基于多变量公钥密码系统的环机密交易协议

洪璇，袁梦玲

引用本文

洪璇，袁梦玲. 基于多变量公钥密码系统的环机密交易协议[J]. 计算机科学, 2023, 50(6A): 220100157-6.

HONG Xuan, YUAN Mengling. Ring Confidential Transaction Protocol Based on Multivariate Public-key Cryptosystem [J]. Computer Science, 2023, 50(6A): 220100157-6.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220100157

基于多变量公钥密码系统的环机密交易协议

洪 璇 袁梦玲
上海师范大学信息与机电工程学院 上海 200234
上海师范大学上海智能教育大数据工程技术研究中心 上海 200234
(hong@shnu.edu.cn)

摘 要 与比特币类似,门罗币也是一种加密货币。最初的门罗币是基于CryptoNote协议,该协议使用环签名和一次密钥来隐藏交易双方的真实身份,但是具体的交易金额却暴露在区块链中,存在一定的安全风险。为了解决这个安全漏洞,Shen Noether提出了环机密交易协议(RingCT),利用一个随机数来隐藏真正的交易金额。目前门罗币社区使用的环机密交易协议是基于离散对数难题的。然而随着量子计算机的发展,基于传统数论问题的方案将变得不再安全,后量子方案是一个很好的替代选择。多变量公钥密码学是后量子密码的主要研究方向之一,并且相较于其他后量子密码方案,基于多变量的签名方案往往在签名和验证过程中计算速度快、所需计算资源少,具有很好的研究价值。在多变量环签名方案的基础上,设计了一个基于多变量的环机密交易协议。该协议利用多变量签名方案公钥的加法同态性实现了对交易金额的承诺,并对此承诺进行环签名,通过随机选择区块链中的用户公钥成环,来混淆交易中实际的交易参与者的身份。同时在交易产生过程中会利用交易者的私钥生成唯一一个key-image,并让其参与签名生成过程,成为签名的一部分,通过比对此部分可以有效防止交易双花。在随机预言机模型中证明了本文方案的安全性,并且相比基于格的后量子安全的环机密交易协议,所提方案在签名效率以及验证效率方面都更具优势。

关键词:多变量公钥密码;后量子;环签名;环机密交易协议;同态承诺
中图法分类号 TN918

Ring Confidential Transaction Protocol Based on Multivariate Public-key Cryptosystem

HONG Xuan and YUAN Mengling
College of Information, Mechanical and Electrical Engineering, Shanghai Normal University, Shanghai 200234, China
Shanghai Engineering Research Center of Intelligent Education and Bigdata, Shanghai Normal University, Shanghai 200234, China

Abstract Similar to Bitcoin, Monero is also a cryptocurrency. The original Monero is based on the CryptoNote protocol, which uses ring signatures and one-time keys to hide the real identities of both parties to the transaction, but the specific transaction amount is exposed in the area. In the blockchain, there are certain security risks. To address this security hole, Shen Noether proposed ring confidential transactions(RingCT), which utilizes a random number to hide the real transaction amount. The ring confidential transaction protocol currently uses by the Monero community is based on the discrete logarithm problem. However, with the development of quantum computers, solutions based on traditional number theory problems will become no longer secure. Post-quantum solutions are a good alternative. Multivariate public key cryptography is one of the main research directions of post-quantum cryptography, and compared with other post-quantum cryptographic schemes, multivariate-based signature schemes tend to have faster computing speed and less computing resources in the process of signature and verification. It has good research value. Based on the multivariable ring signature scheme, this paper designs a multivariable ring confidential transaction protocol. The protocol uses the additive homomorphism of the public key of the multivariable signature scheme to realize the commitment to the transaction amount, and performs a ring signature on the commitment. By randomly selecting the user public key in the blockchain to form a ring, the identity of the actual transaction participants in the transaction is confused. At the same time, during the transaction generation process, the trader's private key will be used to generate a unique key-image, and it will participate in the signature generation process and become a part of the signature. By comparing this part, the transaction double-spending can be effectively prevented. The security of the proposed scheme is proved in the random oracle model, and compared with the lattice-based post-quantum secure ring confidential transaction protocol, the proposed scheme has more advantages in signature efficiency and verification efficiency.

Keywords Multivariate public-key cryptosystem, Post-quantum, Ring signature, Ring confidential transactions protocol, Homomorphic commitment

---

基金项目:上海师范大学科研发展基金(309-C-9000-21-309203)
This work was supported by the Shanghai Normal University Scientific Research Development Fund Project(309-C-9000-21-309203).
通信作者:袁梦玲(yuan_mengling@163.com)

1 引言

在当前的数字时代，加密货币是利用虚拟资产和加密机制进行电子支付或转账等操作。这些支付或转账的操作可以直接在账户或钱包之间进行，而不需要第三方参与，也就是说，这些操作是去中心化的[1]。比特币是迄今为止最广为人知、最分散的加密货币[2]。与传统银行作为第三方的交易模式相反，比特币允许在去中心化的 P2P 网络中进行相关电子交易操作。虽然比特币的本意是通过使用假名来实现匿名性，保证用户隐私，但一些分析表明，比特币并不是真正的匿名。比特币的交易信息是公开的，其交易金额和流向可以说是完全暴露的[3]。文献[4]研究发现，利用 Union-Find 算法可以将比特币中公开的地址与实体之间进行关联，从而揭开用户的真实身份。虽然文献[5]中提出了一种可以减少交易之间关系的协议，用来保护诚实的支出者的信息不会被不诚信的接收者暴露，但这个协议只是尽可能地避免暴露，在实际应用中并不能保证完全的安全性。因此，比特币只是一种伪匿名加密货币。

