基于新型公平盲签名和属性基加密的食用农产品溯源方案

张学旺*①② 林金朝③ 黎志鸿① 姚亚宁①

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：为解决食用农产品溯源中存在的身份隐私易泄露、难监管以及溯源数据共享困难等问题，该文提出一种基于新型公平盲签名和属性基加密的食用农产品溯源方案。该方案在联盟链授权访问、不可篡改特性的基础上，结合椭圆曲线和零知识证明提出一种新型公平盲签名方法，实现了食用农产品数据上传者身份条件匿名并通过双重ID机制避免了签名方陷害问题；方案同时采用Asmuth-Bloom门限改进的属性基加密结合智能合约技术实现了权限分层的食用农产品溯源数据秘密共享。各项分析及实验结果表明，该方案具备良好的安全性和功能性。

关键词：农产品溯源；公平盲签名；属性基加密；身份隐私；联盟链

中图分类号：TN918.4; TP309 **文献标识码**：A **文章编号**：1009-5896(2023)03-0836-11

DOI: 10.11999/JEIT221077

Traceability Scheme of Edible Agricultural Products Based on Novel Fair Blind Signature and Attribute-based Encryption

ZHANG Xuewang①② LIN Jinzhao③ LI Zhihong① YAO Yaning①

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 Photoelectronic Information Sensing and Transmitting Technology, Chongqing* 400065, *China*)

Abstract: In order to solve the problems of identity privacy easy to leak, difficult to monitor and difficult to share the traceability data in the existing edible agricultural products traceability scheme, a traceability schema of edible agricultural products based on novel fair blind signature and attribute-based encryption is proposed. Based on the authorized access and non-tampering characteristics of consortium blockchain, a novel fair blind signature method is proposed by combining elliptic curve and zero-knowledge proof, which achieves anonymity of the identity of the edible agricultural product data uploader and avoids the problem of enmiting the signer through the double ID mechanism. At the same time, the attribute-based encryption improved by Asmuth-Bloom threshold combined with smart contract technology is adopted to realize the secret sharing of traceability data of edible agricultural products with hierarchical permissions. The analysis and experimental results demonstrate that the proposed scheme has good security and functionality.

Key words: Traceability of agricultural products; Fair blind signature; Attribute-based encryption; Identity privacy; Consortium blockchain

收稿日期：2022-08-16；改回日期：2023-02-28；网络出版：2023-03-03

*通信作者： 张学旺 zhangxw@cqupt.edu.cn

基金项目：国家自然科学基金联合重点项目(U21A20447)，南充市科技计划(21YFZJ0033)

Foundation Items: The Natural Science Foundation Key Project of China (U21A20447), The Science and Technology Program of Nanchong (21YFZJ0033)

1　引言

近年来，世界各地陆续出现“毒鸡蛋”、“瘦肉精”、“毒奶粉”等食用农产品质量安全问题，人们对于食用农产品质量安全的关注度居高不下；为解决该问题国内外相继出台了相应的法律法规[1,2]，社会各界对食用农产品质量安全的可追溯性提出了新要求。以是否运用区块链技术为分割点，食用农产品质量安全溯源技术可分为传统溯源研究和基于区块链技术的溯源研究两大类。

传统溯源普遍运用2维码[3]、无线射频[4]、互补金属氧化物半导体/电荷耦合器件(Complementary Metal Oxide Semiconductor/Charge Coupled Device, CMOS/CCD)相机[5]等物联网技术采集农产品供应链的数据，再由相关企业将数据录入到溯源数据库中。企业可对溯源数据库中的数据随意修改，导致数据的可信度不高；且农产品供应链中各企业数据相对独立，出现安全问题时准确追责的难度较高[6]。因此，传统溯源并不能较好完成食用农产品质量安全信息的追溯。

区块链技术具有匿名、可追溯、公开共享等特性[7]；将它应用于溯源，能有效解决传统溯源存在的数据可信度低及数据孤岛问题[8]。国内外对基于区块链技术的食用农产品质量安全溯源研究从多方面展开。Feng等人[9]提出区块链的架构设计框架和适用性应用分析流程图，为使用区块链技术提高食品可持续性产生了积极影响；于合龙等人[10]基于区块链技术实现了水稻供应链溯源，并结合椭圆曲线和对称加密算法解决了溯源数据泄密问题。Cao等人[11]研究基于区块链的供应链实施，有效解决了跨境牛肉的安全可信问题。Salah等人[12]应用基于区块链的溯源技术结合星际文件系统有效实现了对大豆质量安全的可信追溯。任守纲等人[13]从农产品产业链角度出发，设计实现基于区块链的农作物全产业链信息溯源平台，提出基于信誉监督机制共识算法CSBFT (Credit-Supervisor Byzantine Fault Tolerance)以提高联盟链场景下共识机制的安全性和效率。刘双印等人[14]提出“On-Chain + Off-Chain”农产品质量安全溯源信息协同管理存储策略，解决了农产品溯源区块链网络中各节点数据存储压力大、查询效率低和数据爆炸等问题。Zhang等人[15]基于区块链和密文策略的属性加密(Ciphertext Policy Attribute Based Encryption, CP-ABE)提出一种安全可信的农产品追溯系统(secure and trusted agricultural product traceability system, BCST-APTS)，解决了农产品产业链各方之间的互信、隐私保护、细粒度访问控制等问题。由于区块链中全账本节点的数据库中都存有全链数据[16]，依靠区块链技术难以实现溯源数据的安全多方秘密共享；基于区块链的溯源可通过交易信息快速定位溯源数据的发布者，身份信息的无条件透明性为发布者的隐私带来威胁；Kamilaris等人[17]指出基于区块链的溯源技术有利于实现透明食品供应链，但目前仍存在区块链账户对应的私钥可能泄露、区块链协议可扩展困难、区块链隐私泄露、数据共享困难、监管困难等问题。

针对食用农产品溯源技术存在的身份隐私易泄露、溯源数据共享困难以及监管困难等不足，本文基于联盟链技术提出一种结合公平盲签名和属性基加密的食用农产品溯源方案，其贡献如下：

(1)提出一种基于椭圆曲线和零知识证明的新型公平盲签名方法并应用于食用农产品溯源。能耗方面：降低密钥生成中心的工作强度，减少联盟链网络存储负担，同时提高签名效率；功能方面：在对食用农产品供应链参与方身份匿名的同时，实现对供应链全阶段溯源信息的监管以及问题阶段的精准追责；并通过双重ID机制有效避免恶意签名方对普通交易用户的陷害问题。

(2)采用Asmuth-Bloom门限改进的属性基加密技术结合智能合约技术，同时依靠联盟链账本间数据公开共享的特性，在实现溯源数据按权限分层共享的基础上，提升溯源效率。

2　相关技术

2.1　食用农产品全产业链

农产品产业链参与的主体众多，涉及节点多且各节点信息化水平参差不齐、信息多源异构等[14]。以农作物为例，农作物全产业链包含产前、产中和产后多阶段，是关联原料购买、种植管理、仓储服务、加工生产、物流运输、分级销售、监管取证等多环节的完整链状结构，结构如图1 所示[13]。

