软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2021,32(9):2935−2944 [doi: 10.13328/j.cnki.jos.006019]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

抗量子计算的多变量盲签名方案*

俞惠芳, 付帅凤

(西安邮电大学 网络空间安全学院,陕西 西安 710121)

通讯作者: 俞惠芳, E-mail: yuhuifang@xupt.edu.cn

摘 要: 盲签名是一种特殊的数字签名,可广泛应用于各种匿名场合.目前,大多数盲签名的安全性主要基于大整数分解问题或离散对数问题的难解性.然而,实用量子计算机的即将诞生会使得传统的盲签名不再安全,而且量子算法的出现对传统的盲签名亦提出了挑战.因此,构造能够防御量子计算攻击的盲签名方案具有重要的意义.多变量公钥密码是后量子密码的主要候选者之一.在多变量公钥密码和盲签名的理论基础上,设计了一种新颖的多变量公钥密码体制下的盲签名方案.该密码方案借助另一非线性可逆变换 $L:F^r\to F^r$ 将签名的公私钥分离,减少了公私钥之间的线性关系,提高了盲签名的安全性.分析表明:该密码方案不仅具有盲性、不可伪造性和不可追踪性,而且还具有计算复杂度低及抗量子计算攻击的优点.

关键词: 多变量;盲签名;非满射中心映射;后量子安全

中图法分类号: TP309

中文引用格式: 俞惠芳,付帅凤.抗量子计算的多变量盲签名方案.软件学报,2021,32(9):2935−2944. http://www.jos.org.cn/1000-9825/6019.htm

英文引用格式: Yu HF, Fu SF. Post-Quantum blind signature scheme based on multivariate cryptosystem. Ruan Jian Xue Bao/ Journal of Software, 2021,32(9):2935−2944 (in Chinese). http://www.jos.org.cn/1000-9825/6019.htm

Post-quantum Blind Signature Scheme Based on Multivariate Cryptosystem

YU Hui-Fang, FU Shuai-Feng

(School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an 710121, China)

Abstract: Blind signature is a special digital signature, which is widely used in various anonymity environments. At present, the security of most blind signature schemes is mainly based on the intractability of large integer factoring (LIF) or discrete logarithm (DL) problems. However, with the birth of practical quantum computers, the traditional public key cryptosystem will be unsecure; moreover, the quantum algorithms make it face severe challenges. Hence, it is of great value to construct blind signature schemes that can resist the quantum computing attacks. One of main candidates of post-quantum cryptosystems is multivariate public key cryptosystem (MPKC). On the basis of the theory of MPKC and blind signature, a post-quantum blind signature scheme is proposed based on MPKC. The proposed cryptographic scheme separates the public and private keys of the signature by using another nonlinear reversible transformation $L:F^r\to F^r$, which reduces the linear relationship between the public and private keys. Accordingly, it improves the security of the blind signature scheme. Analysis shows that this cryptographic scheme has the blindness, unforgeability, and untraceability; in addition, it has the merits of low computational complexity and resisting quantum computing attacks.

Key words: multivariate; blind signature; nonsurjective center mapping; post-quantum security

1983 年,Chaum[1]首次提出了盲签名的概念.盲签名是一种具有消息盲化特性的签名.假设消息拥有者想要签名者对待签消息进行签名,但是又不想让签名者知道待签消息的具体内容,即使以后签名者又见到了该消息

* 基金项目: 陕西省自然科学基金基础研究计划(2020JZ-54); 西安邮电大学研究生创新基金(CXJJLY2018076)

Foundation item: Key Program of Natural Science Basic Research Plan of Shaanxi Province (2020JZ-54); Innovation Foundation of Postgraduate of Xi'an University of Posts & Telecommunications (CXJJLY2018076)

收稿时间: 2019-04-14; 修改时间: 2019-11-20, 2020-01-03; 采用时间: 2020-02-06; jos 在线出版时间: 2021-04-20

签名,也不确定什么时候他签署了这个签名,这种情况下就可以用到盲签名.盲签名可以理解为将需要签名的文件放在装有复印纸的文件袋中,签名者看不到文件的具体内容,他只需要在文件袋上签名,这样签名可以通过复印纸印在文件上.盲签名主要用于电子现金支付、电子投票等需要匿名性和认证性的应用场合中[2−4].自 1983 年以后,盲签名引起了广泛的关注,学者们也提出了众多盲签名方案[5−7],但是目前大多数盲签名都是基于传统公钥密码体制的[8−10].传统公钥密码体制的安全性主要依赖于大整数分解问题或离散对数问题的难解性.随着量子计算[11]的发展,使得基于传统公钥密码体制的盲签名方案受到了严重威胁.为此,研究具有抗量子计算特性的盲签名方案具有重要的意义.多变量公钥密码作为后量子密码的主要候选者之一,其安全性基于有限域上二次多变量多项式方程组(multivariate quadratic,简称 MQ)问题和多项式同构(isomorphism of polynomials,简称 IP)问题的难解性,已有的量子算法目前还不能很好地解决 MQ 问题和 IP 问题.多变量公钥密码具有计算效率高、运算速度快等优点,非常适用于计算能力有限的设备.文献[12,13]提出了多变量环签名方案;文献[14]运用公平划分的思想,将文献[12]转化为多变量门限环签名方案;文献[15,16]提出了多变量代理签名方案;文献[17]提出了多变量群签名方案;文献[18]提出了多变量盲签名方案,但是该方案运用传统的多变量签名模型,为了产生一个有效的签名,采用了两个非满射中心映射,其只能应用在已知安全的多变量公钥密码体制下,而且安全性低、计算效率低;文献[19]提出了一个交互式的多变量盲签名方案,但是其公钥长度和签名长度较大.