Dash 是最初在加密货币中添加匿名性的加密货币，它通过合币、链式混合及盲化的技术来隐藏交易中的实际金额及交易双方的地址[6]。另一个在加密货币中提供匿名性的尝试是 Zerocash，它使用零知识非交互式知识论证(zk-SNARKs)技术提供匿名性与形式化安全证明；同时通过 mint 与 pour 技术，保证了 Zerocash 中交易金额、交易双方的保密性[7]。然而，Zerocash 需要通过可信第三方来生成和销毁初始化参数，这在一定程度上违背了去中心化的思想。

门罗币(Monero)是于 2014 年 4 月创建的一种开源加密货币，注重隐私、去中心化和可扩展性[8]。与许多作为比特币衍生品的加密货币不同，门罗币基于 CryptoNote 协议[9]，利用一次性地址解决交易输入输出地址的关联性问题，利用环签名的“验证者无法分辨环中的实际签名者”的特性[10]，来提供交易双方的匿名性。但是 CryptoNote 协议存在一个巨大的安全漏洞，即使只有一个用户在交易过程中没有使用 mixin 来模糊交易的真正输入，那么就有可能导致整个门罗币系统的不可追溯性被破坏[11]。为了解决这个安全漏洞，Shen Noether 引入比特币社区核心人物 Maxwell 提出的的机密交易(CT)协议[12]，并结合了多层可链接自发匿名组签名(MLSAG)，为门罗币构建了环机密交易协议(RingCT)[13]。MLSAG 中的自发(或称 ad-hoc)的意思是，用户可以任意选择某几个用户进行组签名，而无须告知组内被选择的其他用户。这一特性保证了方案无须依赖可信第三方，满足去中心化的特性，且生成的签名不会存在暴露签名者身份的信息，在验证者看来这个签名有可能是组内任意一个用户所签，这就增强了匿名性。同时机密交易协议中的 Pedersen 承诺[14]技术实现了对交易中实际金额的隐藏。

可链接环签名是 RingCT 协议保证匿名性的基础。它是环签名的变体，在不破坏环签名匿名性的基础上，添加了可链接的属性，提供了可链接性和匿名性：验证者并不能从签名中得到签名者的身份信息，只知道他/她是环中的用户之一。而对于给定的任何两个可链接环签名，验证者可以通过验证链接标签是否相等来得知它们是否由同一个签名者产生[15]。Pedersen 承诺使一方能够对选定的秘密值进行承诺，同时对其他方进行隐藏，以后可以打开这个承诺[14]。这种密码学原语是同态的，允许各方通过计算同态的输入和输出账户来证明账户余额。

本文设计了一个基于多变量的环机密交易协议，作为后量子方案，该协议可以很好地抗量子计算机攻击，并且与基于格的方案相比，所需的计算资源少；此外该协议利用环签名技术，隐藏交易发起者的身份，并在环签名中添加了一个链接标签，作为 key-image 以防止双花。同时还构建了基于多变量的同态承诺，用于隐藏交易中的金额，便于验证交易中输入和输出之间的关系。在随机预言机模型中证明了本文方案具有匿名性、不可伪造性和平衡性。

2 多变量公钥密码学

目前实践中使用的绝大多数密码方案的安全性都是基于传统的数论问题，例如基于大整数分解问题的 RSA 方案[16]和基于求解离散对数问题的 DSA 方案。然而，Shor 算法指出，传统数论问题在量子领域可以在多项式时间内得到解决[17]。换言之，量子计算机的发展将会严重威胁现有数字签名的安全性。因此，需要建立新的公钥密码方案，用于代替传统的基于数论问题的密码方案，以确保不受量子计算攻击。基于多变量[18]、格[19]、编码和哈希的密码方案都可以抵抗量子计算攻击。这些符合条件的公钥密码方案被称为后量子密码方案[20]。本文主要关注多变量密码方案。

多变量公钥密码方案的基础是有限域 $GF(2^n)$ 上的多变量二次多项式方程组，如下所示：

$$\begin{cases} \bar{f}^{(1)}(x_1,\cdots,x_n)=\sum_{i=1}^{n}\sum_{i=j}^{n}\alpha_{ij}^{(1)}\cdot x_i x_j+\sum_{i=1}^{n}\beta_i^{(1)}\cdot x_i+\gamma_0^{(1)} \\ \bar{f}^{(2)}(x_1,\cdots,x_n)=\sum_{i=1}^{n}\sum_{i=j}^{n}\alpha_{ij}^{(2)}\cdot x_i x_j+\sum_{i=1}^{n}\beta_i^{(2)}\cdot x_i+\gamma_0^{(2)} \\ \quad\cdots \\ \bar{f}^{(m)}(x_1,\cdots,x_n)=\sum_{i=1}^{n}\sum_{i=j}^{n}\alpha_{ij}^{(1)}\cdot x_i x_j+\sum_{i=1}^{n}\beta_i^{(m)}\cdot x_i+\gamma_0^{(m)} \end{cases}$$

