计算机科学
COMPUTER SCIENCE

基于同态加密的区块链混币方案

王冬, 李政, 肖冰冰

引用本文

王冬, 李政, 肖冰冰. 基于同态加密的区块链混币方案[J]. 计算机科学, 2024, 51(3): 335-339.

WANG Dong, LI Zheng, XIAO Bingbing. Blockchain Coin Mixing Scheme Based on Homomorphic Encryption [J]. Computer Science, 2024, 51(3): 335-339.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230100059

基于同态加密的区块链混币方案

王 冬[1] 李 政[1,2] 肖冰冰[1,2]
1 河南大学软件学院 河南 开封 475001
2 河南省智能网络理论与关键技术国际联合实验室 河南 开封 475001
(Juliawdd@qq.com)

摘 要 区块链混币技术是一种保护交易隐私、实现交易的不可链接性的重要方案。然而,其结合了 Pedersen 承诺的验证过程,需要数百字节的空间开销,极大地降低了可用性。利用国密 SM2 算法、同态加密和混淆地址,提出了一种新的区块链混币方案。该方案通过使用 EC-ElGamal 半同态加密技术加密交易金额,在链上交易过程中完全隐藏交易金额,将隐藏金额后的交易进行两次验证和一次重随机化后发送到一次性的混淆地址中,打破交易发起方和接收方的联系,实现了交易的不可链接性和不可追踪性。所提方案能够有效提高交易数据隐私保护的强度,增强对分析攻击、密钥重放攻击和女巫攻击的抵抗能力,同时单次交易的空间占用减少了 82.25%,交易吞吐量显著提高。

关键词:区块链;混币;混淆地址;隐私保护
中图分类号 TP311.13

Blockchain Coin Mixing Scheme Based on Homomorphic Encryption

WANG Dong[1],LI Zheng[1,2] and XIAO Bingbing[1,2]
1 School of Software,Henan University,Kaifeng,Henan 475001,China
2 Henan International Joint Laboratory of Intelligent Network Theory and Key Technology,Kaifeng,Henan 475001,China

Abstract Coin mixing is important for protecting transaction privacy and realizing transaction unlinkability. However,hundreds of bytes of space overhead is necessary because of its verification process with pedersen commitment,which severely reduces its usability. A new coin mixing scheme is proposed by using SM2 algorithm,homomorphic encryption and stealth address technology in this paper. The on-chain transaction information is completely hide by using EC-ElGamal partially homomorphic encryption technology to encrypt the transaction value. Then the confidential transaction is sent to one-time stealth addresses after twice verification and once re-randomization,thus breaking the connection between the payer and payee of the transaction to achieve unlinkability and untraceability of the transaction. This scheme can severely increase the privacy degree of transaction and transaction per second(TPS) while 82.25% reduction in the size of one transaction is achieved. At the same time,it enhances the resistance to analysis attacks,key replay attacks and sybil attacks.

Keywords Blockchain,Coin mixing,Stealth address,Privacy protection

1 引言

区块链通过加密算法、共识机制、时间戳等技术手段,在分布式系统中实现了不依赖于某个信用中心的点对点交易、协调和协作,从而规避了中心化机构普遍存在的数据安全、协同效率和风险控制等问题[1-2],成为行业创新和建立数字化新生态的核心力量,受到政府、金融、物流、医疗、教育等多个行业的广泛关注。

然而,区块链的公开透明和全节点验证使其无法很好地保护隐私数据,因此自区块链诞生以来,隐私保护一直就是该领域需要解决的关键问题。目前大多数区块链系统是通过椭圆曲线加密(Elliptic Curves Cryptography,ECC)的不记名地址(假名,pseudonymity)来实现交易的匿名性,但是其隐私保护的强度仍然不能满足实际应用的需要,无法实现通信过程中的隐私性要求:1)不可链接性(Unlinkability),一个用户拥有多个账户时,攻击者从外部无法区分某些账户是否为同一人

到稿日期:2023-01-11 返修日期:2023-05-18
基金项目:国家自然科学基金面上项目(61872125);2023 年河南省高等学校重点科研项目(23A520035);南京大学计算机软件新技术国家重点实验室开放课题(KFKT2022B08)
This work was supported by the National Natural Science Foundation of China General Program(61872125),Colleges and Universities Key Research Project of Henan Province(23A520035) and Foundation of National Key Laboratory for Novel Software Technology, Nanjing University (KFKT2022B08).
通信作者:李政(Li992435997@163.com)

