基于公平盲签名和分级加密的联盟链隐私保护方案

张学旺[1,2]，黎志鸿[1]，林金朝[3]

（1. 重庆邮电大学软件工程学院，重庆 400065；2. 重庆大学微电子与通信工程学院，重庆 400004；
3. 重庆邮电大学光电信息感测与传输技术重庆市重点实验室，重庆 400065）

摘 要：为了解决联盟链应用场景中身份信息、交易数据存在的安全隐患，以及单级加密方法耗时的问题，提出了一种基于公平盲签名和分级加密的联盟链隐私保护方案。一方面，考虑公平盲签名方案存在中心化强、安全性差的缺陷，结合零知识证明技术对其重新设计，使之适用于联盟链应用场景；另一方面，基于 Paillier 同态加密算法，设计出可监管的分级加密方法。安全性分析及仿真实验结果表明，所提方案在实现对加密后的交易数据信息监管的同时，减少了加解密过程的时间开销；能有效抵抗篡改、窃听等恶意攻击，并使加密效率明显提升。

关键词：联盟链；公平盲签名；零知识证明；同态加密；隐私保护；分级加密

中图分类号：TP393

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022162

Privacy protection scheme based on fair blind signature and hierarchical encryption for consortium blockchain

ZHANG Xuewang[1,2], LI Zhihong[1], LIN Jinzhao[3]

1. School of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. College of Microelectronic and Communication Engineering, Chongqing University, Chongqing 400004, China
3. Chongqing Key Laboratory of Photo Electronic Information Sensing and Transmitting Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: To solve the security hazards of identity information and transaction data and the time-consuming problem of traditional single-level encryption methods in the current application scenarios of consortium blockchain, a privacy protection scheme of consortium blockchain based on fair blind signature and hierarchical encryption was proposed. Considering the strong centrality and poor security of the existing fair blind signature scheme, it was redesigned with zero-knowledge proof technology to be applicable for consortium blockchain application scenario. Based on the Paillier homomorphic encryption algorithm, a supervisable hierarchical encryption method was designed, and the method realized the supervision of encrypted transaction data information and reduced the time cost of the encryption and decryption process. The security analysis and simulation results show that the proposed scheme can effectively resist malicious attacks such as tampering and eavesdropping and significantly improve the encryption efficiency.

Keywords: consortium blockchain, fair blind signature, zero-knowledge proof, homomorphic encryption, privacy protection, hierarchical encryption

0 引言

区块链技术为能源交易[1]、供应链金融[2-3]、车辆自组网[4]、智能家居[5]、数字档案[6]等一系列行业带来了较大影响。区块链技术的蓬勃发展，得益于其去中心化、可追溯、信息不可篡改等特性[7-8]，但

收稿日期：2022−05−18；**修回日期：**2022−08−05

基金项目：国家重点研发计划基金资助项目（No.2019YFC1511300）；国家自然科学基金资助项目（No.U21A20447）；南充市科技计划基金资助项目（No.21YFZJ0033）

Foundation Items: The National Key Research and Development Program of China (No.2019YFC1511300), The National Natural Science Foundation of China (No.U21A20447) , The Science and Technology Program of Nanchong (No.21YFZJ0033)

这些特性也使链上交易数据以及用户身份的隐私安全难以得到保障。安全隐私问题是区块链技术中的重要问题，交易数据以及用户身份的链上安全成为亟待解决的问题[9-10]。

针对目前区块链领域中的用户身份隐私保护问题，国内外学者不断进行研究探索，出现了以群签名[11]、环签名[12]、多方安全计算[13]为代表的去中心化混币机制和以盲签名[14]为代表的中心化混币机制 2 个研究方向。Zhang 等[15]将群签名与区块链结合应用于移动边缘计算，提出了一种可验证区块的群签名方案，解决了区块链存在的诸多安全漏洞。群签名匿名性不足的缺点，限制了其应用场景。2007 年，一种不需要中间节点参与签名过程的、无条件匿名的签名方法——环签名被提出[12]。Li 等[16]将具有无条件匿名性的环签名与区块链技术相结合，提出了一种完全匿名的区块链隐私保护方案，使用户成员不依赖于群主节点和其他成员便可进行签名。Chaum[14]首次提出盲签名，其因签名者对授权交易不可追溯的特点，目前广泛应用于电子现金和不记名投票等领域；但盲签名的运用使交易用户完全匿名，难以对用户的恶意行为进行有效监管。Stadler 等[17]提出公平盲签名的思想，该思想将盲签名的无条件匿名转换为条件匿名，解决了盲签名的不可追溯问题。

针对区块链交易数据隐私保护的研究以哈希上链、密钥加密、同态加密[18]、零知识证明[19]等方向为主，区块链数据隐私安全的重要性不言而喻，同时链上数据的安全可验证性也很重要[20]。李宇溪等[21]结合同态加密算法提出一种 K-近邻搜索方案，用于解决移动社交网络的身份隐私保护问题。Dowlin 等[22]将同态加密算法应用于生物信息领域，为解决基因数据等隐私信息的泄露问题提供了新的手段。2009 年，Gentry[23]提出了第一个真正意义上满足全同态运算的同态加密算法，即全同态加密算法，但其极度复杂的计算过程导致其运算十分耗时。虽然之后陆续有更优的全同态加密算法被提出[24]，但依旧未能解决这一短板。半同态加密算法虽然效率优于全同态加密算法，但其加解密过程的耗时相比于对称密码仍高出不少。

综上所述，针对联盟链中存在的用户身份与链上交易数据的隐私安全隐患及现行方案存在的不足，本文提出一种基于公平盲签名和分级加密的联盟链隐私保护方案。该方案的主要贡献如下。

1) 对已有公平盲签名方法进行了针对联盟链应用场景的重新设计，结合零知识证明提出一种基于联盟链身份隐私保护的可行性方案。该方案可在保护用户身份隐私的同时，实现对恶意交易的追溯。

2) 设计并实现了一种分级加密方法。针对单级加密无效耗时，该方法在实现对已脱敏交易数据可监管的同时，有效减少了加解密过程的时间损耗，降低了交易过程的响应时效。

1 相关知识概述

1.1 联盟链

区块链根据其应用场景和开放程度[25]的不同，可分为公有链、私有链和联盟链三类。其中，私有链与传统的分布式存储方案几乎没有区别，由于私有链不具有开放性和可扩展性，其使用范围一般限于公司内部，公司掌握了全链的写入能力，智能合约的部署以及节点共识的达成都只由该公司的内部成员完成。公有链具有开放透明的特点，但出块缓慢限制了其应用场景。相比于公有链和私有链，联盟链在兼具开放性的同时具有更强大的数据处理能力、数据私密性以及共识机制的可扩展性。

Linux 基金会为推动区块链数字技术的发展，于 2015 年牵头发起了开放式账本项目；同年年底，项目名称由开放式账本改为 Hyperledger 区块链开源项目[26]。Hyperledger 拥有 Burrow、Cello、Fabric 和 Iroha 等多个顶级项目，项目可分为框架和工具两类，其中，框架类项目 Fabric 的影响最大。Hyperledger Fabric[27]的提出旨在推动区块链技术跨行业领域的应用，使区块链的应用场景不再局限于金融贸易行业。

