

## 按需披露的区块链隐私保护机制

李少卓, 王娜, 杜学绘

(信息工程大学, 河南 郑州 450000)

**摘要:** 隐私保护已经成为区块链技术真正从理论到现实应用必须解决的关键问题。实际应用中存在一种按需披露的隐私保护需求, 受组播安全通信机制的启发, 提出一种按需披露的区块链隐私保护机制 (PPM-ODB, privacy protection mechanism of on-demand disclosure on blockchain)。该机制通过改进基于 RSA 的匿名多接收者加密方案来实现隐私信息一对多的加解密、知情者的匿名性保护和隐私泄露的可追溯, 通过采用 Quorum 链隐私保护机制来实现密钥在隐私信息拥有者和知情者间的安全高效分发。实验证明了 PPM-ODB 机制可保证隐私数据的保密性, 及其在时间和存储开销上的优越性, 并建议知情者的个数少于 100, 以获得良好的用户体验。

**关键词:** 区块链; 隐私保护; Quorum; 匿名多接收者方案

**中图分类号:** TP309

**文献标识码:** A

**doi:** 10.11959/j.issn.2096-109x.2020033

## Privacy protection mechanism of on-demand disclosure on blockchain

LI Shaozhuo, WANG Na, DU Xuehui

Information Engineering University, Zhengzhou 450000, China

**Abstract:** Privacy protection has become the key problem that blockchain technology must solve from theory to practice. There is a privacy protection requirement of on-demand disclosure in practical applications. Inspired by multicast secure communication mechanism, a privacy protection mechanism of on-demand disclosure on blockchain was proposed. This mechanism improves the RSA based anonymous multi receiver encryption scheme to realize the disclosure of the private data on the blockchain only to the permitted informed, the anonymity protection of the informed and the traceability of the privacy disclosure. The Quorum blockchain privacy protection mechanism is adopted to realize the safe and efficient distribution of the key between the owner of the private information and

收稿日期: 2020-03-07; 修回日期: 2020-04-30

通信作者: 李少卓, 494187944@qq.com

基金项目: 国家重点研发计划(2018YFB0803603, 2016YFB0501901); 国家自然科学基金(61502531, 61702550, 61802436)

**Foundation Items:** The National Key R&D Program of China (2018YFB0803603, 2016YFB0501901), The National Natural Science Foundation of China (61502531, 61702550, 61802436)

论文引用格式: 李少卓, 王娜, 杜学绘. 按需披露的区块链隐私保护机制[J]. 网络与信息安全学报, 2020, 6(3): 19-29.

LI S Z, WANG N, DU X H. Privacy protection mechanism of on-demand disclosure on blockchain[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 19-29.

the informed. Finally, it is proved that PPM-ODB mechanism can guarantee the privacy of privacy data and its superiority in time and storage cost, and it is suggested that the number of informed people should be less than 100 to obtain a good user experience.

**Key words:** blockchain, privacy protection, Quorum, anonymous multi receiver encryption scheme

## 1 引言

区块链是一种去中心化、去信任化的分布式账本技术,是利用块链式数据结构来验证与存储数据,利用分布式节点共识算法来生成和更新数据,利用密码学技术来保证数据传输和访问的安全,利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式,具有去中心化、开放性、防篡改、匿名性、可追溯性等特点<sup>[1]</sup>。目前,区块链技术在金融、医疗、物联网、电子政务、食品药品溯源、身份认证等领域的应用已经成为人们关注和研究的热点。

但是,区块链开放性的技术特点和公共总账的本质使其在应用中面临着用户隐私泄露的风险。隐私保护已经成为区块链技术真正从理论到现实应用必须解决的关键问题<sup>[2]</sup>。目前,区块链隐私保护技术分为用户匿名技术和链上数据隐私保护技术两类。用户匿名技术是为了解决攻击者通过分析链上用户的全部交易信息而导致的用户真实身份泄露问题<sup>[3]</sup>。典型方案包括达世币<sup>[4]</sup>,其引入链式混合和盲化技术,通过混合多个用户来实现用户匿名;门罗币<sup>[5]</sup>,其使用隐藏地址和环签名的方法来实现交易地址的隐藏;零钞<sup>[6]</sup>,其使用 zkSNARK 零知识证明的方法来实现匿名性。链上数据隐私保护技术是为了解决链上隐私数据的泄露问题,典型技术包括实现了交易双方间交易数据隐私保护的 Zcoin<sup>[7]</sup>和 Quorum<sup>[8]</sup>隐私保护技术;在基于同态加密和区块链技术的车联网隐私保护方案<sup>[9]</sup>中,设计了基于同态加密的区块,使用 Paillier 加密算法<sup>[10]</sup>对隐私数据进行加密,能够完成数据在密文状态下的处理。

本文发现实际应用中存在一种按需披露的隐私保护需求。例如,在医疗区块链应用中,病人的病历信息只能披露给为其看病的医生和护士,对于其他医生和护士而言该病人的病历信息是保密的。按需披露隐私保护具体包含以

下需求:① 链上的隐私数据只披露于许可知情者,对于其他用户而言是保密、非公开的;② 知情者的匿名性,即保证知情者在不暴露身份的情况下解密隐私密文,因为知情者身份、职业等背景信息的暴露仍然会在一定程度上带来隐私数据的泄露;③ 隐私泄露的可追溯性,即在用户的隐私信息泄露后,能够追溯到泄露的知情者。

目前的链上数据隐私保护技术只能实现一次交易中交易双方间的一对一的交易数据保护,难以有效地解决按需披露隐私保护问题。按需披露的隐私保护本质上是一对多的隐私数据保护,如果采用目前的链上数据隐私保护技术,隐私信息拥有者节点需要对多个知情者节点分别加密隐私数据、分发隐私数据,只需在链上存储一次的隐私数据会在链上以不同形式被重复记录,显著增加了存储开销。而且,目前的链上数据隐私保护技术不能同时保证知情者的匿名性和隐私泄露的可追溯性。

