doi:10.11959/j.issn.1000-436x.2017024

基于多项式同构的代理重签名方案

李慧贤[1]，邵璐[1]，庞辽军[2]
（1. 西北工业大学计算机学院，陕西 西安 710072；2. 西安电子科技大学综合业务网国家重点实验室，陕西 西安 710071）

摘 要：由于目前的代理重签名方案几乎都是基于大数分解、离散对数和椭圆曲线等问题设计的，无法抵抗量子攻击，提出了一个新的代理重签名方案。该方案通过借助多项式同构和秘密仿射变换技术，能够高效地完成代理重签名功能并且可以抵抗量子攻击。通过分析表明，该方案不但满足正确性与一致性，并且在随机预言机模型下具有不可伪造性。与现有的代理重签名方案相比，该方案不仅继承了多变量公钥密码体制的高效性与抗量子攻击性，还具有复用性、透明性和秘密代理性等特点。
关键词：代理重签名；多变量公钥密码体制；多项式同构；仿射变换
中图分类号：TP309 **文献标识码**：A

Proxy re-signature scheme based on isomorphisms of polynomial

LI Hui-xian[1], SHAO Lu[1], PANG Liao-jun[2]
(1. School of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an 710072, China;
2. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China)

Abstract: Most of the existing proxy re-signature schemes were based on the hardness of big integer factoring, discrete logarithm, elliptic curve. However, none of them can resist the attack by a quantum computer. Motivated by these concerns, a new proxy re-signature scheme was proposed. By employing secret affine transformations and homogeneous polynomials, the proposed scheme could implement the signature transformation with high-efficiency, and meanwhile it was secure against the attack by a quantum computer. The results of analysis showed that the proposed scheme was correct and consistent, and had the unforgeability in the random oracle model. Compared with the existing schemes, the proposed scheme not only inherits the resistance to quantum attack and high efficiency from the multivariate public key cryptosystems, but also has the properties of multi-use, transparent and private proxy.
Key words: proxy re-signature, multivariate public key cryptosystem, isomorphisms of polynomial, affine transformation

1 引言

随着计算机科学技术的不断发展，数字签名技术也随之飞速发展。许多具有不同功能的签名类型被陆续提出，如代理签名[1]、群签名[2]和多重签名[3]等。近年来，代理重签名[4]也成为该领域的一个新兴研究方向。由于代理重签名在特定路径的遍历证明、透明认证、管理群组签名以及数字证书的共享与转换等方面有较好的应用前景，所以，近 10 年来许多研究人员都在研究设计安全可靠的代理重签名方案。

1998 年，Blaze 等[4]首先提出了代理重签名的概念：存在一个拥有重签名密钥的半可信的代理，它可以将 Alice 针对某一消息的签名转换为 Bob 对同一消息的签名。自 1998 年代理重签名方案[4]的概念被提出后，由于其方案本身安全性不高以及未详

收稿日期：2016-10-10；**修回日期**：2016-12-27
基金项目：国家自然科学基金资助项目（No.61103178, No.61473214）；陕西省自然科学基础研究计划基金资助项目（No.2015JM6294, No.2016JM6002）；中央高校基本科研业务费专项基金资助项目（No.3102015JSJ0003）
Foundation Items: The National Natural Science Foundation of China (No.61103178, No.61473214), The Natural Science Basic Research Plan in Shaanxi Province of China (No.2015JM6294, No.2016JM6002), The Fundamental Research Funds for the Central Universities (No.3102015JSJ0003)

细说明其应用领域等问题，代理重签名并没有引起足够的重视。直到 2005 年，Ateniese 等[5]对代理重签名的性质和应用领域提出了新的定义，他们指出之前方案的缺陷并提出了更安全的代理重签名方案，通过引入双线性映射来设计代理重签名方案，从而利用计算性 Diffie-Hellman（CDH）问题和二元离散对数（2-DL）问题保证其安全性。同时，形式化地定义了代理重签名的算法及安全模型。自此，代理重签名引起了广泛的关注，具有不同性质的代理重签名方案开始陆续被提出。

2007 年，Shao 等[6]提出了 2 个新的代理重签名方案，第 1 个方案引用了 Waters[7]的签名方案进行签名从而提高方案的安全性，第 2 个方案在此基础上设计出一个基于身份的代理重签名方案。该方案使用基于 ID 的密钥，从而省去了证书管理的麻烦。2008 年，Libert 等[8]提出了一个可以提高代理者的重签名密钥安全性的代理重签名方案。该方案使用了 2 层签名设计出具有更高安全性的代理重签名方案，但该方案具有计算量和占用空间较大的缺点。之后，代理重签名领域的研究渐渐兴起，为了满足更多的应用场景与用途，针对代理重签名的研究不仅局限于代理重签名算法本身，还根据不同的性质要求，开始将代理重签名算法与其他算法相结合，产生了一系列的具有更多应用场景的代理重签名方案。

Yang 等[9]提出了基于门限的代理重签名方案，该方案第一次定义了门限代理重签名的模型，并且基于 Ateniese 等[5]和 Shao 等[6]的方案，使用 Shamir 的门限秘密共享方法[10]将代理者的权利分散，防止代理者滥用代理签名权。Yang 等[11]提出了可变门限的代理重签名方案，该方案基于 Ateniese 等[5]的方案设计出可变门限代理重签名方案，它相对于普通门限方案的优势是可以根据被签署文档的重要性来改变阈值和代理者的数量。Feng 等[12]提出了基于身份的代理重签名方案，该方案在保证安全性的同时使用较短的系统参数降低计算成本，简化密钥管理。Zhang 等[13]提出基于身份的门限代理重签名方案。该方案将 Shamir 的门限秘密共享方法应用于 Shao 等[6]的基于身份的代理重签名方案，从而避免了传统公钥证书中管理存储开销的问题。

到目前为止，几乎所有的代理重签名方案都是基于大数分解、离散对数和椭圆曲线等问题的。然而，Shor[14]量子计算算法的出现使量子计算机会威胁到 ECC、DSA、RSA、ElGamal 等算法以及基于大数分解、离散对数和椭圆曲线等问题的代理重签名方案。这就意味着现有的代理重签名方案在量子攻击下并不安全。在量子计算机的研发成为热点的大背景下，如何保证代理重签名方案的安全性是一个值得研究的问题。多变量公钥密码体制就是后量子密码系统中一个可以抵抗量子计算机攻击的公知技术。