持有;2)不可追踪性(Untracability),对于任何交易,所有可能的发送方都是等可能的[3]。通过地址聚类和标签分析进行污点分析[4],画出用户的交易图,再通过社会工程学确认用户的身份。

为了提高区块链交易过程的隐私强度,更好地保护交易双方的身份信息,本文提出了一种新的混币方案。该方案利用同态加密技术在本地加密交易金额,能有效保护交易金额信息的隐私性,同时创新地利用乘法同态加密取代 Pedersen 承诺,不再使用 Commitment 进行数据验证,使得单次交易空间占用减少了 82.25%,之后将密文再次进行随机加密并输出到一次性混淆地址上,完全隐藏接收方的信息,从而实现了交易的不可链接性和不可追踪性。

2 相关工作

Maxwell 在 2013 年提出的 CoinJoin[5] 是最早的混币方案,该方案通过将多笔交易合并为一笔,混淆了交易参与者的身份,实现了交易的不可链接性,但交易金额仍暴露在网络中。自 CoinJoin 后,混币逐渐分为中心化混币和去中心化混币。

去中心化混币不需要可信的第三方,利用混币的参与者,通过部署在链上的智能合约或嵌在钱包中的混币脚本主动寻找参与者共同组成交易。其面临的主要问题在于难以自举,在交易发起阶段难以找到共同发起交易的参与者,无法达到协议安全运行的最低标准,使得参与者想要实现一次安全的混币所需的时间成本大大增加。典型的去中心化混币有 Tornado Cash[6], Coinshuffle[7] 和 Coinparty[8] 等。Tornado Cash 的信息存储在由所有参与者共同维护的链上,其最早部署在以太坊上,虽然也有拓展到其他链上,但因为使用智能合约,对于不具有图灵完备的链仍无法使用。Coinshuffle 及使用了 DC-Net 的 Coinshuffle++[7,9] 能够在每次混币失败后找出恶意节点,但代价是参与者发起交易时必须同时在线,而且只能发起特定金额的交易;Coinparty 在存在一定恶意节点的情况下也能实现有效混币,同时允许单笔混币交易。

中心化混币通过中心化的混币器,降低了自举的难度,参与者需要将货币发到第三方中间服务器上,由服务器将交易合并广播,存在第三方将隐私泄露的风险。典型代表为 Mixcoin[10] 和 Blindcoin[11] 等。Mixcoin 通过设计随机的手续费机制,随机将部分用户的混币金额当作该笔混币交易所有参与者的手续费,通过生成随机数,增强混币的外部安全性,一定程度上实现了不可伪造,并可以监督混币运营商是否存在盗窃行为。Blindcoin 在 Mixcoin 的基础上使用了盲签名生成数字签名作为 Commitment,隐藏交易输出地址,进一步提高了混币过程的隐私性,但其只能发起特定金额的交易,且对恶意行为的追责效率过低。

为了同时解决去中心化混币难以自举和中心化混币的中心化问题,研究者试图构建独立运行的中心化节点。如去信任第三方平台的去中心化链下混币协议 TumbleBit[12] 使用了 2PC 和 LOE 模型,以及以牺牲效率为代价实现不可伪造性的 A^2L^+ 和 A^2L^{UC}[13]。此外,还有很多研究者从整体出发,构建了更具安全性的匿名项目,例如所有交易都参与混币的 Dash[14]、使用环签名机制实现混币的 Monero[15]。Wang 等[16]将聚合签名和混币结合,实现了全匿名区块链,但依旧存在验证速率过低的问题。

本文设计了一种新的混币方案,构建了行为受限的 Hub 节点,在交易发起前后加密交易信息,在网络中隐藏交易金额,实现交易的不可链接性,增强抗密钥重放攻击;利用 EC-ElGamal 的加法同态加密特性保证混币前后的输入和输出一致;使用乘法同态加密验证交易金额,不需额外空间存储 Commitment 验证信息。最后,将混币的输入地址设置为一次性地址,实现不可追踪性。