1.2 Paillier 同态加密

同态加密是指通过使用某种特殊函数对数据明文进行加密处理后再进行加或乘运算的结果，与直接对明文进行相应运算的结果是等价的。同态加密算法的合理运用为许多应用场景的数据隐私泄露问题提供了解决方法[24,28-29]。同态加密算法可对密文进行运算的特性使其能应对脱敏后信息的二次处理和监管需求。

Paillier 同态加密算法[30]于 1999 年提出，该算法满足 $\mathrm{Enc}(m_1)\mathrm{Enc}(m_2)=\mathrm{Enc}(m_1+m_2)\bmod n^2$，其中，Enc 为加密操作，$n$ 为 2 个大素数的乘积，m_1 和 m_2 为明文，即使用 Paillier 同态加密算法加密后的密文

可以直接进行加减运算，解密密文加减后的结果，与直接对明文进行计算的结果相同。Paillier 同态加密基于复合剩余类的困难问题，其功能如图 1 所示。用户通过客户端调用 Paillier 库对数据进行加密，再将加密后数据提交到服务器端进行计算，最后调用 Paillier 库对计算结果解密即得到相关数据的计算结果。

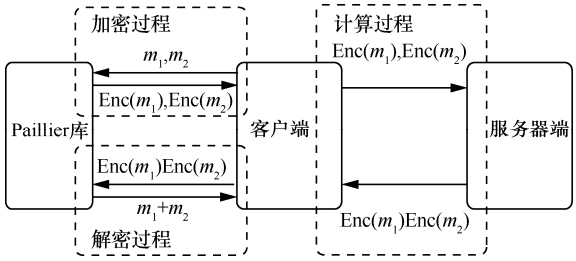


图 1　Paillier 同态加密功能

1.3　公平盲签名

在许多区块链应用中，用户需要授权机构验证自己的身份，并授予参与某项目的权限，还要确保授权机构在授权后不能对授权发起追溯。例如，在电子投票时，选民需要在领取到选票后，再进行匿名投票；在现实生活中实现该类需求并不困难，但程序却难以实现。盲签名技术的出现为解决匿名投票类难题提供了一种可行性方案。不难分析盲签名依赖数据的盲化和解盲过程实现匿名性；虽然用户的身份隐私得到了保障，但也让恶意用户的行为难以监管。本节通过以下 4 个步骤解释基于盲签名进行匿名授权的过程。

步骤 1　用户在本地利用盲因子对数据的哈希值进行盲化处理。

步骤 2　用户将盲化后的数据哈希值传递给授权组织机构进行授权操作，待授权组织验明用户身份后，通过签名算法，使用其私钥对待授权盲化数据的哈希值进行签名授权。

步骤 3　授权组织机构签名授权后将完成签名授权的盲化数据的哈希值传递给用户。

步骤 4　用户对授权后的盲化数据的哈希值进行解盲操作，得到授权后的原始数据的哈希值。

公平盲签名是具有条件匿名性的盲签名，其通过引入除用户、授权组织机构外的可信第三方（TTP, trusted third party），由可信第三方保管用户的盲因子及用户信息，当授权组织机构需要追溯恶意交易数据信息的来源时，可信第三方查询交易的发起用户，完成对恶意用户的追溯。

2　本文方案描述

2.1　本文方案中的实体

本文方案主要涉及 6 个实体，包括交易发起者（TO, transaction originator）、追溯者（Tracer）、密钥生成中心（KGC, key generation center）、联盟链（CB, consortium blockchain）、组织机构（ORG, organization）、可信第三方（TTP, trusted third party），各实体描述如下。

1) TO 是指数据的真实拥有者，依赖其所属的 ORG 向 CB 中发布交易；TO 的身份是对外匿名的，ORG 外部并不知道其存在，ORG 本身也无法通过交易独立追溯 TO 的真实身份。

2) Tracer 一般指交易的接收方，当其发现交易有恶意时，向 ORG 发起追溯。

3) KGC 在联盟链系统搭建的初始阶段，为所有 ORG 和 TTP 生成并分发密钥对。

4) CB 在本文方案中指由 TTP 发起并联合 ORG 建立的联盟链，CB 中的 TTP 和各 ORG 都拥有至少 2 个节点参与共识。

5) ORG 是由多个 TO 组成的组织，为 TO 发起交易提供混币服务，并在 Tracer 发起追溯时，联合 TTP 完成对恶意 TO 的追溯。

6) TTP 是 CB 的发起者，拥有 CB 的访问权限和节点加入权限，并负责 CB 的监管工作，同时协同 ORG 实现对 TO 的追溯。

2.2　需求与隐患

在联盟链实际应用场景中， TO 存在隐匿敏感信息的需求，但区块链中全账本节点都存有链上交易数据的完整副本，使 TO 的需求仅靠区块链技术难以满足，故运用密码学等技术手段对数据信息进行脱敏处理不可避免。但面对脱敏后的交易数据，TTP 利用传统技术难以实现有效监管；而且将现有公平盲签名方案应用于 CB 中 TO 身份隐私保护存在如下安全隐患。

TTP 经手 TO 的身份隐私信息，隐私信息的安全性完全依赖于 TTP 对 TO 做出的承诺；事实上，所有隐私信息都存在被 TTP 选择性保存在其本地数据库中的可能，该行为并不受限制。即使考虑 TTP 诚实，仍存在数据库被敌手攻击，导致所有 TO 的身份隐私信息被泄露的风险。由于 TTP 集中掌握了大量关键的交易数据信息，使联盟链交易具有单中心化的特征，与区块链去中心化的

思想相违背。

2.3 方案构建

为解决 2.2 节中的需求及安全隐患，本文提出一种基于公平盲签名和分级加密的联盟链隐私保护方案，结合零知识证明技术实现公平盲签名的联盟链去中心化；并提出了一种分级加密方法，将待处理的数据按敏感度进行分级，对不同分级的数据提供不同级别的加密，实现数据隐私保护的灵活性。方案主要包括联盟链初始化、数据加解密、数据上链及数据分析等 4 个阶段。

阶段 1 联盟链初始化。

步骤 1 TTP 与各 ORG 一同组建 CB，KGC 为 ORG 和 TTP 生成其全局密钥对。以 ORG 密钥对的生成为例，选取 2 个大素数 p和q，并计算 $n=pq$ 和 $\Phi(n)=(p-1)(q-1)$。