1996 年，Patarin 等[15]提出一种多变量公钥密码体制中的基于多项式同构（IP，isomorphisms of polynomial）问题的非交互的零知识证明方案。Tang 等[16]简化了该方案，提出一种更为简洁高效的基于多项式同构问题的签名方案，在本文中将其简称为 IP 签名。本文基于 Tang 等[16]提出的多变量公钥密码体制中的 IP 签名技术设计一个新的代理重签名方案——基于多项式同构问题的代理重签名方案。由于 IP 签名方案的验证过程是通过寻找同类型的 2 个不同映射的同构多项式来进行的，所以 IP 签名是基于 NP 难题中的 IP 问题设计的，因此，其具有抗量子攻击的特性。基于 IP 签名技术进行代理重签名的构造可以利用秘密仿射变换进行重签名密钥的巧妙构造使重签名过程简洁可行，并且利用 IP 问题保证了重签名过程的安全性。本文提出的代理重签名方案在保证了复用性、透明性和秘密代理性等优点的同时，还继承了 IP 签名方案具有的抗量子攻击与高效性的特性。

2　预备知识

由于本文的代理重签名方案是基于多项式同构（IP）问题构造的，所以本文先介绍一下 IP 问题以及代理重签名方案的通用模型结构。

2.1　IP 问题

Patarin 等[15]说明了 IP 问题，即多项式同构问题。所有的运算均在阶为 2^k 的有限域 K 上，有正整数 u、n。A 为具有 n 个变量 $x_1,x_2,\cdots,x_n$ 的 u 阶二次多项式方程组，μ_{ik} 为一次项的系数。

$$A:\ y_k=\sum_i\sum_j\gamma_{ijk}x_ix_j+\sum_i\mu_{ik}x_i+\delta_k,k=1,2,\cdots,u$$

B 为具有 n 个变量 $x_1',\cdots,x_n'$ 的 u 阶二次多项式方程组。

$$B:y_k'=\sum_i\sum_j\gamma_{ijk}'x_i'x_j'+\sum_i\mu_{ik}'x_i'+\delta_k',\ \ k=1,2,\cdots,u$$

S 为具有 u 个变量 $y_1,y_2,\cdots,y_u$ 的双射仿射变换。

$$S(y_1,y_2,\cdots,y_u)=(y_1',y_2',\cdots,y_u')$$

T 为具有 n 个变量 $x_1',x_2',\cdots,x_n'$的双射的仿射变换。

$$T(x_1',x_2',\cdots,x_n')=(x_1,x_2,\cdots,x_n)$$

如果存在(S,T)可以使 $B=S\circ A\circ T$，就可以说 A、B 是同构的，其中，“∘”表示仿射变换运算，双射仿射变换对(S,T)可以称为 A、B 的同构多项式。

IP 问题。已知 2 个 u 阶二次多项式方程组 A、B，并且它们是同构的，从而寻找到它们的同构多项式(S,T)。IP 问题是 NP 难题，所以通常用来隐藏私钥信息 S、T。

2.2 代理重签名模型

代理重签名中存在一个可以对签名进行转换的半可信代理者，它利用自己的重签名密钥将 Alice 在消息 m 上的签名转换成 Bob 在 m 上的签名。但这个代理者并不能单独替代 Alice 或 Bob 对任一消息进行签名。代理重签名的一般模型是由以下 6 个算法（Globle-Setup、KeyGen、ReKey、Sign、ReSign、Verify）构成。

Globle-Setup：由一信任方运行算法，生成系统全局参数。

KeyGen：输入系统参数，密钥生成算法 KeyGen 生成签名者公私钥对(pk,sk)。

ReKey：输入受托者 Alice 和委托者 Bob 的公私钥对(pk_A,sk_A)、(pk_B,sk_B)（不一定全部都需要），重签名密钥生成算法 ReKey 输出代理重签名密钥 $rk_{A\to B}$，代理者应用该密钥可将受托者签名转换为委托者签名。

Sign：输入待签名消息 m、私钥 sk，签名算法 Sign 进行运算后输出对消息 m 的签名 σ。

ReSign：输入 ReKey 生成的代理重签名密钥、消息 m、受托者 Alice 的公钥 pk_A，以及 Alice 对 m 的签名 σ_A。首先验证 Verify$(pk_A,m,\sigma_A)=1$，若签名通过验证，则重签名算法 ReSign 输出生成的新签名 σ_B，该签名则为委托者 Bob 在消息 m 上的签名。否则输出⊥。

Verify：输入公钥 pk、消息 m 以及对应消息 m 的签名 σ。验证算法运算 Verify$(pk,m,\sigma)=1$，如果签名算法 Sign 和重签名算法 ReSign 生成的签名都可以满足上式的验证，即运行 Verify 算法输出的结果均为 1 时，则证明该重签名方案是正确的。

2.3 基于游戏的代理重签名安全模型

定义 1 若不存在任何多项式有界敌手 A 以不可忽略的优势赢得游戏，则称该基于多项式同构问题的代理重签名方案在选择消息攻击下具有不可伪造性。

由攻击者 A 与挑战者 C 进行的游戏过程如下所示。

1) 预言机查询

O_{KeyGen}：用户密钥预言机，攻击者 A 输入查询由密钥生成算法 KeyGen 合法生成的用户公钥 pk，则用户密钥预言机 O_{KeyGen} 返回攻击者 A 公钥所对应的私钥 sk。

O_{ReKey}：重签名密钥预言机，攻击者 A 输入查询由密钥生成算法 KeyGen 合法生成的用户公钥 pk_A、pk_B。重签名密钥预言机 O_{ReKey} 返回攻击者 A 重签名密钥 $rk_{A\to B}$。

O_{Sign}：签名预言机，攻击者 A 输入查询由密钥生成算法 KeyGen 合法生成的用户公钥 pk、消息空间中任意消息 m。签名预言机 O_{Sign} 返回给攻击者 A 签名 V，其签名可用对应加密私钥 sk 的公钥 pk 验证。

O_{ReSign}：重签名预言机，攻击者 A 输入查询(pk_A, pk_B, m, V)。其中，pk_A、pk_B 为密钥生成算法 KeyGen 合法生成的用户公钥，V 是对应公钥 pk_A 的消息 m 的签名。重签名预言机 O_{ReSign} 返回 A 重签名 V_b。