2009 年,Wang 等人[20]提出了一种多变量签名模型改进的方案,本质上是增加一个秘密仿射变换 M 来分离签名私钥和验证公钥之间的线性关系.2012 年,Lu 等人[21]对 Wang 等人的方案进行了分析,指出:可以通过合法用户的 r+1 个已知签名建立线性方程组,使 Wang 等人的方案转化为一般的签名方案,进而说明增加秘密仿射变换 M 并不能提高原有签名方案的安全性.Lu 等人[22]提出使用非线性可逆变换 L 替代秘密仿射变换 M,减少签名私钥和验证公钥的线性关系,提高了签名方案的安全性.Yasuda 等人[23]提出利用非满射中心映射构造多变量公钥密码,具有隐藏代数矩阵和线性对等线性性质.

本文在盲签名和多变量公钥密码的理论基础上,借鉴文献[22]改进的多变量签名模型和文献[23]的非满射中心映射,提出一种多变量公钥密码体制下的后量子盲签名方案.由于所提方案只有一个非满射中心映射,为了使方案可以产生一个有效的签名,本文借鉴文献[24]对消息增加几个随机比特的思想.所提方案的公私钥之间没有线性关系,使得盲签名的安全性得到提高.经过安全性分析,证明了该密码方案满足盲性、不可伪造性和不可追踪性,而且计算效率高还能防御量子计算攻击.

1 预备知识

1.1 多变量公钥密码

多变量公钥密码的单向陷门函数形式是有限域 F 上的多变量二次多项式映射,公钥的一般形式如下:

$$P=(p_1(x_1,x_2,\ldots,x_n),\ldots,p_r(x_1,x_2,\ldots,x_n)).$$

每个方程 $p_i(i=1,2,\ldots,r)$是一个关于 $x=(x_1,x_2,\ldots,x_n)$的非线性二次方程:

$$p_i(x_1,x_2,...,x_n):=\sum_{1\leqslant j\leqslant k\leqslant n}\gamma_{ijk}x_jx_k+\sum_{j=1}^{n}\beta_{ij}x_j+\alpha_i,$$

其中,方程的系数$\gamma_{ijk},\beta_{ij},\alpha_i\in F(1\leqslant i\leqslant n,1\leqslant j\leqslant k\leqslant n)$,变量 $x_j,x_k\in F$.多变量公钥密码的安全性主要依赖于 MQ 问题和 IP 问题的难解性.

定义 1(MQ 问题). 给定有限域 F_q(q 为有限域 F 的阶)中的 r 个 n 元方程式的非线性方程组:

$$p_1(x_1,x_2,\ldots,x_n),p_2(x_1,x_2,\ldots,x_n)=\ldots=p_r(x_1,x_2,\ldots,x_n)=0.$$

求解该方程组的问题被称为 MQ 问题.已经证明 MQ 问题是非确定多项式(nondeterministic polynomials,简称 NP)困难问题,即使是在最小的有限域 F_2 上.

定义 2(IP 问题). 设 P 和 Q 是有限域 F_q 上随机选取的 r 个 n 元方程的多变量方程组,且 P 和 Q 同构,则有 $P=T\circ Q\circ S$,其中,T 和 S 分别为两个可逆仿射变换,则称寻找从 Q 到 P 同构的(T,S)问题为 IP 问题[16].

多变量公钥密码的签名和验证过程如下:

签名

$$v\in F^r \xrightarrow{T^{-1}} y\in F^r \xrightarrow{Q^{-1}} x\in F^n \xrightarrow{S^{-1}} \sigma\in F^n$$

$$v'\in F^r \xleftarrow{\qquad P=T\circ Q\circ S\qquad} \sigma\in F^n$$

验证

这里的 S 和 T 分别是 $F^n\to F^n$ 和 $F^r\to F^r$ 的两个可逆仿射变换,Q 是 $F^n\to F^r$ 的中心映射,公钥为 $P=T\circ Q\circ S$,私钥为$\{T,Q,S\}$.

签名:如果要对消息 m 进行签名,先计算消息 m 的哈希值 $v\in F^r$,然后依次计算 $y=T^{-1}(v)\in F^r$,$x=Q^{-1}(y)\in F^n$ 和 $\sigma=S^{-1}(x)\in F^n$,σ就是消息 m 的签名.

验证:如果要对签名σ进行验证,先利用公钥 $P=T\circ Q\circ S$ 计算 $v'=P(\sigma)$:如果 $v'=v$,则说明签名是有效的;否则,签名是无效的.

1.2 盲签名的形式化定义

1.2.1 算法定义

盲签名是一种具有消息盲化特性的签名,确保了签名者在不知道具体待签消息内容的情况下进行签名,即使签名者以后又见到了该消息签名,也不确定自己什么时候签署了这个签名.一个盲签名方案由以下几个算法组成.

- 系统初始化:输入安全参数λ,输出系统参数;
- 密钥生成:输入系统参数,输出签名者 B 的公私钥对;
- 盲签名:该算法由如下 3 个子算法组成.
  (1) 盲化:输入系统参数,消息拥有者 O 随机选取一个盲因子 e,对消息 m 进行盲化处理,将盲化后的消息发送给 B;
  (2) 签名:B 用私钥对盲化后的消息进行签名,得到盲签名σ';
  (3) 去盲化:O 用 B 的公钥和盲化后的消息对盲签名σ'进行验证:若成立,O 对盲签名σ'去盲化处理,输出最终的签名σ;否则,签名无效;
- 验证:输入系统参数、消息 m 和 B 的公钥对签名σ进行验证:如果签名有效,输出 1;否则,输出 0.

一般地,对于消息 m,如果签名者按照正确的步骤对消息 m 进行签名,而且在传播的过程中签名没有被篡改,那么签名σ可以通过验证.

1.2.2 安全模型

1. 盲性

定义 3. 签名者 B 对消息 m 进行签名,但是不知道消息 m 的具体内容.