多变量公钥密码方案的安全性是基于 MQ 问题的。

MQ 问题：在有限域 $GF(2^n)$ 上，对于上述多变量二次多项式方程组 $\bar{f}^{(i)}(x_1,\cdots,x_n)(i\in[1,m])$，求一个解向量 $\bar{\boldsymbol{x}}=(\bar{x}_1,\cdots,\bar{x}_n)$，使得 $\bar{f}^{(1)}(\bar{x}_1,\cdots,\bar{x}_n)=\cdots=\bar{f}^{(m)}(\bar{x}_1,\cdots,\bar{x}_n)=0$。当方程组中方程的个数 m 和变量个数 n 相差不大时，MQ 问题的求解是指数级别的，在文献[21]中已经证明 MQ 问题是一个 NP 困难问题。即使是使用量子计算机对基于 MQ 问题的方案进行攻击，也不能在多项式时间内解决。因此，与基于传统数论难题的方案相比，基于 MQ 问题的多变量密码方案对抗量子计算机的攻击有着更好的抵抗能力[18]。

多变量签名方案的一般构造如下。

密钥生成：$k=GF(q^l)$ 是一个有限域，中心映射 F 是一个二次映射 $F:k^n\to k^m$，$L_1:k^m\to k^m$ 和 $L_2:k^n\to k^n$ 是两个可逆仿射映射。由此可以得到私钥为 (L_1,F,L_2)。公钥由三映射复合组成：

$$\begin{aligned} PK&=\overline{F}=L_1\circ F\circ L_2 \\ &=(f_1(x_1,\cdots,x_n),\bar{f}_2(x_1,\cdots,x_n),\cdots,\bar{f}_m(x_1,\cdots,x_n)) \end{aligned}$$

签名算法：假设 $(y_1',\cdots,y_m')\in k^m$ 是将被签名的消息，签名者通过计算：$(x_1',\cdots,x_n')=\overline{F}^{-1}(y_1',\cdots,y_m')=L_2^{-1}\circ F\circ L_1^{-1}(y_1',\cdots,y_m')$ 得到消息 $(y_1',\cdots,y_m')$ 的签名是 $(x_1',\cdots,x_n')$。

验证算法:为了验证签名$(x_1',\cdots,x_n')$是否为消息$(y_1',\cdots,y_m')$的签名,验证者需要确认公式$y_i'=\bar{f}_i(x_1',\cdots,x_n'),i=1,2,\cdots,m$是否成立,如果成立,则确定签名$(x_1',\cdots,x_n')$是合法的,否则认为签名不合法。

3　RingCT 的形式化定义和安全模型

环机密交易(RingCT)协议的目的是在门罗币中保护支出者的匿名性以及交易的隐私。在实际应用中,该协议将 Pedersen 承诺与可链接环签名相结合,在隐藏交易金额的同时,通过环签名来混淆真实输出者身份,创建环保密交易。

RingCT 的概念最早是于 2015 年由 Shen Noether[13]提出,由于门罗币中所使用的 CryptoNote 协议中存在的安全漏洞,Shen Noether 将机密交易协议扩展到环签名上使用,提出了 RingCT 协议。

但是 Shen Noether 只是对 Ring CT 直接进行了实例化,因此,2017 年,Sun 等[22]提出了 RingCT v2.0 并对 RingCT 协议进行了完善的安全分析,给出了 RingCT 协议的形式化语法定义及安全定义。在该方案中他们并没有直接使用可链接环签名,而是通过使用单向累加器以及知识签名(SoK)来实现隐藏交易双方真实信息的功能,以此来缩小交易的规模。但是该方案会产生大量的零知识证明,会导致签名与验证阶段效率的降低。并且,此方案还需要一个公共可信设置,这会产生一定的安全性风险,并且也不符合去中心化的思想。

为了解决上述问题,2020 年 Yuen 等建立了一种高效的环签名方案[23],该方案删除了文献[22]中使用的可信设置假设,并提出了一个低成本区块链 RingCT 3.0 协议。

以上 RingCT 协议的安全性均依赖于经典数论假设,如求解离散对数的困难性。随着量子计算机的发展,基于传统数论问题的方案将面临巨大威胁。这种情况下,就需要构造相应的后量子密码方案,以对抗量子计算机攻击。

2018 年 Alberto 等提出了第一个后量子 RingCT 协议[24],并将其命名为 Lattice RingCT v1.0。在该方案中,他们首先利用 Fiat-Shamir 变换和 BLISS 签名方案设计了一种基于格的可链接环签名方案(L2RS),并以此签名方案为基础,添加同态承诺,设计了第一个基于格的 RingCT 协议。

然而,基于 L2RS 所提出的 Lattice RingCT v1.0 交易仅限于单输入和单输出(SISO)钱包,并且该方案中所产生的签名是一次性的,也就是说,在每次的交易中都需要生成一个新的输入钱包。因此在 2019 年,Alberto 等将文献[24]的 SISO.LRCT 方案进行了泛化,提出了可以实现多输入多输出(MIMO)钱包交易的 Lattice RingCT v2.0[25],并增加了范围证明以抵抗超出范围的攻击。