2) 伪造

攻击者 A 最终输出(pk^*,m^*,V^*)，需满足下列条件。

V^*是可用公钥 pk^*验证的关于 m^*的有效重签名；

pk^*不是密钥预言机 O_{KeyGen} 的查询；

(pk^*, m^*)不是签名预言机 O_{Sign} 的查询；

(Δ,pk^*)不是重签名密钥预言机 O_{ReKey} 中的查询，Δ为任意用户公钥；

$(\Delta,pk^*, m^*,\square)$不是重签名预言机的查询，$\square$为任意签名。

如果攻击者 A 最终输出的(pk^*,m^*,V^*)满足上述条件，则称 A 赢得这场游戏。攻击者 A 在游戏后成功伪造重签名的优势定义为 Adv_A。

3 基于 IP 问题的代理重签名方案

3.1 方案初始化过程

令 K 为运算所在的阶为 2^k 的有限域，n、u、q、k 为正整数。其中，n 表示二次多项式方程组变量

个数的正整数，u 表示二次多项式方程组阶数的正整数，q 表示散列函数 $H(x)$运算后的二进制值的位数。H:$\{0,1\}^{*}\to\{0,1\}^{q}$，$H$ 为一抗碰撞的散列函数，将任意长度 0、1 字符串转换成 q bit 长度。令 $H=H(P)$，其中，P 为任意长度的 0、1 字符串。本文用 $H[i]\in\{0,1\}$表示 H 中第 i 比特位的值，其中，$i=1,2,\cdots,q$。

在本文的代理重签名方案中，Alice 为受托者，即原始签名者；Bob 为委托者，即被转换后的签名所属者。在该方案中，首先需要由第三方随机选择一个具有 n 个变量的 u 阶二次多项式方程组 Q，如

$$\overline{y_k}=\sum_i\sum_j\overline{\gamma_{ijk}}\,\overline{x_i}\,\overline{x_j}+\sum_i\overline{\mu_{ik}}\,\overline{x_i}+\overline{\delta_k},\ k=1,2,\cdots,u \quad (1)$$

Alice 首先随机选择可逆仿射变换(M,N)，如

$$M:\ M(\overline{y_1},\overline{y_2},\ldots,\overline{y_u})=(y_1,y_2,\ldots,y_u)$$

$$N:\ N(x_1,x_2,\ldots,x_n)=(\overline{x_1},\overline{x_2},\ldots,\overline{x_n})$$

使 $A=M\circ Q\circ N$。

Alice 再随机选择可逆仿射变换(S,T)作为它的私钥，如

$$S:\ S(y_1,y_2,\cdots,y_u)=(y_1',y_2',\cdots,y_u') \quad (2)$$

$$T:\ T(x_1',x_2',\cdots,x_n')=(x_1,x_2,\cdots,x_n) \quad (3)$$

对应的公钥为(A,B)，满足

$$A=M\circ Q\circ N$$

$$B=S\circ A\circ T$$

其中，A、B 为具有 n 个变量的 u 阶二次多项式方程组，如

$$A:\ y_k=\sum_i\sum_j\gamma_{ijk}x_ix_j+\sum_i\mu_{ik}x_i+\delta_k,\ \ k=1,2,\cdots,u \quad (4)$$

$$B:\ y_k'=\sum_i\sum_j\gamma_{ijk}'x_i'x_j'+\sum_i\mu_{ik}'x_i'+\delta_k',\ \ k=1,2,\cdots,u \quad (5)$$

同样地，Bob 随机选择可逆仿射变换(M_b, N_b)，如

$$M_b:\ M_b(\overline{y_1},\overline{y_2},\cdots,\overline{y_u})=(y_1,y_2,\cdots,y_u)$$

$$N_b:\ N_b(x_1,x_2,\cdots,x_n)=(\overline{x_1},\overline{x_2},\cdots,\overline{x_n})$$

使 $A_b=M_b\circ Q\circ N_b$。

Bob 再随机选择可逆仿射变换(S_b,T_b)作为它的私钥，与上文 (S,T)形式相同。对应的公钥为(A_b,B_b)，满足

$$A_b=M_b\circ Q\circ N_b$$

$$B_b=S_b\circ A_b\circ T_b$$

其中，A_b、B_b 分别为如式(4)和式(5)所示的 u 阶二次多项式方程组。

3.2　方案描述

本文的代理重签名方案和一般代理重签名方案一样分为以下 6 个算法(Globle-Setup、KeyGen、ReKey、Sign、ReSign、Verify)。

Globle-Setup：系统生成参数(n, u, q, K, Q)。运算所在有限域 K，n、u、q 为正整数；H:$\{0,1\}^{*}\to\{0,1\}^{q}$ 为一抗碰撞的散列函数；Q 为具有 n 个变量的 u 阶二次多项式方程组。

KeyGen：根据方案初始化赋值阶段，由 Globle-Setup 给定的方程组 Q，Alice、Bob 分别选择各自可逆仿射变换(M,N)、(M_b,N_b)，计算出各自的部分公钥 A、A_b；再分别选择可逆仿射变换 $sk_A=(S,T)$、$sk_B=(S_b,T_b)$作为各自签名的私钥；通过计算，得出各自对应的公钥 $pk_A=(A,B)$、$pk_B=(A_b,B_b)$。

ReKey：重签名密钥为 $rk_{A\to B}=(rk_1, rk_2, rk_3, rk_4)$，重签名密钥生成过程如下。

1) 代理者秘密随机选择形如 S 的可逆仿射变换 C 和 E；选择形如 T 的可逆仿射变换 D 和 F。

2) 代理者将 C、D、E、F 发送给 Alice，Alice 进行计算将$(C\circ M,N\circ D,E\circ S\circ M,N\circ T\circ F)$发送给 Bob。

3) Bob 收到后进行计算，将$(C\circ M\circ M_b^{-1}, N_b^{-1}\circ N\circ D,E\circ S\circ M\circ M_b^{-1}\circ S_b^{-1},T_b^{-1}\circ N_b^{-1}\circ N\circ T\circ F)$发送给代理者。