2.2　公平盲签名

公平盲签名思想源于盲签名技术[18]，盲签名与以群、环签名[19,20]为代表的去中心化混币机制不同，其功能的实现依赖于第三方混币机构。盲签名技术因具有完全匿名的特性被广泛应用，不足在于敌手的恶意行为难以被监管方所追溯。公平盲签名解决了传统盲签名技术存在的不可追溯问题[21]，它在盲签名的基础上引入第三方，以联盟链场景为例，交易用户在向签名方申请对交易的签名授权前，需先提交相应身份信息获取第三方对交易的背书，第三方存储交易用户的身份信息；当恶意交易出现时，签名方可以通过第三方对发起恶意交易的用户进行追溯。

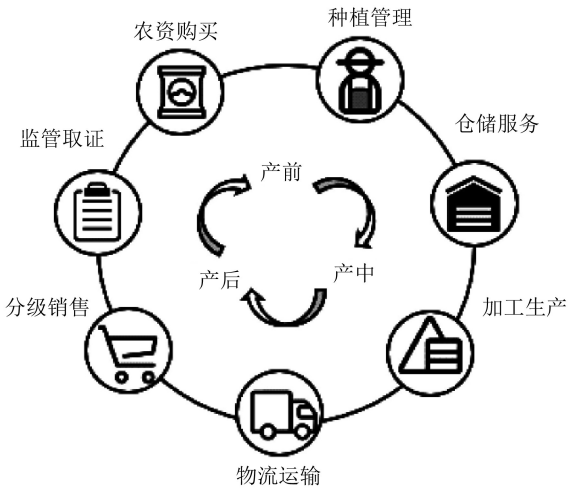

图 1 农作物全产业链

2.3 属性基加密

属性基加密实现了对数据信息的1次加密多方共享。根据访问策略的不同，可将属性基加密分为密文策略的属性加密(CP-ABE)和密钥策略的属性加密(Key Policy Attribute Based Encryption, KP-ABE)两类；基于多方秘密共享的特性，属性基加密目前已应用于多个领域[22–24]。本文重点研究基于CP-ABE的溯源数据多方秘密共享，CP-ABE工作流程有以下4个步骤：

(1) $\text{Setup}(\lambda)\to(\text{PK},\text{MK})$：输入隐式安全参数$\lambda$，输出系统公钥PK和主私钥MK；

(2) $\text{KeyGen}(\text{MK},S)\to(\text{SK})$：输入主私钥MK和属性集合$S$，根据策略为数据访问用户输出其私钥SK, SK与$S$相关；

(3) $\text{Encrypt}(\text{PK},M,T)\to(\text{CT})$：数据拥有者输入系统公钥PK、明文$M$以及访问结构$T$进行加密，输出包含访问结构$T$的密文CT，只有满足特定属性集的数据访问用户才能对数据进行访问；

(4) $\text{Decrypt}(\text{SK},\text{CT},\text{PK})\to(M)$：数据访问者输入私钥SK，密文CT和系统公钥PK，若SK对应的S满足CT中的T，则可正确解密得到明文M。

2.4 Asmuth-Bloom门限方案

Asmuth-Bloom门限方案[25]基于中国剩余定理，选择(m,n)门限对明文M进行加密，使用任意m个影子就能恢复M。影子选取分为4个步骤。

(1) 随机选择一个大于M的大素数p。

(2) 选取n个小于p的数$\{d_1,d_2,\cdots,d_n\}$满足以下条件：

(a) d_i需按升序排列，即$d_i<d_{i+1}$；

(b) 对$d_i\in\{d_1,d_2,\cdots,d_n\}$和$d_k\in\{d_1,d_2,\cdots,d_n\}$，当$i\neq k$时，$\gcd(d_i,d_k)=1$；

(c) 对任意$d_i\in\{d_1,d_2,\cdots,d_n\}$，有$\gcd(d_i,p)=1$；

(d) $\prod_{i=1}^{m}d_i>p\prod_{k=n-m+2}^{n}d_k$。

(3) 计算$d_{\text{mult}}=\prod_{i=1}^{n}d_i$，选取$r\in[0,\dfrac{d_{\text{mult}}}{p+1}]$，使用$r$和$p$对明文$M$进行处理得到$M'=M+rp$。

(4)根据$k_i=M'\bmod d_i$计算$\{k_1,k_2,\cdots,k_n\}$。

3 基于新型公平盲签名和属性基加密的食用农产品溯源方案

基于新型公平盲签名和属性基加密的食用农产品溯源方案(简称本方案)，详述如下：

3.1 方案模型

本方案使用的主要术语如表1所示。

本方案支持溯源数据上传者匿名对其加密的溯源数据进行基于属性的细粒度访问控制及身份条件匿名；溯源数据的访问者通过基于自身属性的私钥SK对特定溯源数据进行安全访问。本方案模型框架涉及7个实体，包括溯源数据拥有者TDO、溯源数据访问者TDV、授权组织机构AO、联盟链CB、密钥生成中心KGC、星际文件系统IPFS、第三方监管机构TPR。方案模型如图2所示，其中共享链表示溯源数据的上传和获取流程，追溯链表示对问题溯源数据的TDO追溯流程。结合食用农产品溯源场景对各实体的详细描述如下：

(1) TDO是指食用农产品全产业链上的产前、产中和产后各阶段实际参与溯源数据上传的用户。TDO是溯源数据的来源，具有数据的所有权和访问控制权。TDO通过客户端加密溯源数据后上传IPFS，使用属性基加密技术加密对称密码算法的密钥得到密文CT，并将IPFS返回的哈希值和密文CT存储到联盟链中。

表 1 主要术语

符号	符号表示的含义
TDO	Traceability Data Owner, 溯源数据拥有者
TDV	Traceability Data Visitor, 溯源数据访问者
AO	Authorized Organization, 授权组织机构
CB	Consortium Blockchain, 联盟链
KGC	Key Generation Center, 密钥生成中心
IPFS	Inter Planetary File System, 星际文件系统
TPR	Third Party Regulator, 第三方监管机构
PK	非对称密码算法的公钥
SK	非对称密码算法的私钥
MK	主私钥
CT	密文
M	明文
S	属性集
T	访问树
K	对称密码算法的密钥