3 预备知识

E_p:有限域上由 a 和 b 定义的一条椭圆曲线:$y^2=x^3+ax+b, 4a^3+27b^2\neq 0$;$F_q$:包含 q 个元素的素域;$E(F_q)$:F_q 上椭圆曲线 E_p 的所有有理点(包括无穷远点)组成的集合;L:椭圆曲线 E_p 的基点;n:基点 L 的阶;G:椭圆曲线 E_p 上除无穷远点之外的一个点;Q:k 个 G 相加被称为 G 的 k 倍点运算,记作 $Q=[k]G$;r:随机数;p:大素数;R:明文交易信息;$E:=(C_1,C_2)$:明文 R 经 EC-ElGamal 加密后的密文;Alice, Bob, Hub:系统的参与者,默认 Alice 是发送方,Bob 是接收方,Hub 是生成混币交易的脚本;$((a,A),(b,B),(sk,PK))$:用户的密钥,其中(a,A)为用户的钱包密钥对,(b,B)为生成混淆地址所需的密钥对,(sk,PK)为 *EC-ElGamal* 密钥对;(d,D):生成混淆地址时产生的交易密钥对;P,P':混淆地址和验证地址;$TXin,TXout$:交易输入、交易输出;$Cin,Cout$:交易输入、输出密文。

SM2[17] 椭圆曲线公钥密码算法的安全性基于椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem, ECDLP)。ECDLP:已知椭圆曲线 $E(F_q)$、阶为 n 的点 $G\in E(F_q)$ 及 $Q\in\langle p\rangle$,椭圆曲线离散对数问题是指确定整数 $l\in[0,n-1]$,使得 $Q=[l]p$ 成立。

ElGamal 加密算法[18] 是由迪菲-赫尔曼密钥交换协议演变而来的非对称加密算法。EC-ElGamal 加密算法将 ElGamal 移植到椭圆曲线上实现,属于 ECC 范畴,具有同态加密特性,支持椭圆曲线点加⊕、点乘⊗运算。

4 方案设计

本文提出的混币方案主要分为 3 个阶段:链下构建交易密文、交易广播、交易接收。

4.1 链下构建交易密文

本阶段主要使用 EC-ElGamal 加密方案 Π_{EC} 和一次性地址生成算法 Π_{SA} 生成交易的密态金额和输出地址。加密后的交易金额在整个交易过程中都不可见,有效保护了交易金额信息的隐私性,可抵抗对区块链交易数据的分析攻击,增强混币的内部隐私性。

$\Pi_{EC}:=(KeyGen,Encrypt,Decrypt)$

$\Pi_{SA}:=(kGen,SAGen,SAMatch)$

Step1 交易接收方 Bob 使用 $keyGen()$ 和 $kGen()$ 创建自己的密钥对$((a,A),(b,B),(sk,PK))$,并将公钥广播。

Step2 交易发起方 Alice 使用 PK 加密交易金额 R 生成

密态金额 $E \leftarrow Encrypto()$。

$Encrypt := \{(C_1, C_2) | C_1 \leftarrow rG, C_2 \leftarrow R + rPK\}$

在交易金额变为密文后，可有效抵抗对区块链交易数据的分析攻击。

Step3　Alice 使用公钥 B 生成一次性混淆地址 $P \leftarrow SA\text{-}Gen()$，以此作为 Bob 此次交易的一次性接收地址。

$SA := Hash(dA)G + B$

在之后的交易过程中，Bob 的真实身份会被隐藏在一次性地址之后，即使是 Hub 节点也无法识别。

Step4　Alice 将 E，P 和生成一次性地址的公钥 $D \leftarrow dG$ 发送给 Hub 节点。

4.2　交易验证广播

本方案利用 EC-ElGamal 的乘法同态和加法同态特性，创新地构建了一个含有两次交易验证和一次重随机加密的 Hub 节点：Π_{Hub}，从而保证 Hub 接收到的交易金额在一个合理的范围内（大于等于 0 且小于当前货币总发行量 Max），不会出现非法交易。