4) 代理者收到后进行计算，得到$(C^{-1}\circ C\circ M\circ M_b^{-1},\ N_b^{-1}\circ N\circ D\circ D^{-1},\ E^{-1}\circ E\circ S\circ M\circ M_b^{-1}\circ S_b^{-1},\ T_b^{-1}\circ N_b^{-1}\circ N\circ T\circ F\circ F^{-1})$，即代理重签名密钥为$(rk_1, rk_2, rk_3, rk_4)=(M\circ M_b^{-1},N_b^{-1}\circ N,\ S\circ M\circ M_b^{-1}\circ\ S_b^{-1},\ T_b^{-1}\circ N_b^{-1}\circ N\circ T)$。

Sign：输入待签名消息 m、Alice 的公私钥对(A,B)和(S,T)。Alice 随机选择 q 对可逆仿射变换$((S_1',T_1'),(S_2',T_2'),\cdots,(S_q',T_q'))$，对 m 进行签名。签名过程分为以下 2 步。

1) 输入参数：输入 m、(S,T)、(A,B)。m 为待签名消息，(S,T)为私钥，(A,B)为公钥。

2) 运算过程：首先，Alice 随机选择 q 对双射仿射变换对$(S_1',T_1'),(S_2',T_2'),\cdots,(S_q',T_q')$，进行仿射变换的计算。

$$S_1'(y_1,y_2,\cdots,y_u)=(y_1^{(1)},y_2^{(1)},\cdots,y_u^{(1)})$$

$$S_2'(y_1,y_2,\cdots,y_u)=(y_1^{(2)},y_2^{(2)},\cdots,y_u^{(2)})$$

$$\vdots$$

$$S_q'(y_1,y_2,\cdots,y_u)=(y_1^{(q)},y_2^{(q)},\cdots,y_u^{(q)})$$
$$T_1'(x_1^{(1)},x_2^{(1)},\cdots,x_n^{(1)})=(x_1,x_2,\cdots,x_n)$$
$$T_2'(x_1^{(2)},x_2^{(2)},\cdots,x_n^{(2)})=(x_1,x_2,\cdots,x_n)$$
$$\vdots$$
$$T_q'(x_1^{(q)},x_2^{(q)},\cdots,x_n^{(q)})=(x_1,x_2,\cdots,x_n)$$

其次，Alice 进行计算

$$C_1=S_1'\circ A\circ T_1',\ C_2=S_2'\circ A\circ T_2',\cdots,\ C_q=S_q'\circ A\circ T_q'$$

然后，Alice 计算散列值：$H=H(m\|C_1\|C_2\|\cdots\|C_q)$，其中，符号“‖”表示级联。

Alice 计算(S_i,T_i)值为

$$(S_i,T_i)=\begin{cases}(S_i',T_i'),H[i]=0\\(S_i'\circ S^{-1},T^{-1}\circ T_i'),H[i]=1\end{cases}$$

其中，$i=1,2,\cdots,q$，$H[i]$表示 H 中第 i 比特的值。

最后，Alice 计算

$$V=(H,(S_1,T_1),(S_2,T_2),\cdots,(S_q,T_q)) \tag{6}$$

输出生成的签名 V，$V=(H,(S_1,T_1),(S_2,T_2),\cdots,(S_q,T_q))$。

ReSign：输入签名 V、重签名密钥 $rk_{A\to B}=(rk_1,rk_2,rk_3,rk_4)$、原始签名者 Alice 的公钥$(A,B)$和消息 m。

1) 验证签名正确性。输入 m、V 和(A,B)，根据验证算法（Verify）的过程进行运算，若 Verify$(m,V,(A,B))=1$，则证明签名验证成功，进行下一步重签名生成；否则，输出⊥，结束运算。

2) 重签名生成。输入签名 V 和重签名密钥 $rk_{A\to B}=(rk_1,rk_2,rk_3,rk_4)$，计算

$$(S_{ib},T_{ib})=\begin{cases}(S_i\circ rk_1,rk_2\circ T_i),H[i]=0\\(S_i\circ rk_3,rk_4\circ T_i),H[i]=1\end{cases},i=1,2,\cdots,q$$

3) 输出签名

$$V_b=(H,(S_{1b},T_{1b}),(S_{2b},T_{2b}),\cdots,(S_{qb},T_{qb})) \tag{7}$$

Verify：输入待签名消息 m、Bob 的公钥(A_b,B_b)，转换后的签名 V_b，进行签名验证过程。

签名的验证过程分为以下 3 步。

1) 输入参数：输入 m、V、(A,B)。m 为待签名消息，V_b 为对应消息 m 生成的签名，(A,B)为签名者公钥。

2) 运算过程：验证者计算

$$C_i'=\begin{cases}S_i\circ A\circ T_i,H[i]=0\\S_i\circ B\circ T_i,H[i]=1\end{cases},i=1,2,\cdots,q$$

其中，$H[i]$表示 H 中第 i 比特的值。

验证者计算散列值 $H'=H(m\|C_1'\|C_2'\|\cdots\|C_q')$后，将 H'与签名阶段中 H 值进行对比。

3) 输出过程：当 $H'=H$ 时，签名通过验证，即 Verify$(m,V,(A,B))=1$ 返回 true。否则签名验证失败，返回 false。

验证者根据上述签名验证阶段的过程进行运算，若 Verify$(m,V_b,(A_b,B_b))=1$，则代理重签名验证成功；否则，输出⊥。

4 方案的正确性与性能分析

本节对提出的代理重签名方案的正确性、一致性和不可伪造性进行证明，并对该方案的效率和代理重签名特性进行讨论分析。

4.1 代理重签名方案正确性分析

定理 1 基于多项式同构问题的代理重签名方案满足正确性。代理重签名方案满足正确性必须满足条件：对于在消息空间内的任意消息 m 以及由算法 KeyGen 产生的公私钥对$(pk_i,sk_i)=((A_i,B_i),(S_i,T_i))$，由算法 Sign 生成的签名 V 满足 Verify$(m,V,(A_i,B_i))=1$。由算法 ReSign 生成的签名需满足 Verify$(m,\text{ReSign}(rk_{A\to B},m,V),(A_b,B_b))=1$。

证明 由于已知 IP 签名方案满足正确性，所以只需证明该代理重签名过程的正确性，即可证明代理重签名方案满足正确性。本文首先对 Alice 签名过程中的重要步骤做一个简要分析。