上述两种后量子 RingCT 方案均是基于格的方案,都存在运算效率低、所需计算资源过多的问题。在电子交易中,所需计算资源越大,交易过程的花费也会增加,而基于多变量的方案不仅可以抗量子计算机攻击,并且在实际应用中只需要适量的计算资源,是一种很好的后量子方案[19]。

3.1　RingCT 的形式化定义

定义 2　RingCT 协议由多项式时间算法(Setup,KeyGen,Mint,Spend,Verify)组成,分别生成系统参数、用户密钥、硬币密钥,支出者生成交易信息及相关签名,验证支出合法性。

$pp\leftarrow Setup(1^\lambda)$:Setup 算法输入安全参数$\lambda\in N$,输出公共系统参数 pp。以下所有算法均隐含公共参数 pp 作为其输入的一部分。

$(pk,sk)\leftarrow KeyGen(pp)$:密钥生成算法将公共参数 pp 作为输入,输出用户的公私钥对(pk,sk)。在门罗币中,pk 始终设置为一次性地址,该地址与硬币一起构成一个账户。

$(cn_{pk},ck)\leftarrow Mint(pk,a)$:Mint 算法将金额 a 和一次性地址 pk 作为输入,输出地址 pk 所对应的硬币 cn_{pk} 以及相关的硬币密钥 ck。硬币 cn_{pk} 和一次性地址 pk 一起构成一个账户 $act\triangleq(pk,cn_{pk})$,其对应的私钥是$ask\triangleq(sk,ck)$。

$(tx,\pi)\leftarrow Spend(m,i,K_s,A_s,R)$:输入支出者索引 i 以及相应的支出者密钥 K_s,输入账户 $A_s=\{act_{\text{in}}\}$,输出地址 $R=\{pk_{\text{out}}\}$,和一些交易字符串 $m\in\{0,1\}^*$,该算法输出交易 tx 和证明 π。

$0/1\leftarrow Verify(tx,\pi)$:输入交易 tx 和证明 π 时,算法将验证该次交易是否正确有效,并输出有效或无效支出。

3.2　RingCT 的安全模型

RingCT 协议应满足以下的安全属性。

定义 3(完全正确性)　完全正确性要求如果对于任意概率多项式时间攻击者 A,RingCT 协议 Π($Setup$,$KeyGen$,$Mint$,$Spend$,$Verify$)满足:

$$\Pr\left[\begin{array}{c}(pk,sk)\leftarrow KeyGen(pp);\\ Verify(tx,\pi)=1:(cn_{pk},ck)\leftarrow Mint(pk,a);\\ (tx,\pi)\leftarrow Spend(m,i,K_s,A_s,R);\end{array}\right]=1$$

则认为该协议是完全正确的。

定义 4(匿名性)　匿名性要求在支出过程中使用相同的交易字符串 m,输入账户集合 A_s 和输出账户集合 R,以及不同的两个支出账户集合 A_{s_0},$A_{s_1}\in A_s$ 生成的一个证明 π,对于任意概率多项式时间,攻击者 S 不能区分 π 是由哪一个支出账户所生成的,也就是说,实际支出者的账户成功隐藏在所有诚实用户中。

我们定义如下预言机:

支出预言机(Spend Oracle):对于输入的交易字符串 m,账户集合 $A_s=\{act^k\}_{k\in[w]}$ 以及相应的账户密钥 $K_s=\{ask^k\}_{k\in[w]}$,输出地址的集合 $R=\{pk_{\text{out},j}\}_{j\in[t]}$,支出预言机返回一个有效证明 π。

"腐败"预言机(Corruption Oracle):对于输入的索引 $i\in\{1,\cdots,n\}$,返回该索引相应的私钥 SK_i。

攻击者 S 和挑战者 C 的匿名性游戏如下:

(1)挑战者 C 通过密钥生成算法生成公私钥对(PK,SK),并把所有的公钥发送给攻击者 S,自己保留所有私钥。

(2)攻击者 S 允许访问支出预言机 SO。

(3)攻击者 S 选取一个交易字符串 m,两个不同的支出账户 A_{s_0},A_{s_1},一个包含 A_{s_0},A_{s_1} 的任意集合 A_s,输出地址的集合 $R=\{pk_{\text{out},j}\}_{j\in[t]}$,将其发送给挑战者 C。

(4)挑战者 C 随机选取一个支出账户 A_{s_b},通过访问支出预言机 SO,获得一个证明 π_b,并将其发送给攻击者 A。

5)攻击者 S 输出一个数 b^*。

如果对于任意概率多项式时间攻击者 A,RingCT 协议 Π($Setup$,$KeyGen$,$Mint$,$Spend$,$Verify$)满足:

$$Pr\left[\begin{array}{c}pp\leftarrow Setup(1^\lambda);\\ b^*=b:(pk,sk)\leftarrow KeyGen(pp);\\ b\leftarrow\{0,1\};\\ \pi_b\leftarrow Spend(m,b,K_{s_b},A_{s_b},R)\end{array}\right]-\frac{1}{2}\leqslant nefl(\lambda)$$

