[文章编号] 1673 - 2944(2017)01 - 0071 - 05

基于对角自同构群的离散对数问题的盲签名方案

潘 平, 洪 歧
(陕西理工大学 数学与计算机科学学院, 陕西 汉中 723000)

[摘 要] 为了能够抵抗已知的量子算法攻击,非交换密码已成为后量子密码时代的研究方向之一。采用非交换群构造了一个签名方案,并在此基础上设计了一个盲签名方案。新方案的安全性依赖于单位三角矩阵群的对角自同构群上的离散对数问题。新的盲签名方案满足盲性和多一不可伪造性安全,并且只需要更短的公钥和更少的存储空间;采用平方-乘算法计算两个自同构的乘积,减少了计算成本。

[关 键 词] 非交换群; 对角自同构群; 离散对数; 盲签名
[中图分类号] TP309 [文献标识码] A

非交换密码(non-commutative cryptography)作为密码学研究领域的专业术语,首次出现于 2010 年"符号计算与密码"国际会议。2011 年,Myasnikov、Shpilrain 和 Ushakov 合著《非交换密码及群论问题复杂性》[1],从此,非交换密码开始登上了现代密码学的舞台。密码学原语的数学平台从"交换"到"非交换"的拓广并不是一个简单的概念类推,而是有着深刻的背景和丰富的内涵,可以说是后量子密码学的一个极其重要的研究方向之一。

盲签名是一类特殊的数字签名,除了满足数字签名的一般要求之外,还有自身的特点,即签名者不知道自己所签消息的具体内容。正是这一特点使得盲签名广泛应用于许多领域,比如电子支付、电子选举等。直观上讲,所谓盲签名,就是把需要隐藏的文件放进一个信封里,此时这个信封里的文件内容是任何人都不知道的。然后在信封里放一张复写纸,当签名者在信封上签名时,他的签名便透过复写纸签到了这个文件上。

一个好的盲签名应该具有以下性质:

(1) 盲性:签名者对所签消息的具体内容是不知道的。盲性也蕴含如下属性,对于脱盲后的签名,即便是签名者本人也不能联系是哪个用户在何时请求该签名的。

(2) 多一(One-More)不可伪造性:由于盲签名的脱盲操作从本质上赋予了普通用户"伪造"合法签名的能力,因此盲签名的不可伪造性的定义要略费周折。2000 年,Pointcheval 和 Stern [2] 给出了所谓的"多一"不可伪造性的概念:对某个整数 l(这里假定 l 为安全参数 k 的多项式),一个攻击者与签名者进行 l 次交互后获得 $l+1$ 个有效的签名是不可行的。

收稿日期:2016-09-20 修回日期:2016-11-22
基金项目:国家自然科学基金资助项目(61370194);陕西省教育厅自然科学研究基金资助项目(2013JK0598,16JK1163);陕西理工学院博士科研基金资助项目(SLGQD13-24)
作者简介:潘平(1975—),女,甘肃省天水市人,陕西理工大学讲师,博士,主要研究方向为信息安全、密码学;洪歧(1961—),男,浙江省东阳市人,陕西理工大学副教授,博士,主要研究方向为大数据处理、体视化技术。

自 1982 年 Chaum[3] 首次给出基于 RSA 的盲签名方案以来,人们基于交换群的密码难题假设提出了许多盲签名方案。然而,1994 年,Shor[4] 提出了高效求解大整数分解问题和交换群上的离散对数问题的量子算法,这些成果对现行的盲签名体制的安全性投下了阴影。近年来,运用非交换群(如辫群、特殊线性群、有限 p 群等)来构造公钥密码系统已引起人们的广泛关注,也相继出现了一些优秀的研究成果[5-15]。但是目前运用非交换群构造签名及盲签名方案的研究成果甚少。Paeng 等人[8] 用特殊线性群的内自同构群构造一个公钥加密系统,称为 MOR 密码系统。MOR 密码系统是 ElGamal 加密系统在非交换群上的推广。此后,研究者[15-16] 相继分析了基于矩阵群与循环群的半直积的内自同构群上的离散对数问题是亚指数时间复杂度。很自然地,希望非交换群的自同构群在公钥密码系统中能有更广泛的应用。文献[13]构造了基于非交换群的内自同构群的离散对数问题的盲签名方案,但已分析出其效率低。因此,通过选择适当的非交换群及其自同构,可以构造一个更安全高效的签名及盲签名方案。