选取 ORG 的公钥指数 e_{org}，满足 $\gcd\left(e_{\text{org}},\Phi(n)\right)=1, e_{\text{org}}<\Phi(n)$，通过逆运算求出 ORG 的私钥指数 d_{org}，如式(1)所示。

$$d_{\text{org}}\equiv e_{\text{org}}^{-1}\left(\bmod \Phi(n)\right) \tag{1}$$

这样，KGC 就完成了对 ORG 公钥 $O_{\text{pub}}=\{e_{\text{org}},n\}$ 及私钥 $O_{\text{prv}}=\{d_{\text{org}},n\}$的生成。TTP 的密钥生成类似，可参照 ORG 密钥对的生成过程，此处不再赘述；生成的 TTP 密钥对为 $T_{\text{pub}}=\{e_{\text{ttp}},n\}$和 $T_{\text{prv}}=\{d_{\text{ttp}},n\}$。

步骤 2 ORG 与 TTP 协定方程 $\xi=q^{\alpha}\bmod p$ 用于数据上链阶段 ORG 成员 TO 的身份验证。ξ,p,q 值由 ORG 与 TTP 双方共享；ORG 为其 TO 发放 α 作为组织凭证。

阶段 2 数据加解密

步骤 1 TO 录入交易数据后，客户端根据交易数据敏感度的不同，将原始交易数据拆分为可公开数据和不可公开数据两类。按其是否需要进行监管处理，将不可公开数据继续细分为需要进行监管处理的动态数据和不需要进行监管处理的静态数据两类。交易数据细粒度分级如图 2 所示。

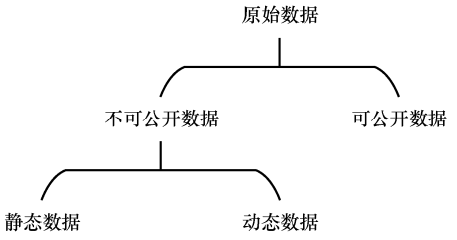


图 2 交易数据细粒度分级

步骤 2 客户端对可公开数据进行 RLP（recursive length prefix）编码处理；可公开数据在区块链网络中以编码后的形式进行传输和存储。

步骤 3 对于静态数据，客户端先对其进行 RLP 编码操作，再使用对称加密算法进行脱敏处理，如算法 1 所示。

算法 1 静态数据脱敏

输入 明文 M，加密密钥 MK，系统参数 FK，固定参数 CK

输出 密文 M'

1) $(K_0,K_1,K_2,K_3)=(\text{MK}_0\oplus\text{FK}_0,\text{MK}_1\oplus\text{FK}_1,\text{MK}_2\oplus\text{FK}_2,\text{MK}_3\oplus\text{FK}_3)$

2) for $i=1$ to 32 by 1 do

3) $\quad \text{rk}_i=K_i\oplus T'(K_{i+1}\oplus K_{i+2}\oplus K_{i+3}\oplus CK_i)$

4) end for

5) 将 M 按照 128 bit 大小分组读取，得到 n 组 $X_{128}=(X_1,X_2,X_3,X_4)$

6) while $X_{128}\neq\varnothing$

7) $\quad$ for $i=1$ to 32 by 1 do

8) $\quad\quad X_{i+4}=X_i\oplus T(X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus \text{rk}_i)$

9) $\quad$ end for

10) $\quad$ 反序变换：$Y_{128}=(X_{32},X_{33},X_{34},X_{35})\rightarrow(X_{35},X_{34},X_{33},X_{32})$

11) $\quad M'=M'+Y_{128}$

12) $\quad$ next X_{128}

13) end while

14) return M'

步骤 4 对于需要进行监管处理的动态数据，客户端进行 RLP 编码后使用 Paillier 同态加密算法进行加解密处理。具体处理过程如下。

1) 密钥生成

选取 2 个大素数 p 和 q，满足 $\gcd(n,\Phi(n))=1$，分别计算 $n=pq$ 和 $\Phi(n)=(p-1)(q-1)$，根据欧几里得算法计算 $\lambda=\gcd(p-1,q-1)$，为便于阐述，以下将 $p-1$ 表示为 x，将 $q-1$ 表示为 y。由于 p 和 q 均为大素数，故 $x\geqslant y>0$。使用带余数的除法，得 $x=k_1y+r_1,0\leqslant r_1<y$。

若 $r_1=0$，则 $\gcd(x,y)=y$；若 $r_1\neq0$，则必定存在 $\lambda\mid x$ 和 $\lambda\mid y$，故一定有 $\lambda\mid(x-k_1y)$，即 $\lambda\mid r_1$。由于 $y>r_1$，得 $y=k_2r_1+r_2,0\leqslant r_2<r_1$。

以上迭代过程中，余数将不断递减且为正整数，当余数递减为 0 时，计算出 λ 的值。选取 g 满

足 $g<n^2$，且 g 的选取要使如式(2)所示的 μ 存在。

$$\mu=\frac{n}{g^{\lambda} \bmod n^2-1} \bmod n \tag{2}$$

密钥对生成完成，私钥为 $\{\lambda,\mu\}$，公钥为 $\{n,g\}$。

2) 加密

选取随机数 r，满足 $r\in\mathbb{Z}_n^*$，$\gcd(r,n)=1$；使用公钥 $\{n,g\}$ 加密明文 m，生成密文 c。

$$c=g^m r^n \bmod n^2 \tag{3}$$

3) 解密

$$m=\frac{c^{\lambda} \bmod n^2-1}{n}\mu \bmod n \tag{4}$$

密钥交换可以通过线下交换的方式进行，或者在使用非对称加密算法加密密钥后，在安全网络环境条件下进行在线交换。分级加密方法如图 3 所示，用户通过客户端调用相关库函数接口对不同敏感度分级的数据进行加密处理后，将数据组装成交易并发送到联盟链节点中。

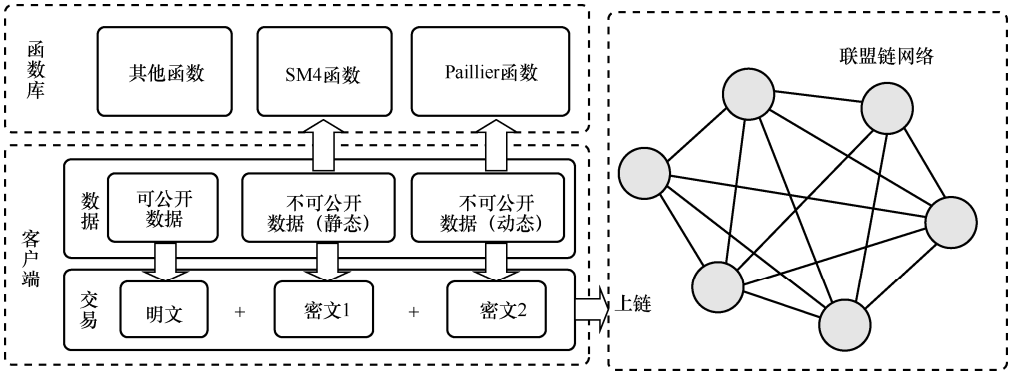


图 3　分级加密方法

阶段 3　数据上链

TO 通过客户端将编码后的可公开数据的明文、静态数据密文以及动态数据密文重新组装成完整的交易数据 m。最后计算其哈希值 Hash(m)。TO 使用基于零知识证明的公平盲签名方案对 Hash(m) 进行签名授权。数据上链的流程如图 4 所示。具体由以下几个步骤组成。相关符号如表 1 所示。