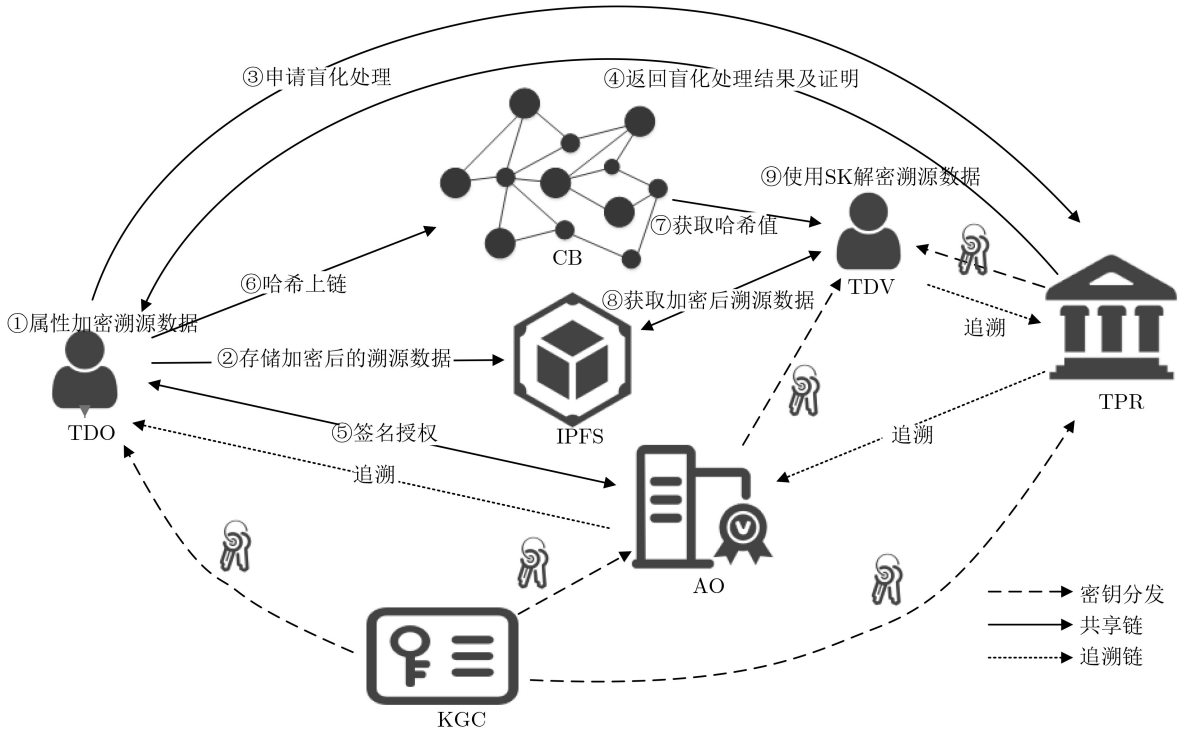

图 2 方案模型

(2) TDV是指访问溯源数据的用户，包括AO和TPR中的部分用户如生产管理者、仓储管理者、监管者等；该类用户能使用KGC生成的密钥SK对特定溯源数据进行安全访问。

(3) AO是指食用农产品全产业链上的产前、产中和产后各阶段实际参与溯源数据上传的用户所在组织机构，包括农产品生产机构、各级企业、物流公司等。TDO上传溯源数据前，通过AO对交易进行背书和授权操作，联盟链其余成员很难通过分析交易直接找到其TDO，实现了TDO对外的身份隐藏；其本地数据库采用分布式架构。

(4) CB在此处特指该食用农产品全产业链各AO和TPR节点所组成的联盟链结构；当TDO通过客户端发起交易时，CB各节点采用约定俗成的共识机制对交易进行合法性验证并完成后续操作。

(5) KGC为整个系统生成系统公钥PK和主私钥MK，利用主私钥MK和属性集S为TDV生成私钥SK，系统建立时为供应链各节点生成其密钥对并定时更新，同时实现密钥的分发操作。

(6) IPFS用于存放TDO加密后的溯源数据，IPFS分布式存储的特性在其与CB良好结合的基础上，有效避免了存储节点的单点故障问题。

(7) TPR拥有最大的溯源数据访问权限，能对食用农产品全产业链产前、产中和产后各阶段溯源数据进行安全访问，并且能协同AO对TDO的真实身份发起追溯，实现了TDO的身份条件匿名，其本地数据库使用分布式架构。

3.2 方案构建

本方案通过公平盲签名思想对TDO的身份信息进行条件匿名处理，并采用属性基加密技术结合联盟链与IPFS协同架构实现对溯源数据的链上链下协同存储及多方秘密共享。方案构建主要包括：联盟链系统搭建、溯源数据加密、溯源数据存储、溯源数据共享、TDO身份追溯。具体方案如下：

阶段1　联盟链系统搭建。TPR与各AO共建食用农产品溯源联盟链，系统搭建分为节点构建、系统初始化、属性密钥生成、节点密钥生成、令牌分发和ID生成6个步骤，如下所示：

(1) 节点构建：TPR与AO分别创建多个CB节点；

(2) 系统初始化：KGC选择隐式安全参数λ，并随机选择一个阶为素数p的双线性群G_0, G_0的大小由λ决定；用g表示群G_0的一个生成元，随机选取加密指数α,β满足$\alpha,\beta\in\mathbb{Z}_P$。如式(1)所示生成系统公钥PK和主私钥MK

$$\left.\begin{aligned}&\mathrm{PK}=(G_0,g,g^{\beta},g^{1/\beta},e(g,g)^{\alpha})\\&\mathrm{MK}=(\beta,g^{\alpha})\end{aligned}\right\}\tag{1}$$

(3) 属性密钥生成：KGC收集该食用农产品溯源链上所有TDV的属性，构成属性集S；随后选取任意数$\gamma\in\mathbb{Z}_P$，并为每一个属性$S_{\mathrm{i}}\in S$，随机生成

一个随机数$\gamma_i \in \mathbb{Z}_P$。如式(2)计算TDV私钥SK，并对其进行加密处理

$$\begin{aligned}&\mathrm{SK} = (D = g^{\frac{\alpha+\gamma}{\beta}}, D'_{S_i} = g^{\gamma_{S_i}},\\&\forall S_i \in S : D_{S_i} = g^{\gamma} \cdot H(S_i)^{\gamma_{S_i}})\end{aligned} \tag{2}$$

(4) 节点密钥生成：KGC重复如下4个步骤分别为TPR与各AO生成其密钥对用以后续溯源数据存储阶段的签名验签操作：

(a) 选择有限域GF(q)上的椭圆曲线E；

(b) 基于安全性选择大素数$n > 2^{160}$，同时满足n整除$\#E(\mathrm{GF}(q))$且$n > 4\sqrt{q}$；

(c) 由西格尔定理知E上的整点个数是有限的，选择基点$G = (x_G, y_G) \in E(\mathrm{GF}(q))$，并随机生成整数$k \in \mathbb{Z}_n^*$，计算$R$=$kG$；

(d) 生成密钥对$\{d, Q = dG\}, d \in \mathbb{Z}_n^*$。

KGC定期为TPR与各AO生成新的密钥对，避免因密钥长时间使用增加的泄露风险；

(5) 令牌分发：首先AO与TPR协定方程$\xi = \alpha^{\mathrm{Token}} \mathrm{mod} \beta$用以后续TDO的身份认证，其中$\xi, \alpha, \beta$均为公开参数，其次AO为组织内的各TDO分发Token作为其身份令牌；

(6) ID生成：AO和TPR为TDO生成并分发双重ID, ID分别表示为$\mathrm{ID}_{\mathrm{AO}}$和$\mathrm{ID}_{\mathrm{TPR}}$。