那么就认为该协议是满足匿名性的。

定义 5(不可伪造性) 不可伪造性要求一个不诚实用户生成的证明 π 不能通过验证算法 Verify 返回该证明有效。

我们定义如下不可伪造性游戏：

(1)挑战者 C 生成系统参数并将其发送给攻击者 A。

(2)攻击者 A 根据需要自适应访问支出预言机 SO 和"腐败"预言机 CO。

(3)攻击者 A 选取一个交易字符串 m，支出账户 A_s，输出地址的集合 $R=\{pk_{\text{out},j}\}_{j\in[t]}$，并访问支出预言机 SO 得到证明 π_s。

如果对于任意概率多项式时间攻击者 A，RingCT 协议 $\Pi(Setup,KeyGen,Mnt,Spend,Verify)$ 满足：

$$Pr\left[\begin{array}{l}pp\leftarrow Setup(1^{\lambda});\\(pk,sk)\leftarrow KeyGen(pp);\\Verify(\pi_s)=1:SK_i\leftarrow Corruption-Oracle(i);\\\pi_s\leftarrow Spend(m,s,K_s,A_s,R)\end{array}\right]$$

$$\leqslant nefl(\lambda)$$

则认为该协议满足不可伪造性。

定义 6(平衡性) 平衡性(Balance)要求任何恶意用户不能有以下行为：

(1)花费一个诚实用户的任何账户；

(2)花费其账户的输入金额与输出金额的总和；

(3)双花其任何一个账户。

如果对于任意概率多项式时间攻击者 A，RingCT 协议 $\Pi(Setup,KeyGen,Mnt,Spend,Verify)$ 满足：

$$Pr\left[\begin{array}{l}pp\leftarrow Setup(1^{\lambda});\\(pk,sk)\leftarrow KeyGen(pp);\\Verify(\pi_s)=1:SK_i\leftarrow Corruption-Oracle(i);\\\pi_s\leftarrow Spend(m,s,K_s,A_s,R)\\a_{\text{out}}=a_{\text{out}}+a_{\text{in}};I_1=I_2\end{array}\right]$$

$$\leqslant nefl(\lambda)$$

则认为该协议满足平衡性。

4 基于多变量的环机密交易协议

4.1 多变量公钥承诺方案

环机密交易协议方案中隐藏交易金额的重要技术是 Pedersen 承诺。这是一种用于提供机密交易(特别是加密货币)的加密技术，其中最重要的属性就是加法同态性。利用具有加法同态性的 Pedersen 承诺，就可以在不透露实际交易金额的情况下，向验证者证明输入金额等于输出金额。

有限域上的基于多变量的签名方案的公钥是加法同态的，即 $PK(a)+PK(b)=PK(a+b)$，因此非常便于构建用于隐藏交易金额的基于多变量的加法同态承诺。对于想要隐藏的交易金额 a，随机选择一个数 $r\in GF(q^l)$，我们做如下基于多变量的承诺：

$$Com(r,a)=PK(r+PK(a))$$

加法同态承诺还需要满足：

$$\begin{aligned}Com(r,a_1)\oplus Com(r,a_2)&\triangleq Com(r,a_1)+Com(r,a_2)\ \bmod q\\&=Com(r+r,a_1+a_2)\ \bmod q\\Com(r,a_1)\ominus Com(r,a_2)&\triangleq Com(r,a_1)-Com(r,a_2)\ \bmod q\\&=Com(r-r,a_1-a_2)\ \bmod q\\&=Com(0,a_1-a_2)\ \bmod q\end{aligned}$$

如果满足公式：

$$Com(r,a)=Com(r,a_1)+Com(r,a_2)$$

且 $a=a_1+a_2$，则表示成功利用盲化因子 r 隐藏了实际交易金额 a,a_1,a_2。

4.2 方案的描述

基于多变量的环机密交易协议方案的实现步骤如下。

初始化阶段(Setup)：选择一个阶为 q^l 的有限域 $k=GF(q^l)$，和两个哈希函数 $H_1:\{0,1\}^*\rightarrow k^m$，$H_2:\{0,1\}^*\rightarrow k^n$，令 m 是多项式中方程的个数，n 是多项式中的变量个数。如此，得到公共参数集：

$$pp=\{k,q,l,m,n,H_1,H_2\}$$

密钥生成阶段(KeyGen)：对于输入的公共参数集 pp，密钥生成算法输出一对用户公钥和私钥(PK,SK)，其中，公钥为：$PK=\overline{F}=L_1\circ F\circ L_2$，私钥 $SK=(L_1,F,L_2)$。

硬币生成阶段(Mint)：对于输入的交易金额 a，门罗币钱包随机选择一个数 $ck=r_{ck}\in GF(q^l)$作为该硬币的私钥，并计算该硬币的承诺：

$$cn=Com(ck,a)=Com(r_{ck},a)=\overline{F}(r_{ck}+\overline{F}(a))$$

由此得到一个账户 $act=(PK,cn)$，其相应私钥为 $ask=(SK,ck)$。

支出者花费阶段(Spend)：

(1)支出者调用步骤(3)创建输出钱包(OW)，对于输出金额 a_{out}，利用随机数 $ck_{\text{out}}=r_{\text{out}}\in GF(k^l)$创建承诺：

$$cn_{\text{out}}=Com(ck_{\text{out}},a_{\text{out}})=\overline{F}(r_{\text{out}}+\overline{F}(a_{\text{out}}))$$