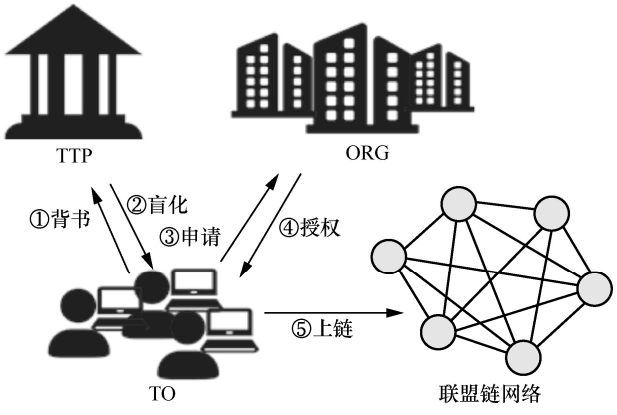


图 4　数据上链流程

步骤 1　TO 持 Hash(m) 向 TTP 提交交易注册申请，并使用零知识证明向 TTP 证明其所在机构 ORG；完整身份证明过程如以下 4 个步骤所示。

表 1　**相关符号及其含义**

符号	含义
m	用户交易的原始交易数据
m'	经盲化处理后的交易数据
k	盲因子
$(O_{\text{pub}},O_{\text{prv}})$	组织机构 ORG 的密钥(公钥，私钥)
$(T_{\text{pub}},T_{\text{prv}})$	可信第三方 TTP 的密钥(公钥，私钥)
ω^*	组织机构 ORG 的签名
σ^*	可信第三方 TTP 的签名
Hash(∗)	数据 ∗ 的哈希值

步骤 1-1　TO 生成 i 个随机数 $\{r_1,r_2,\cdots,r_i\}$，其中 i 满足 $i\geqslant 16$，r_i 满足 $r_i<p-1$；计算 $\xi_i=q^{r_i} \bmod p$，将 $\{\xi_1,\xi_2,\cdots,\xi_i\}$ 发送给 TTP。

步骤 1-2　TTP 与 TO 根据算法 2 产生 i 个随机位 $\{\beta_1,\beta_2,\cdots,\beta_i\}$。

算法 2　随机位生成

输入　$\{a_1,a_2,\cdots,a_i\}$

输出　$\{\beta_1,\beta_2,\cdots,\beta_i\}$

1)for　k = 1 to　i　by 1 do

2)　TTP 计算 a_i 的奇偶性 t_1（t_1=1 表示 a_i 为奇数，t_1=0 表示 a_i 为偶数）

3) TTP 计算 $\text{Hash}(a_i)\to \text{TO}$

4) TO 根据 $\text{Hash}(a_i)$ 猜测 a_i 的奇偶性 t_2

5) if $t_2==t_1$ then

6) $\beta_i=0$

7) else

8) $\beta_i=1$

9) end if

10)end for

11) return $\{\beta_1,\beta_2,\cdots,\beta_i\}$

步骤 1-3 根据随机位开始身份验证，若 $\beta_i=0$，TO 向 TTP 发送 r_i；若 $\beta_i=1$，TO 向 TTP 发送 $(r_i-r_v)\bmod(p-1)$，$v=\min\{i|\beta_i=1\}$，TTP 验证式(5)是否成立。

$$\xi_i=q^{(r_i-r_v)\bmod(p-1)}\xi_v \bmod p \tag{5}$$

步骤 1-4 TO 向 TTP 发送 $(\alpha-r_v)\bmod(p-1)$，TTP 验证式(6)是否成立。

$$\xi=q^{(\alpha-r_v)\bmod(p-1)}\xi_v \bmod p \tag{6}$$

若以上 $i+1$ 个等式均成立，则证明 TO 属于该 ORG。TTP 为 TO 生成 k，$k\in(1,n)$；并将 $\text{Hash}(m)$、k 存于本地数据库中。通过 TO 所在机构的公钥 O_{pub} 和 k 对 $\text{Hash}(m)$ 盲化处理，生成签名 $\sigma^*_{m'}$，并向 TO 返回 $(m',k,\sigma^*_{m'})$。

$$\begin{aligned}&m'=\text{Hash}(m)k^{e_{\text{org}}} \bmod n\\&\text{Sig}_{\text{ttp}}(m')=(m')^{d_{\text{ttp}}} \bmod n\end{aligned} \tag{7}$$

步骤 2 TO 使用 T_{pub} 对返回的 $\sigma^*_{m'}$ 进行认证，确认签名的信息没有被篡改；认证通过后，TO 向 ORG 提交授权申请，并把 m' 传递给 ORG。

步骤 3 ORG 使用 T_{pub} 对 $\sigma^*_{m'}$ 进行认证，认证通过后则对 m' 授权，生成 $\omega^*_{m'}$，并将 $\omega^*_{m'}$ 返回给 TO，签名过程如式(8)所示；ORG 的本地数据库中保存 $\omega^*_{m'}$ 和 TO 的个人信息。

$$\text{Sig}_{\text{org}}(m')=(m')^{d_{\text{org}}} \bmod n \tag{8}$$

步骤 4 TO 使用 k 对 $\omega^*_{m'}$ 进行解盲处理，得到 $\omega^*_{\text{Hash}(m)}$，解盲过程如式(9)所示。

$$\text{Sig}_{\text{org}}\big(\text{Hash}(m)\big)=\frac{\text{Sig}_{\text{org}}(m')}{k} \bmod n \tag{9}$$

步骤 5 TO 通过客户端将 $\omega^*_{\text{Hash}(m)}$ 打包完整的交易后，调用相关 API 将其提交到 CB 节点等待验证。验证及共识达成后交易随区块存储。

TTP 与 ORG 存储用户信息时，选用分布式集群存储方案，避免将全部信息存储于同一个数据库中，防止单存储节点故障导致的数据丢失。

阶段 4 数据分析

步骤 1 TTP 通过 CB 获取到相关数据后，对其进行分解从而提取到加密后的动态数据信息 c。

步骤 2 TTP 利用同态加密算法同态运算的性质对数据密文进行处理，处理算法如式(10)所示，其中，$\text{Enc}(m_1)$ 和 $\text{Enc}(m_2)$ 分别表示明文 m_1 和 m_2 加密后生成的密文，k 为任意标量。

$$\begin{aligned}&\text{Enc}(m_1)\text{Enc}(m_2)=\\&(g^{m_1}r_1^n(\bmod n^2))(g^{m_2}r_2^n(\bmod n^2))=\\&g^{m_1+m_2}(r_1r_2)^n(\bmod n^2)=\\&\text{Enc}(m_1+m_2)\\&(\text{Enc}(m_1))^k=(g^{m_1}r_1^n)^k \bmod n^2=\\&g^{m_1\times k}(r^k)^n \bmod n^2=\text{Enc}(km_1)\end{aligned} \tag{10}$$