$\Pi_{Hub} := (Vf_m, Vf_a, reRan)$

Step1　Hub 接收来自 Alice 的交易信息。

Step2　该阶段设计了一种新的交易合法性验证方法，Hub 使用乘法同态加密验证函数 $Vf_m := E_1 \otimes E_2$ 进行验证。当 $Vf_m((C_1, C_2), -1) > 0$ 时，说明交易输入输出金额均为非负数；利用加法同态验证函数 $Vf_a := E_1 \oplus E_2$ 验证 $Vf_a((C_1, C_2), -Max) < 0$，小于 Max 时符合安全范围。本方案利用同态加密验证取代了臃肿的 Pedersen 承诺和零知识证明方案，不需要额外生成 Commitment，空间占用相较于 Wang 等[16]的方案减少了 208 B，相较于 Bulletproof[19]方案减少了 626 B。

Step3　Π_{Hub} 利用加法同态加密特性再次验证，以此来识别交易的输入与输出总额是否发生变化。

$$\sum_{i=1}^{x} Cin_i \stackrel{?}{=} \sum_{i=1}^{x} Cout_i$$

由于随机化的交易金额密文对 Hub 依旧保持着不可见的状态，因此，本方案设计了 $Vf_a()$ 验证来防止出现交易输入与输出不一致的恶意交易行为。

Step4　Alice 的交易信息通过验证之后，Hub 会进行一次重随机加密 $reRan() := E \otimes r$ 以增强交易的安全性。重随机加密后的密文使得攻击者无法简单地通过分析混币前后的密文联系交易的输入和输出，增强了混币的外部隐私性。

Step5　Hub 将多笔交易合并为一笔混合交易广播。

4.3　交易接收

Step1　Bob 使用 $x \leftarrow SAMatch()$ 查找属于自己的交易输出地址 P。

$SAmatch() := p \stackrel{?}{=} Hash(aD)G + bG$ /* $\stackrel{?}{=}$ 意为是否相等 */

Step2　Bob 运行解密函数，得到交易金额明文 $R \leftarrow Decrypt()$。

如果 Bob 想要借助交易的匿名性来否认这笔交易，Alice 可以公开 d 来打破这笔交易的匿名性，使得任何人都可以验证该交易，且不会影响到其他交易输入与输出的匿名性。

4.4　方案算法描述

该方案算法描述如算法 1 所示。

算法 1　交易生成与验证算法

输入：椭圆曲线 E_p 和 E_p 上的点 G；交易输入与输出金额 TXin，TXout

输出：交易输出

1. /* Alice 链下构建交易密文 */
2. a，b，$sk \stackrel{\$}{\leftarrow} E_p$ /* Bob 随机选取私钥 */
3. A=aG，B=bG，PK=skG /* Bob 根据私钥计算公钥 */
4. Get(PK，A，B) /* Alice 获取 Bob 的公钥对 */
5. r，$d \stackrel{\$}{\leftarrow} E_p$，D=dG /* Alice 生成 Bob 的混淆地址密钥对 */
6. P=Hash(dA)G+B /* Alice 生成 Bob 的混淆地址 */
7. $Cin_{1\sim x}$=Encrypt($Rin_{1\sim x}$，r)
   $Cout_{1\sim x}$=Encrypt($Rout_{1\sim x}$，r) /* Alice 加密交易的输入和输出金额，使其转换为密态金额 */
8. Send() /* Alice 将密态金额和混淆地址传送给 Hub */
9. /* Hub 验证交易 */
10. if($Vf_m(Cout_{1\sim x}, -1) \geqslant 0$ && $Vf_a((C_1, C_2), -Max) < 0$) then
    tag=1
    end if /* Hub 验证输出密态金额是否在合理范围，通过 tag=1，不通过 tag=0 */
11. if($\sum_{i=1}^{x} Cin_i = \sum_{i=1}^{x} Cout_i$) then
    tag=1
    end if /* Hub 验证输入输出是否相等，通过 tag=1，不通过 tag=0 */
12. if(tag==1) then
    $Vf_m(Cout_{1\sim x}, r_i)$
    end if /* 两次验证通过，tag=1，Hub 将这笔交易的输出和随机数重新进行乘法同态加密 */
13. Broadcast() /* Hub 广播该交易 */
14. /* Bob 匹配接收交易 */
15. P′=Hash(aD)G+bG /* Bob 根据 D 计算对应的混淆地址 */
16. $P \stackrel{?}{=} P'$ /* Bob 验证 P 是否与 P′相等，相等则打开交易 */

交易生成、广播、加解密算法流程如图 1 所示：Bob 生成公钥给 Alice，然后参与到混币交易中进行 Verify、Re-Random、Broadcast 隐蔽传输至 Bob 的一次性地址，从而实现交易隐藏。

