS 中，验证签名需判断两个整数是否相等，

表 1 3 种签名体制所需各种运算的次数

运算	REP-SS	SCSS	CSS	ECSS
乘法	$\leqslant 4p$	2	8	4
求逆	0	0	1	1
哈希	1	1	1	1
共轭判断	0	1	5	2

但这种运算与辫群上的运算相比可忽略不计，因此也不包含在表内。

根据文献[8,12]，当辫指数 n 和辫元正规长度给定时，辫群上各种运算的复杂性如表 2 所示。其中，在求逆运算中，l' 表示输入辫元的正规长度；在乘法和共轭判断运算中，l' 表示参与运算的两个辫元的正规长度的最大值。显然，共轭判断运算的复杂性大于乘法运算。因此，当辫指数 n 和正规长度 l' 相同时，只要 p 不过大，REP-SS 在计算上比 SCSS，CSS 和 ECSS 更有效。

表 2 辫群上各种运算的复杂性

运算	输入	输出	复杂性
乘法	辫元	辫元	$\mathcal{O}(l'n)$
求逆	辫元	辫元	$\mathcal{O}(l'n)$
共轭判断	辫元	是/否	$\mathcal{O}(l'n^3)$

下面比较各签名体制的签名长度。根据文献[8]，正规长度为 l' 的辫元可以用 $l'n\lg n$ 比特二进制数表示。当 $n=30$，$l'=15$ 时，$l'n\lg n>1800$。REP-SS 的签名中，整数 c 小于素数 p，当素数 p 较小时，与辫元长度相比 c 的长度可忽略不计。SCSS 和 ECSS 的签名为 1 个辫元，CSS 则为 3 个辫元。因此，REP-SS 的签名长度与 SCSS，ECSS 相当，约是 CSS 的 1/3。SCSS 存在同时共轭弱点，故 4 种签名体制中 REP-SS 具有最好的应用前景。

5　结束语

辫群作为构造密码协议的新平台，一经提出就成为研究热点。本文对辫群上的签名体制进行了研究，首次提出了基于求根问题难解性的签名体制。与几种共轭签名体制相比，新的签名体制在计算效率和签名长度上都有优势。基于该签名体制还可以构造各种特性数字签名体制。

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] Kitaev A. Quantum measurements and the abelian stabilizer problem. http://arxiv.org/quant-ph/9511026. 2008.8.

[3] Hashimoto Y and Sakurai K. On the construction of signature schemes based on birational permutations over noncommutative rings[EB/OL]. http://eprint.iacr.org/2008/340, 2008.10.

[4] Ogura N and Uchiyama S. Cryptanalysis of the birational permutation signature scheme over a noncommutative ring[EB/OL]. http://eprint.iacr.org/2009/066, 2009.8.

[5] Artin E. Theory of braids[J]. *Annals of Mathematics Studies*, 1947, 48(2): 101–126.

[6] Ko K H, Lee S J, and Cheon J H, *et al*.. New public key cryptosystem using braid groups[C]. Proceedings of Crypto-2000, Lecture Notes in Computer Science, Benlin: Springer-Verlag, 2000, 1880: 166–183.

[7] Anshel I, Anshel M, and Fisher B, *et al*.. New key agreement protocol in braid group cryptography[C]. Topics in Cryptology- CT- RSA 2001, Lectures Notes in Computer Science, Benlin: Springer Verlag, 2001, 2020: 1–15.

[8] Cha J C, Ko K H, and Lee S J, *et al*.. An efficient implementation of braid groups[C]. Advances in Cryptology: Proceedings of ASIACRYPT 2001, Lecture Notes in Computer Science, Benlin: Springer-Verlag, 2001, 2248: 144–156.

[9] Sibert H, Dehornoy P, and Girault M. Entity authentication schemes using braid word reduction[EB/OL]. http://eprint.iacr.org/ 2002/187, 2008.8.

[10] Lal S and Chaturvedi A. Authentication schemes using braid groups. http://arXiv.org/cs.CR/0507066. 2008.8.

[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.
Tang X M, Hong F, and Cui G H. A public key encryption algorithm on braid groups[J]. *Journal of Software*, 2007, 18(3): 722–729.

[12] Ko K H, Choi D H, and Cho M S, *et al*.. New signature scheme using conjugacy problem[EB/OL]. http://eprint.iacr.org/2002/168. 2008.8.

[13] 丁勇, 田海博, 王育民. 一种改进的基于辫群的签名体制[J]. 西安电子科技大学学报, 2006, 33(1): 50–52.
Ding Y, Tian H B, and Wang Y M. An improved signature scheme based on the braid group[J]. *Journal of Xidian University*, 2006, 33(1): 50–52.

[14] Thomas T and Lal A K. Group signature scheme using braid groups[EB/OL]. http://arXiv.org/cs.CR/0602063. 2008.8.

[15] Verma G K. Blind signature schemes over braid groups [EB/OL]. http://eprint.iacr.org/2008/027, 2008.10.

[16] Verma G K. A proxy signature scheme over braid groups [EB/OL]. http://eprint.iacr.org/2008/160, 2008.10.

[17] Zhang L L and Zeng J W. Proxy signature based on braid

group[J]. *Journal of Mathematical Study*, 2008, 41(1): 56–64.

[18] Manoj K. Linkability of blind signature schemes over braid groups[EB/OL]. http://eprint.iacr.org/2009/192, 2009.10.

[19] Lal S and Verma V. Some proxy signature and designated verifier signature schemes over braid groups[EB/OL]. http://arXiv.org/cs.CR/09043422. 2009.5.

[20] Manoj K. On the security of a proxy blind signature scheme over braid groups[EB/OL]. http://eprint.iacr.org/2009/361, 2009.10.

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

[22] Wei Y, Xiong G H, and Zhang X K, *et al.*. Security analysis and design of proxy signature schemes over braid groups [EB/OL]. http://eprint.iacr.org/2009/458, 2009.10.

[23] Wei Y, Xiong G H, and Bao W S, *et al.*. A strong blind signature scheme over braid groups[EB/OL]. http://eprint.iacr.org/2009/622, 2009.12.

[24] Myasnikov A and Ushakov A. Length based attack and braid groups: cryptanalysis of Anshel-Anshel-Goldfeld key(AAGK) exchange protocol[C]. Proceedings of PKC2007, Lecture Notes in Computer Science, Benlin: Springer-Verlag, 2007, 4450: 76–88.

[25] Kalka A G. Representation attacks on the braid Diffie-Hellman public key encryption[J]. *Applicalbe Algebra in Engineering, Communication and Computing* (*AAECC*), 2006, 17(3-4): 257–266.

[26] Pointcheval D and Stern J. Security arguments for digital signatures and blind signatures[J]. *Journal of Cryptology*, 2000, 13(3): 361–396.

隗 云： 女，1982 年生，博士生，研究方向为密码理论、数字签名.

熊国华： 男，1963 年生，高级工程师，博士后，博士生导师，研究方向为密码学与编码理论等.

鲍皖苏： 男，1966 年生，教授，博士生导师，研究方向为信息安全与密码理论等.