3 分析及实验

3.1 正确性分析

分析 1 证明式(4)的正确性，根据卡迈克尔定理 $\left|\mathbb{Z}^*_{n^2}\right|=\Phi(n^2)=n\Phi(n)$，对于任意 $\omega\in\mathbb{Z}^*_{n^2}$ 都有

$$\begin{cases}\omega^{\lambda}=1 \bmod n\\ \omega^{n\lambda}=1 \bmod n^2\end{cases}$$

$$\begin{aligned}&\lambda(n^2)=\text{lcm}(\lambda(q^2),\lambda(p^2))=\\&\text{lcm}(\Phi(q^2),\Phi(p^2))\ =\\&\text{lcm}(q(q-1),p(p-1))=\\&pq(\text{lcm}(p-1,q-1))=n\lambda(n)\to\\&\omega^{\lambda(n^2)}=\omega^{n\lambda}\equiv 1 \bmod n^2\end{aligned} \tag{11}$$

因此，有

$$\begin{aligned}&c^{\lambda} \bmod n^2=g^{m\lambda}r^{n\lambda}\equiv g^{m\lambda} \bmod n^2=\\&(1+n)^{m\lambda} \bmod n^2=\ (1+nm\lambda)\bmod n^2\\&g^{\lambda} \bmod n^2=(1+n)^{\lambda} \bmod n^2=\\&(1+n\lambda)\bmod n^2\end{aligned} \tag{12}$$

$$\text{①}\ \ \frac{c^{\lambda} \bmod n^2-1}{n}=m\lambda \bmod n^2$$

$$\text{②}\ \ \frac{g^{\lambda} \bmod n^2-1}{n}=\lambda \bmod n^2\to m=\frac{\text{①}}{\text{②}} \bmod n \tag{13}$$

分析 2 证明本文方案中公平盲签名过程的正

确性，即式(7)～式(9)的正确性。

由欧拉定理得 $e^{\Phi(k)\bmod k}=ed \bmod k \ de \bmod \Phi(n)=1$

$\rightarrow de=st+1$

其中，$s=\Phi(n), t\in\mathbb{Z}$；

$$\mathrm{Sig}(m)=\frac{\mathrm{Sig}(m')}{k}\bmod n=$$

$$\frac{\mathrm{Sig}(mk^e)}{k}\bmod n=\frac{(mk^e)^d \bmod n}{k}\bmod n=$$

$$\frac{m^d k^{ed} \bmod n}{k}\bmod n=m^d k^{ed-1}\bmod n=$$

$$m^d \bmod n k^{st}\bmod n=$$

$$m^d \bmod n(k^s \bmod n)t=m^d \bmod n(1\bmod n)$$

$$m^d \bmod n=\mathrm{Sig}(m) \tag{14}$$

3.2　安全性分析

本节分别从用于身份隐私保护的公平盲签名和用于交易数据保护的分级加密方法两方面展开安全性分析。此处给出以下 4 种定理并进行证明，以说明本文方案的安全性。

定理 1　在 ORG 的私钥未泄露的前提下，若敌手对盲化后的交易数据进行篡改，其成功的概率是可忽略的。

证明　TTP 对交易进行盲化处理后，基于公平盲签名的授权认证一旦签发，认证的原始数据不能任意改变；公平盲签名基于离散对数数学难题，对于其安全性分析考虑方程 $\xi=q^{\alpha}\bmod p$；对于给定的 p、y、q，最多仅需执行 x 次乘法运算便可计算出 y 的值；相反，对于给定的 ξ,p,q 计算 α 的值异常困难，其计算的难度级别为 $e^{\left((\ln p)^{\frac{1}{3}}(\ln(\ln p))^{\frac{2}{3}}\right)}$。当选取的随机数为足够大的素数时，根据 ξ、p、q 计算 α 的值是计算不可行的。

若敌手想窃取签名者的私钥 O_{prv}，则必须计算出 $\Phi(n)$ 的值；考虑一般情形分析有

$$n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$$

$$\Phi(n)=\prod_{i=1}^{k}\left(p_i^{e_i}-p_i^{e_i-1}\right) \tag{15}$$

根据式(15)，该计算为大整数的因子分解难题。故交易篡改成功的概率可忽略。证毕。

定理 2　敌手攻击 TTP 与 ORG 中的一个或多个节点，导致指定 TO 信息泄露的概率可以忽略。

证明　将 TTP 的节点表示为集合 $\{T_1,T_2,\cdots,T_n\}$，假设敌手攻击 TTP 的节点 T_i，致使节点 T_i 中存储的用户信息泄露，泄露的信息包括 Hash(m) 及其对应的 k。敌手通过 TTP 节点 T_i 中存储的信息，仅能通过式(7)计算 m'；无法得知该笔交易数据对应 TO 的身份隐私信息。同理，若敌手攻击 ORG 节点集合为 $\{O_1,O_2,\cdots,O_n\}$ 中的节点 O_i，获取 ORG 节点 O_i 中存储的 TO 部分信息；根据节点 O_i 中存有的 $\omega^*_{m'}$ 以及 TO 身份信息，敌手无法对泄露的数据信息进行合理应用。若同时攻击 TTP 和 ORG 的多个节点，敌手分别从两方节点中获取了 TO 部分信息。因 TTP 和 ORG 对 TO 的部分信息进行存储时，使用分布式集群存储的方案；敌手通过攻击 TTP 节点得到的 TO 交易信息与攻击 ORG 节点得到的 TO 交易信息比对上的可能性极低。证毕。

定理 3　具有窃听能力的敌手窃听到 CB 上的交易数据并对其进行有效分析的概率可以忽略。

证明　本文方案的分级加密方法中，对交易数据的保护基于 SM4 对称加密算法和 Paillier 同态加密算法。SM4 加密算法的安全程度与 128 bit 的 AES 相当，可抵抗差分攻击和线性攻击，目前并没有发现有效的攻击手段。Paillier 同态加密算法基于复合剩余类的困难问题；在私钥保存完好的情况下，并没有行之有效的攻击手段。在对 SM4 对称加密算法和 Paillier 同态加密算法的密钥进行在线传输时，本文方案使用基于离散对数难题的椭圆曲线加密算法对其进行加密后，再在安全网络环境下进行线上传输，通过协同加密手段为交易数据的安全保护链建立闭环，故定理 3 成立。证毕。

定理 4　对于敌手发动的恶意交易攻击，本文方案虽无法对恶意交易的发起进行阻止，但能对恶意交易进行追溯。

证明　根据公平盲签名的条件匿名性，ORG 可以与 TTP 对恶意交易发起联合追溯。恶意交易追溯如图 5 所示，具体追溯过程分为以下 5 个步骤。

步骤 1　恶意交易发生时，Tracer 通过 $\omega^*_{\mathrm{Hash}(m)}$ 追查到恶意交易的签名方 ORG。

步骤 2　Tracer 向 ORG 提供恶意交易的数据信息，并委托 ORG 追溯该笔交易的发起者。

步骤 3　ORG 向 TTP 申请合作，向 TTP 提交 m 和 $\omega^*_{\mathrm{Hash}(m)}$；并向 TTP 提供其私钥 O_{prv} 以证明身份。