对于盲性的安全模型,通过游戏 Game1 进行形式化定义.

Game1:敌手 A(模拟签名者 B)和挑战者 C 的盲签名交互过程如下所述.

(1) C 通过运行系统初始化算法生成系统参数,同时,通过运行密钥生成算法生成签名的公私钥对,然后将系统参数和私钥发送给 A;
(2) A 随机选取两个等长的不同的消息 m_0 和 m_1 发送给 C;
(3) C 随机选取两个等长的不同的盲因子 $e_c\in F$ 和 $e_{1-c}\in F$,然后随机选择 $c\in\{0,1\}$.最后运行盲签名中的盲化算法生成盲化消息 b_c 和 b_{1-c},并将 b_c 和 b_{1-c} 随机发送给 A;
(4) A 对 b_c 和 b_{1-c} 依次执行盲签名中的签名算法,得到盲签名 σ'_c 和 σ'_{1-c},并将 σ'_c 和 σ'_{1-c} 依次发送给 C;
(5) C 利用盲因子 e_c 和 e_{1-c} 对盲签名 σ'_c 和 σ'_{1-c} 去盲化处理,得到签名σ_c和σ_{1-c};然后,将σ_c和σ_{1-c}依次发送给 A;
(6) A 输出一个 c 的猜测值 $c'\in\{0,1\}$.

敌手 A 赢得挑战的优势为 $Adv_A^{Game1}=|\Pr(c=c')-1/2|$,其中,$\Pr(c=c')$是 $c=c'$的概率.若敌手 A 以不可忽略的优势猜测正确,则挑战成功.

2. 不可伪造性

定义 4. 对于任意的消息 m,敌手 A 通过盲签名交互过程,成功伪造一个有效的签名并能通过验证的概率是可以忽略的.

对于不可伪造性的安全模型,通过游戏 Game2 进行形式化定义.

Game2:敌手 A 和消息拥有者 O 的盲签名交互过程如下所述.

(1) O 通过运行系统初始化算法生成系统参数,同时,通过运行密钥生成算法生成签名的公私钥对,然后将系统参数和公钥发送给 A;

(2) O 访问随机预言机,A 通过公开的公钥猜测签名的私钥,与随机预言机分别进行 t 次盲签名交互过程,得到签名 δ_j 和 $\sigma_j(j=1,2,\ldots,t)$;

(3) 经过验证算法,签名 δ_j 和 σ_j 都验证成功.

如果敌手赢得游戏的事件用 Win 表示,则敌手 A 获胜的优势可定义为 $Adv_A^{Game2}=\Pr[Win]$.如果等式 $\delta_j=\sigma_j$ 成立的概率可以忽略,则敌手 A 赢得挑战的优势可以忽略,故而盲签名具有不可伪造性.

3. 不可追踪性

定义 5. 签名 σ 公布以后,即使留有当时的盲消息,签名者 B 也无法确定是他何时签署的.

对于不可追踪性的安全模型,通过下面 Game3 进行形式化定义.

Game3:挑战者 C(模拟签名者 B)和消息拥有者 O 的盲签名交互过程如下所述.

(1) O 通过运行系统初始化算法生成系统参数,同时,通过运行密钥生成算法生成签名的公私钥对,并将系统参数和私钥发送给 C;

(2) O 随机选取两个等长的不同的盲因子 e_θ 和 $e_{1-\theta}$,然后选择一个随机的比特 $\theta\in\{0,1\}$,将消息 m 作为输入,执行盲签名中的盲化算法,生成盲化消息 b_θ 和 $b_{1-\theta}$,并将 b_θ 和 $b_{1-\theta}$ 随机发送给 C;

(3) C 对 b_θ 和 $b_{1-\theta}$ 依次执行盲签名中的签名算法,生成盲签名 σ'_θ 和 $\sigma'_{1-\theta}$,然后将 σ'_θ 和 $\sigma'_{1-\theta}$ 依次发送给 O;

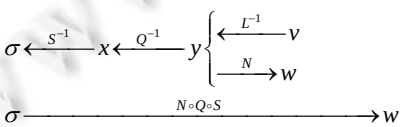
(4) O 利用盲因子 e_θ 和 $e_{1-\theta}$ 对盲签名 σ'_θ 和 $\sigma'_{1-\theta}$ 去盲化处理,得到签名 σ_θ 和 $\sigma_{1-\theta}$,然后,将 σ_θ 和 $\sigma_{1-\theta}$ 依次发送给 C;

(5) C 输出一个 θ 的猜测值 $\theta'\in\{0,1\}$.

挑战者 C 赢得挑战的优势为 $Adv_C^{Game3}=|\Pr(\theta=\theta')-1/2|$,其中,$\Pr(\theta=\theta')$是 $\theta=\theta'$ 的概率.若挑战者 C 以不可忽略的优势猜对,则挑战成功.

1.3 Lu等人改进的多变量签名模型

Lu 等人[22]改进了 Wang 等人[20]的签名模型,即把文献[20]中的秘密仿射变换 M 改为非线性可逆变换 L,其结构如下.



私钥:L,S 和 Q 中的某些参数.

公钥:$h\circ L^{-1},h\circ N^{-1}$ 和 $N\circ Q\circ S$,其中,$N(N\neq E,N\neq L)$是一秘密仿射变换,E 表示恒等变换,h 是一个保密的单向不可逆哈希函数.

签名:设 v 是消息 m 的哈希值,依次计算 $y=L^{-1}(v),x=Q^{-1}(y)$ 和 $\sigma=S^{-1}(x)$,σ 即为签名.

验证:输入公钥 $P=N\circ Q\circ S$ 和签名 σ,输出 $w=N\circ Q\circ S(\sigma)$,验证 $h\circ L^{-1}(v)=h\circ N^{-1}(w)$是否成立:若成立,则接受签名;否则,拒绝签名.