本文首先在单位三角矩阵群的对角自同构群上的离散对数问题困难假设下提出了一个签名方案,最后对这些方案的安全性和效率进行了分析。本文工作是基于单位三角矩阵群的对角自同构群构造了一个签名方案,该方案类似于有限域交换群上的 DSA 算法,是 DSA 算法在非交换群上的推广。然后在这个签名方案的基础上,进行了盲化改造,给出了盲签名方案。新的签名和盲签名方案的安全性建立于单位三角矩阵群的对角自同构群的离散对数问题。

1 单位三角矩阵群及对角自同构

用于构造新方案的非交换群是特征为 p(p 为素数)的有限域 F_q 上的单位三角矩阵群。

定义 1[10] 设 F_q 为有限域,F_q 上的一个 $n\times n$ 的单位三角矩阵是主对角线左下方的元素全为零、主对角线的元素全为 1 的矩阵,形如

$$\begin{bmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix},$$

单位三角矩阵群是指 F_q 上的所有 $n\times n$ 的单位三角矩阵构成的集合,记作 UT(n,q)。

令 e_{ij} 表示第(i,j)上元素为 1、其余元素为 0 的矩阵(其中 $i<j$),那么 UT(n,q)中任意一个元素可表示为 $I+\sum_{i<j} a_{ij}e_{ij}$,$a_{ij}\in F_q$,$I$ 为 UT(n,q)的单位阵。

对任意 $I+ae_{ij}$,$I+be_{kj}\in$ UT(n,p),a,$b\in F_q$,有

$$(I+ae_{ij})(I+be_{ij}) = I+(a+b)e_{ij},$$

$$[I+ae_{ij},I+be_{ij}] = \begin{cases} I+abe_{il}, & j=k,i\neq l, \\ I-abe_{kj}, & i=l,j\neq k, \\ I, & \text{其他}, \end{cases}$$

这里 $[x,y]=x^{-1}y^{-1}xy$ 是元素 x,$y\in G$ 的交换子,G 是群。

UT(n,q)是一般线性群的 p 子群,其阶为 $q^{n(n-1)/2}$。UT(n,q)也是一个多重循环群。如果存在一个有限长的子群列 $G=G_0>G_1>G_2>\cdots>G_k>G_{k+1}=1$,其中 G_{i+1} 是 G_i 的正规子群且 G_{i+1}/G_i($i=1,2,\cdots,k$)是循环群,这样的群称为多重循环群。

定义 2[10] 设 $\boldsymbol{D}$ 是一个 n 阶对角矩阵,其定义为:主对角线元素均是有限域 F_q 上的非零元素,其余元素均为 0 的矩阵,形如

$$\begin{bmatrix} * & 0 & \cdots & 0 \\ 0 & * & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{bmatrix},$$

对角矩阵 $\boldsymbol{D}$ 可表示为 $[\omega_1,\omega_2,\cdots,\omega_n]$,非零元素 $\omega_i\in F_q$。

定义 3 [17]　群 G 的自同构是指群 G 到自身的同构,用 $\mathrm{Aut}(G)$ 表示群 G 的全体自同构组成的集合。对于映射的乘法,$\mathrm{Aut}(G)$ 组成一个群,叫做 G 的自同构群。

定义 4 [10]　$\mathrm{UT}(n,q)$ 上的对角自同构定义为

$$\Phi(a) = \boldsymbol{D}^{-1}a\boldsymbol{D},\quad a \in \mathrm{UT}(n,q),$$

即 $\Phi(a) = I + \sum_{i<j}(\omega_i^{-1}a_{ij}\omega_j)e_{ij}$,$a = I + \sum_{i<j}a_{ij}e_{ij}$。显然,$\Phi^m(a) = \boldsymbol{D}^{-m}a\boldsymbol{D}^m$,　$m \in N$。为了方便表述,$\Phi^m(a)$ 简记为 Φ^m。$\mathrm{UT}(n,q)$ 的全体对角自同构的集合是单位三角矩阵群的对角自同构群。