步骤 4　TTP 收到 ORG 的合作请求时，先通过 O_{prv} 验证该笔交易是否由提出追溯申请的 ORG 签名授权。若验证通过，则 TTP 计算 Hash(m)，将其与本地数据库中存储的 k 以及 O_{pub} 结合，计算

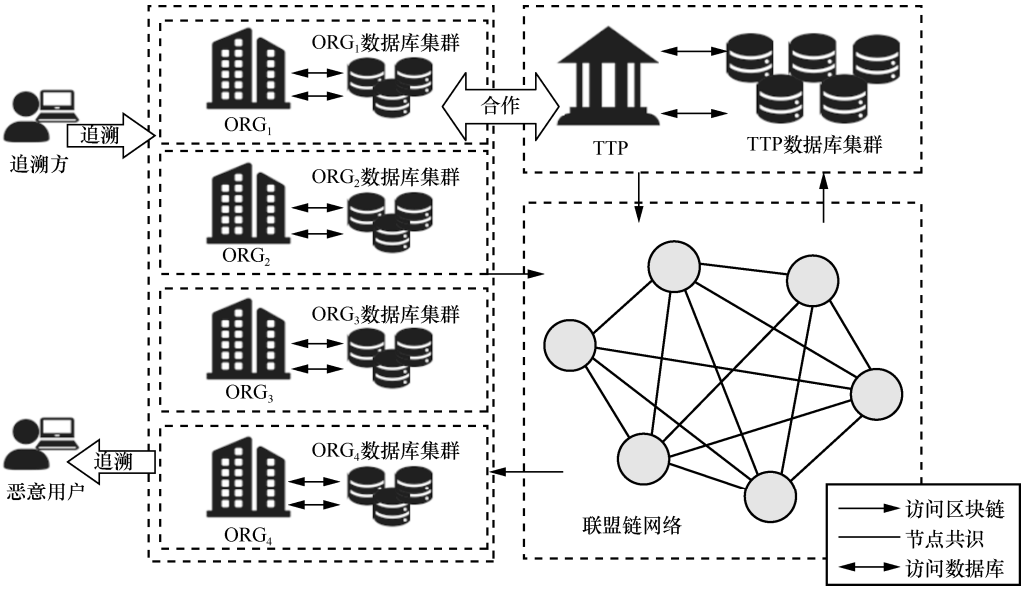


图 5 恶意交易追溯

表 2 效率分析对比

方案	加密理论时间开销	解密理论时间开销	加密体制	同态属性	密文可监管
文献[28]方案	$2T_{\mathrm{E}}+T_{\mathrm{X}}$	$2(T_{\mathrm{E}}+T_{\mathrm{X}})$	概率型	加法	是
文献[31]方案	$2k(2T_{\mathrm{E}}+T_{\mathrm{X}})$	$2(T_{\mathrm{m}}+kT_{\mathrm{E}})$	概率型	加法	是
文献[32]方案	T_{E}	T_{E}	确定型	乘法	是
本文方案	$X\%T_{\mathrm{SM4}}+Y\%(2T_{\mathrm{E}}+T_{\mathrm{X}})$	$X\%T_{\mathrm{SM4}}+Y\%2(T_{\mathrm{E}}+T_{\mathrm{X}})$	概率型	加法	是

$m'=\mathrm{Hash}(m)k^{e_{\mathrm{org}}} \bmod n$；将 m' 返回给 ORG。ORG 使用 O_{prv} 与 m' 计算得出 $\omega_{m'}^{*}=(m')^{d_{\mathrm{org}}} \bmod n$。

步骤 5 ORG 通过 $\omega_{m'}^{*}$ 查询本地数据库，得到被追溯的恶意交易发起用户的身份信息，联合监管部门对其进行相应处罚；至此追溯完成。

证毕。

3.3 效率分析及实验

本文方案中的分级加密方法拟在保护交易数据安全的基础上提高加解密过程的效率。分级加密方法的计算代价分别来自对称加密和同态加密两方面。定义符号 T_{X} 表示模乘运算的时间开销，T_{E} 表示模幂运算的时间开销，T_{SM4} 表示执行一次 SM4 加解密运算的时间开销，T_{m} 表示执行一次乘法运算的时间开销。将文献[28,31-32]方案与本文方案进行效率对比分析，其效率分析对比如表 2 所示，其中 $X\%+Y\%<1$。

根据表 2 分析可知，文献[31]方案因加密过程需进行 k 次循环，理论时间开销大于其他方案；而文献[28]方案对于数据信息的保护选择了改进的同态加密算法进行单级加密处理，一定程度上降低了加解密过程的耗时；文献[32]方案的加密过程基于 RSA 同态加密算法，其理论时间开销最低。将本文所提分级加密方法与表 2 中其他方案进行仿真实验对比真实效率，仿真实验选用 Java 为主要编程语言实现代码编写，代码基于 bouncycastle 库实现分级加密方法，调用 java.math.BigInteger 类实现大整数的运算；实验设备及其参数如表 3 所示。

表 3 实验设备及其参数

设备	参数
CPU 型号	AMD Ryzen 7 5800H
CPU 主频/GHz	3.20
内存/GB	16
系统类型	Win10-64 bit
软件平台	IntelliJ IDEA & JDK 1.8

考虑到区块链中的每一个区块都是大小有限的数据（一般不超过 1 Mbit），区块分为区块头和区块体；仿真实验选取 5～50 kbit 的 10 组不同大小的测试文件模拟 10 个不同的区块体进行加解密测试，并且对每组测试用例进行 5 次测量，实验结果取 5 次测量值的平均值。实际应用中需要进行二次

计算的数据量往往仅占数据总量的一小部分，为模拟真实情况，测试用例中的静态数据量占比应高于动态数据，故设置敏感度数据比例为 1:2:1；同时考虑控制变量原则，此处所使用的敏感度数据比例始终保持 1:2:1；即可公开数据:不可公开数据(静态):不可公开数据(动态) = 1:2:1。不同方案加密开销对比如图 6 所示，实验数据如表 4 所示。

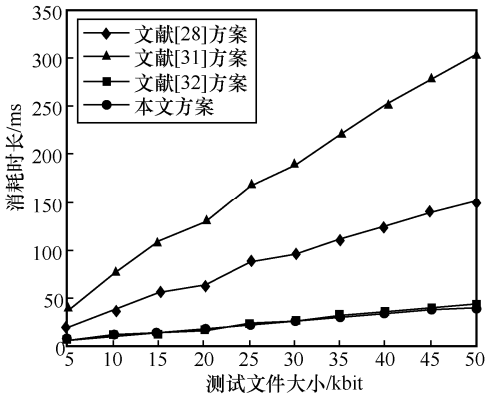


图 6　不同方案加密开销对比

表 4　不同方案加密开销对比

文件大小/kbit	消耗时长/ms			
	文献[28]方案	文献[31]方案	文献[32]方案	本文方案
5	19.161	37.132	6.723	5.173
10	37.718	75.923	12.684	10.002
15	55.892	109.851	14.015	13.746
20	62.902	129.55	18.762	16.714
25	87.91	166.82	22.516	23.619
30	95.725	189.345	26.271	25.272
35	111.94	219.876	31.151	29.485
40	125.856	253.451	36.417	33.167
45	140.121	277.623	39.438	36.931
50	150.85	303.67	43.787	39.043