按需披露隐私保护与安全组播通信比较相似,本质上都是实现一对多的消息安全传输,不同之处在于安全组播通信不需要实现隐私泄露的可追溯性。基于此,本文提出了一种按需披露的区块链隐私保护机制(PPM-ODB),该机制通过改进安全组播通信中的基于 RSA 的匿名多接收者加密方案,实现了隐私信息一对多的加解密、知情者的匿名性保护和隐私泄露的可追溯,然后通过采用 Quorum 链隐私保护机制实现了密钥在隐私信息拥有者和知情者间的安全高效分发,从而实现了链上数据的按需披露隐私保护。最后,本文分析了 PPM-ODB 机制的安全性和性能,证明了该机制可保证隐私信息的保密性,及相较于 Quorum 链在按需披露隐私保护时间和存储开销上的优越性,且为获得良好的用户体验,建议知情者的个数少于 100。总结来看,本文主要作出了以下贡献。

1) 深入分析了区块链实际应用中存在的按

需披露隐私保护需求，提出了一种按需披露的区块链隐私保护机制，实现了隐私信息拥有者和多个知情者间密钥的安全高效分发和隐私信息的安全披露。

2) 改进了基于 RSA 的匿名多接收者加密方案，通过将隐私信息与知情者身份绑定，实现了隐私信息一对多的加解密、知情者的匿名性和隐私泄露的可追溯。

3) 证明了 PPM-ODB 机制可保证隐私信息的保密性，实验表明在实现按需披露隐私保护的时间和存储开销上，PPM-ODB 机制优于 Quorum 链，并建议知情者的个数少于 100，以获得良好的用户体验。

## 2 相关研究

### 2.1 基于 RSA 的匿名多接收者加密方案

目前的匿名多接收者加密方案主要用于提供组播通信中传输消息的保密性和接收者匿名性的保护。即在采用了匿名多接收者加密方案的组播通信中，发送者通过加密明文消息得到唯一的密文，并将密文发送给所有的接收者，每个接收者在收到密文后，可在不暴露身份的情况下分别独立地解密密文获得明文消息。

在组播安全通信的应用场景下，匿名多接收者加密方案多采用基于身份的密码体制实现<sup>[11-18]</sup>。因为该密码体制不需要数字证书，用户的公钥通过用户的身份信息获得且只与用户的身份信息相关，从而避免了公钥基础设施（PKI, public key infrastructure）的部署和管理等问题，能够更好地满足组播通信的安全需求。

因为区块链本身采用了 RSA 算法，链中节点都已拥有公私钥对，所以本文对基于 RSA 的匿名多接收者加密方案<sup>[19]</sup>进行了研究。该方案基于中国剩余定理使采用不同的公私钥对可产生唯一的密文，并且在把密文发送给所有的接收者后，拥有相关私钥的接收者可以对密文进行解密，在这个过程中没有用到任何与接收者相关的身份信息，从而保证了接收者的匿名性。

下面对中国剩余定理的原理进行阐述。

设  $m_1, m_2, \dots, m_k$  为两两互素的  $k$  个正整数，其中  $k \geq 2$ ，则同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases} \quad (1)$$

有整数解，并且在模  $M = m_1 m_2 \dots m_k$ ， $1 \leq i \leq k$  的情况下有唯一解，解为

$$x \equiv M_1 b_1 M'_1 + M_2 b_2 M'_2 + \dots + M_k b_k M'_k \pmod{M} \quad (2)$$

其中， $M_i M'_i \equiv 1 \pmod{m_i}$ ， $M_i \equiv \frac{M}{m_i}$ ， $i = 1, 2, \dots, k$ 。

基于 RSA 的匿名多接收者加密方案的详细过程如下（假设存在  $n$  个接收者）。

1) 密钥生成阶段：分别生成  $n$  个接收者的 RSA 公私钥对，要保证生成的  $n$  对公私钥中的  $N_i$  两两互素（ $1 \leq i \leq n$ ），满足中国剩余定理所需条件。

2) 加密阶段：设所需加密的消息为  $M$ ，并且保证  $0 < M < N'$ ，其中  $N'$  为  $\{N_1, N_2, \dots, N_n\}$  中最小的模值，首先，发送者  $S$  计算  $N = N_1 N_2 \dots N_n$  和

$$\begin{aligned} c_1 &= M^{e_1} \pmod{N_1}; \\ c_2 &= M^{e_2} \pmod{N_2}; \\ &\vdots \\ c_n &= M^{e_n} \pmod{N_n} \end{aligned} \quad (3)$$

根据中国剩余定理可知，下面这个方程组有公共解  $C$ 。

$$\begin{aligned} C &= c_1 \pmod{N_1}; \\ C &= c_2 \pmod{N_2}; \\ &\vdots \\ C &= c_n \pmod{N_n} \end{aligned} \quad (4)$$

然后，发送者  $S$  给所有接收者发送消息  $M$  的密文  $C$ 。

3) 解密阶段：当接收者  $U_i$  收到密文  $C$  后，首先利用自己的公钥  $N_i$  把密文还原为  $c_i = C \pmod{N_i}$ ，然后用自己的私钥  $d_i$  解密  $c_i$  获得明文消息  $M$ ，即  $M = c_i^{d_i} = (M^{e_i})^{d_i} \pmod{N_i}$ （ $1 \leq i \leq n$ ）。因为  $0 < M < N'$ ，所以所有接收者都可以得到相同的消息  $M$ 。

### 2.2 Quorum 链隐私保护机制

Quorum 链是由摩根大通开发的企业级分布式账本和智能合约平台<sup>[6]</sup>，它在以太坊的基础上增加了对交易数据的隐私性保护，适用于需要高速交易以及高吞吐量处理联盟间隐私交易的应用



值, 得到  $H(E_{K_s}(\text{PriInfo}))$ ;

④ 使用步骤 1) 中 privateFor 字段中记录的 Party A 和 Party B 的公钥分别加密  $K_s$ , 生成一个新的数组 EnArray: ["key\_encrypted\_by\_publickey\_A", "key\_encrypted\_by\_publickey\_B"];

⑤ 将  $E_{K_s}(\text{PriInfo})$ 、 $H(E_{K_s}(\text{PriInfo}))$ 、EnArray 返回给 Transaction Manager A。