(2)使用用户的公钥 PK_i 来代表一个用户，假设实际支出者为 PK_π，让其对输出钱包的承诺 cn_{out}进行环签名。首先令随机选择的来自区块链的 $w-1$ 个用户组成一个集合 $R'=\{PK_i\}|_{i\in[0,w-1],i\neq\pi}$，将实际签名者 π 加入集合 R'组成用户集合 $R=(PK_0,PK_1,\cdots,PK_{w-1})$。

(3)计算本次交易的密钥图像(key-image)：$I=PK_\pi^{-1}(H_1(a,cn_{\text{out}}))$。

(4)签名者随机选择一个秘密参数 $\alpha\in k^n$，计算 $c_{\pi+1(\bmod w)}=H_2(R,cn_{\text{out}},\overline{F}_\pi(\alpha),I)$。

(5)对于 $i=\pi+1,\cdots,w-1,0,1,\cdots,\pi-1$，统一选择 $s_i\in k^n$，并计算：

$$c_{i+1(\bmod w)}=H_2(R,cn_{\text{out}},\overline{F}_i(c_i)+\overline{F}_i(s_i),I)$$

由此计算得到 $s_\pi=PK_\pi^{-1}(\overline{F}_\pi(\alpha)-\overline{F}_\pi(c_\pi))$。

(6)输出签名：

$$\sigma_R(cn_{\text{out}})=(c_0,s_0,\cdots,s_{w-1},I)$$

(7)令交易 $TX=(R,\sigma_R,cn_{\text{out}})$，并输出 TX 和签名 $\sigma_R(cn_{\text{out}})$

验证阶段(Verify)：

(1)首先检索区块链上是否已经存在一个交易的密钥图像 I，如果不存在，则继续验证，否则拒绝本次交易。

(2)对于 $i=0,\cdots,w-1$，计算：

$$c_{i+1(\bmod w)}=H_2(R,cn_{out},\overline{F}_i(c_i)+\overline{F}_i(s_i),I)$$

验证 c_0 和 c_w 是否相等，相等则认为该签名有效，否则拒绝该签名。

(3)验证输入金额是否等于输出金额：首先分别计算输入钱包和输出钱包承诺总和 Σcn_{in} 和 Σcn_{out}，如果 $\Sigma cn_{\text{in}}=\Sigma cn_{\text{out}}$，则表示交易中的输入金额和输出金额相等。

4.3 安全性分析

结论 1(完全正确性) 本文提出的基于多变量的环机密交易协议满足正确性要求。

证明:假设验证者接收到一笔交易 TX 和对于环 $R=(PK_0,PK_1,\cdots,PK_{W-1})$ 的签名 $\sigma_R(cn_{\text{out}})$,如果,交易 TX 和签名都是根据上述步骤得到,并且在传输过程中没有被篡改,那么,根据生成交易 TX 和签名 $\sigma_R(cn_{\text{out}})$ 的算法,我们可以得到:

$$c_{1(\bmod w)}=H_2(R,cn_{\text{out}},\overline{F}_0(c_0)+\overline{F}_0(s_0),I)$$

$$c_{2(\bmod w)}=H_2(R,cn_{\text{out}},\overline{F}_1(c_1)+\overline{F}_1(s_1),I)$$

$$\cdots$$

$$c_{w-1(\bmod w)}=H_2(R,cn_{\text{out}},\overline{F}_{w-2}(c_{w-2})+\overline{F}_{w-2}(s_{w-2}),I)$$

$$c_{w(\bmod w)}=H_2(R,cn_{\text{out}},\overline{F}_{w-1}(c_{w-1})+\overline{F}_{w-1}(s_{w-1}),I)=c_0$$

因此,一个诚实的用户生成交易 TX 和签名 $\sigma_R(cn_{\text{out}})$,并且在传输过程中不发生错误,那么在验证算法中,就会接受此次交易和签名。

结论 2(匿名性)　本文提出的基于多变量的环机密交易协议满足匿名性要求。

证明:根据 2.2 节中的定义的匿名性安全游戏,我们需要证明在 Spend 阶段产生的签名 $\sigma_R(cn_{\text{out}})$ 是匿名的。假设攻击者 S 选取两个不同的支出账户 PK_{π_0},PK_{π_1},并将其发送给挑战者 C,挑战者 C 随机选取 PK_{π_b}($b\in\{0,1\}$)通过访问支出预言机得到证明:

$$\sigma_{\pi_b}\leftarrow Spend(cn_{\text{out}},SK_{\pi_b},\{PK_0,\cdots,PK_{w-1}\})$$

对于支出预言机产生的证明 $\sigma_{\pi_b}=(c_0,s_0,\cdots,s_{w-1},I)$,由于在其生成过程中,$s_i(i\neq\pi_b)$ 是随机选取的,而 $s_{\pi_b}=\overline{F}_{\pi_b}^{-1}(\overline{F}_{\pi_b}(\alpha)-\overline{F}(c_{\pi_b}))$,其中,秘密参数 α 是签名者随机选择的,因此,可以认为 s_{π_b} 也是一个随机值。此外从公式计算中可以得知 $c_0=c_w=H_2(R,cn_{\text{out}},\overline{F}_{w-1}(c_{w-1})+\overline{F}_{w-1}(s_{w-1}),I)$。从之前的分析可知 s_{w-1} 是一个随机数,由此可以认为 c_0 也是 k^m 上的随机数。针对密钥图像 $I=PK_\pi^{-1}(H_1(a,cn_{\text{out}}))$,在这里,$a$ 是交易金额,在实际中,交易金额 a 是被隐藏的,在攻击者看来,a 就是一个随机生成的数,从而可以认为密钥图像 I 也是一个随机数。