从图 6 和表 4 可以看出，本文方案的加密开销比对比方案中理论耗时最少的文献[32]方案低 15%以上，与同样满足加法同态运算的文献[28,31]方案相比，效率提升明显。为测试本文方案应对不同数据时的效率变化，选取对 3 组不同敏感度分级的测试用例，分别使用相同的 10 组测试文件进行测试比较，并且对每组测试用例进行 5 次测量，最终结果取其平均值。不同分级比例加密开销对比如图 7 所示，实验数据如表 5 所示，其中，a 表示可公开数据:不可公开数据(静态):不可公开数据(动态)=1:2:1，b 表示可公开数据:不可公开数据(静态):不可公开数据(动态) =1:3:1，c 表示可公开数据:不可公开数据(静态):不可公开数据(动态)=1:5:1。

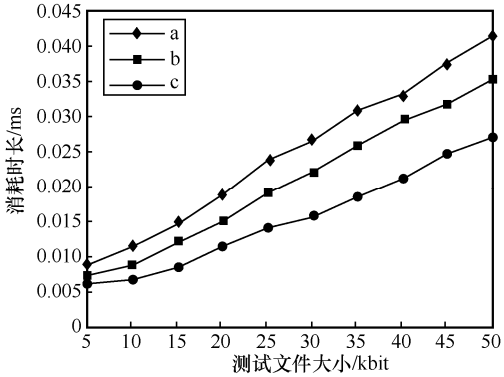


图 7　不同分级比例加密开销对比

表 5　不同分级比例加密开销对比

文件大小/kbit	消耗时长/ms		
	a	b	c
5	5.173	5.137	5.062
10	10.002	8.911	6.932
15	13.746	12.141	8.633
20	16.714	15.147	11.535
25	23.619	19.103	14.13
30	25.272	22.168	15.521
35	29.485	25.843	18.525
40	33.167	29.37	21.318
45	36.931	31.905	24.725
50	39.043	35.413	27.107

从图 7 和表 5 可以看出，随着静态数据在总文件数据中所占比例的不断增加，分级加密方法在时间开销上的优势呈不断增加的趋势。为进一步对比分析本文分级加密方法与其他方法的解密过程真实效率，选取上述加密测试实验的结果数据作为新的测试文件；为保证数据可靠性，此处同样对每组测试用例进行 5 次测量，最终结果取其平均值。不同方案解密开销对比如图 8 所示，实验数据如表 6 所示。

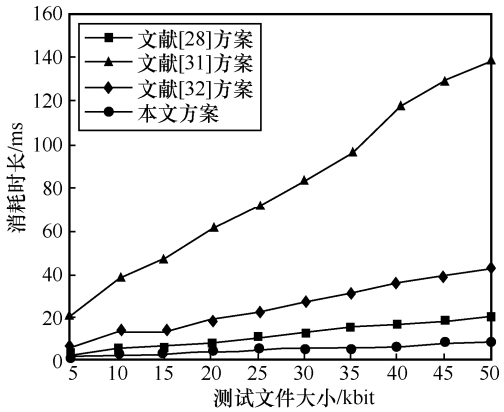


图 8　不同方案解密开销对比

表 6　　不同方案解密开销对比

文件大小/kbit	消耗时长/ms			
	文献[28]方案	文献[31]方案	文献[32]方案	本文方案
5	2.218	21.055	6.702	1.065
10	4.093	36.302	12.661	1.606
15	6.315	47.413	13.937	2.438
20	7.957	60.399	18.758	2.979
25	10.126	69.764	22.488	3.732
30	13.093	82.301	26.250	4.643
35	15.411	95.621	31.083	5.413
40	16.258	115.632	36.389	5.965
45	18.539	128.456	39.217	6.534
50	21.145	137.031	42.856	7.586

从图 8 和表 6 可以看出，本文方案的解密时间开销相比文献[31]方案明显减少；较文献[28]方案和文献[31]方案，本文方案的解密时间开销分别降低约 62%和 83%。选取 50 kbit 的数据文件进行加解密总时间开销对比，结果如图 9 所示，实验数据如表 7 所示。

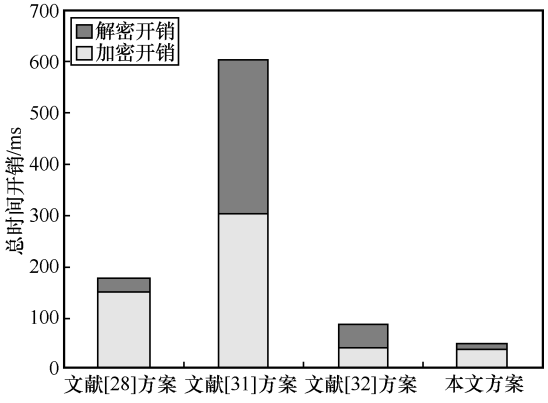


图 9　加解密总时间开销对比

表 7　　加解密总时间开销对比

方案	加密时长/ms	解密时长/ms	总时长/ms
文献[28]方案	150.85	21.145	171.995
文献[31]方案	303.67	137.031	440.701
文献[32]方案	43.787	42.856	86.643
本文方案	39.043	7.586	46.629

从图 9 和表 7 可以看出，本文方案与对比方案中耗时最短的文献[32]方案相比，总消耗时间降低约 46%。综上所述，本文方案能在保证对部分数据进行同态运算的同时，有效降低交易数据加解密过程的时间开销，在联盟链实际应用中具有一定的使用价值。

4　结束语

本文方案基于公平盲签名的条件匿名性以及同态加密算法的同态运算特性，分别从用户身份隐私保护和链上交易数据的隐私安全两方面展开研究。通过对现有公平盲签名进行重新设计，结合零知识证明技术，实现了对联盟链用户身份隐私的保护；安全性分析证明，重新设计的公平盲签名方案能有效抵抗攻击者窃取用户身份信息，并能够对恶意交易进行追溯。另一方面，基于 Paillier 同态加密算法，根据敏感级别对数据进行细粒度划分设计出一套分级加密方法；安全性分析和仿真实验对比检测证明，该分级加密方法具备良好的安全性和能效性。在确保方案功能完备的前提下，进一步完善公平盲签名的联盟链身份隐私保护方案，降低分级加密方法中加密解密过程的时间开销，是下一步研究的主要工作。

参考文献：

[1] GAI K K, WU Y L, ZHU L H, et al. Privacy-preserving energy trading using consortium blockchain in smart grid[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3548-3558.

[2] DU M X, CHEN Q J, XIAO J, et al. Supply chain finance innovation using blockchain[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1045-1058.