5) Transaction Manager A 把  $E_{K_s}(\text{PriInfo})$  和 EnArray 保存在本地, 以  $H(E_{K_s}(\text{PriInfo}))$  作为索引, 并将  $E_{K_s}(\text{PriInfo})$ 、 $H(E_{K_s}(\text{PriInfo}))$ 、EnArray 发送给 Transaction Manager B。Transaction Manager B 收到后, 将  $E_{K_s}(\text{PriInfo})$  和 EnArray 保存在本地, 以  $H(E_{K_s}(\text{PriInfo}))$  作为索引, 并向 Transaction Manager A 返回一个成功的回执。

6) Transaction Manager A 收到成功回执后, 将  $H(E_{K_s}(\text{PriInfo}))$  发送给 Quorum Node A。Quorum Node A 设置隐私交易值  $\text{PriTX} = H(E_{K_s}(\text{PriInfo}))$ , 将 PriTX 的  $V$  值设置为 37 或者 38 (37 或 38 是隐私交易的标识)。

7) Quorum Node A 将隐私交易 PriTX 通过 P2P 方式广播给整个网络。

8) PriTX 被记入当前区块链中。

9) 当其他节点发现某次交易的  $V$  值为 37 或者 38 时, 会认定该交易为隐私交易, 然后将隐私交易值传给自己的 Transaction Manager。以 Party C 为例, 因为 Party C 没有参与该隐私交易, 所以 Transaction Manager C 根据隐私交易值无法检索到相应的加密隐私数据。查找失败后, Transaction Manager C 会返回给 Quorum Node C 一个 TX Not Found 的回执, Quorum Node C 就不会更新自己的 Private State。

10) 对于参与隐私交易的 Party B 来说, Transaction Manager B 可根据隐私交易值  $H(E_{K_s}(\text{PriInfo}))$  查找到  $E_{K_s}(\text{PriInfo})$  和 EnArray, 然后向 Enclave B 发出解密请求。

11) Enclave B 收到解密请求后, 利用 Party B 的私钥来解密 EnArray, 获得对称密钥  $K_s$ , 然后利用  $K_s$  解密  $E_{K_s}(\text{PriInfo})$ , 解密成功后将明文 PriInfo 发送给 Transaction Manager B。

12) Transaction Manager B 收到明文 PriInfo 后, 通过 EVM 执行 PriInfo 的内容, 执行后将执

行结果返回给 Quorum Node B, 并更新 Quorum Node B 的 Private State, 完成完整的隐私交易过程。

### 3 按需披露的隐私保护机制

按需披露的隐私保护机制 PPM-ODB 流程如图 2 所示, 它分为信任关系建立、隐私信息加密、隐私信息解密与追溯 3 个阶段。在这个过程中, 本文对 Quorum 链隐私保护机制进行了一定的修改来保证 PPM-ODB 机制的实现, 在步骤 1) 中将  $\text{PriInfo}_i$  中隐私交易数据替换为披露公私钥, 在步骤 7) 中增加了含有隐私密文的证书的网络广播, 并增加了步骤 13), 向 Party B 的用户传输对应的密钥交易  $\text{TX}_i$  和含有隐私密文的证书 Certificate。

下面将详细阐述 3 个阶段的原理。

#### 3.1 信任关系建立

为了实现隐私信息的按需披露, 首先需要在隐私信息拥有者 (下文中称为发送者  $S$ ) 和  $n$  个知情者之间建立信任关系, 也就是完成隐私信息拥有者和知情者间的密钥分发工作, 这一过程采用 Quorum 链完成。

假设在信任关系建立之前, 每个节点都已拥有一个 RSA 公私钥对, 私钥节点自己保存, 公钥公开。该假设与实际情况相符合, 每个区块链节点都拥有一个 RSA 公私钥对, 为了和后面区分, 将其称为节点公私钥对。

信任关系建立的过程如下。

1) 发送者  $S$  分别为  $n$  个知情者生成披露公私钥  $(d_i, (e_i, N_i))$ , 其中  $N_i$  两两互素, 可利用中国剩余定理进行加密操作; 在本地存储  $(d_i, (e_i, N_i))$  和知情者  $i$  的节点公钥的对应关系, 便于后续隐私泄露的追溯 ( $1 \leq i \leq n$ )。

2) 发送者  $S$  生成要发送给知情者  $i$  的密钥交易  $\text{TX}_i$ , 密钥交易数据  $\text{PriInfo}_i = [\text{sig}(d_i, (e_i, N_i), \text{PK}_s), (d_i, (e_i, N_i)), \text{PK}_s]$ 。其中,  $\text{sig}(d_i, (e_i, N_i), \text{PK}_s)$  为发送者  $S$  用自己节点私钥进行的签名, 以防止  $((d_i, (e_i, N_i)), \text{PK}_s)$  被篡改、实现知情者  $i$  对发送者  $S$  的源认证和发送者  $S$  的不可否认,  $\text{PK}_s$  为发送者  $S$  的节点公钥 ( $1 \leq i \leq n$ )。

3) 发送者  $S$  基于 Quorum 链加密传输  $\text{PriInfo}_i$  到知情者  $i$  ( $1 \leq i \leq n$ )。