阶段2 溯源数据加密。TDO对拟上传的溯源数据进行脱敏处理，处理分为两个步骤，如下所示：

(1) 原始数据脱敏：TDO选用SM4算法通过客户端对拟上传的溯源数据进行脱敏处理。

(2) 密钥加密：TDO使用属性加密技术加密SM4算法的对称密钥K，首先通过属性集S和主私钥MK构建访问树T，T中任意非叶子节点都为一个(m, n)门限，用以表现子节点之间的逻辑关系，当$m = n$时逻辑关系表示为与门，$m < n$时则表示为或门；T中任意叶子节点则用于存储TDO设置的秘密分割值、属性以及其对应的属性值，最终通过访问树T对K加密得到包含T的密文CT。传统CP-ABE进行秘密分割采用拉格朗日插值法，选用Asmuth-Bloom门限进行分割，秘密分割从T的根节点自顶向下展开，算法1展示一个非叶子节点的秘密分割过程。随机选取全局公开参数r，满足$r < (n/p) - 1$。

算法1 Asmuth-Bloom秘密分割

输入：m, n, S, MK

输出：$\{K_1, K_2, \cdots, K_n\}$

(1)选择素数$p >$ MK

(2)根据2.3节步骤2中条件，选取n个小于p的数$\{d_1, d_2, \cdots, d_n\}$

(3)使用$\{d_1, d_2, \cdots, d_n\}$计算$d_{\mathrm{mult}} = \prod_{i=1}^{m} d_i$

(4)对MK进行处理得到$K' = \mathrm{M}K + rp$

(5)**for** i 1 to n by 1 **do**

(6) $K_i = K' \bmod d_i$

(7)end **for**

(8)return $\{K_1, K_2, \cdots, K_n\}$

阶段3 溯源数据存储。TDO通过客户端完成溯源数据的脱敏操作后，将M'上传到IPFS中，得到IPFS返回的索引哈希值$H(M')$；TDO使用$\mathrm{ID}_{\mathrm{TPR}}$通过SM3杂凑算法计算$H(H(M')||\mathrm{CT}||\mathrm{ID}_{\mathrm{TPR}})$，将其与$H(M')$和CT组成Tx的data字段；Tx′表示未签名的交易，对Tx′进行编码处理后计算其哈希值$H(\mathrm{Tx}')$。交易基本结构如表2所示。

TDO, AO, TPR 3方通过新型公平盲签名对$H(\mathrm{Tx}')$进行条件匿名授权操作，具体过程分为6个步骤，如下所示：

(1) TDO使用$H(\mathrm{Tx}')$和Token向TPR发出交易注册申请，TPR通过零知识证明验证该TDO所属的AO；具体验证过程如下

(a) TDO通过客户端生成n个随机数表示为$\{t_1, t_2, \cdots, t_n\}$，其中$n \geq 16$且$t_n \in \mathbb{Z}_{\alpha-1}^*$；计算$\xi_n = \alpha^{t_n} \mathrm{mod} \beta$，将$\{\xi_1, \xi_2, \cdots, \xi_n\}$发送给TPR；

(b) TPR与TDO根据硬币投掷协议协同产生n个随机位$\{\tau_1, \tau_2, \cdots, \tau_n\} \to \{\eta_1, \eta_2, \cdots, \eta_n\}$；

(c) 若$\eta_i = 0$，TDO向TPR发送t_i；若$\eta_i = 1$，TDO向TPR发送$(t_i - t_v) \mathrm{mod}(\alpha - 1)$，其中$v = \min\{i | \beta_i = 1\}$；TPR验证式(3)是否成立

$$\xi_i = \beta^{(t_i - t_v) \mathrm{mod}(\alpha-1)} \xi_v \mathrm{mod} \alpha \tag{3}$$

(d) TDO向TPR发送$(\tau - t_v) \mathrm{mod}(\alpha - 1)$，TPR验证式(4)是否成立

$$\xi = \beta^{(\tau - t_v) \mathrm{mod}(\alpha-1)} \xi_v \mathrm{mod} \alpha \tag{4}$$

若以上验证均成立，TPR生成$\eta, \delta, \gamma \in \mathbb{Z}_n^*$作为盲因子，计算$A = \eta R + \delta G + \gamma Q = (x, y)$；通过盲化处理得到$\mathrm{Tx}'' = \eta^{-1}(H(\mathrm{Tx}') - \delta) \mathrm{mod} n$，向TDO返回参数$(A, \eta, \gamma, \mathrm{Tx}'', \sigma^*_{\mathrm{Tx}''} = \mathrm{Sig}_{\mathrm{TPR}}(\mathrm{Tx}''))$；

(2) TDO验证$\sigma^*_{\mathrm{Tx}''}$真实性后使用$(\sigma^*_{\mathrm{Tx}''}, \mathrm{Tx}'')$以及$\mathrm{ID}_{\mathrm{AO}}$向AO申请签名授权；

表 2 交易基本结构

字段	相关描述
nonce	TDO生成的唯一随机数，用于标示交易
fromAddress	根据交易的签名计算出AO的地址
toAddress	交易接收方的地址，即智能合约的地址
gas	本次交易允许最多消耗的gas数量
gasPrice	本次交易的gas单价
data	$H(H(M')\|\|\mathrm{CT}\|\|\mathrm{ID}_{\mathrm{TPR}})$, $H(M')$和CT

(3) AO验证$\sigma^*_{\mathrm{Tx}''}$及$\mathrm{ID}_{\mathrm{AO}}$真实性后，向TDO返回$\omega^*_{\mathrm{Tx}''}=\mathrm{Sig}_{\mathrm{AO}}(\mathrm{Tx}'')=d_{\mathrm{AO}}^{-1}(k-\mathrm{Tx}'')\mathrm{mod}n$；

(4) TDO验证$\omega^*_{\mathrm{Tx}''}$真实性后，根据式(5)对其进行解盲操作，得到$\omega^*_{H(\mathrm{Tx}')}$

$$\omega^*_{H(\mathrm{Tx}')}\equiv(\eta\omega^*_{\mathrm{Tx}''}+\gamma)\mathrm{mod}n \tag{5}$$

(5) TDO将参数$(A,e=H(\mathrm{Tx}'),\omega^*_{H(\mathrm{Tx}')})$作为签名组与Tx′结合后得到完整交易Tx，对其编码后计算哈希得到$H(\mathrm{Tx})$，并通过客户端向CB发起交易请求后，Tx存于交易池中；

(6) CB中leader节点选择交易池中交易Tx进行验签操作，计算判断等式$e=H(\mathrm{Tx}')$和$eG+\omega^*_{H(\mathrm{Tx}')}Q=A$是否成立，若成立则将交易打包进新区块中，通过CB各节点验证及共识达成后，溯源数据通过智能合约完成上链。

阶段4　溯源数据共享(如图3)。本方案将溯源数据共享分为直接共享和间接共享；直接共享指具有数据访问权限的TDV通过其SK对数据进行安全访问的过程，间接共享指最终购买该食用农产品的用户通过扫描产品2维码进行溯源的过程；间接共享与直接共享最本质的区别在于间接共享不是通过访问CB和IPFS获取溯源数据，而是通过TPR查询后为其选择性返回的部分溯源数据展示页面。间接共享依赖于直接共享，此处仅讨论直接共享过程。TDV通过CB查询溯源数据的索引$H(M')$和CT，并通过SK和访问树T恢复对称密码算法的密钥K；以(m,n)门限为例，对称密码算法的密钥K恢复具体过程如算法2所示。