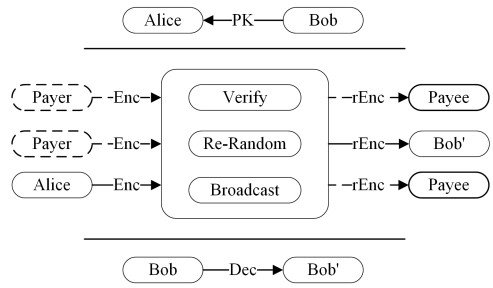

图 1　方案流程图

Fig. 1　Protocol flowchart

5　性能分析

本文所使用的 SM2 国密算法和 EC-ElGamal 加密算法主要使用了 Alibaba 开发的开源密码学和通信安全协议基础库“铜锁/Tongsuo”[20]。SM2 椭圆曲线 $y^2 = x^3 + ax + b$ 使用了推荐的椭圆曲线参数。实验环境为 Intel(R) Core(TM) i5-

8400 CPU @ 2.80 GHz, NVIDIA GeForce GTX 1060, 16.0GB RAM, Windows10 22H2 系统，数据来自比特币链上真实数据[21]。

5.1 效率分析

过去一年间(2021-08-17－2022-08-16)，比特币区块链的平均区块大小约为 1.13 MB，平均每个区块包含 1 753 笔交易[21]，扣除区块头约占用空间 100 B，每个交易的大小约为 676 B，平均每笔交易有 3.97 个输入和输出；在极限情况下，只有 1 个输入时有 11.42 个输出，有 5.17 个输入时只有 1 个输出(不考虑 MS 和 Segwit 等情况)。将这些数据在不同的匿名方案之间进行对比，如表 1 所列。

表 1 签名与密文长度

Table 1 Signature and ciphertext length

	SigLength/B	CipherValue/B	TxsNumber 3.97in-3.97out	TxsNumber 1in-11.42out	TxsNumber 5.17in-1out
Maxwell[22]	$(N+1)*64$	33	1 258	870	1 523
Wang 等[23]	64	512	215	90	475
Wang 等[16]	64	256	714	331	1 310
Ours	64	48	1 369	1 038	1 563

通过比较表 1 中各方案在不同交易输入与输出数量时的区块容量可知，文中方案的签名长度显著缩短，有效增加了单个区块所能容纳的交易数量，提高了交易吞吐量。

在数字签名长度上，Maxwell[22] 使用了 Borromean 环签名。构建签名时的环越多，安全性越高，空间开销越大，当在 n 个环上使用 N 个验证密钥进行签名时，签名长度为 $N+1$。Pedersen 承诺还需要交易发起方和接收方建立额外的通信信道，增加了通信开销，而且无法实现不可追踪性。相比于 Maxwell 的方案，本方案将原来的椭圆曲线参数 Secp256k1：$y^2=x^3+7$ 改为 SM2 推荐的椭圆曲线参数，达到了安全可控范围内的最短长度，相同签名长度下具有更高的安全强度。

在密文长度上，Wang 等[23] 和 Wang 等[16] 分别使用 Paillier 同态加密和 BGN06 加密构造了复杂的交易隐私保护方案，达到了较好的匿名效果，但却大大增加了区块的交易数据大小，同时存在验证速率过低的问题，而且同样需要额外信道来传输 Commitment。本方案采用的 EC-ElGamal 加密方案的密文是明文的两倍，虽然引进了混淆地址，需要使用空间传输交易公钥 D，即 $length=2*Value+D$，但得益于所设计的乘法同态加密验证方案，相比于使用了零知识证明和 Pedersen 承诺的Wang 等[23] 和 Wang 等[16] 方案所产生的 512B 和 256B 密文，本文方案在保证相同的安全性的情况下，仅产生了 48B 密文，空间开销显著下降。

签名长度和密文长度的降低，使得单个区块所能容纳的交易数量显著增加，相比于同类型的 Wang 等[23] 和 Wang 等[16] 方案，在交易输入输出数量相等、交易输入数量为 1 和交易输出数量为 1 的极限情况下，所能容纳的交易数量分别提升了 536.7%，1 053.3%，229% 和 91.7%，213.5%，19.3%；相比于 Maxwell[22] 的明文方案，本方案的交易量有一定提升。