4) 知情者  $i$  解密获得明文  $\text{PriInfo}_i$  后, 首先

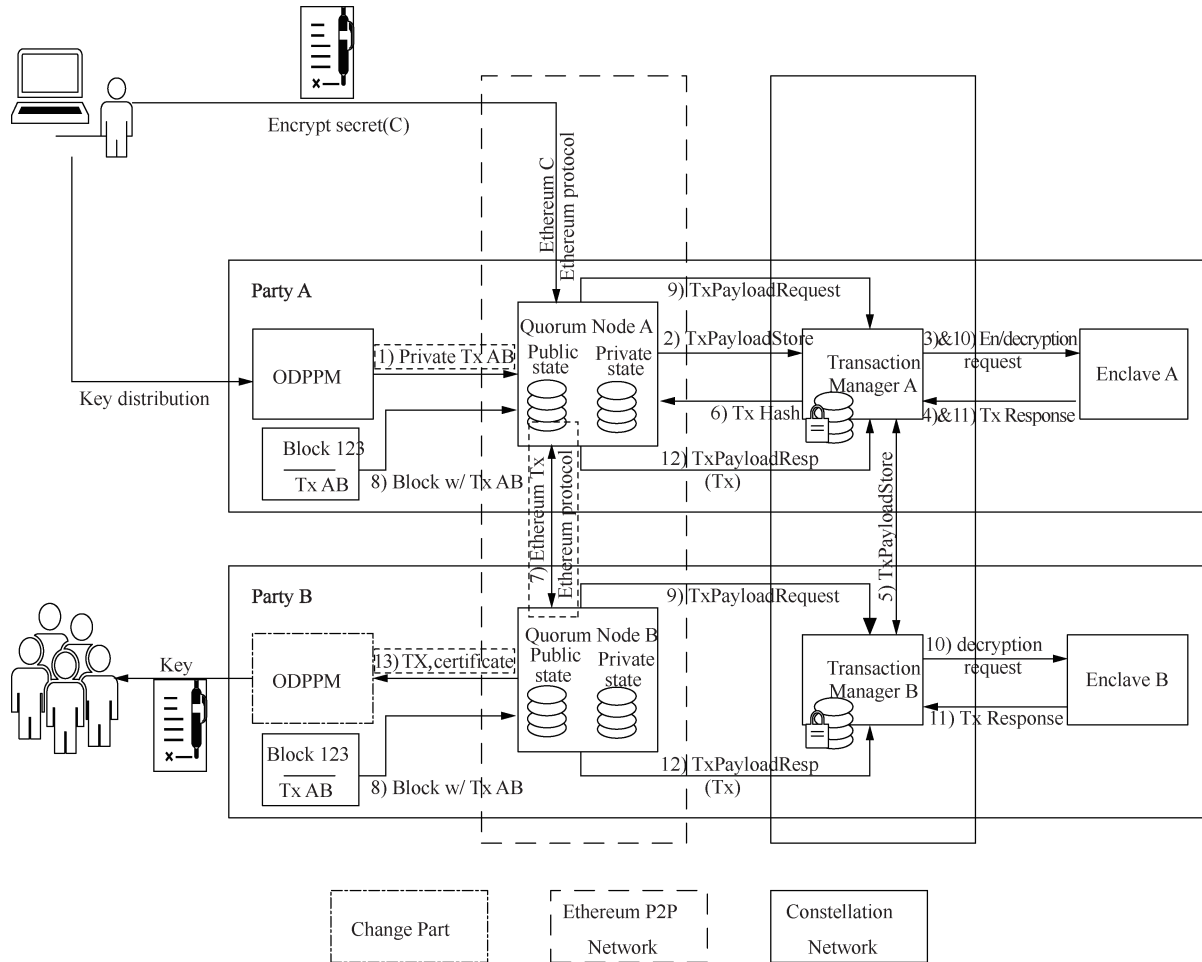


图 2 PPM-ODB 流程  
Figure 2 Flow chart of PPM-ODB

对  $\text{PriInfo}_i$  中签名  $\text{sig}(d_i, (e_i, N_i), \text{PK}_s)$  进行验证, 验证成功后, 在知情者  $i$  的 Private State 中存储  $\text{PriInfo}_i$ , 并以发送者  $S$  的节点公钥  $\text{PK}_s$  为索引, 便于后续解密隐私信息时, 查询获得相应的披露私钥。

Quorum 链可保护传输的密钥交易  $\text{TX}_i$  的保密性, 实现发送者  $S$  和  $n$  个知情者间披露公私钥  $(d_i, (e_i, N_i))$  的安全高效分发。

### 3.2 隐私信息加密

因为基于 RSA 的匿名多接收者加密方案无法实现隐私泄露后的可追溯, 本文对该方案进行了改进。改进的基本思想是针对每个知情者生成包含隐私信息  $M$  的不同的知情隐私信息  $Z$ , 且将该信息与知情者身份绑定, 以便当发生隐私信息泄露时, 通过比对信息  $Z$  和知情者身份的绑定关

系, 找到隐私信息的泄露者。

设计发送给知情者  $i$  的知情隐私信息为  $Z_i = [M, r_i, \text{sig}(M, r_i)]$ , 其中,  $r_i$  为随机数, 用于区分不同的知情者  $i$ ,  $\text{sig}(M, r_i)$  为发送者  $S$  用自己的节点私钥对隐私信息  $M$  和随机数  $r_i$  的签名 ( $1 \leq i \leq n$ ), 以防止有人伪造隐私信息, 且在隐私信息泄露后, 用于确认所泄露的隐私信息是否真实。

将基于 RSA 的匿名多接收者加密方案中的消息  $M$  替换为  $Z_i$  ( $1 \leq i \leq n$ )。因为中国剩余定理成立的前提条件是  $N_i$  互素, 这里的替换操作并没有破坏这一条件, 所以仍可生成相同的密文  $C$ , 保持多接收者的匿名性。

下面给出具体的加密过程。

1) 发送者  $S$  生成  $n$  个随机数  $r_i$  和每个知情者

对应的信息  $Z_i$  ( $1 \leq i \leq n$ )。

2) 发送者  $S$  存储信息  $Z_i$  与披露公私钥  $(d_i, (e_i, N_i))$  的映射关系 ( $1 \leq i \leq n$ )，以为隐私信息泄露后的追溯提供数据支持。

3) 发送者  $S$  根据  $Z_i$  和相应知情者的披露公钥  $N_i$  ( $1 \leq i \leq n$ )，计算需要在链上写入的密文  $C$ 。首先，计算

$$\begin{aligned} c_1 &= Z_1^{e_1} \bmod N_1 \\ c_2 &= Z_2^{e_2} \bmod N_2 \\ &\vdots \\ c_n &= Z_n^{e_n} \bmod N_n \end{aligned} \quad (5)$$

因为  $N_i$  互素，利用中国剩余定理求解方程组

$$\begin{aligned} C &= c_1 \bmod N_1 \\ C &= c_2 \bmod N_2 \\ &\vdots \\ C &= c_n \bmod N_n \end{aligned} \quad (6)$$

最后得到隐私密文  $C$ 。

### 3.3 隐私信息解密和追溯

当知情者要获取某用户的隐私信息时，需要对隐私密文进行解密，下面阐述链上隐私密文的解密过程。

1) 某隐私信息的知情者  $i$  从链上获得该隐私密文后，其对应的 Quorum Node 会根据隐私信息发送者  $S$  的节点公钥  $PK_s$  检索 Private state 数据库，获得相应的 PriInfo <sub>$i$</sub> 。