在签名过程中，Alice 随机选择 q 对双射仿射变换对$((S_1',T_1'),(S_2',T_2'),\cdots,(S_q',T_q'))$，进行仿射变换的计算。

$$A=M\circ Q\circ N$$

所以

$$C_1=S_1'\circ A\circ T_1'=S_1'\circ M\circ Q\circ N\circ T_1'$$
$$C_2=S_2'\circ A\circ T_2'=S_2'\circ M\circ Q\circ N\circ T_2'$$
$$\vdots$$
$$C_q=S_q'\circ A\circ T_q'=S_q'\circ M\circ Q\circ N\circ T_q'$$

Alice 计算散列值：$H=H(m\|C_1\|C_2\|\cdots\|C_q)$，其中，符号“‖”表示级联。

Alice 计算(S_i,T_i)值为

$$(S_i,T_i)=\begin{cases}(S_i',T_i'),H[i]=0\\(S_i'\circ S^{-1},T^{-1}\circ T_i'),H[i]=1\end{cases}$$

其中，$i=1,2,\cdots,q$，$H[i]$表示 H 中第 i 比特的值。

最后，Alice 计算 $V=(H,(S_1,T_1),(S_2,T_2),\cdots,(S_q,T_q))$。代理进行转换后的签名为

$$(S_{ib},T_{ib})=\begin{cases}(S_i\circ rk_1,rk_2\circ T_i)=(S_i\circ M\circ M_b^{-1},\\ N_b^{-1}\circ N\circ T_i),\ H[i]=0\\ (S_i\circ rk_3,rk_4\circ T_i)=(S_i\circ S\circ M\circ M_b^{-1}\circ S_b^{-1},\\ T_b^{-1}\circ N_b^{-1}\circ N\circ T\circ T_i),\ H[i]=1\end{cases}$$

其中，$i=1,2,\cdots,q$，S_i、T_i 为 Alice 在签名阶段生成的(S_i,T_i)值。本文将(S_i,T_i)值代入继续进行化简。

$$(S_i,T_i)=\begin{cases}(S_i',T_i'),\ H[i]=0\\ (S_i'\circ S^{-1},T^{-1}\circ T_i'),\ H[i]=1\end{cases},i=1,2,\cdots,q$$

所以，

$$(S_{ib},T_{ib})=\begin{cases}(S_i'\circ M\circ M_b^{-1},\\ N_b^{-1}\circ N\circ T_i'),\ H[i]=0\\ (S_i'\circ M\circ M_b^{-1}\circ S_b^{-1},\\ T_b^{-1}\circ N_b^{-1}\circ N\circ T_i'),H[i]=1\end{cases},i=1,2,\cdots,q$$

本文可以看作代理转换后的签名中 Bob 签名时选取的 q 对仿射变换对为$(S_1'\circ M\circ M_b^{-1},N_b^{-1}\circ N\circ T_1')$,$(S_2'\circ M\circ M_b^{-1},N_b^{-1}\circ N\circ T_2')$,$\cdots$,$(S_q'\circ M\circ M_b^{-1},N_b^{-1}\circ N\circ T_q')$。因为

$$A_b=M_b\circ Q\circ N_b$$

所以

$$\begin{aligned}C_{1b}&=S_1'\circ M\circ M_b^{-1}\circ A_b\circ N_b^{-1}\circ N\circ T_1'\\&=S_1'\circ M\circ M_b^{-1}\circ M_b\circ Q\circ N_b\circ N_b^{-1}\circ N\circ T_1'\\&=S_1'\circ M\circ Q\circ N\circ T_1'=C_1,\\C_{2b}&=S_2'\circ M\circ M_b^{-1}\circ A_b\circ N_b^{-1}\circ N\circ T_2'\\&=S_2'\circ M\circ Q\circ N\circ T_2'=C_2,\\&\vdots\\C_{qb}&=S_q'\circ M\circ M_b^{-1}\circ A_b\circ N_b^{-1}\circ N\circ T_q'\\&=S_q'\circ M\circ Q\circ N\circ T_q\leftarrows C_q。\end{aligned}$$

由于消息值 m 相同，所以

$$H_b=H(m\|C_{1b}\|C_{2b}\|\cdots\|C_{qb})=H(m\|C_1\|C_2\|\cdots\|C_q)=H$$

所以输出转换后的签名

$$V_b=(H,(S_{1b},T_{1b}),(S_{2b},T_{2b}),\cdots,(S_{qb},T_{qb}))$$

证毕

4.2　代理重签名方案一致性分析

定理 2　基于多项式同构问题的代理重签名方案满足一致性。方案若满足一致性，则必须满足条件：对于在消息空间内的任意消息 m、公钥 $pk_i=(A_i,B_i)$ 以及签名 V，2 次调用算法 Verify$(m,V,(A_i,B_i))$，得到的结果必定相同。

证明　在本文方案中，无论是 Sign(pk_i,m)或 Resign(pk_A,pk_B,m_j,V)生成的签名，由于验证过程中条件不变，所以对于 $V=(H,(S_1,T_1),(S_2,T_2),\cdots,(S_q,T_q))$，$H'=H(m\|C_1'\|C_2'\|\cdots\|C_q')$，恒有 $H'=H$，也就是 2 次验证结果是相同的。所以，代理重签名方案的一致性得以验证。

证毕

4.3　代理重签名方案不可伪造性证明

定理 3　在随机预言模型中，如果存在一个敌手 A，能够在多项式时间内以ε的优势赢得游戏，而且攻击者 A 最多能够查询 Q_S 次签名预言机 O_{Sign}、Q_K 次用户密钥预言机 O_{KeyGen}、Q_{RK} 次重签名密钥预言机 O_{ReKey}、Q_{RS} 次重签名预言机 O_{ReSign}、Q_H 次散列查询预言机 O_{Hash}。那么存在一个算法 C，能够在多项式时间内以ε'优势解决 IP 问题。其中，有

$$\varepsilon'>\frac{\varepsilon(1-\frac{1}{2^q})}{Q_HQ_K(Q_{RS}+Q_S)}$$

证明　不失一般性，本文将(S_t,T_t)设为算法 C 的目标私钥，C 把 A 作为它的子程序并扮演游戏中挑战者的角色。

1) 初始化

首先建立攻击者 A 的公开参数：(n,u,q,K,Q)。有限域 K，n、u、q 为正整数；Q 为具有 n 个变量的 u 阶二次多项式方程组，如式 (1)。$H(\cdot):\{0,1\}^*\rightarrow\{0,1\}^q$ 为一个随机预言机。