在时间开销上，本方案为了实现乘法同态加密验证，增加了负数解密。负数解密时，构建解密表、查询解密表和点运算时间开销较大，导致本方案在时间开销上相较于其他方案并无明显减少，这也是需要进一步改进的地方。

5.2 安全性分析

在所提方案中，每个参与者有 3 对密钥((a,A)，(b,B)，(sk,PK))，其中(a,A)，(b,B)由 $kGen()$ 函数产生，其安全性依赖于哈希难题的强度。本文方案采用 SHA256 算法。根据 NIST[24] 按照当前硬件发展推荐的密钥长度标准，SHA256 算法能够满足区块链当前的安全要求。(sk,PK)则是 EC-ElGamal 加密算法的密钥对，ElGamal 加密算法基于 DLP 难题，符合 CPA 安全。

混币过程第二阶段的加法同态特性和乘法同态特性主要是在椭圆曲线上做点加⊕和点乘⊗运算，根据椭圆曲线的加法阶数难求问题，在椭圆曲线群上运行⊕和⊗运算时，其逆运算求解是困难的。

对于发起的交易仅有一个交易输入和一个交易输出时，因为加密后的密文往往比作为明文的交易金额更具独特性，如果发起单对单交易，很容易通过对比混币前后的密文来判断输入和输出之间的对应关系。本方案采取了重加密策略，即将加密信息再次加密，彻底切断交易发起方和接收方的联系。由于每个新的混淆地址都是根据原有的地址产生，因此不必担心出现地址复用的问题[25]。

当非本次混币的参与者想要打破交易的匿名性，获取交易信息时，由于所有的交易金额信息都为通过 Π_{EC} 加密后的密态金额，输出地址都为根据 Bob 钱包地址产生的无任何记录的一次性地址，攻击者无法从中获得任何有效信息，实现了交易的不可追踪性。

当混币过程的参与者存在恶意攻击者试图打破混币的匿名性，获得其他参与者的交易信息时，由于交易合并过程由 Hub 节点完成，因此每个参与者仅知道自己的交易信息，无法得知其他节点的交易信息；而且混币交易具有正外部性[26]，即每个参与者的加入都会增强此次混币交易的安全性，参与人数越多，匿名集越大，系统的安全性越高，抗分析攻击能力和不可链接性越强。

当多个恶意攻击者或者一个恶意节点发起女巫攻击参与到一次混币过程中时，参与者的安全性随恶意攻击者数量的增加而逐渐降低。极端情况下，即 n 个参与者中有 $n-1$ 个攻击者时，唯一一个诚实节点的交易输出和输入之间的映射关系会被暴露，但即便如此，交易金额仍处于密文状态，Bob 的一次性混淆地址，暴露的信息仅为原来就属于公开信息的 Alice 地址。因此，本方案具有较好的内部隐私性和抗女巫攻击能力。

表 2 分析了当前主流混币方案的特点，可以看出当前混币机制主要面临的问题在于内部隐私性和抗女巫攻击能力

不足。本方案通过加密交易金额的方式实现了内部隐私性，增强了抗女巫攻击能力。

表 2　混币方案的安全性对比

Table 2　Securitycomparison of mixing scheme

	不可追踪性	不可链接性	外部隐私性	内部隐私性	资产安全性	抗女巫攻击
CoinJoin[10]	N	Y	Y	N	Y	N
Coinshuffer[12]	Y	Y	Y	Y	Y	N
Mixcoin[15]	N	Y	Y	N	Y	Y
TumbleBit[16]	Y	Y	Y	Y	Y	N
Ours	Y	Y	Y	Y	Y	Y

结束语　本文设计的新型混币方案，结合了同态加密算法发起验证区块链的匿名交易，保护了用户的交易隐私和身份隐私，实现了不可追踪性和不可链接性。相较于 Wang 等[16]提出的方案，本文方案空间占用减少了 208 B，在交易输入和输出数量相等的情况下，每个区块能够多容纳 91.7% 的交易，提高了匿名区块链的交易速率。

下一步的工作将主要集中在扩充现有方案和迭代现有方案模块，压缩解密表长度，平衡时间开销与空间开销，将其控制在一个合理的范围，以期进一步提高方案的性能和安全性。

参 考 文 献

[1] SATOSHI N. Bitcoin: A Peer-to-Peer Electronic Cash System [OL]. [2008-06-02]. https://bitcoin.org/bitvoin.pdf.