2) 利用 PriInfo <sub>$i$</sub>  中的披露公私钥  $(d_i, (e_i, N_i))$  进行以下计算，获得信息  $Z_i$ 。

$$\begin{aligned} c_i &= C \bmod N_i \\ Z_i &= (Z_i^{e_i})^{d_i} \bmod N = c_i^{d_i} \end{aligned} \quad (7)$$

3) 得到信息  $Z_i = [M, r_i, \text{sig}(M, r_i)]$  后，如果隐私信息  $M$  是具有完整语义的，则可以保证  $M$  没有被篡改，为减少计算开销，可不对  $Z_i$  中的签名进行验证。如果需要进一步验证，通过验证签名  $\text{sig}(M, r_i)$  可以检查  $M$  是否被篡改。

在隐私密文的解密过程中，只有相关的知情者能够对隐私密文进行解密，且解密过程在本地进行，并不需要暴露知情者的身份信息，从而实现知情者的匿名性保护。

在隐私密文解密后，存在某个知情者有意或者无意泄露隐私信息的情况。针对这种情况，

PPM-ODB 可实现对隐私信息泄露者的追溯。如果某个节点声称其所透露的信息为某个用户的隐私信息，但没有该用户对隐私信息的签名时，本文不称其为隐私信息的泄露，因为该隐私信息没有公信力，任何节点都可以随意发布用户的隐私信息。

在 PPM-ODB 中除了加密过程中生成的信息  $Z_i$  外，再没有出现过发送者  $S$  对隐私信息的签名，也就是说只有  $Z_i$  中包含具有公信力的隐私信息。发送者  $S$  发现含有自己隐私信息的  $Z_i$  泄露后，追溯的过程如下。

1) 发送者  $S$  根据自己在隐私信息加密过程中记录的信息  $Z_i$  与知情者  $i$  披露公私钥  $(d_i, (e_i, N_i))$  的对应关系，通过  $Z_i$  可查找到对应的披露公私钥  $(d_i, (e_i, N_i))$ 。

2) 发送者  $S$  根据自己在信任关系建立过程中记录的披露公私钥  $(d_i, (e_i, N_i))$  与知情者节点公钥的对应关系，由披露公私钥  $(d_i, (e_i, N_i))$  可查找到对应的知情者节点公钥，从而实现对隐私泄露者的追溯。

## 4 安全性分析

针对 PPM-ODB 中隐私信息的保密性要求，本节通过定义多项式时间算法，进行模拟攻击游戏对其进行了安全性分析，并证明了在安全性有保证的情况下，PPM-ODB 满足隐私信息的保密性。下面对证明过程进行详细阐述。

**结论** 若 Quorum 的隐私交易机制满足安全性，基于 RSA 的匿名多接收者加密方案满足安全性，RSA 算法满足安全性，则本文机制满足隐私信息的保密性。

**证明** 定义  $A_{\text{IBAnony}}$  为攻击本文机制隐私信息保密性模拟攻击游戏的敌手， $A_{\text{Quorum}}$  为攻击 Quorum 隐私交易机制的敌手， $A_{\text{AME}}$  为攻击基于 RSA 的匿名多接收者加密方案的敌手， $A_{\text{RSA}}$  为破解 RSA 算法的敌手。定义一个多项式时间算法  $A \in (A_{\text{Quorum}}, A_{\text{AME}}, A_{\text{RSA}})$ ，包含以上所有攻击者的能力，通过模拟攻击游戏中  $A_{\text{IBAnony}}$  和  $A$  的交互来构造  $A$ ，使其能够完成以上攻击。即如果  $A_{\text{IBAnony}}$  成功攻击了本文机制中隐私信息的保密性，那么  $A$  能在一定概率下成功攻击其他部分。

**初始化** 算法初始化系统, 运行 PPM-ODB 机制, 把隐私信息加密后的隐私密文  $C$  和区块中 Public State 数据交给攻击者  $A_{IBAnony}$ , 保留 Private State 数据和密钥交易 TX 消息。

**询问** 敌手  $A_{IBAnony}$  向算法  $A$  进行多项式有界次数询问。

请求询问加密后隐私信息  $C$  相对应的知情者身份, 算法  $A$  通过运行  $A_{Quorum}$ 、 $A_{AME}$ 、 $A_{RSA}$  攻击 Quorum 链隐私交易机制和基于 RSA 的匿名多接收者加密方案, 可以获取  $PriInfo_i$  中标识字段 privateFor 或者直接破解基于 RSA 的匿名多接收者加密方案的匿名性, 返回知情者身份给  $A_{IBAnony}$ 。

请求询问对应知情者收到的披露公私钥对, 算法  $A$  通过运行  $A_{Quorum}$ 、 $A_{AME}$ 、 $A_{RSA}$  攻击 Quorum 的隐私交易机制和对 RSA 算法进行破解, 从 Private State 数据中获取到相关的  $PriInfo_i$  信息或者破解 Enclave 产生的加密信息, 将其中的披露公私钥对  $(d_i, (e_i, N_i))$  交给攻击者  $A_{IBAnony}$ 。

**挑战** 当攻击者  $A_{IBAnony}$  结束询问后,  $A$  首先选取两个加密后的信息  $C_0$  和  $C_1$ , 并获取相应的 Public State 数据, 然后随机选择一个比特  $\mu \in \{0, 1\}$ , 接着执行上述的各个部分, 得到知情者身份和披露公私钥对  $(d_i, (e_i, N_i))$ , 最后得到隐私消息  $Z_i$  并返回给  $A$ 。