[3] 李娟娟, 袁勇, 王飞跃. 基于区块链的数字货币发展现状与展望[J]. 自动化学报, 2021, 47(4): 715-729.
LI J J, YUAN Y, WANG F Y. Blockchain-based digital currency: the state of the art and future trends[J]. Acta Automatica Sinica, 2021, 47(4): 715-729.

[4] ZHANG X H, CHEN X F. Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network[J]. IEEE Access, 2019, 7: 58241-58254.

[5] SHE W, GU Z H, LYU X K, et al. Homomorphic consortium blockchain for smart home system sensitive data privacy preserving[J]. IEEE Access, 2019, 7: 62058-62070.

[6] 谭海波, 周桐, 赵赫, 等. 基于区块链的档案数据保护与共享方法[J]. 软件学报, 2019, 30(9): 2620-2635.
TAN H B, ZHOU T, ZHAO H, et al. Archival data protection and sharing method based on blockchain[J]. Journal of Software, 2019, 30(9): 2620-2635.

[7] ZHENG Z B, XIE S A, DAI H N, et al. Blockchain challenges and opportunities: a survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352.

[8] 朱立, 俞欢, 詹士潇, 等. 高性能联盟区块链技术研究[J]. 软件学报, 2019, 30(6): 1577-1593.
ZHU L, YU H, ZHAN S X, et al. Research on high-performance consortium blockchain technology[J]. Journal of Software, 2019, 30(6): 1577-1593.

[9] FENG Q, HE D B, ZEADALLY S, et al. A survey on privacy protec-

tion in blockchain system[J]. Journal of Network and Computer Applications, 2019, 126: 45-58.

[10] 王晨旭, 程加成, 桑新欣, 等. 区块链数据隐私保护：研究现状与展望[J]. 计算机研究与发展, 2021, 58(10): 2099-2119.
WANG C X, CHENG J C, SANG X X, et al. Data privacy-preserving for blockchain: state of the art and trends[J]. Journal of Computer Research and Development, 2021, 58(10): 2099-2119.

[11] CHAUM D, HEYST V E. Group signatures[C]//Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'91). Berlin: Springer, 1991: 257-265.

[12] KOMANO Y, OHTA K, SHIMBO A, et al. Toward the fair anonymous signatures: deniable ring signatures[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2007, E90-A(1): 54-64.

[13] LINDELL Y, PINKAS B. Secure multiparty computation for privacy-preserving data mining[J]. Journal of Privacy and Confidentiality, 2012, 25(2): 761-766.

[14] CHAUM D. Blind signatures for untraceable payments[C]//Advances in Cryptology. Berlin: Springer, 1983: 199-203.

[15] ZHANG S J, LEE J H. A group signature and authentication scheme for blockchain-based mobile-edge computing[J]. IEEE Internet of Things Journal, 2020, 7(5): 4557-4565.

[16] LI X F, MEI Y R, GONG J, et al. A blockchain privacy protection scheme based on ring signature[J]. IEEE Access, 2020, 8: 76765-76772.

[17] STADLER M, PIVETEAU J M, CANENISCH J. Fair blind signatures[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1995: 209-219.

[18] 李瑞琪, 贾春福, 王雅飞. 基于 NTRU 的多密钥同态代理重加密方案及其应用[J]. 通信学报, 2021, 42(3): 11-22.
LI R Q, JIA C F, WANG Y F. Multi-key homomorphic proxy re-encryption scheme based on NTRU and its application[J]. Journal on Communications, 2021, 42(3): 11-22.

[19] 王后珍, 蔡鑫伟, 郭岩, 等. 基于矩阵填充问题的五轮零知识身份认证方案[J]. 通信学报, 2021, 42(11): 79-86.
WANG H Z, CAI X W, GUO Y, et al. 5-pass zero-knowledge identity authentication scheme based on matrix completion problem[J]. Journal on Communications, 2021, 42(11): 79-86.

[20] ZHANG R, XUE R, LIU L. Security and privacy on blockchain[J]. ACM Computing Surveys, 2020, 52(3): 1-34.

[21] 李宇溪, 周福才, 徐紫枫. 支持 K-近邻搜索的移动社交网络隐私保护方案[J]. 计算机学报, 2021, 44(7): 1481-1500.
LI Y X, ZHOU F C, XU Z F. Privacy-preserving K-nearest-neighbor search over mobile social network[J]. Chinese Journal of Computers, 2021, 44(7): 1481-1500.

[22] DOWLIN N, GILAD-BACHRACH R, LAINE K, et al. Manual for using homomorphic encryption for bioinformatics[J]. Proceedings of the IEEE, 2017, 105(3): 552-567.

[23] GENTRY C. A fully homomorphic encryption scheme using ideal lattices[C]//Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 169-178.

[24] ACAR A, AKSU H, ULUAGAC A S, et al. A survey on homomorphic encryption schemes: theory and implementation [J]. ACM Computing Surveys, 2018, 51(4): 1-35.

[25] 于戈, 聂铁铮, 李晓华, 等. 区块链系统中的分布式数据管理技术: 挑战与展望[J]. 计算机学报, 2021, 44(1): 28-54.
YU G, NIE T Z, LI X H, et al. The challenge and prospect of distributed data management techniques in blockchain systems[J]. Chinese Journal of Computers, 2021, 44(1): 28-54.

[26] CHRISTIAN C. Architecture of the hyperledger blockchain fabric[C]//Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers. New York: ACM Press, 2016: 14-17.

[27] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of the Thirteenth EuroSys Conference. New York: ACM Press, 2018: 1-30.

[28] 徐文玉, 吴磊, 阎允雪. 基于区块链和同态加密的电子健康记录隐私保护方案[J]. 计算机研究与发展, 2018, 55(10): 2233-2243.
XU W Y, WU L, YAN Y X. Privacy-preserving scheme of electronic health records based on blockchain and homomorphic encryption[J]. Journal of Computer Research and Development, 2018, 55(10): 2233-2243.

[29] PHONG L T, AONO Y, HAYASHI T, et al. Privacy-preserving deep learning via additively homomorphic encryption[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(5): 1333-1345.

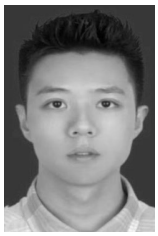
[30] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//Proceedings of EUROCRYPT 1999. Berlin: Springer, 1999: 223-238.

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

[32] GAUTAM P, ANSARI M D, SHARMA S K. Enhanced security for electronic health care information using obfuscation and RSA algorithm in cloud computing[J]. International Journal of Information Security and Privacy, 2019, 13(1): 59-69.

[作者简介]

张学旺（1974− ），男，湖南祁东人，重庆大学博士生，重庆邮电大学副教授，主要研究方向为数据安全与隐私保护、区块链与物联网等。



黎志鸿（1997− ），男，四川成都人，重庆邮电大学硕士生，主要研究方向为区块链技术、互联网软件技术及安全等。

林金朝（1966− ），男，四川蓬溪人，博士，重庆邮电大学教授、博士生导师，主要研究方向为无线通信传输技术、BAN 与信息处理技术等。