定义 5 [10]　对角自同构群的离散对数问题:设 G 是一个单位三角矩阵群,Φ 是 G 的对角自同构,给定 Φ 和 Φ^x,计算 $x \in F_q$。

2　盲签名方案

作为一个过渡,先构造基于对角自同构群的离散对数问题的签名方案,这个方案可以说是签名方案从交换群到非交换群的延伸。

系统参数:设 G 是群,Φ: $G \to G$ 是自同构。设 $\hbar$: $G \to F_q$ 和 h: $\{0,1\}^* \to F_q$ 均是抗碰撞哈希函数。

密钥生成:随机选择 $x \in F_q$,计算 $y = \Phi^x$。则私钥为 x,公钥为 y。

签名:待签名消息 m,签名者做如下的计算:

1) 选择 $k \in F_q$,计算 $v = \Phi^k$;

2) 计算 $s = k^{-1}(h(m) + rx)$,其中 $r = \hbar(v)$;

则消息 m 的签名 (r,s)。

验证:验证者接收到消息 m 的签名 (r,s) 后:

1) 计算 $u_1 = h(m)s^{-1}$ 和 $u_2 = rs^{-1}$;

2) 由 y 和 u_2 计算 y^{u_2};

3) 计算 $w = \Phi^{u_1}(y^{u_2})$;

验证等式 $w = v$ 是否成立。若成立,则接受 (m,r,s) 是一个有效的签名;否则拒绝接受签名。

在上述签名方案的基础上,非交换群上的盲签名方案描述如下:

系统参数:设 G 是群,Φ: $G \to G$ 是自同构。设 $\hbar$: $G \to F_q$ 和 h: $\{0,1\}^* \to F_q$ 均是抗碰撞哈希函数。

密钥生成:选择随机数 $x \in F_q$,计算 Φ^x,则私钥为 x,公钥为 Φ^x。

盲化:

1) 签名者选择随机数 $k \in F_q$,计算 Φ^k 及 $e = \hbar(\Phi^k)$,发送 (Φ^k,e) 给用户;

2) 用户选择随机数 $a,b \in F_q$,①计算 Φ^a,②由 Φ^k 计算 Φ^{bk},③由 Φ^a 和 Φ^{bk} 计算 Φ^{a+bk},④计算 $f = h(m,r)$,其中 $r = \hbar(\Phi^{a+bk})$;

3) 用户计算 $m' = fber^{-1}$,并发送 m' 给签名者。

签名:签名者接收到盲化消息 m' 后,计算 $s' = m'k - ex$,并发送 s' 给用户。

去盲:用户接收到 s' 后,计算 $s = s're^{-1} + af$,则消息 m 的签名为 (r,s)。

验证:验证者接收到消息 m 的签名 (r,s) 后,

1) 计算 Φ^s;

2) 由 Φ^x 计算 Φ^{xr};

3) 由 Φ^s 和 Φ^{xr} 计算 Φ^{s+xr};

4) 计算 $\Phi^{(s+xr)f^{-1}}$,其中 $f = h(m,r)$。

验证等式 $\Phi^{(s+xr)f^{-1}} = \Phi^{a+bk}$ 是否成立。若成立,则接受 (m,r,s) 是一个有效的签名;否则拒绝接受签名。

定理 1　任何人都可通过公开的签名 (m,r,s) 验证新的盲签名方案中签名的有效性。

证明　需要证明签名 (m,r,s) 满足验证等式 $\Phi^{(s+xr)f^{-1}} = \Phi^{a+bk}$ 成立。

首先签名参数 s:

$$s = s're^{-1} + af,$$

其中

$$s' = m'k - ex,$$
$$m' = fber^{-1},$$

则

$$s = (fber^{-1}k - ex)re^{-1} + af,$$

整理得到

$$(s + xr)f^{-1} = a + bk。$$

则上述方程两边都变成 Φ 的幂方:

$$\Phi^{(s+xr)f^{-1}} = \Phi^{a+bk},$$

即(m,r,s)是一个有效的签名。

3 安全性及效率分析

定理2 上述盲签名方案满足盲性。

证明: 要证明方案的盲性,即给定签名(r,s),存在唯一的盲因子 a 和 b。

假定消息 m 的签名为(r,s),在方案中签名者完全知道参数 k、Φ^k、e、m'、$s' = m'k - ex$,则对盲因子 a 和 b,下列等式必成立:

$$s = s're^{-1} + af, \quad (1)$$
$$m' = fber^{-1}, \quad (2)$$
$$\Phi^{a+bk} = \Phi^{(s+xr)f^{-1}}。 \quad (3)$$