阶段5　TDO身份追溯。如步骤3所述，TDO在上传溯源数据时隐匿了身份，即TDV通过CB访问溯源数据时最多只能查询到该数据上传者所属的AO。本方案的身份隐匿方式为条件匿名，当食用农产品的质量在某一阶段出现问题时，该阶段的AO可以和TPR协同完成对该TDO真实身份的追溯。具体追溯过程分为3个步骤，如下所示：

(1) TDV通过$\omega^*_{H(\mathrm{Tx}')}$追溯到该笔交易的签发机构AO1并向TPR发出追溯申请。

(2) TPR通过$H(\mathrm{Tx}')$在本地数据库查询到对应的盲因子(η,γ)，将其与AO1的公钥相结合，根据式(7)计算得出$\omega^*_{\mathrm{Tx}''}$，并将$\omega^*_{\mathrm{Tx}''}$发送与AO1，监督其完成最后的追溯流程

$$\omega^*_{\mathrm{Tx}''}\equiv\eta^{-1}(\omega^*_{H(\mathrm{Tx}')}-\gamma)\mathrm{mod}n \tag{7}$$

(3) AO1验证追溯真实性后，通过$\omega^*_{\mathrm{Tx}''}$查询本地数据库找到对应TDO的身份信息，并将其返回与TPR，至此完成追溯。

算法2　对称密码算法的密钥K恢复

输入：SK, p, r

输出：K

(1) 客户端通过KGC解密SK后从SK中获取集合$\{K_1,K_2,\cdots,K_m\}$及集合$\{d_1,d_2,\cdots,d_m\}$；

(2)使用$\{d_1,d_2,\cdots,d_m\}$计算$d_{\mathrm{mult}}=\prod_{i=1}^{m}d_i$；

(3)根据中国剩余定理，求出下列同余方程组在模d_{mult}下的唯一解K'

$$\left.\begin{array}{l}X\equiv K_1(\mathrm{mod}d_1)\\X\equiv K_2(\mathrm{mod}d_2)\\\cdots\\X\equiv K_m(\mathrm{mod}d_m)\end{array}\right\} \tag{6}$$

求得：$X=\sum_{i=1}^{m}K_iD_iD_i{}^{-1}$，其中$D_i=d_{\mathrm{mult}}/d_i$；

$K'=X \bmod d_{\mathrm{mult}}$

(4)使用K',p,r计算$K=K'-rp$

(5)return K

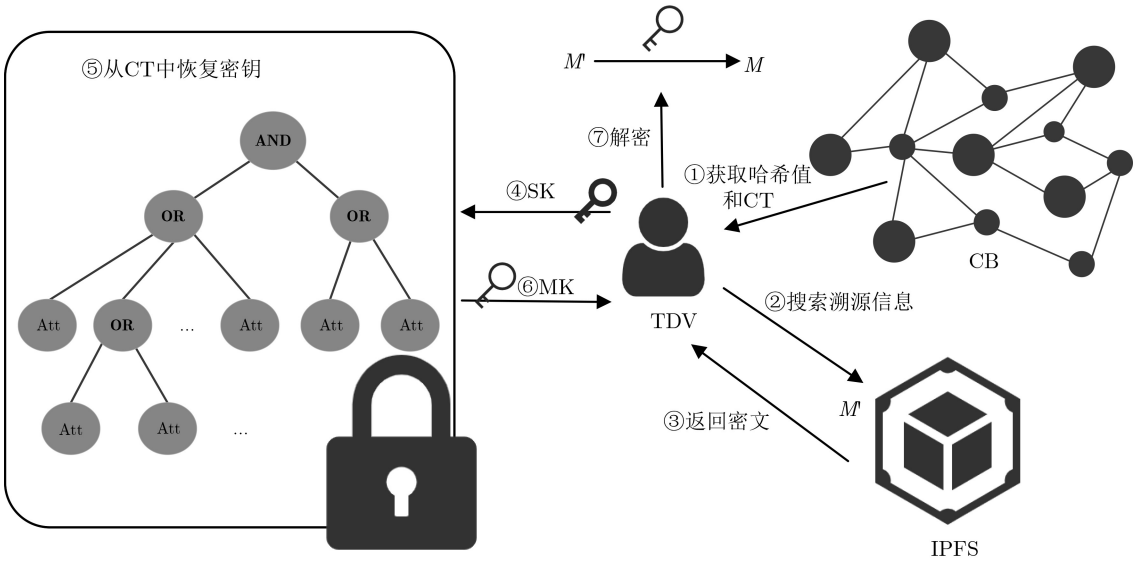

图 3 溯源数据共享

3.3 智能合约设计

本案例使用Golang语言基于Hyperledger fabric开源的shim和peer依赖包，设计提出智能合约Trace, TDO和TDV通过调用Trace合约可以实现溯源数据的链上存储和共享；Trace合约的基本业务设计如表3所示。

Trace合约定义了结构体data，变量hash3, hash1和 ct分别对应$H(H(M')||\mathrm{CT}||\mathrm{ID}_{\mathrm{TPR}})$, $H(M')$和密文CT；两种功能函数的具体实现如算法3、算法4所示。

4 方案分析

4.1 正确性分析

分析1 为验证本方案所提新型公平盲签名的正确性，即等式$eG+\omega^{*}_{H(\mathrm{Tx}')}Q=A$成立，作如式(8)的分析

$$\begin{aligned}eG+\omega^{*}_{H(\mathrm{Tx}')}Q=&(e+(\eta\omega^{*}_{\mathrm{Tx}''}+\gamma)d_{\mathrm{AO}})G\\=&(e+(\eta d^{-1}_{\mathrm{AO}}(k-\mathrm{Tx}'')+\gamma)d_{\mathrm{AO}})G\\=&(e+\eta(k-\mathrm{Tx}'')+\gamma d_{\mathrm{AO}})G\\=&(e+\eta k-\eta\mathrm{Tx}''+\gamma d_{\mathrm{AO}})G\\=&(e+\eta k-\eta(\eta^{-1}(e-\delta))+\gamma d_{\mathrm{AO}})G\\=&(\eta k+\delta+\gamma d_{\mathrm{AO}})G\\=&\eta R+\delta G+\gamma Q=A\end{aligned}\tag{8}$$

表 3 Trace合约业务设计

功能	合约方法	相关描述
数据上链	saveTraceData()	存储溯源数据信息
数据查询	getTraceData()	通过hash3查询溯源数据

算法3 存贮TraceData函数

```
func (t *SimpleChaincode) saveTraceData(stub
shim.ChaincodeStubInterface, args []string) pb.Response {
    hash3 := args[0]
    hash1 := args[1]
    ct := args[2]
    //检查是否存在该记录
    dataAsBytes, err := stub.GetState(hash3)
    if err != nil {
        return shim.Error(“获取数据失败:” + err.Error())}
    else if dataAsBytes != nil {
        return shim.Error(“该记录已存在: ” + hash3)}
    //创建新的data对象并通过marshal转为JSON
    data := &data{hash3, hash1, ct}
    dataJSONasBytes, err := json.Marshal(data)
    if err != nil {return shim.Error(err.Error())}
    //数据上链
    err = stub.PutState(hash3, dataJSONasBytes)
    if err != nil {return shim.Error(err.Error())}
    return shim.Success(nil)}
```