由以上分析可知,经过正确的签名算法步骤得到的证明 $\sigma_{\pi_b}=(c_0,s_0,\cdots,s_{w-1},I)$ 是完全随机分布的,攻击者 S 无法区分该证明 σ_{π_b} 是由支出账户 PK_{π_0},PK_{π_1} 中的哪一个生成。因此,本方案满足匿名性要求。

结论 3(不可伪造性)　本文提出的基于多变量的环机密交易协议满足不可伪造性要求。

证明:若需证明一个方案是不可伪造的,则需将所提出的方案的安全性规约到一个或几个数学难题上。但是,本文所基于的多变量方案的安全性不仅需要考虑 MQ 问题的困难性,还需要考虑是否存在 IP 问题。目前人们对 IP 问题的了解有限,因此大多基于多变量的方案的安全性依靠各种攻击算法来检测。

假设攻击者 S 获得了由密钥生成算法生成的所有公钥 $PK_i(i=0,\cdots,w-1)$。通过访问"腐蚀"预言机,攻击者 S 最多可以知道 $w-1$ 个成员私钥,(假设实际支出者 π 的私钥不可知)并且掌握多种针对多变量公钥密码方案的已知攻击方法,如秩攻击、直接攻击、线性化方程攻击、差分攻击等。攻击者 S 想要模仿一个诚实的支出者进行支出操作,可以通过以下两种途径。

(1)攻击者 S 像合法的签名用户一样进行支出操作。根据支出算法的步骤可知,为了生成有效的证明 σ_π,攻击者首先需要利用签名者私钥计算交易 key-image 的值,然后利用该值与一个随机选择的数一起进行哈希预算得到 $c_{\pi+1}$ 的值。证明 σ_π 是由分量 c_0,I 以及 s_i 组成的,对于除签名者之外的其他环中用户,可以随机选择 s_i 的值,但是计算签名者的 $s_\pi=PK_\pi^{-1}(c_{\pi+1})-c_\pi$ 则需要知道签名者实际的私钥。这相当于破坏底层的多变量公钥方案实例,而在多变量公钥方案中,公钥的设置是一个单向陷门函数,通过公钥求得签名者私钥是不可行的。

(2)攻击者 S 直接求出所有的 $s_i=\overline{F}_i^{-1}(c_{i+1})-c_i$ 的值,这里 $i\in\{0,w-1\}$。其中,除了 s_i 是未知的,c_i 也是未知的,即使攻击者 S 通过"腐败"预言机获得了 $w-1$ 个成员的私钥,仍然无法求得所有 s_i 的值。

通过上述分析可以证明本文提出的基于多变量的环机密交易协议是安全的,满足不可伪造性。

结论 4(平衡性)　本文提出的基于多变量的环机密交易协议满足平衡性要求。

证明:根据平衡性(Balance)属性要求,任何恶意用户不能有以下行为:

(1)花费一个诚实用户的任何账户;

(2)花费其账户的输入金额与输出金额的总和;

(3)双花其任何一个账户。

因此,平衡性可以看作是匿名性和不可伪造性的结合,根据上述对匿名性和不可伪造性的证明可知,本方案满足平衡性。

4.4　效率分析

对于环机密交易协议的效率分析,本文主要考虑其在支出(Spend)和验证(Verify)阶段的计算成本。在此根据这两个因素,分别分析了本文所构造的基于多变量的环机密交易协议及 Alberto 等的 Lattice RingCT v1.0[24] 和 Lattice RingCT v2.0[25],结果如表 1 所列。

表 1　环机密交易协议效率比较

Table 1　Comparison of efficiency of RingCT

Protocol	Signature Size	Spend Process	Verify Process
Lattice RingCT v1.0[24]	$O(n)$	$(5n+3)E+nH+1$	$(4n+2)E+nH+2$
Lattice RingCT v2.0[25]	$O(n^2)$	$(5n+3)E+nH$	$(2n*n+n+2)E+nH+1$
Our Method	$O(n)$	$(3n+2)E+nH$	$2nE+nH+1$

表 1 中,n 为环中的用户数量,E 为做一次格/多变量运算的开销,H 为做一次哈希运算的开销。

从表 1 可以看出,本文提出的基于多变量的环机密交易协议在签名长度、支出开销和验证开销上相比基于格的方案均具有优势,在签名长度上要优于 Lattice RingCT v2.0,在支出阶段和验证阶段的运行效率上明显优于 Lattice RingCT v1.0 和 Lattice RingCT v2.0,是一个较好的抗量子攻击的环机密交易协议方案。