已知盲化消息 m'、e、f 与 p 互素,由等式(1)和(2)可得唯一的 a 和 b:

$$a = (s - s're^{-1})f^{-1},$$
$$b = m'f^{-1}e^{-1}r,$$

从而验证了等式(1)—(3)均成立:

$$\Phi^{a+bk} = \Phi^{(s+xr)f^{-1}}。$$

上述盲签名方案在一般群模型下满足多一不可伪造性安全。该方案的证明思路类似于文献[18]的安全性证明。

上述新方案建立于单位三角矩阵群 $\mathrm{UT}(2,q)$,则 $g = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ 是 $\mathrm{UT}(2,q)$ 的生成元。由于自同构是对角自同构 Φ,则

$$\Phi(g) = \boldsymbol{D}^{-1}g\boldsymbol{D}, \quad g \in \mathrm{UT}(2,q),$$

那么

$$\Phi^x(g) = \boldsymbol{D}^{-x}g\boldsymbol{D}^x。$$

所以新方案的安全性依赖于单位三角矩阵群的对角自同构群上的离散对数问题。假如公开 Φ 和 Φ^x,攻击者要求 x,需先计算 $\boldsymbol{D}^x$,这是一个共轭搜索问题,在一般线性群上是不难的,但是 $\boldsymbol{D}$ 与 $\boldsymbol{D}^x$ 不唯一,$\boldsymbol{DZ}$ 与 $\boldsymbol{D}^x\boldsymbol{Z}$ 也是共轭问题的解,这里 Z 是 $\mathrm{UT}(2,q)$ 的中心。只要保证 $\mathrm{UT}(2,q)$ 的中心足够大,攻击者需要穷举才能找到中心 Z。

现在考虑新盲签名方案的参数大小。新方案中素数 q 为160比特。由于 $g \in \mathrm{UT}(2,q)$,$\Phi(g) \in \mathrm{UT}(2,q)$,那么只需要1个元素就可表示出 $\Phi(g)$,因此 g 和 $\Phi(g)$ 都只需要160比特。表1给出了新方案所需参数大小,同时,也列出了文献[13]中盲签名方案所需参数大小。通过比较,显然新盲签名方案在系统参数和公钥上仅需

表1 盲方案所需存储空间的大小比较

	文献[13]		新方案	
	参数	大小(bits)	参数	大小(bits)
系统参数	p,g	640	q,g	320
公钥	$Inn(g)$	960	$\Phi(g)$	160
私钥	x	160	x	160
签名	(r,s)	320	(r,s)	320
总计	–	2080	–	960

要更短的参数大小，私钥和签名两者保持相同的大小。

总而言之，本文盲签名方案总共需要 960 比特的存储空间，而文献［13］的方案需要 2080 比特，大约是新方案的 2 倍多。因此新盲签名方案更节省存储空间。根据文献［12］，采用平方-乘算法计算两个自同构的乘积，最坏情形下的复杂度为 $16p$ 域乘。显然，新方案所需计算成本优于文献［13］的方案。

4 结　论

在单位三角矩阵群的对角自同构群上的离散对数问题困难假设下，首先给出了一个非交换群的盲签名方案，新方案建立于非交换群的签名方案的基础之上。新的盲签名方案满足盲性和多一不可伪造性，通过比较，新方案既能节省了大量的存储空间，也减少了计算成本。如果考虑其他的非交换群（如循环矩阵群、幂零群等）或者自同构的复合运算（如对角自同构与置换自同构的复合、图自同构与域自同构的复合等），也许方案更安全，这将是以后需要进一步深入研究的工作。

［参　考　文　献］

［1］ MYASNIKOV A G，SHPILRAIN V，USHAKOV A. Non-commutative Cryptography and Complexity of Group-theoretic Problems［M］. Amer. Math. Soc. Surveys and Monographs，2011.

［2］ POINTCHEVAL D，STERN J. Security Argument for Digital Signatures and Blind Signatures［J］. Journal of Cryptology，Springer-Verlag，2000，13（3）：361-396.

［3］ CHAUM D. Blind Signatures for Untraceable Payments［C］. Crypto 1982，California，1983.

［4］ SHOR P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer［J］. SIAM Journal on Computing，1997，26：1484-1509.

［5］ KO K H，CHOI D H，CHO M S，et al. New signature scheme using conjugacy problem［EB/OL］. Cryptography ePrint Archive.［2016-08-20］. http：//eprint. iacr. org/2002/168，2002.