分析2 本方案所用新型属性基加密方法基于CP-ABE，若CP-ABE保证其正确性，且改良后的溯源数据能正确恢复，则本方案所用新型属性基加密方法具有正确性；故针对溯源数据能否正确恢复，即算法2的正确性作如下分析：

K值正确性证明 根据$D_i=d_{\mathrm{mult}}/d_i\rightarrow D_i\mathrm{mod}d_k=0$，可知对任意$k\in\mathbb{Z}^{*}_m$且$k\neq i\rightarrow K_iD_iD_i^{-1}\equiv 0(\mathrm{mod}m_k)$；

显然有：$K_iD_iD_i^{-1}\equiv K_i(\mathrm{mod}m_i)$

由模运算的加法分配率，即$(\alpha+\beta)\mathrm{mod}p=(\alpha\mathrm{mod}p+\beta\mathrm{mod}p)\mathrm{mod}p$

将$X=\sum_{i=1}^{m}K_iD_iD_i^{-1}$代入原同余方程组中，方程组成立。 证毕

K值唯一性证明 对同余方程组进行分析，假设已有一组解为X_1，另一组不相同的解为$X_2=X_1+h$，h不为$d_i\in\{d_1,d_2,\cdots,d_m\}$的倍数$i\in\mathbb{Z}^{*}_m$；解$X_1,X_2$都应满足原同余方程组，即$X_1\equiv K_i\mathrm{mod}d_i$，$X_2\equiv K_i\mathrm{mod}d_i\rightarrow X_1+h\equiv K_i\mathrm{mod}d_i$，可推得$X_1\equiv(X_1+h)\mathrm{mod}d_i\rightarrow h=0$即$X_1=X_2$，与假设相矛盾。 证毕

故算法2中恢复值对称密码算法的密钥K正确且唯一。

4.2 安全性分析

本节将分别从用户身份隐私和溯源数据安全两方面展开分析，通过以下3种定理及其证明过程，阐述本方案的安全性。

定理1 本方案使用的基于Asmuth-Bloom门限改进的属性加密方法能有效抵抗合谋攻击。

证明 考虑将TDV持有的SK表示为集合$\{\mathrm{SK}_1,\mathrm{SK}_2,\cdots,\mathrm{SK}_n\}$，假设$\mathrm{TDV}_1$,$\mathrm{TDV}_2$,$\cdots$,$\mathrm{TDV}_i$为AD，其中$i\in(1,n)$；AD分离SK中的影子$\{K_1,K_2,\cdots,K_i\}$，$\{K_1+K_1'',K_2+K_2'',\cdots,K_i+K_i''\}$隐藏自身身份，并不断将假影子组成新的SK进行试探

算法4 获取TraceData函数

```
func (t *SimpleChaincode) getTraceData(stub
shim.ChaincodeStubInterface, args []string) pb.Response {
    var hash3, jsonResp string
    var err error
    if len(args) != 1 {return shim.Error("请输入hash3")}
    hash3 = args[0]
    valAsbytes, err := stub.GetState(hash3)
    if err != nil {
        jsonResp = "{\"Error\":\"获取数据信息失败"\"}"
        return shim.Error(jsonResp)}
    else if valAsbytes == nil {
        jsonResp = "{\"Error\":\"未查找到该数据信息"\"}"
        return shim.Error(jsonResp)}
    return shim.Success(valAsbytes)}
```

攻击，每次会返回一个假的秘密K''。AD(TDV_1, TDV_2,…,TDV_i)根据同余方程可求出$K''' = X'' \bmod p$

$$\begin{cases} X = K_1'(\bmod d_1) \\ X = K_2'(\bmod d_2) \\ \cdots \\ X = K_i'(\bmod d_i) \end{cases} \cdots \begin{cases} X = K_1'(\bmod d_1) \\ X = 0(\bmod d_2) \\ \cdots \\ X = 0(\bmod d_i) \end{cases} \tag{9}$$

计算$K' = K'' - K'''$得到K'，代入$K' = K + rp$中求出K值。本方案通过在密钥生成阶段KGC对SK进行加密操作使AD无法拆分出$\{K_1, K_2, \cdots, K_i\}$，能有效抵抗合谋攻击。　　证毕

定理2　敌手(AD, ADversary)攻击AO或TPR中1个或多个本地存储节点，导致TDO身份暴露的可能性可以忽略。

证明　本方案溯源数据存储过程中，TDO分别向AO和TPR提交了部分信息，考虑这些信息被AO和TPR全部存储于本地数据库。现将TPR的存储节点表示为$T = \{T_1, T_2, \cdots, T_n\}$，AO的存储节点表示为$A = \{A_1, A_2, \cdots, A_n\}$；分别对3种攻击行为进行分析：

(1) AD攻击单个TPR节点：考虑被攻击的节点为T_i，分布式存储环境下T_i中存有特定TDO信息的可能性可以忽略，若AD进行泛攻击或T_i中恰好存有特定TDO的部分身份信息$(k, H(\mathrm{Tx}'))$，AD根据$(k, H(\mathrm{Tx}'))$计算TDO身份是不可行的；

(2) AD攻击单个AO节点：考虑被攻击的节点A_i中恰好存有特定TDO的部分信息，AD窃取信息后，没有k对签名进行解盲，难以将其与特定交易对应获取TDO身份信息，且同样分布式存储环境下A_i中存有特定TDO信息的可能性可以忽略；

(3) AD同时攻击TPR和AO节点：假设被攻击的节点为T_i和A_k，根据上述分析，T_i和A_k中存有特定TDO信息的可能性较低；若AD进行泛攻击，将T和A中节点排列组合计算匹配的概率为$1/n^2$，当n值较大时T_i和A_k中存有同一TDO的身份信息的可能性可以忽略，且T_i和A_k中存有多个TDO的身份信息，AD无法直接将其进行匹配。　　证毕

定理3　AO无法利用已有信息私自伪造溯源数据对TDO进行陷害。

证明　本方案采用双重ID 的方法来避免恶意AO对TDO的陷害。在联盟链搭建的初始阶段，TPR和AO为TDO生成了双重ID$(\mathrm{ID_{AO}}, \mathrm{ID_{TPR}})$；两种ID在功能上互不干扰，TDO通过TPR授予的$\mathrm{ID_{TPR}}$对上传的溯源数据信息进行了防伪授权，即$H(H(M')||CT||\mathrm{ID_{TPR}})$；AO对溯源数据授权则是通过$\mathrm{ID_{AO}}$来确认TPO的身份，AO在追溯问题溯源数据时也无需向TPR查询$\mathrm{ID_{TPR}}$；即AO若要伪造溯源信息需获取到TPR 的$\mathrm{ID_{TPR}}$，AO虽然可以通过追溯权限追溯到TPR的$H(M')$和CT值，但SM3杂凑算法抗碰撞攻击、抗原像攻击、抗区分器攻击体现出的高安全性，使得AO破解$H(H(M')||\mathrm{CT}||\mathrm{ID_{TPR}})$获取$\mathrm{ID_{TPR}}$的行为是计算不可行的，故如定理3所述。　　证毕