**猜测** 攻击者  $A_{IBAnony}$  还可以和之前一样对  $A$  进行多项式有界次数询问, 但不允许询问  $C_0$ 、 $C_1$  的知情者身份和披露公私钥对。

**输出** 攻击者  $A_{IBAnony}$  输出猜测  $\mu' \in \{0, 1\}$ , 如果  $\mu' = \mu$ , 则说明攻击者  $A_{IBAnony}$  赢得了游戏, 敌手  $A_{IBAnony}$  成功的概率为

$$\begin{aligned} \text{Adv}_{A_{IBAnony}}(k) &= \Pr[\text{Exp}_{A_{IBAnony}}(k) = 1] = \\ &= \Pr[A_{IBAnony}(\text{guess}) = 1 \mid \mu = 1] \cdot \Pr[\mu = 1] + \\ &+ \Pr[A_{IBAnony}(\text{guess}) = 0 \mid \mu = 0] \cdot \Pr[\mu = 0] = \\ &= \frac{1}{2} \left( \Pr \left[ \begin{array}{l} A_{Quorum}(\text{guess}) = 1 \\ A_{AME}(\text{guess}) = 1 \mid \mu = 1 \end{array} \right] + \right. \\ &\quad \left. \Pr \left[ \begin{array}{l} A_{Quorum}(\text{guess}) = 0 \\ A_{AME}(\text{guess}) = 0 \mid \mu = 0 \end{array} \right] \right) + \\ &\quad \frac{1}{2} \left( \Pr[A_{RSA}(\text{guess}) = 1 \mid \mu = 1] \cdot \Pr[\mu = 1] + \right. \\ &\quad \left. \Pr[A_{RSA}(\text{guess}) = 0 \mid \mu = 0] \cdot \Pr[\mu = 0] \right) = \\ &= \Pr[\text{Exp}_{A_{Quorum}}(k) = 1] + \Pr[\text{Exp}_{A_{AME}}(k) = 1] + \\ &+ \Pr[\text{Exp}_{A_{RSA}}(k) = 1] = \\ &= \text{Adv}_{A_{Quorum}}(k) + \text{Adv}_{A_{AME}}(k) + \text{Adv}_{A_{RSA}}(k) \end{aligned}$$

$$\begin{aligned} &\Pr \left[ \begin{array}{l} A_{Quorum}(\text{guess}) = 0 \\ A_{AME}(\text{guess}) = 0 \mid \mu = 0 \\ A_{RSA}(\text{guess}) = 0 \end{array} \right] < \\ &\frac{1}{2} \left( \Pr[A_{Quorum}(\text{guess}) = 1 \mid \mu = 1] \cdot \Pr[\mu = 1] + \right. \\ &\quad \left. \Pr[A_{Quorum}(\text{guess}) = 0 \mid \mu = 0] \cdot \Pr[\mu = 0] \right) + \\ &\frac{1}{2} \left( \Pr[A_{AME}(\text{guess}) = 1 \mid \mu = 1] \cdot \Pr[\mu = 1] + \right. \\ &\quad \left. \Pr[A_{AME}(\text{guess}) = 0 \mid \mu = 0] \cdot \Pr[\mu = 0] \right) + \\ &\frac{1}{2} \left( \Pr[A_{RSA}(\text{guess}) = 1 \mid \mu = 1] \cdot \Pr[\mu = 1] + \right. \\ &\quad \left. \Pr[A_{RSA}(\text{guess}) = 0 \mid \mu = 0] \cdot \Pr[\mu = 0] \right) = \\ &= \Pr[\text{Exp}_{A_{Quorum}}(k) = 1] + \Pr[\text{Exp}_{A_{AME}}(k) = 1] + \\ &+ \Pr[\text{Exp}_{A_{RSA}}(k) = 1] = \\ &= \text{Adv}_{A_{Quorum}}(k) + \text{Adv}_{A_{AME}}(k) + \text{Adv}_{A_{RSA}}(k) \end{aligned}$$

如果攻击者  $A_{Quorum}$  成功攻击 Quorum 链隐私交易机制,  $A_{AME}$  成功攻击基于 RSA 的匿名多接收者方案,  $A_{RSA}$  成功破解 RSA 算法, 则  $A_{IBAnony}$  在本文方案匿名性模拟攻击游戏中获胜, 但根据上述算法的安全性可知, 敌手  $A_{IBAnony}$  攻击成功的概率可以忽略不计, 因此 PPM-ODB 机制满足隐私消息保密性。

## 5 性能分析

本文选择 1 024 bit 的 RSA 算法, 定义  $E$  为指数运算的时间开销,  $H$  为哈希运算的时间开销,  $n$  为知情者个数。所有的仿真实验在 Win10 64 位、Inter(R) Core(TM) i7-7700@3.6 GHz、16 GB 内存 PC 机上进行。

### 实验 1 PPM-ODB 的时间开销

忽略乘法、加法运算, PPM-ODB 各阶段时间开销的估计值如表 1 所示。

由表 1 可知, 在忽略乘法、加法运算情况下, PPM-ODB 的总时间开销估计为  $7nE + 5nH$ 。密钥交易加密、知情隐私信息  $Z$  生成以及隐私密文解密算法均可以并行运算, 而密钥交易生成和知情隐私信息  $Z$  加密算法要直接与用户交互, 用户必须等待其运算完毕才能进行下一步工作。所以本文对密钥交易生成算法和知情隐私信息  $Z$  加密算法进行了仿真实验, 评估算法的时间开销与知情

者个数  $n$  的关系, 并将其与理论估计值 (根据仿真实验环境下  $E$ 、 $H$  运算的时间开销计算得到) 进行比较。实验中隐私信息大小设为 1 kB。

表 1 PPM-ODB 各阶段时间开销理论估计值  
Table 1 Theoretical estimation of time cost in each stage of PPM-ODB

| 阶段     | 算法名称        | 时间开销      |
|--------|-------------|-----------|
| 信任关系建立 | 密钥交易生成      | $2n(E+H)$ |
|        | 密钥交易加密      | $n(E+H)$  |
| 隐私信息加密 | 知情隐私信息 Z 生成 | $n(E+2H)$ |
|        | 知情隐私信息 Z 加密 | $nE$      |
| 隐私信息解密 | 隐私密文解密      | $2nE$     |

从图 3 和图 4 可以看出: ①在  $n < 50$  时, 密钥交易生成算法和 Z 加密算法在时间开销上理论估计值与实验结果基本相符; ②在  $n > 50$  时, 随着  $n$

的增大, 理论估计时所忽略的乘法和加法运算带来的时间开销越来越大, 尤其是 Z 加密算法, 随着  $n$  的增大, 理论估计误差越来越大; ③在  $n > 100$  时, 密钥交易生成算法和 Z 加密算法的时间开销基本在 1 s 以上。