1.4 Yasuda等人提出的非满射中心映射

设 r 是多变量方程组的个数,n 是变量的个数.这里的 r 和 n 均为有限的正整数,并且满足 $n=z^2$,$r=z(z+1)/2$. Yasuda 等人[23]利用非满射来构造多变量的中心映射,具体结构如下:

$$f_{\tilde{\delta},\tilde{B}}(\boldsymbol{X})=\boldsymbol{X}\tilde{\boldsymbol{B}}\boldsymbol{A}_{\tilde{\delta}}\tilde{\boldsymbol{B}}^T\boldsymbol{X}^T,$$

其中,$f_{\tilde{\delta},\tilde{B}}(\boldsymbol{X}):F^n\to F^r$ 为多变量的非满射中心映射,$\boldsymbol{X}$ 是一个 $z\times z$ 的矩阵变量,$\tilde{\boldsymbol{B}}$ 是一个 $z\times z$ 的正规矩阵,$\boldsymbol{A}_{\tilde{\delta}}$ 是一个 $z\times z$ 的对称矩阵,上标 T 表示矩阵的转置.

2 方案实例

本节给出了一个具体的抗量子计算的多变量盲签名方案.详细算法细节如下所述.

1. 系统初始化(Setup)

生成系统参数(F,p,l,r,n,H),其中,$F=GF(p^l)$是特征为 p 的有限域,r 是多变量方程组的个数,n 是变量的个数,哈希函数 $H:\{0,1\}^*\to F^r$.这里的 p 是素数,l,r 和 n 均为有限的正整数.

2. 密钥生成(KeyGen)

生成签名者 B 的私钥 $sk:\{L^{-1},G^{-1},S^{-1}\}$和公钥 $pk:\{N\circ G\circ S,h\circ L^{-1},h\circ N^{-1}\}$,公开公钥,其中,$G:F^n\to F^r$ 是非满射中心映射,具体结构参照本文第 1.4 节和文献[23]中的 $f_{\tilde{\delta},\tilde{B}}$.$L:F^r\to F^r$ 是随机选取的非线性可逆变换,N 和 S 分别是 $F^r\to F^r$,$F^n\to F^n$ 随机选取的可逆仿射变换,h 是一个保密的单向不可逆哈希函数.

3. 盲签名(BlindSIG)

(1) 对消息 m 增加几个随机比特 m'[24];

下面介绍如何给消息 m 增加几个随机比特 m':

a) 计算 $W=H(H(m)\oplus\tilde{S})$,其中,$\tilde{S}$ 为 r-bit 字符串,值为 00…00;

b) 令 $m'=[W]_{0\to 2}$ 为 2-bit 字符串.

(2) 盲化(Blind):O 随机选取盲因子 $e\in F$,计算 $b=eH(m\|m')$,将盲化后的消息 b 发送给 B;

(3) 签名(Sign):B 收到 b 后,用私钥 $sk:\{L^{-1},G^{-1},S^{-1}\}$依次计算 $y=L^{-1}(b)$,$x=G^{-1}(y)$,若 y 没有与之对应的原像 x,则返回步骤(1),并用 $H(W)$替换步骤 a)中的 W;否则继续计算$\sigma'=S^{-1}(x)$,然后将盲签名σ'发送给 O;

现在说明一下签名失败的概率:根据文献[24]的证明,对消息 m 增加几个随机比特 m',在签名过程中,y 没有与之对应的原像 x 的概率约为 2^{-85},即签名失败的概率约为 2^{-85}.这个概率是可以完全忽略不计的,因此对签名过程的效率影响可以忽略不计.

(4) 去盲化(MoveBlind):O 收到 B 的盲签名σ'后,先验证 $h\circ N^{-1}(N\circ G\circ S(\sigma'))=h\circ L^{-1}(b)$是否成立:若成立,$O$ 对盲签名σ'去盲化处理,计算$\sigma=\sigma'/e^2$,得到签名σ;否则,签名无效.

4. 验证(Verify)

输入系统参数、消息 $m\|m'$和 B 的公钥,验证者计算 $h\circ L^{-1}(H(m\|m'))$,并用公钥 $N\circ G\circ S$ 和 $h\circ N^{-1}$ 验证等式 $h\circ L^{-1}(H(m\|m'))=h\circ N^{-1}(N\circ G\circ S(\sigma))$是否成立:若等式成立,则签名有效;否则,签名无效.

3 正确性分析

根据第 1.2.1 节中盲签名的定义,只有合法的盲签名才能通过验证.在证明本文方案满足正确性之前,先介绍用到的相关性质.

性质 1[23]. 若一有限域 F,V 是有限域 F 上的 n 维向量空间.当映射$\varphi:V\to F$ 具有二次形式时,有:

$$\varphi(ax)=a^2\varphi(x),$$

其中,$a\in F,x\in V$.

定理 1. 本文提出的抗量子计算的多变量盲签名方案是正确的.

证明:对消息 m 增加几个随机比特 m',假设对 $m\|m'$进行盲签名交互过程,可以产生一个有效的签名.若接收

方收到消息 $m||m'$的签名σ是按上述签名步骤进行的,并且在传播过程中没有被篡改,则:

$$h\circ N^{-1}(N\circ G\circ S(\sigma))=h\circ N^{-1}(N\circ G\circ S(\sigma'/e^2))=h\circ N^{-1}(N\circ G\circ S(sk(eH(m||m'))/e^2)).$$

根据性质 1 可得:

$$sk(eH(m||m'))=e^2sk(H(m||m')).$$

所以,

$$h\circ N^{-1}(N\circ G\circ S(\sigma))=h\circ N^{-1}(N\circ G\circ S(sk(H(m||m'))))=h\circ L^{-1}(H(m||m')).$$

可见,验证等式 $h\circ L^{-1}(H(m||m'))=h\circ N^{-1}(N\circ G\circ S(\sigma))$成立.这说明所构造的抗量子计算的多变量盲签名方案是正确的.证毕. □

4 安全性分析

4.1 盲 性

定理 2. 本文提出的抗量子计算的多变量盲签名方案满足盲性.