4.3　功能对比分析

本节从存储方式、存储技术、数据共享方式、数据加密以及身份匿名保护5个方面将本方案与文献[10,12,15]进行对比。如表4所示，文献[10]无法实现数据1次加密多次共享，且使用本地数据库存储数据信息存在拓展难、成本高的缺陷；文献[12]使用IPFS对数据明文直接进行存储，数据安全存在严重隐患；文献[15]使用CP-ABE技术实现了对数据的多方秘密共享，但将数据直接上链为区块链网络带来极大的负担；且文献[10,12,15]都未对上传者的身份隐私进行保护，上传者隐私信息存在泄露隐患。本方案选用对称加密结合改进CP-ABE完成对数据的脱敏处理，并采取IPFS分布式存储数据密文保证了数据的安全性；同时使用本文所提的新型公平盲签名方法实现了上传者身份条件匿名，保护了上传者的隐私安全。故本方案较对比的文献[10,12,15]，功能更完善。

5　性能测试

仿真实验使用Java语言基于JPBC(Java Pairing-Based Cryptograply)库和java.security包进行代码编写，在16 GB内存、AMD Ryzen 7 5800H CPU, Windows10操作系统环境下运行。

5.1　新型公平盲签名性能

为验证提出的新型公平盲签名方法较RSA公平盲签名方法具有性能优势，分别对其存储性能和时间性能进行对比实验。

表 4　功能对比分析

方案	存储方式	存储技术	数据共享方式	数据加密	身份匿名保护
文献[10]	链上链下	本地数据库+区块链	1对1	对称加密+ECC	未匿名
文献[12]	链上链下	IPFS+区块链	1对多	未加密	未匿名
文献[15]	链上	区块链	1对多	对称加密+CP-ABE	未匿名
本文方案	链上链下	IPFS+区块链	1对多	对称加密+改进CP-ABE	条件匿名

5.1.1 存储性能

选取224 bit 新型公平盲签名和2048 bit RSA公平盲签名进行存储性能实验。实验环境模拟为由3个TPR节点和12个AO节点构成的CB，根据图4显示，新型公平盲签名对空间的需求更小，能有效节省区块链网络的存储资源。

5.1.2 时间性能

分别对两种方案进行效率测试，测试选用密码安全强度范围112～192 bit，测试结果如表5所示。

随着密码强度的不断增加，RSA公平盲签名的耗时几乎成指数增长，结合图5分析，新型公平盲签名耗时增长缓慢。

5.2 溯源性能

为对本方案在溯源场景下的实际性能进行更精准的评估，根据表4选取同样实现多方秘密共享的文献[15]与本方案进行效率对比实验。两种方案在溯源时除秘密恢复过程外均相同，为使实验更具针对性，将秘密恢复作为溯源过程的测试点，此处考虑对测试数据进行溯源的个体数量为20。

根据图6显示，随溯源次数不断增加本方案耗时增幅小且始终低于文献[15]，考虑本方案并未增加额外存储空间，故本方案在溯源场景下的效率较文献[15]有较大优势。

6 结束语

本方案通过使用改进的CP-ABE实现溯源数据信息分层秘密共享，在提高了共享效率的同时能有效抵抗合谋攻击；使用新型公平盲签名方法在TDO, AO, TPR 3方之间实现了对TDO的身份匿名保护，相比传统RSA公平盲签名方案在减少时间损耗和存储压力的同时能有效抵抗陷害攻击。本方案还存在一些不足：单KGC工作强度大且强中心化；所提新型公平盲签名验签耗时较高。下一步工作重心是进一步优化本方案，解决存在的问题。

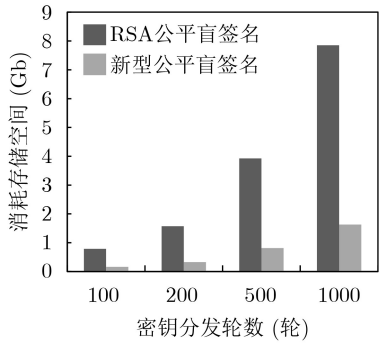

图 4 密钥存储损耗

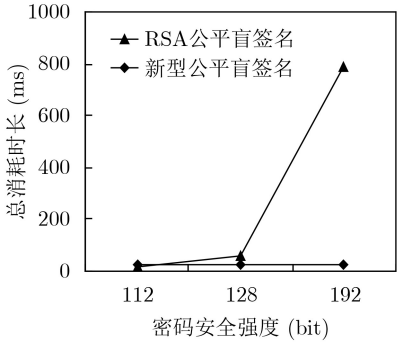

图 5 效率对比

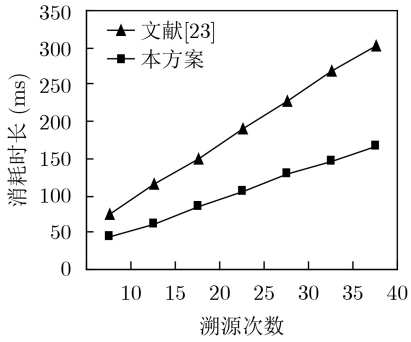

图 6 溯源效率对比

参 考 文 献

[1] 何晖, 郭富朝, 郭泽颖. 新《食品安全法实施条例》评述[J]. 食品科学, 2020, 41(11): 336–343. doi: 10.7506/spkx1002-6630-20191202-015.

HE Hui, GUO Fuchao, and GUO Zeying. Commentary on the new regulation on the implementation of the food safety

表 5 效率测试

密码强度(bit)	签名方案	盲化耗时(ms)	签名耗时(ms)	解盲耗时(ms)	验签耗时(ms)	总耗时(ms)
112	2048bit RSA公平盲签名	3.6087	6.9396	0.5977	7.138	18.284
112	224 bit 新型公平盲签名	0.0233	0.3707	0.0363	25.8827	26.313
128	3072 bit RSA公平盲签名	11.2375	22.1061	0.9382	22.0228	56.3046
128	256 bit 新型公平盲签名	0.0354	0.3546	0.0491	26.7625	27.2016
192	7680 bit RSA公平盲签名	155.6723	309.3041	3.6179	317.4969	786.0912
192	384 bit 新型公平盲签名	0.0599	0.3812	0.0464	28.192	28.6795

law of the people's republic of China[J]. *Food Science*, 2020, 41(11): 336–343. doi: 10.7506/spkx1002-6630-20191202-015.

[2] TILMAN D, CASSMAN K G, MATSON P A, *et al*. Agricultural sustainability and intensive production practices[J]. *Nature*, 2002, 418(6898): 671–677. doi: 10.1038/nature01014.

[3] KIM Y G and WOO E. Consumer acceptance of a quick response (QR) code for the food traceability system: Application of an extended technology acceptance model (TAM)[J]. *Food Research International*, 2016, 85: 266–272. doi: 10.1016/j.foodres.2016.05.002.

[4] WANT R. RFID: A key to automating everything[J]. *Scientific American*, 2004, 290(1): 56–65. doi: 10.1038/scientificamerican0104-56.

[5] OKI K, MITSUISHI S, ITO T, *et al*. An agricultural monitoring system based on the use of remotely sensed imagery and field server web camera data[J]. *GIScience & Remote Sensing*, 2009, 46(3): 305–314. doi: 10.2747/1548-1603.46.3.305.