因为密钥交易生成算法和 Z 加密算法在用户与区块链交互的过程中运行, 只有完成这两个过程, 用户才能够继续后续的操作, 所以当  $n > 100$  时, 算法的时间开销对于用户而言变得难以接受, 尤其是隐私信息加解密的过程。本文建议在实际应用中知情者  $n$  不超过 100 (即  $n \leq 100$ ), 以获得良好的用户体验。

## 实验 2 PPM-ODB 与 Quorum 链在按需披露隐私保护性能开销上的比较

首先测试评估在知情者个数  $n$  确定的情况

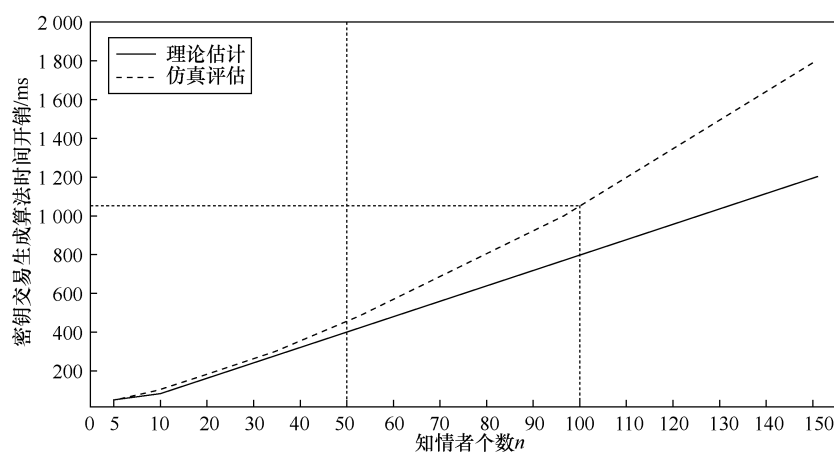


图 3 密钥交易生成算法时间开销和  $n$  的关系

Figure 3 The relationship between the time cost of key transaction generation algorithm and  $n$

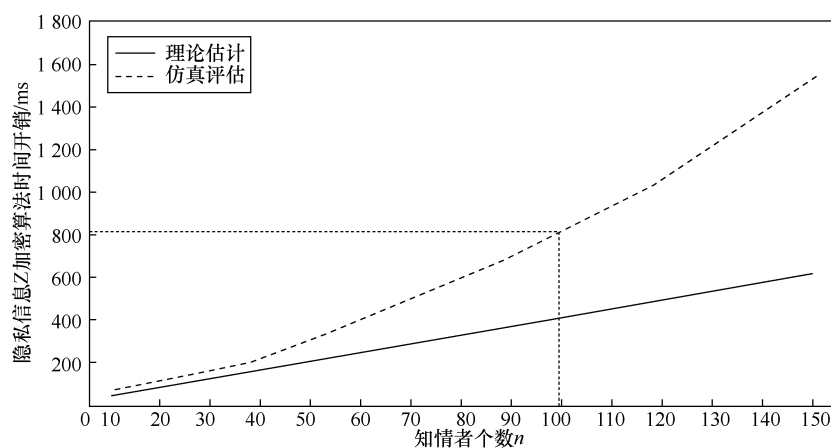


图 4 隐私信息 Z 加密算法时间开销和  $n$  的关系

Figure 4 The relationship between the time cost of privacy Z encryption algorithm and  $n$

下,采用 PPM-ODB 和 Quorum 链分别实现按需披露隐私保护的时间开销。这里,时间开销指隐私信息的加密、共识上链以及解密完整过程的时间开销,实验中设置  $n=50$ , 因为 Quorum 链以以太坊为基础,以太坊中单笔交易允许携带最大数据量约为 44 kB, 所以实验中隐私信息大小最大设置为 44 kB。实验结果如图 5 所示。

从图 5 可以看出在隐私信息较小时, Quorum 链与 PPM-ODB 耗时相近,但随着隐私信息的增大, Quorum 链的时间开销逐渐大于 PPM-ODB 机制。这主要是因为采用 Quorum 链实现按需披露的隐私保护时,隐私信息需要  $n$  次加密上链,随着隐私信息的增大,受到网络带宽和 Quorum 链共识时间的共同影响,上链耗时显著增加,然而 PPM-ODB 只需上链 1 次,所以随着隐私信息的增大,采用 Quorum 链实现按需披露隐私保护的时间开销显著大于 PPM-ODB 机制。可见,隐私信息越大,PPM-ODB 在时间开销上越占优势。

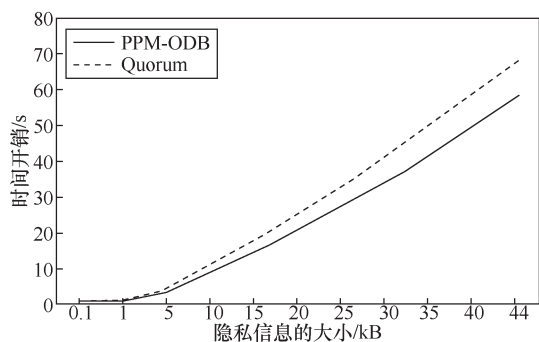


图5 PPM-ODB 与 Quorum 链时间开销与隐私信息大小的关系  
Figure 5 The relationship between the time cost of PPM-ODB and Quorum blockchain and the size of privacy information

另外,采用 Quorum 链实现按需披露的隐私保护时,因是向  $n$  个知情者分别发送隐私信息,隐私信息会在链上存储  $n$  份,所以 Quorum 链的存储开销是 PPM-ODB 的  $n$  倍。对于区块链系统而言,由于链中数据只增不减,所以如何减少存储开销对于目前区块链系统来说是急需解决的问题<sup>[20]</sup>,如比特币截至 2020 年 4 月,完整节点的数据量已经达到约 700 GB。Quorum 链所增加的  $n-1$  倍的存储开销会严重影响区块链系统的运行效率,所以从存储开销对比看 PPM-ODB 是更优的方案。