证明:利用第 1.2.2 节中的 Game1 安全模型证明所提方案满足盲性.假设敌手 A 伪装成签名者 B 与挑战者 C 进行盲签名交互过程.

(1) C 通过运行系统初始化算法生成系统参数(F,p,l,r,n,H),同时,通过运行密钥生成算法生成签名的公私钥对,并将系统参数和私钥发送给 A;

(2) 对消息 m 增加几个随机比特 m',假设对 $m||m'$进行盲签名交互过程,可以产生一个有效的签名;

(3) A 随机选取两个等长的不同的消息 $m_0\,\|\,m_0'$ 和 $m_1\,\|\,m_1'$ 发送给 C;

(4) C 随机选取两个等长的不同的盲因子 $e_c\in F$ 和 $e_{1-c}\in F$,然后再选择一个随机的比特 $c\in\{0,1\}$,接着计算 $b_c=e_cH(m_c\,\|\,m_c')$ 和 $b_{1-c}=e_{1-c}H(m_{1-c}\,\|\,m_{1-c}')$,并将 b_c 和 b_{1-c} 以随机顺序发送给 A;

(5) A 先后分别依次计算:

$$y_c=L^{-1}(b_c),x_c=G^{-1}(y_c),\sigma_c'=S^{-1}(x_c),y_{1-c}=L^{-1}(b_{1-c}),x_{1-c}=G^{-1}(y_{1-c}),\sigma_{1-c}'=S^{-1}(x_{1-c}).$$

然后,将盲签名 σ_c' 和 σ_{1-c}' 先后发送给 C;

(6) C 利用盲因子 e_c 和 e_{1-c} 去计算 $\sigma_c=\sigma_c'/e_c^2$ 和 $\sigma_{1-c}=\sigma_{1-c}'/e_{1-c}^2$,然后将签名$\sigma_c$和$\sigma_{1-c}$先后发送给 A;

(7) A 输出一个 c 的猜测值 $c'\in\{0,1\}$.

现在分析敌手 A 猜对 c 的概率.因为盲因子 e_c 和 e_{1-c} 是在有限域 F 上随机选取的,并且选取的过程完全独立于消息 $m_c\,\|\,m_c'$ 和 $m_{1-c}\,\|\,m_{1-c}'$,因此经过盲签名交互过程后,盲因子 e_c 和 e_{1-c}、消息 $m_c\,\|\,m_c'$ 和 $m_{1-c}\,\|\,m_{1-c}'$、签名 σ_c 和σ_{1-c}这三者完全相互独立.对于敌手 A,$c\in\{0,1\}$是随机选取的,即使一个攻击者拥有无限的计算能力,c 也在计算上具有不可区分性,敌手 A 猜对 c 的概率只有 1/2,即 $\Pr(c=c')=1/2$,则敌手 A 赢得挑战的优势为

$$Adv_A^{Game1}=|\Pr(c=c')-1/2|=0.$$

可见,敌手 A 无法以不可忽略的优势赢得挑战.从而证明了所构造的抗量子计算的多变量盲签名方案满足盲性.证毕. □

4.2 不可伪造性

定理 3. 如果 IP 问题在有限域 F 上是困难的,那么本文提出的抗量子计算的多变量盲签名方案满足不可伪造性.

- 证法 1

证明:利用第 1.2.2 节中的 Game2 安全模型,采用反证法证明所提方案满足不可伪造性.对于一个消息 m,先对消息 m 增加几个随机比特 m',假设对 $m||m'$进行盲签名交互过程,可以产生一个有效的签名.以一次盲签名交互过程为例,假设敌手 A 成功地伪造了一个有效的盲签名δ,同时,随机预言机产生了一个真实的盲签名σ',并且经过消息拥有者 O 去盲化后,得到的签名δ和σ都能够通过验证.

(1) 若$\delta=\sigma$,根据去盲化过程,有:

$$\delta/e^2=\sigma'/e^2.$$

根据签名过程,有:

$$\delta=sk(eH(m||m'))'=e^2sk(H(m||m'))',\sigma'=sk(eH(m||m'))=e^2sk(H(m||m')),$$

则:

$$e^2sk(H(m||m'))'/e^2=e^2sk(H(m||m'))/e^2,sk(H(m||m'))'=sk(H(m||m')).$$

若想要上式成立,那么敌手 A 必须得到签名者 B 的私钥$\{L^{-1},G^{-1},S^{-1}\}$.由于 h 是一个保密的单向不可逆哈希函数,所以通过 $h\circ L^{-1}$ 和 $h\circ N^{-1}$ 求得 L^{-1} 和 N^{-1} 是不可行的,由 $N\circ G\circ S$ 得到 N^{-1},G^{-1},S^{-1} 是不可行的,这相当于解决 IP 困难问题.

(2) 若$\delta\neq\sigma$,根据去盲化过程,有:

$$\delta/e^2\neq\sigma'/e^2.$$

根据签名过程,有:

$$e^2sk(H(m||m'))'/e^2\neq e^2sk(H(m||m'))/e^2,sk(H(m||m'))'\neq sk(H(m||m')).$$

通过上式可知,敌手 A 不可能伪造一个有效的签名.