2) 攻击阶段

O_{KeyGen}：C 随机选择(S_i,T_i)，若询问的用户未被攻陷，则返回$(pk_i,sk_i)=(A_i,B_i)$，其中，$A_i=M_i\circ Q\circ N_i$，$B_i=S_i\circ A_i\circ T_i$；其中，$M_i$，$S_i$ 形如式(2)，其中，N_i、T_i 形如式(3)。若询问的用户已被攻陷，则返回公私钥对$(pk_i,sk_i)=((A_i,B_i),(S_i,T_i))$。

O_{Sign}：接收到 A 查询输入(pk_i,m_j)，C 随机选取 S_p'和 T_p'，$p=1,2,\cdots,q$。

① 若 pk_i 已被攻陷，则进行计算

$$\begin{aligned}C_1&=S_1'\circ A_i\circ T_1'\\C_2&=S_2'\circ A_i\circ T_2'\\&\vdots\\C_q&=S_q'\circ A_i\circ T_q'\end{aligned}$$

签名者计算散列值为

$$H=H(m_j\|C_1\|C_2\|\cdots\|C_q)$$

计算(S_p,T_p)值为

$$(S_p,T_p)=\begin{cases}(S_p',T_p'),\ H[p]=0\\(S_p'\circ S_i^{-1},T_i^{-1}\circ T_p'),\ H[p]=1\end{cases}$$

$$p=1,2,\cdots,q$$

最后，返回签名值 $V=(H,(S_1,T_1),(S_2,T_2),\cdots,(S_q,T_q))$。

② 若 pk_i 未被攻陷，选择 M(构造形式如式(2))和 N(构造形式如式(3))，计算

$$A_i=M\circ Q\circ N,\ S_p^*=S_p'\circ M^{-1},\ T_p^*=N^{-1}\circ T_p'$$

计算

$$C_1=S_1^*\circ A_i\circ T_1^*=S_1'\circ Q\circ T_1'$$
$$C_2=S_2^*\circ A_i\circ T_2^*=S_2'\circ Q\circ T_2'$$
$$\vdots$$
$$C_q=S_q^*\circ A_i\circ T_q^*=S_q'\circ Q\circ T_q'$$

然后，签名者计算散列值：$H=H(m_j\|C_1\|C_2\|\cdots\|C_q)$。

计算

$$(S_p,T_p)=\begin{cases}(S_p'\circ M^{-1},N^{-1}\circ T_p'),\ H[p]=0\\(S_p'\circ M^{-1}\circ S_i^{-1},T_i^{-1}\circ N^{-1}\circ T_p'),\ H[p]=1\end{cases}$$

其中，$p=1,2,\cdots,q$。

最后，返回签名值 $V=(H,\ (S_1,T_1),\ (S_2,T_2),\cdots,\ (S_q,T_q))$。

未被攻陷时，签名正确性验证过程如下所示。

$$C_p'=\begin{cases}S_p\circ A_i\circ T_p\\=S_p'\circ M^{-1}\circ A_i\circ N^{-1}\circ T_p',\ H[p]=0\\S_p\circ B_i\circ T_p\\=S_p'\circ M^{-1}\circ S_i^{-1}\circ B_i\circ T_i^{-1}\circ N^{-1}\circ T_p',\\H[p]=1\end{cases},$$

其中，$p=1,2,\cdots,q$。

由于 $A_i=M\circ Q\circ N$，$B_i=S_i\circ A_i\circ T_i$，

$$C_p'=\begin{cases}S_p\circ A_i\circ T_p\\=S_p'\circ Q\circ T_p',\ H[p]=0\\S_p\circ B_i\circ T_p\\=S_p'\circ Q\circ T_p',\ H[p]=1\end{cases},p=1,2,\cdots,q$$

于是，$H(m_j\|C_1'\|C_2'\|\cdots\|C_q')=H(m_j\|C_1\|C_2\|\cdots\|C_q)=H$。

O_{ReKey}：接收到 A 查询输入(pk_i,pk_j)后，若(pk_i,pk_j)均已被攻陷或(pk_i,pk_j)均未被攻陷，C 返回重签名密钥 $rk_{i\to j}(rk_1,\ rk_2,\ rk_3,\ rk_4)=(M_i\circ M_j^{-1},\ N_j^{-1}\circ N_i,\ S_i\circ M_i\circ M_j^{-1}\circ S_j^{-1},T_j^{-1}\circ N_j^{-1}\circ N_i\circ T_i)$。否则，中止。

O_{ReSign}：接收到攻击者 A 输入查询$(pk_A,\ pk_B,\ m_j,\ V)$。首先验证 $\text{Verify}(pk_A,m_j,V)=1$，否则，中止。调用 O_{Sign} 输出 $O_{\text{Sign}}(pk_B,m_j)$。

O_{Hash}：该预言机根据攻击者的查询信息，构造表 L，若接收到 A 查询输入是$(m_k,C_1,C_2,\cdots,C_q)$时，如果表 L 中存在相应记录，那么 C 返回相应的存储记录；否则，随机选取 $\omega\in Z_q$ 并在表 L 中记录。

3) 伪造阶段

在进行多项式有界次上述询问后，A 输出伪造密文为 $V''=(H'',(S_1'',T_1''),(S_2'',T_2''),\cdots,(S_q'',T_q''))$。

通过上述分析可知，此模拟等同实际的攻击环境，敌手 A 伪造成功，则必须得到(S_t,T_t)。可获得正确(S_t,T_t)的概率至少为 $\dfrac{1}{Q_{\text{RS}}+Q_{\text{S}}}$。$C$ 将$(S_t,\ T_t)$其作为 IP 问题的输出。

下面，本文来分析 C 成功概率：A 正确猜出目标用户的概率为 $\dfrac{1}{Q_{\text{K}}}$。A 正确猜出伪造信息 m^*的概率为 $\dfrac{1-\dfrac{1}{2^q}}{Q_{\text{H}}}$。

因此，本文可以得出：$\varepsilon'>\dfrac{\varepsilon(1-\dfrac{1}{2^q})}{Q_{\text{H}}Q_{\text{K}}(Q_{\text{RS}}+Q_{\text{S}})}$。