［6］ BAUMSLAG G，FAZIO N，NICOLOSI A R，et al. Generalized learning problems and applications to non-commutative cryptography［C］. In ProvSec'11，Springer，LNCS 6980，2011：324-339.

［7］ HASHIMOTO Y，SAKURAI K. On the construction of signature schemes based on birational permutations over noncommutative rings［EB/OL］.［2016-08-20］. http：//eprint. iacr. org/2008/340，2008.

［8］ PAENG S H，HA K C，KIM J H，et al. New public key cryptosystem using finite non-abelian groups［C］. CRYPTO2001，Berlin：Springer-Verlag，LNCS 2139，2001：470-485.

［9］ MAHALANOBIS A. A simple generalization of the ElGamal cryptosystem to non-abelian groups II［J］. Communications in Algebra，2012，40：3583-3596.

［10］ MAHALANOBIS A. The automorphism group of the group of unitriangular matrices over a field［J］. International Journal of Algebra，2013，7（15）：723-733.

［11］ MAHALANOBIS A. The MOR cryptosystem and extra-special p-groups［EB/OL］. Proceedings of WCC 2012，Castro Urdiales，Spain 9-13 July 2012.［2016-08-20］. http：//arxiv. org/abs.

［12］ MAHALANOBIS A. The MOR cryptosystem and finite p-groups［EB/OL］.［2016-08-20］. http：//arxiv. org/abs.

［13］ 潘平，王励成，杨义先. 内自同构群上的盲签名［J］. 北京邮电大学学报，2012，35（6）：20-23.

［14］ PAN Ping，WANG Li-cheng，YANG Yi-xian，et al. Chameleon Hash Functions and One-Time Signature Schemes from Inner Automorphism Groups［J］. Fundamenta Informaticae，2013，126（1）：103-119.

［15］ PAENG S H. On the security of cryptosystem using the automorphism groups［J］. Information Proceedings Letters，2003，88（6）：293-298.

［16］ TOBIAS C. Security analysis of the MOR cryptosystem［C］. PKC 2003，Berlin：Springer-Verlag，LNCS 2567，2003：175-186.

［17］ 徐明曜，曲海鹏. 有限 p 群［M］. 北京：北京大学出版社，2010.

［18］ BROWN R L. Generic group，Collision resistance，and ECDSA［J］. Designs，Codes and Cryptography，2005，35（1）：119-152.

［责任编辑：魏　强］

（下转第 92 页）

Research on the evaluation of traffic facilities in large parks based on AHP-FEC

LIU Xing, LUO Jia, LI Bang-lan, HE Lin, BAN Yue
(School of Traffic & Transportation, Chongqing Jiaotong University, Chongqing 400074, China)

Abstract: Large park is an important part of the modern city, and it plays a positive role in improving the image of the city and improving the quality of life of the people, but at present, many large park construction after the completion of its supporting traffic facilities is not perfect in that it's difficult to meet the travel needs of tourists. A case study of Central Park in Chongqing City has been conducted using level analysis method to construct the large park supporting transport facilities status evaluation index system. Based on fuzzy comprehensive evaluation method to establish the supporting transport facilities situation evaluation model, the paper discusses and analyses the present situation of supporting traffic facilities in Central Park of Chongqing City, and works out the existing problems, and finally proposes corresponding measures.

Key words: analytic hierarchy process; fuzzy comprehensive evaluation method; large parks; traffic facilities

---

(上接第 75 页)

Blind signature based on the discrete logarithm over diagonal automorphism group

PAN Ping, HONG Qi
(School of Mathematics and Computer Science, Shaanxi Sci-Tech University, Hanzhong 723000, China)

Abstract: In order to resist currently known quantum algorithm attacks, non-commutative cryptography has become one of research directions in post-quantum cryptography era. A signature scheme over non-commutative group is proposed. Based on the signature scheme, a blind signature scheme is presented. The security of the schemes relies on the discrete logarithm problem over the diagonal automorphism group of the group of unitriangular matrices. The new blind signature scheme satisfies blinding and one-more unforgery, and only requires shorter public keys and smaller storage space. Since the multiplication of two automorphisms is computed using the square and multiply algorithm, the computing cost is reduced.

Key words: non-commutative group; diagonal automorphism group; discrete logarithm; blind signature