综上所述,经过 t 次盲签名交互过程,所得到的有效签名δ_j和σ_j都通过验证,若想要签名$\delta_j=\sigma_j(j=1,2,\ldots,t)$,则必须得到签名者 B 的私钥$\{L^{-1},G^{-1},S^{-1}\}$.由公钥 $N\circ G\circ S,h\circ L^{-1}$ 和 $h\circ L^{-1}$ 得到私钥$\{L^{-1},G^{-1},S^{-1}\}$,这相当于解决 IP 问题.因此,敌手 A 无法以不可忽略的优势赢得挑战,假设不成立.从而证明了若 IP 问题在有限域 F 上是困难的,则所构造的抗量子计算的多变量盲签名方案满足不可伪造性.证毕. □

- 证法 2

证明:对于一个消息 m,先对消息 m 增加几个随机比特 m',假设对 $m||m'$进行盲签名交互过程,可以产生一个有效的签名.分别用列表 L_H,L_S 和 L_V 记录 H 询问、签名询问和验证询问,所用列表初始均为空.最多可以执行 q_{L_H} 次 H 询问、 q_{L_S} 次签名询问和 q_{L_V} 次验证询问.假设敌手 A 以不可忽略的优势ε成功伪造签名,则存在挑战者 C 以不可忽略的优势ε'解决 IP 问题.

挑战者 C 运行系统初始化算法和密钥生成算法,将系统参数(F,p,l,r,n,H)和公钥发送给敌手 A.

(1) H 询问:当 A 向 C 请求关于 $m||m'$的 H 询问时,首先,C 查询列表 L_H:若 L_H 中存在相应的记录$(m||m',H)$,则 C 直接返回结果 H 给 A;否则,C 随机选取 $H\in F^r$ 发送给 A,同时将$(m||m',H)$添加到列表 L_H 中;

(2) 签名询问:当 A 向 C 请求关于 $m||m'$的签名询问时,首先,C 查询签名列表 L_S:若 L_S 中存在相应的记录,则返回签名σ;否则,调用 H 询问(若在此询问之前,表中已经存在此询问记录,则伪造签名失败),再执行盲签名算法得到签名σ,然后将此记录添加到签名列表 L_S 中;

(3) 验证询问:当 A 向 C 请求关于 $m||m'$的验证询问时,首先,C 查询验证列表 L_V:若 L_V 中存在相应的记录,则返回消息 $m||m'$;否则,执行验证算法得到 $m||m'$.再对 L_H 进行查找:若存在相应的记录,则返回 $m||m'$;否则,拒绝这个签名.

经过多次盲签名交互过程后,A 提交一个伪造的签名σ^*.

通过上面的询问,如果敌手 A 想要伪造一个有效的签名σ^*,他必须得到签名者 B 的私钥$\{L^{-1},G^{-1},S^{-1}\}$.由$N\circ G\circ S,h\circ L^{-1}$ 和 $h\circ N^{-1}$ 得到私钥$\{L^{-1},G^{-1},S^{-1}\}$,这相当于解决 IP 问题.

我们用 E_1 和 E_2 表示敌手 A 伪造签名失败的事件.

1) E_1:当在步骤(2)签名询问时,重新调用的 H 询问已经在步骤(1)中所记录,则伪造签名失败.这个优势为:

$$\Pr[E_1]\leqslant(q_{Ls}+q_{L_H})2^{-r};$$

2) E_2:当在步骤(3)验证询问时,拒绝了一个有效的签名.这个优势为 $\Pr[E_2]\leqslant q_{L_V}2^{-r}$.

另外, $\Pr[E_3]\leqslant q_{L_s}^{-1}$ 表示在步骤(3)签名询问阶段得到了一个有效签名的优势.$\Pr(E_4)=\varepsilon$表示敌手 A 成功伪造签名的优势.

因此,挑战者 C 解决 IP 问题的优势是$\varepsilon'=\Pr[E_1\wedge E_2\wedge E_3\wedge E_4]$.又因为各事件之间是相互独立的,所以挑战者 C 解决 IP 问题的优势为

$$\varepsilon'=\Pr[E_1\wedge E_2\wedge E_3\wedge E_4]=\Pr[E_1]\cdot\Pr[E_2]\cdot\Pr[E_3]\cdot\Pr[E_4]\geqslant\frac{\varepsilon}{q_{L_S}}\left(1-\frac{q_{L_S}+q_{L_H}}{2^r}\right)\left(1-\frac{q_{L_V}}{2^r}\right).$$

可见,挑战者 C 无法以不可忽略的优势ε'解决 IP 问题.从而证明了如果 IP 问题在有限域 F 上是困难的,那么所构造的抗量子计算的多变量盲签名方案满足不可伪造性.证毕. □

4.3 不可追踪性

定理 4. 本文提出的抗量子计算的多变量盲签名方案满足不可追踪性.

证明:利用第 1.2.2 节中的 Game3 安全模型证明所提方案满足不可追踪行性.下面介绍挑战者 C(模拟签名者 B)和消息拥有者 O 的盲签名交互过程.

(1) O 通过运行系统初始化算法生成系统参数(F,p,l,r,n,H),同时,通过运行密钥生成算法生成签名的公私钥对,并将系统参数和私钥发送给 C;

(2) 对消息 m 增加几个随机的比特 m',假设对 $m||m'$进行盲签名交互过程可以产生一个有效的签名;

(3) O 随机选取两个等长的不同的盲因子 $e_0\in F$ 和 $e_1\in F$;

(4) O 选择一个随机的比特值$\theta\in\{0,1\}$,然后计算 $b_\theta=e_\theta H(m||m')$和 $b_{1-\theta}=e_{1-\theta}H(m||m')$,然后将 b_θ和 $b_{1-\theta}$以随机顺序发送给 C;

(5) C 先后分别依次计算:

$$y_\theta=L^{-1}(b_\theta),x_\theta=G^{-1}(y_\theta),\sigma'_\theta=S^{-1}(x_\theta),y_{1-\theta}=L^{-1}(b_{1-\theta}),x_{1-\theta}=G^{-1}(y_{1-\theta}),\sigma'_{1-\theta}=S^{-1}(x_{1-\theta}),$$

然后,先后发送盲签名 σ'_θ 和 $\sigma'_{1-\theta}$ 给 O;

(6) O 利用盲因子 e_θ和 $e_{1-\theta}$计算签名 $\sigma_\theta=\sigma'_\theta/e_\theta^2$ 和 $\sigma_{1-\theta}=\sigma'_{1-\theta}/e_{1-\theta}^2$,并将$\sigma_\theta$和$\sigma_{1-\theta}$先后发送给 C;

(7) C 输出一个θ的猜测值$\theta'\in\{0,1\}$.