证毕

4.4　代理重签名方案效率分析

通常，代理重签名方案的时间开销主要包括重签名算法和验证算法过程的时间开销，本文方案在整个算法过程中具有较低时间消耗。表 1 通过分析经典代理重签名方案以及本方案在重签名阶段与验证阶段的计算时间消耗以及公私钥开销来对本方案的效率进行分析。

表 1　　**方案效率对比分析**

方案	重签名阶段	验证阶段	公钥开销	私钥开销
BBS[4]	$ke+h$	$3ke+h$	$\|p\|$	$\|q\|$
AH[5]	$2e+h$	$2P+h$	$\|2^k\|$	$\|q\|$
SCW[6]	$6e+h$	$3P+h$	$\|p\|$	$\|q\|$
LV[8]	$7e+h$	$6P+h$	$\|p\|$	$\|p\|$
本文方案	h	$2h$	$8u(n+1)(n+2)$	$8u(u+1)+8n(n+1)$

表 1 中 k 是方案中安全参数，e 表示一次幂运算时间消耗，h 表示一次散列运算时间消耗，P 表示一次对数运算时间消耗，u、n 均为本方案所选取的整数，p、q 为文献[4~6,8]方案选取群中的大素数。

幂运算和对数运算均为低效运算[17]。由表 1 可知，本文方案由于基于多变量公钥密码体制中的 IP 签名算法，所以在重签名阶段与验证阶段并未使用计算消耗大的幂运算与对数运算。通过与表 1 中的所有方案对比，本文方案具有最低时间消耗，因此在计算方面具有高效性。为保证在量子计算机攻击下本文方案的安全性，本文参数选择与 IP 签名方案的参数相同时处于同等安全级别。根据文献[21]中针对 IP 签名攻击方法的分析，本文方案中参数选取为 K=GF(2^8)，n=18，u=10，q=64 时，本文方案的攻击计算复杂度即可达到安全级别所需的 2^{80}。在此参数基础上，本文方案的公钥大小为 $8u(n+1)(n+2)$=8×10×(18+1)×(18+2)=30 400 bit，私钥大小为 $8u(u+1)+n(n+1)$=8×10×(10+1)+ 8×18×(18+1)=3 616 bit。而对比文献[4~6,8]主要基于离散对数困难问题，按照普通安全要求，其所选取的大素数一般为 1 024 bit，即公、私钥大小都为 1 024 bit，因此，本文方案较其他方案相比，在公私钥开销方面相对较大，这也是 IP 签名技术固有的缺陷，也是本领域值得进一步探讨的公开问题。

4.5 代理重签名方案特性分析

1) 双向性

代理重签名方案满足双向性即代理重签名密钥 $rk_{A\to B}$ 不仅可以将 Alice 签名转换为 Bob 签名,也可将 Bob 签名转换为 Alice 签名。

定理 4　在基于多项式同构问题的代理重签名方案中，如果可以将 Alice 签名转换为 Bob 签名的重签名密钥 $rk_{A\to B}$ 得到将 Bob 签名转换为 Alice 签名的重签名密钥 $rk_{B\to A}$，则称该代理重签名方案满足双向性。

证明　根据本方案的算法设计可知，本方案的代理重签名算法得到的代理重签名密钥为 $rk_{A\to B}$=$(M\circ M_b^{-1}, N_b^{-1}\circ N, S\circ M\circ M_b^{-1}\circ S_b^{-1}, T_b^{-1}\circ N_b^{-1}\circ N\circ T)$。

因为由可逆仿射变换的性质可知$(M_b\circ M^{-1})^{-1}$=$(M\circ M_b^{-1})$，同理可得$(M_b\circ M^{-1},\ N^{-1}\circ N_b,\ S_b\circ M_b\circ M^{-1}\circ S^{-1},\ T^{-1}\circ N^{-1}\circ N_b\circ T_b)$。

如果要将 Bob 的签名转换为 Alice 的签名，需要得到的重签名密钥为 $rk_{B\to A}$=$(M_b\circ M^{-1},\ N^{-1}\circ N_b,\ S_b\circ M_b\circ M^{-1}\circ S^{-1}, T^{-1}\circ N^{-1}\circ N_b\circ T_b)$。

因此，可以通过求逆方法从 $rk_{A\to B}$ 得到 $rk_{B\to A}$。满足定理 4，所以本方案满足双向性。

证毕

2) 复用性

代理重签名方案满足复用性即由重签名方案中的 Sign、ReSign 算法产生的签名均可作为 ReSign 算法的输入。

定理 5　在基于多项式同构问题的代理重签名方案中，ReSign 算法的输入为 V，如果 Sign、ReSign 算法输出的签名形式满足 V=$(H,(S_1,T_1),(S_2,T_2),\cdots,(S_q,T_q))$（如式(6)），则该方案满足复用性。

证明　在本文方案中 Sign 算法产生的签名为 V=$(H,(S_1,T_1),(S_2,T_2),\cdots,(S_q,T_q))$，满足定理 5。

ReSign 算法产生的签名为 V_b=$(H,(S_{1b},T_{1b}),\ (S_{2b},T_{2b}),\cdots,\ (S_{qb},T_{qb}))$（如式(6)），与所要求签名形式相同，满足定理 5。

由于 Sign、ReSign 算法产生的签名形式均满足定理 5 要求，所以本方案满足复用性。

证毕

3) 透明性

代理重签名方案满足透明性即仅通过签名是无法判断该签名是 Sign 还是 ReSign 算法产生的。

定理 6　在基于多项式同构问题的代理重签名方案中，如果 Sign 和 ReSign 算法输出的签名形式相同，则该方案满足透明性。

证明　Sign 算法产生的签名为 V=$(H,(S_1,T_1),(S_2,T_2),\cdots,(S_q,T_q))$，ReSign 算法产生的签名为 V_b=$(H,(S_{1b},T_{1b}),(S_{2b},T_{2b}),\cdots,(S_{qb},T_{qb}))$，可直观看出 2 个签名形式完全相同，满足定理 6。

由于 Sign、ReSign 算法输出的签名格式相同，均为$(H,(S_1,T_1),(S_2,T_2),\cdots,(S_q,T_q))$，所以本方案满足透明性。

证毕

4) 秘密代理性

代理重签名方案满足秘密代理性即在代理重签名的过程中，攻击者无法通过代理的输入输出计算出重签名密钥。

定理7　在基于多项式同构问题的代理重签名方案中，如果攻击者无法获得(S_b, T_b, M_b, N_b, S, T, M, N)，即每个参与成员的私钥，则该方案满足秘密代理性。