结束语　本文构造了一个基于多变量的环机密交易协议,为了实现环机密交易协议中对交易金额的隐藏,我们首先构建了一个基于多变量的同态承诺,用于交易双方承诺在交易过程中输入金额的总和会等于输出金额的总和,并且交易金额外部不可见。然后,在支出阶段,利用基于多变量的环签名成功隐藏了支出者身份,并且通过交易中的密钥图像(key-image)防止交易过程中出现双花。相比基于传统数论问题的

方案，本文提出的方案在抗量子计算机攻击方面具有优势。相比基于格的方案，本文方案的计算效率更高，生成证明的速度更快。在安全性方面，通过分析可知，本文的方案满足正确性、匿名性、不可伪造性和平衡性要求。本文所提的后量子方案是基于多变量的，未来可以进一步研究后量子领域的其他方案。

参 考 文 献

[1] ZAGHLOUL E, LI T T, MUTKA M W, et al. Bitcoin and Blockchain: Security and Privacy[J]. IEEE Internet of Things Journal, 2020, 7(10): 10288-10313.

[2] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System [EB/OL]. [2021-12-06]. https:// bitcoin. org/bitcoin. pdf.

[3] KOSHY P, KOSHY D, MCDANIEL P. An Analysis of Anonymity in Bitcoin Using P2P Network Traffic[C]// International Financial Cryptography Association 2014. LNCS 8437, 2014: 469-485.

[4] RON D, SHAMIR A. Quantitative analysis of the full bitcoin transaction graph[C]// Financial Cryptography and Data Security(FC 2013). 2013: 6-24.

[5] WIJAYA D A, LIU J K, STEINFELD R, et al. Anonymizing bitcoin transaction[C]// Information Security Practice and Experience(ISPEC 2016). 2016: 271-283.

[6] DUFFIELD E, DIAZ D. Dash: A Payments-Focused Cryptocurrency [EB/OL]. [2021-12-06]. https://docs. dash. org/en/stable/introduction/about. html # whitepaper.

[7] BEN-SASSON E, CHIESA A, GARMAN C. Zerocash: Decentralized Anonymous Payments from Bitcoin[C]// 2014 IEEE Symposium on Security and Privacy. 2014: 459-474.

[8] KOE, ALONSO K M, NOETHER S. Zero to Monero : Second Edition [EB/OL]. [2021-12-06]. https://www. getmonero. org/library/Zero-to-Monero-2-0-0. pdf.

[9] VAN SABERHAGEN N. CryptoNote v 2. 0 [EB/OL]. [2021-12-06]. https://cryptonote. org/whitepaper. pdf.

[10] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret [C]// 7th International Conference on the Theory and Application of Cryptology and Information Security. 2001: 552-565.

[11] NOETHER S, MACKENZIE A. A Note on Chain Reactions in Traceability in CryptoNote2. 0[EB/OL][2021-12-06]. https://www. getmonero. org/resources/research-lab/pubs/MRL-0001. pdf.

[12] MAXWELL G. Confidential Transactions [EB/OL]. [2021-12-06]. https:// www. weusecoins. com/confidential-transactions/.

[13] NOETHER S. Ring Signature Confidential Transactions for Monero [EB/OL]. [2021-12-06]. https://eprint. iacr. org/2015/1098.

[14] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[M]. Lecture Notes in Computer Science. Springer: Heidelberg, 1992: 129-140.

[15] LIU J K, WEI V K, WONG D S. Linkable spontaneous anonymous group signature for ad hoc groups[M]// Lecture Notes in Computer Science. Heidelberg: Springer, 2004: 325-335.

[16] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

[17] SHOR P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[J]. SIAM Review, 1999, 41(2): 303-332.

[18] DING J, GOWER J E, SCHMIDT D S. Multivariate Public Key Cryptosystems[M]. New York: Springer Science + Business Media, 2006.

[19] BUCHMANN J, LINDNER R, RÜCKERT M. Post-quantum cryptography: lattice signatures[J]. Computing, 2009, 85(1/2): 105-125.

[20] LIU W R. Analysis on the Development of Cryptosystems Against Quantum Computing Attacks[J]. Communication Technology, 2017, 50(5): 1054-1059.

[21] HARTMANIS J. Computers and Intractability: A Guide to the Theory of NP-Completeness[J]. SIAM Review, 1982, 24(1): 90-91.

[22] SUN S F, AU M H, LIU J K. RingCT 2. 0: A Compact Accumulator-Based(Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero[C]// Computer Security — ESORICS 2017. 2017: 456-474.

[23] YUEN T H, SUN S F, LIU J K, et al. RingCT 3. 0 for Blockchain Confidential Transaction: Shorter Size and Stronger Security[C]// Financial Cryptography and Data Securi-ty(FC 2020). 2020: 464-483.

[24] ALBERTO TORRES W A, STEINFELD R, SAKZAD A. Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain(Lattice RingCT v1. 0)[C]// Information Security and Privacy(ACISP 2018). 2018: 558-576.

[25] ALBERTO TORRES W, KUCHTA V, STEINFELD R, et al. Lattice RingCT V2. 0 with Multiple Input and Multiple Output Wallets[C]// Information Security and Privacy(ACISP 2019). 2019: 156-175.

HONG Xuan, born in 1982, Ph. D, professor. Her main research interests include blockchain technology, big data technology, cryptography and network security, etc.

YUAN Mengling, born in 1996, postgraduate. Her main research interests include cryptography and digital signatures.