现在分析挑战者 C 猜对θ的概率.因为盲因子 e_θ和 $e_{1-\theta}$是消息拥有者 O 在有限域 F 上随机选取的,而且选取的过程完全独立于消息 $m||m'$,因此盲因子 e_θ和 $e_{1-\theta}$、消息 $m||m'$、签名σ_θ和$\sigma_{1-\theta}$这三者之间完全相互独立.对于挑战者 C,在不知道盲因子的条件下,无法将消息、盲签名、签名这三者联系起来.因此,即使 C 拥有无限的计算能力,他猜对θ的概率只有 1/2,即 $\Pr(\theta=\theta')=1/2$,则挑战者 C 赢得挑战的优势是:

$$Adv_C^{Game3}=|\Pr(\theta=\theta')-1/2|=0.$$

可见,挑战者 C 无法以不可忽略的优势赢得挑战.从而证明了所构造的抗量子计算的多变量盲签名方案满足不可追踪性.证毕. □

5 效率分析

签名效率主要取决于签名的公钥长度、私钥长度和签名长度.本节依据这 3 个要素分析本文构造的抗量子计算的多变量盲签名方案与类似方案的性能.由文献[24]和 L,N 的构造过程可知,对消息 m 增加几个随机的比特 m'和增加公钥 $h\circ N^{-1},h\circ L^{-1}$ 并不影响整个盲签名交互过程的运算效率.表 1 从签名的公钥长度、私钥长度和签名长度分析文献[18,19]和本文方案的效率.

表 1 中的 r 为多变量方程组的个数,n 为变量的个数.从表 1 可看出:由于本文方案只采用一个非满射中心映射,所以和文献[18]相比,签名的私钥长度减少了 50%;与文献[19]相比,公钥长度和签名长度都有所减少.

Table 1 Comparison of efficiency

表 1 效率比较

方案	公钥长度	私钥长度	签名长度
方案[18]	$r(n+1)(n+2)/2$bit	$2(r(r+1)+n(n+1))$bit	$n$bit
方案[19]	$r(n+1)(n+2)/2+r(r^2+3r+2)/2$bit	$r(r+1)+n(n+1)$bit	$n+r$bit
本文方案	$r(n+1)(n+2)/2$bit	$r(r+1)+n(n+1)$bit	$n$bit

6 结束语

目前,大多数盲签名方案都是基于传统公钥密码体制的.随着量子计算技术的发展,使得传统公钥密码体制下的盲签名受到了严重威胁.本文提出了一种基于多变量的抗量子计算盲签名方案.所提方案运用改进的多变量签名模型,采用一个非满射中心映射,将签名的公私钥分离,减少了公私钥之间的线性关系,提高了盲签名的安全性.和文献[18,19]中的方案相比,计算效率较高.通过安全性分析知,方案具有盲性、不可伪造性和不可追踪性.本文方案可应用在电子现金交易系统、匿名电子投票系统等领域.

References:

[1] Chaum D. Blind signatures for untraceable payments. In: Chaum D, ed. Proc. of the Advances in Cryptology. Boston: Springer-Verlag, 1983. 199−203. [doi: 10.1007/978-1-4757-0602-4_18]

[2] Kumar M, Katti CP, Saxena PC. An untraceable identity-based blind signature scheme without pairing for e-cash payment system. In: Kumar N, ed. Proc. of the Ubiquitous Communications and Network Computing. Cham: Springer-Verlag, 2017. 67−78. [doi: 10.1007/978-3-319-73423-1_7]

[3] Shao AX, Zhang JZ, Xie SC. An e-payment protocol based on quantum multi-proxy blind signature. Int'l Journal of Theoretical Physics, 2017,56(4):1241−1248. [doi: 10.1007/s10773-016-3266-6]

[4] Guo X, Zhang JZ, Xie SC. A trusted third-party e-payment protocol based on quantum blind signature without entanglement. Int'l Journal of Theoretical Physics, 2018,57(9):2657−2664. [doi: 10.1007/s10773-018-3787-2]

[5] Bellare M, Namprempre C, Pointcheval D, Semanko M. The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. Journal of Cryptology, 2003,16(3):185−215. [doi: 10.1007/s00145-002-0120-1]

[6] Sun HM, Hsieh BT, Tseng SM. On the security of some proxy blind signature schemes. Journal of Systems and Software, 2005, 74(3):297−302. [doi: 10.1016/j.jss.2004.02.015]

[7] Fan CI, Chen WK, Yeh YS. Randomization enhanced Chaum's blind signature scheme. Computer Communications, 2000,23(17): 1677−1680. [doi: 10.1016/s0140-3664(00)00254-1]

[8] Nayak SK, Mohanty S, Majhi B. CLB-ECC: Certificateless blind signature using ECC. Journal of Information Processing Systems, 2017,13(4):970−986. [doi: 10.3745/JIPS.03.0029]

[9] Tian JH, Zhang JZ, Li YP. A quantum multi-proxy blind signature scheme based on genuine four-qubit entangled state. Int'l Journal of Theoretical Physics, 2016,55(2):809−816. [doi: 10.1007/s10773-015-2719-7]