证明　Bob 的签名为 V_b=$(H,\ (S_{1b},\ T_{1b}),\ (S_{2b},\ T_{2b}),\cdots,\ (S_{qb},\ T_{qb}))$。

$$(S_{ib},T_{ib})=\begin{cases}(S_i'\circ M\circ M_b^{-1}, N_b^{-1}\circ N\circ T_i'), H[i]=0\\ (S_i'\circ M\circ M_b^{-1}\circ S_b^{-1},\\ T_b^{-1}\circ N_b^{-1}\circ N\circ T_i'), H[i]=1\end{cases}$$

其中，$i=1,2,\cdots,q$。

Bob 的公钥为 $pk_B=(A_b,B_b)$，其中

$$A_b=M_b\circ Q\circ N_b$$

$$\begin{aligned}C_{1b}&=S_1'\circ M\circ M_b^{-1}\circ A_b\circ N_b^{-1}\circ N\circ T_1'\\&=S_1'\circ M\circ M_b^{-}\circ M_b\circ Q\circ N_b\circ N_b^{-1}\circ N\circ T_1'\\&=S_1'\circ M\circ Q\circ N\circ T_1'=C_1,\\C_{2b}&=S_2'\circ M\circ M_b^{-1}\circ A_b\circ N_b^{-1}\circ N\circ T_2'\\&=S_2'\circ M\circ Q\circ N\circ T_2'=C_2,\\&\vdots\\C_{qb}&=S_q'\circ M\circ M_b^{-1}\circ A_b\circ N^{-1}\circ N\circ T_q'\\&=S_q'\circ M\circ Q\circ N\circ T_q'=C_q。\end{aligned}$$

可得 $H=H(m\|C_{1b}\|C_{2b}\|\cdots\|C_{qb})$。

由于 IP 问题的困难性，由上述过程可知根据已知信息求得 Bob 的私钥(S_b, T_b)、(M_b, N_b)与求解 IP 问题困难性相同。对于 Alice 同理，求得 Alice 的私钥(S, T)、(M, N)与求解 IP 问题困难性相同。因而无法求得(S_b, T_b, M_b, N_b, S, T, M, N)。

由上述分析得知本方案满足定理 7，所以本方案满足秘密代理性。

证毕

5 结束语

自代理重签名的概念被提出后，由于其具有广泛的应用前景，具有不同性质的代理重签名方案被陆续提出。本文提出了一个可以应用于量子计算机攻击环境下的代理重签名方案。该方案基于多项式同构问题设计出一个基于多变量公钥密码体制的代理重签名方案。该方案具有正确性、一致性和不可伪造性，并且该方案具有复用性、透明性、秘密代理性、高效性以及抗量子攻击的特性。因此，本文所设计的方案相比现有方案在低能耗硬件与量子计算机攻击下的环境中具有更为高效安全的应用优势。由于本文方案密钥尺寸较大，未来的工作将致力于研究具有较小的密钥尺寸的代理重签名方案以及满足更多应用场景的具有单向性的代理重签名方案。

参考文献：

[1] BOLDYREVA A, PALACIO A, WARINSCHI B. Secure proxy signature schemes for delegation of signing rights[J]. Journal of Cryptology, 2012, 25(1): 57-115.

[2] CHEN X, LENZINI G, MAUW S, et al. A group signature based electronic toll pricing system[C]//International Conference on Availability, IEEE Computer Society. 2011:85-93.

[3] SEVERENS M, FARQUHAR J, DUYSENS J, et al. A multi-signature brain-computer interface: use of transient and steady-state responses[J]. Journal of Neural Engineering, 2013, 10(10): 1160-1166.

[4] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[J]. Lecture Notes in Computer Science, 1998, 1403:127-144.

[5] ATENIESE G, HOHENBERGER S. Proxy re-signatures: new definitions, algorithms, and applications[C]//ACM Conference on Computer and Communications Security. 2005:310-319.

[6] SHAO J, CAO Z, WANG L C, et al. Proxy re-signature schemes without random oracles[C]// Progress in Cryptology-Indocrypt 2007, International Conference on Cryptology in India. 2007:197-209.

[7] WATERS B. Efficient identity-based encryption without random oracles[M]//Advances in Cryptology – EUROCRYPT 2005. Springer Berlin Heidelberg, 2005:114-127.

[8] LIBERT B, VERGNAUD D. Multi-use unidirectional proxy resignatures[C]//ACM Conference on Computer and Communications Security. ACM. 2008: 511-520.

[9] YANG P, CAO Z, DONG X. Threshold proxy re-signature[J]. Journal of Systems Science &Complexity, 2008, 24(4):816-824.

[10] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11):612-613.

[11] YANG X D, ZHANG L, WANG C F. A flexible threshold proxy re-signature scheme with provable security[J]. Computer Engineering & Science, 2014.

[12] FENG J, LAN C H, JIA B R. ID-based proxy resignature scheme with strong unforgeability[J]. Journal of Computer Applications, 2014.

[13] ZHANG Y L, YANG X D, WANG C F. ID-based bidirectional threshold proxy re-signature[J]. Journal of Computer Applications, 2011, 31(1):4920-4926.

[14] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. Siam Review, 1997, 41(2):1484-1509.

[15] JACQUES P. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms[M]// Advances in Cryptology–EUROCRY- PT'96. Springer Berlin Heidelberg, 1996: 33-48.

[16] TANG S, XU L. Proxy signature scheme based on isomorphisms of polynomials[C]//Network and System Security(NSS) 2012. 2012: 113-125.

[17] 刘文浩, 许春香. 无证书两方密钥协商方案[J]. 软件学报, 2011, 22(11):2843-2852.
LIU W H, XU C X. Two party certificateless key agreement schemes[J]. Journal of Software, 2011, 22(11): 2843-2852.

作者简介：

李慧贤（1977-），女，内蒙古乌兰浩特人，博士，西北工业大学副教授，主要研究方向为网络与信息安全、安全协议设计与分析等。

邵璐（1991-），女，陕西咸阳人，西北工业大学硕士生，主要研究方向为安全协议设计与分析。

庞辽军（1978-），男，陕西渭南人，博士，西安电子科技大学教授，主要研究方向为密码学、信息安全等。