[6] BEHZADI G, O'SULLIVAN M J, and OLSEN T L. On metrics for supply chain resilience[J]. *European Journal of Operational Research*, 2020, 287(1): 145–158. doi: 10.1016/j.ejor.2020.04.040.

[7] ZHENG Zibin, XIE Shaoan, DAI Hongning, *et al*. Blockchain challenges and opportunities: A survey[J]. *International Journal of Web and Grid Services*, 2018, 14(4): 352–375. doi: 10.1504/IJWGS.2018.095647.

[8] 谢绒娜, 李晖, 史国振, 等. 基于区块链的可溯源访问控制机制[J]. 通信学报, 2020, 41(12): 82–93. doi: 10.11959/j.issn.1000-436x.2020232.

XIE Rongna, LI Hui, SHI Guozhen, *et al*. Blockchain-based access control mechanism for data traceability[J]. *Journal on Communications*, 2020, 41(12): 82–93. doi: 10.11959/j.issn.1000-436x.2020232.

[9] FENG Huanhuan, WANG Xiang, DUAN Yanqing, *et al*. Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges[J]. *Journal of Cleaner Production*, 2020, 260: 121031. doi: 10.1016/j.jclepro.2020.121031.

[10] 于合龙, 陈邦越, 徐大明, 等. 基于区块链的水稻供应链溯源信息保护模型研究[J]. 农业机械学报, 2020, 51(8): 328–335. doi: 10.6041/j.issn.1000-1298.2020.08.036.

YU Helong, CHEN Bangyue, XU Daming, *et al*. Modeling of rice supply chain traceability information protection based on block chain[J]. *Transactions of the Chinese Society for Agricultural Machinery*, 2020, 51(8): 328–335. doi: 10.6041/j.issn.1000-1298.2020.08.036.

[11] CAO Shoufeng, POWELL W, FOTH M, *et al*. Strengthening consumer trust in beef supply chain traceability with a blockchain-based human-machine reconcile mechanism[J]. *Computers and Electronics in Agriculture*, 2021, 180: 105886. doi: 10.1016/j.compag.2020.105886.

[12] SALAH K, NIZAMUDDIN N, JAYARAMAN R, *et al*. Blockchain-based soybean traceability in agricultural supply chain[J]. *IEEE Access*, 2019, 7: 73295–73305. doi: 10.1109/ACCESS.2019.2918000.

[13] 任守纲, 何自明, 周正己, 等. 基于CSBFT区块链的农作物全产业链信息溯源平台设计[J]. 农业工程学报, 2020, 36(3): 279–286. doi: 10.11975/j.issn.1002-6819.2020.03.034.

REN Shougang, HE Ziming, ZHOU Zhengji, *et al*. Design and implementation of information tracing platform for crop whole industry chain based on CSBFT-Blockchain[J]. *Transactions of the Chinese Society of Agricultural Engineering*, 2020, 36(3): 279–286. doi: 10.11975/j.issn.1002-6819.2020.03.034.

[14] 刘双印, 雷墨鹭兮, 徐龙琴, 等. 基于区块链的农产品质量安全可信溯源系统研究[J]. 农业机械学报, 2022, 53(6): 327–337. doi: 10.6041/j.issn.1000-1298.2022.06.035.

LIU Shuangyin, LEI Moyixi, XU Longqin, *et al*. Development of reliable traceability system for agricultural products quality and safety based on blockchain[J]. *Transactions of the Chinese Society for Agricultural Machinery*, 2022, 53(6): 327–337. doi: 10.6041/j.issn.1000-1298.2022.06.035.

[15] ZHANG Guofeng, CHEN Xiao, FENG Bin, *et al*. BCST-APTS: Blockchain and CP-ABE empowered data supervision, sharing, and privacy protection scheme for secure and trusted agricultural product traceability system[J]. *Security and Communication Networks*, 2022, 2022: 2958963. doi: 10.1155/2022/2958963.

[16] 孟小峰, 刘立新. 基于区块链的数据透明化: 问题与挑战[J]. 计算机研究与发展, 2021, 58(2): 237–252. doi: 10.7544/issn1000-1239.2021.20200017.

MENG Xiaofeng and LIU Lixin. Blockchain-based data transparency: Issues and challenges[J]. *Journal of Computer Research and Development*, 2021, 58(2): 237–252. doi: 10.7544/issn1000-1239.2021.20200017.

[17] KAMILARIS A, FONTS A, and PRENAFETA-BOLDY F X. The rise of blockchain technology in agriculture and food supply chains[J]. *Trends in Food Science & Technology*, 2019, 91: 640–652. doi: 10.1016/j.tifs.2019.07.034.

[18] CHAUM D. Blind signatures for untraceable payments[M]. CHAUM D, RIVEST R L, and SHERMAN A T. Advances in Cryptology. Boston: Springer, 1983: 199–203. doi: 10.1007/978-1-4757-0602-4_18.

[19] CHAUM D and VAN HEYST E. Group signatures[C]. The Workshop on the Theory and Application of of

Cryptographic Techniques. Brighton, UK: Springer, 1991: 257–265. doi: 10.1007/3-540-46416-6_22.

[20] KOMANO Y, OHTA K, SHIMBO A, *et al*. Toward the fair anonymous signatures: Deniable ring signatures [12] appeared in the cryptographers' track at the RSA Conference 2006 (CT-RSA 2006)[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2007, E90-A(1): 54–64. doi: 10.1093/ietfec/e90-a.1.54.

[21] STADLER M, PIVETEAU J M, and CAMENISCH J. Fair blind signatures[C]. The International Conference on the Theory and Applications of Cryptographic Techniques. Saint-Malo, France: Springer, 1995: 209–219. doi: 10.1007/3-540-49264-X_17.

[22] KUMAR P P, KUMAR S P, and ALPHONSE P J A. Attribute based encryption in cloud computing: A survey, gap analysis, and future directions[J]. *Journal of Network and Computer Applications*, 2018, 108: 37–52. doi: 10.1016/j.jnca.2018.02.009.

[23] CHEN Genlang, XU Zhiqian, ZHANG Jiajian, *et al*. Generic attribute revocation systems for attribute-based encryption in cloud storage[J]. *Frontiers of Information Technology & Electronic Engineering*, 2019, 20(6): 773–786. doi: 10.1631/FITEE.1800512.

[24] AMBROSIN M, ANZANPOUR A, CONTI M, *et al*. On the feasibility of attribute-based encryption on internet of things devices[J]. *IEEE Micro*, 2016, 36(6): 25–35. doi: 10.1109/MM.2016.101.

[25] ASMUTH C and BLOOM J. A modular approach to key safeguarding[J]. *IEEE Transactions on Information Theory*, 1983, 29(2): 208–210. doi: 10.1109/TIT.1983.1056651.

张学旺：男，副教授，博士生，研究方向为区块链与物联网、数据安全与隐私保护、大数据与智能数据处理等.

林金朝：男，教授，博士生导师，研究方向为无线通信传输技术、BAN与信息处理技术等.

黎志鸿：男，硕士生，研究方向为区块链、隐私保护.

姚亚宁：男，硕士生，研究方向为区块链、数据安全.

责任编辑：余 蓉