[10] Islam SKH, Amin R, Biswas GP, Obaidat MS. Provably secure pairing-free identity-based partially blind signature scheme and its application in online e-cash system. Arabian Journal for Science and Engineering, 2016,41(8):3163−3176. [doi: 10.1007/s13369-016-2115-5]

[11] Shor PW. Algorithms for quantum computation: Discrete logarithms and factoring. In: Shor PW, ed. Proc. of the 35th Annual Symp. on Foundations of Computer Science. Santa Fe: IEEE, 1994. 124−134. [doi: 10.1109/SFCS.1994.365700]

[12] Wang SP, Ma R, Zhang YL, Wang XF. Ring signature scheme based on multivariate public key cryptosystems. Computers and Mathematics with Applications, 2011,62(10):3973−3979. [doi: 10.1016/j.camwa.2011.09.052]

[13] Liu XQ, Zhao YM. Variant scheme of ring signature based on multivariate public key cryptosystems. Computer Engineering, 2015, 41(2):96−99 (in Chinese with English abstract). [doi: 10.3969/j.issn.1000-3428]

[14] Guo QL, Xiang H, Cai B, Sang J, Xiang T. Threshold ring signature scheme based on multivariate public key cryptosystems. Journal of Cryptologic Research, 2018,5(2):140−150 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000226]

[15] Tang SH, Xu LL. Proxy signature scheme based on isomorphisms of polynomials. In: Bertino E, ed. Proc. of the Network and System Security. Heidelberg: Springer, 2012. 113−125. [doi: 10.1007/978-3-642-34601-9_9]

[16] Sun CY, Li YF, Zhang WZ, Si XM. A new proxy signature scheme based on multivariate cryptosystem. Journal of Sichuan University (Natural Science Edition), 2012,49(3):565−569 (in Chinese with English abstract). [doi: 10.3969/j.issn.0490-6756.2012.03.016]

[17] Yang GD, Tang SH, Yang L. A novel group signature scheme based on MPKC. In: Bao F, ed. Proc. of the Information Security Practice and Experience. Heidelberg: Springer-Verlag, 2011. 181−195. [doi: 10.1007/978-3-642-21031-0_14]

[18] Liu XQ. The research of blind signature and ring signature based on multivariate public key cryptosystems [MS. Thesis]. Shanghai: Fudan University, 2014 (in Chinese with English abstract).

[19] Petzoldt A, Szepieniec A, Mohamed MSE. A practical multivariate blind signature scheme. In: Kiayias A, ed. Proc. of the Financial Cryptography and Data Security. Malta: Springer-Verlag, 2017. 437−454. [doi: 10.1007/978-3-319-70972-7_25]

[20] Wang X, Liu JM, Wang XM. Improvement on multivariate signature scheme sodel. Journal of Beijing University of Posts and Telecommunications, 2009,32(5):124−127 (in Chinese with English abstract). [doi: 10.3969/j.issn.1007-5321.2009.05.027]

[21] Lu XB, Li FD, Tian L, Bao WS. Cryptanalysis of an improved multivariate digital signature scheme. Computer Engineering, 2012,8(22):95−98 (in Chinese with English abstract). [doi: 10.3969/j.issn.1000-3428.2012.22.023]

[22] Lu XB. Research on some kinds of multivariate digital signature scheme [MS. Thesis]. Zhengzhou: PLA Information Engineering University, 2012 (in Chinese with English abstract). [doi: CNKI:CDMD:2.1013.161122]

[23] Yasuda T, Takagi T, Sakurai K. Multivariate signature scheme using quadratic forms. In: Gaborit P, ed. Proc. of the Post-quantum Cryptography. Limoges: Springer-Verlag, 2013. 243−258. [doi: 10.1007/978-3-642-38616-9_17]

[24] Patarin J, Courtois N, Goubin L. Quartz, 128-Bit long digital signatures. In: Naccache D, ed. Proc. of the Cryptographers' Track at the RSA Conf. San Francisco: Springer-Verlag, 2001. 282−297. [doi: 10.1007/3-540-45353-9_21]

附中文参考文献:

[13] 刘筱茜,赵一鸣.基于多变量公钥密码体制的环签名变体方案.计算机工程,2015,41(2):96−99. [doi: 10.3969/j.issn.1000-3428]

[14] 郭秋玲,向宏,蔡斌,桑军,向涛.基于多变量公钥密码体制的门限环签名方案.密码学报,2018,5(2):140−150. [doi: 10.13868/j.cnki.jcr.000226]

[16] 孙昌毅,李益发,张文政,斯雪明.基于多变量密码体制的新型代理签名方案.四川大学学报(自然科学版),2012,49(3):565−569. [doi: 10.3969/j.issn.0490-6756.2012.03.016]

[18] 刘筱茜.基于多变量公钥密码体制的盲签名、环签名研究[硕士学位论文].上海:复旦大学,2014.

[20] 王鑫,刘景美,王新梅.多变量签名模型的改进.北京邮电大学学报,2009,32(5):124−127. [doi: 10.3969/j.issn.1007-5321.2009.05.027]

[21] 鲁晓彬,李发达,田礼,鲍皖苏.一种改进的多变量数字签名方案安全性分析.计算机工程,2012,8(22):95−98. [doi: 10.3969/j.issn.1000-3428.2012.22.023]

[22] 鲁晓彬.几类多变量数字签名方案研究[硕士学位论文].郑州:解放军信息工程大学,2012. [doi: CNKI:CDMD:2.1013.161122]

俞惠芳(1972－),女,博士,教授,CCF 高级会员,主要研究领域为密码学,信息安全.

付帅凤(1996－),女,硕士生,主要研究领域为后量子密码学,信息安全.