[2] BUTERIN V. A next-generation smart contract and decentralized application platform[OL]. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[3] ZHANG A, BAI X Y. Survey of research and practices on blockchain privacy protection[J]. Journal of Software, 2020, 31(5): 1406-1434.

[4] HARRIGAN M, FRETTER C. The Unreasonable Effectiveness of Address Clustering[J]. arXiv: 1605.06369v3, 2016.

[5] MAXWELL G. CoinJoin: Bitcoin privacy for the real world [C]// Post on Bitcoin Forum. 2013.

[6] PERTSEV A, SEMENOV R, STORM R. Tornado Cash Privacy Solution Version 1.4[OL]. https://berkeley-defi.github.io/assets/material/Tornado%20Cash%20Whitepaper.pdf.

[7] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin[C]// European Symposium on Research in Computer Security(ESORICS). New York: Springer-Verlag, 2014.

[8] ZIEGELDORF J H, GROSSMANN F, HENZE M, et al. Coinparty: Secure multi-party mixing of bitcoins[C]// Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. 2015: 75-86.

[9] RUFFING T, MORENO-SANCHEZ P. ValueShuffle: Mixing Confidential Transactions for Comprehensive Transaction Privacy in Bitcoin[C]// International Conference on Financial Cryptography and Data Security. 2017.

[10] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: Anonymity for bitcoin with accountable mixes[C]// International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2014: 486-504.

[11] VALENTA L, ROWAN B. Blindcoin: Blinded, accountable mixes for bitcoin[C]// International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2015: 112-126.

[12] HEILMAN E, ALSHENIBR L, BALDIMTSI F, et al. TumbleBit: an untrusted Bitcoin-compatible anonymous payment hub [C]// Network & Distributed System Security Symposium. 2017.

[13] GLAESER N, MAFFEI M, MALAVOLTA G, et al. Foundations of coin mixing services[C]// Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022: 1259-1273.

[14] DUFFIELD E, DIAZ D. Dash: A payments-focused cryptocurrency [DB/OL]. https://github.com/dashpay/dash/wiki/Whitepaper.

[15] RUFFING T, MORENO-SANCHEZ P, KATE A. P2P Mixing and Unlinkable Bitcoin Transactions[C]// Network & Distributed System Security Symposium. 2017.

[16] WANG Z Y, LIU J W. Full Anonymous Blockchain Based on Aggregate Signature and Confidential Transaction[J]. Journal of Computer Research and Development, 2018, 55(10): 14.

[17] GB/T 32918.4-2016[S/OL]. 北京. 国家密码管理局. https://oscca.gov.cn/sca/xxgk/2010-12/17/content_1002386.shtml.

[18] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.

[19] BUNZ B, BOOTLE J, BONEH D, et al. Bulletproofs: Short Proofs for Confidential Transactions and More[C]// IEEE Symposium on Security and Privacy. IEEE, 2018: 315-334.

[20] ALIBABA. Tongsuo[EB/OL]. https://tongsuo.readthedocs.io/zh/latest/.

[21] BLOCKCHAIR. Blockchair[DB/OL]. https://blockchair.com/.

[22] MAXWELL G. Confidential transactions (2015)[EB/OL]. https://www.weusecoins.com/confidential-transactions/.

[23] WANG Q, QIN B, HU J, et al. Preserving transaction privacy in bitcoin[J]. Future Generation Computer Systems, 2020, 107: 793-804.

[24] NIST. Recommendation forKey Management [OL]. https://doi.org/10.6028/NIST.SP.800-57pt1r5.

[25] WU L, HU Y, ZHOU Y, et al. Towards understanding and demystifying Bitcoin mixing services[C]// Proceedings of the Web Conference 2021. 2021: 33-44.

[26] MÖSER M, BÖHME R. Join me on a market for anonymity [C]// Workshop on Privacy in the Electronic Society. 2016.

WANG Dong, born in 1977, Ph.D, professor, is a member of CCF (No. 22542S). Her main research interest is blockchain and its applications.

LI Zheng, born in 1996, postgraduate. His main research interests include cryptography and Blockchain.

（责任编辑：柯颖）