综上,在按需披露隐私保护的时间和存储开销上,PPM-ODB 显著优于 Quorum 链。

## 6 结束语

区块链开放共识的特点使链上用户隐私信息存在泄露风险。本文主要对区块链上隐私信息按需披露的保护需求进行了研究,提出了一种按需披露的区块链隐私保护机制,该机制基于 Quorum 链实现了隐私信息持有者和知情者间的密钥分发,通过改进基于 RSA 的匿名多接收者加密方案实现了知情者的匿名及隐私信息的加密、解密和追溯。通过安全性分析证明了本文机制满足隐私信息的保密性。仿真实验表明,PPM-ODB 相较于 Quorum 链在实现隐私信息按需披露上不仅减少了时间开销,而且大幅度降低了区块链的存储开销,同时在知情者  $n$  不大于 100 的情况下,运行效率良好,能够有效实现区块链隐私信息的按需披露。

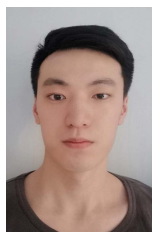
本文所提出的 PPM-ODB 只适用于小规模应用,同一隐私信息的知情者数量不宜超过 100。设计满足大规模应用需求的按需披露隐私保护机制、提高隐私信息上链的处理速度等是下一步需要研究的内容。

## 参考文献:

- [1] 何蒲,于戈,张岩峰. 区块链技术及应用前瞻综述[J]. 计算机科学, 44(4): 1-7, 15.
- [2] HE P, YU G, ZHANG Y F. Overview of blockchain technology and application prospect[J]. Computer Science, 44 (4): 1-7, 15.
- [3] 仲盛,黄欣沂. 区块链应用中的安全隐私专题简介[J]. 中国科学: 信息科学, 2020, 50(3): 461-462.
- [4] ZHONG S, HUANG X Y. Security and privacy in blockchain applications[J]. Chinese Science: Information Science, 2020, 50(3): 461-462.
- [5] 李旭东,牛玉坤,魏凌波. 比特币隐私保护综述[J]. 密码学报, 2019, 6(2): 133-149.
- [6] LI X D, NIU Y K, WEI L B. Bitcoin privacy protection overview[J]. Journal of Cryptologic Research, 2019, 6 (2): 133-149.
- [7] Digital is the Cash[EB].
- [8] NOETHER S. Ring signature confidential transactions for money[J]. IACR Cryptology ePrint Archive, 2015: 1098.
- [9] SASSON E B, CHIESA A, GARMAN C. Zerocash: decentralized anonymous payments from bitcoin[C]//2014 IEEE Symposium on Security and Privacy (SP). 2014: 459-474.
- [10] MIERS I, GARMAN C, GREEN M. Zerocoin: anonymous distributed e-cash from bitcoin[C]// 2013 IEEE Symposium on Security and Privacy (SP). 2013: 397-411.

- [8] Quorum official paper[EB].
- [9] 王瑞锦, 唐榆程, 张巍琦, 等. 基于同态加密和区块链技术的车联网隐私保护方案[J]. 网络与信息安全学报, 2020, 6(1): 46-53.  
WANG R J, TANG Y C, ZHANG W Q, et al. Privacy protection scheme of internet of vehicles based on homomorphic encryption and blockchain technology[J]. Chinese Journal of Network and Information Security, 2020, 6 (1): 46-53..
- [10] PAILLIER P. Public-Key Cryptosystems based on composite degree residuosity classes[C]//International Conference on Advances in Cryptology-enrocrypt. Berlin, Heidelberg: Springer, 1999.
- [11] FAN C I, HUANG L Y, HO P H. Anonymous multireceiver identity-based encryption[J]. IEEE Transactions on Computers, 2010, 59(9):1239-1249.
- [12] FAN C I, TSENG Y F. Anonymous multi-receiver identity-based authenticated encryption with CCA security[J]. Symmetry, 2015, 7(4): 1856-1881.
- [13] ZHANG J, MAO J. An improved anonymous multi-receiver identity-based encryption scheme[J]. International Journal of Communication Systems, 2015, 28(4): 645-658.
- [14] PANG L, GAO L, LI H. Anonymous multi-receiver ID-based signcryption scheme[J]. IET information Security, 2015, 9(3): 194-201.
- [15] 庞辽军, 高璐, 裴庆祺. 基于身份公平的匿名多接收者签密方案[J]. 通信学报, 2013(8): 165-172.  
PANG L J, GAO L, PEI Q Q. Anonymous multi receiver signcryption scheme based on identity fairness[J]. Journal on Communications, 2013 (8): 165-172.
- [16] 李慧贤, 巨龙飞. 对一个匿名多接收者签密方案的安全性分析与改进[J]. 电子学报, 2015, 43(11): 2187-2193.  
LI H X, JU L F. Security analysis and improvement of an anonymous multi receiver signcryption scheme[J]. Acta Electronica Sinica, 2015, 43 (11): 2187-2193.
- [17] 秦艳琳, 吴晓平, 胡卫. 高效的无证书多接收者匿名签密方案[J]. 通信学报, 2016(6): 129-136.  
QIN Y L, WU X P, HU W. Efficient anonymous signcryption scheme for multiple receivers without certificate[J]. Journal on Communications, 2016 (6): 129-136.
- [18] 周彦伟, 杨波, 王青龙. 基于身份的多接收者(多消息)匿名混合签密机制[J]. 软件学报, 2018, 29(2): 442-455.  
ZHOU Y W, YANG B, WANG Q L. Anonymous mixed signcryption mechanism of identity based multi receiver (multi message)[J]. Journal of Software, 2018, 29 (2): 442-455.
- [19] HARN L, CHANG C C, WU H L. An anonymous multi-receiver encryption based on RSA[J]. International Journal of Network Security, 2013, 15(4):307-312.
- [20] 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11): 11-20.  
SHEN X, PEI Q Q, LIU X F. Survey of block chain[J]. Chinese Journal of Network and information Security, 2016, 2(11): 11-20.

#### [作者简介]



李少卓(1995—), 男, 山西大同人, 信息工程大学硕士生, 主要研究方向为信任管理、区块链。



王娜(1980—), 女, 山西临汾人, 博士, 信息工程大学副教授, 主要研究方向为云计算安全、网络空间安全。



杜学绘(1968—), 女, 河南新乡人, 博士, 信息工程大学教授、博士生导师, 主要研究方向为大数据安全、云计算安全和信息系统多级安全。