基于区块链的RFID供应链产品所有权转移方案

陆琪鹏[1,2],刘亚丽[1,2*],刘长庚[1,2],曾聪爱[1,2],陈东东[1,2],宁建廷[3,4]
(1. 江苏师范大学计算机科学与技术学院,江苏徐州 221116;2. 广西密码学与信息安全重点实验室(桂林电子科技大学),广西桂林 541004;3. 武汉大学国家网络安全学院,湖北武汉 430072;4. 澳门城市大学数据科学学院,中国澳门 999078)

摘 要: 将产品转移给不受管理员信任的实体,极易造成产品伪造、窜货和隐私泄露等问题. 因此,本文提出一种基于区块链的RFID供应链产品所有权转移方案BPOTS. 首先,设计了一种基于中国剩余定理与Pedersen承诺的秘密值共享与验证算法,实现了产品在指定新所有者集合的转移,并利用Pedersen承诺的同态性质实现了产品批量转移,提高了产品的转移效率;其次,提出了一种基于对称加密的伪ID生成算法,平衡了供应链的隐私性与透明性;再次,本文对BPOTS进行了安全性分析和性能评估,结果表明:与现有基于区块链的RFID供应链产品所有权转移方案相比,BPOTS有效平衡了供应链的隐私性和透明性,并在产品转移的运行效率上提高了约12倍. 最后,本文在长安链平台上实现了所提出的BPOTS并在Github上开源. 测试结果表明:BPOTS产品转移效率相比于产品串行转移提高了约70.4%,有效降低了供应链节点的成本.

关键词: 区块链;RFID供应链;所有权转移;中国剩余定理;Pedersen承诺

基金项目: 国家自然科学基金(No.61702237,No.61972094,No.62032005);徐州市科技计划项目(No.KC22052);广西密码学与信息安全重点实验室(桂林电子科技大学)研究课题(No.GCIS202114);福建省网络安全与密码技术重点实验室(福建师范大学)开放课题(No.NSCL-KF2021-04);江苏师范大学研究生科研与实践创新计划项目(No.2021XKT1382,No.2022XKT1488,No.2022XKT1545);河南省网络密码技术重点实验室研究课题(No.LNCT2021-A07);教育部产学合作协同育人项目(No.202101374001)

中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2025)02-0451-09

电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20240111

Product Ownership Transfer Scheme of RFID-Enabled Supply Chain Based on Blockchain

LU Qi-peng[1,2], LIU Ya-li[1,2*], LIU Chang-geng[1,2], ZENG Cong-ai[1,2], CHEN Dong-dong[1,2], NING Jian-ting[3,4]
(1. *College of Computer Science and Technology*, *Jiangsu Normal University*, *Xuzhou*, *Jiangsu* 221116, *China*;
2. *Guangxi Key Laboratory of Cryptography and Information Security*, *Guilin University of Electronic Technology*, *Guilin*, *Guangxi* 541004, *China*;
3. *School of Cyber Science and Engineering*, *Wuhan University*, *Wuhan*, *Hubei* 430072, *China*;
4. *Faculty of Data Science*, *City University of Macau*, *Macau* 999078, *China*)

Abstract: Transferring product to the entity which is not trusted by the administrator may lead to some problems, such as product counterfeiting, smuggling, product loss, and privacy leaking, etc. Therefore, in this paper, a product transfer scheme named BPOTS in RFID-enabled supply chain based on blockchain is proposed. Firstly, this paper proposes a secret value sharing and verification algorithm based on Chinese remainder theorem and Pedersen commitment to achieve the transfer of products between the designated new owner sets. And in order to improve system efficiency, we propose a method for the transfer of products in batches based on the homomorphism of Pedersen commitment. Secondly, to balance the transparency and privacy of the supply chain, this paper proposes a pseudo ID generation algorithm based on symmetric encryption. Thirdly, security analysis and performance evaluation are conducted on the BPOTS scheme. The result shows that BPOTS strikes a balance between the transparency and privacy of the supply chain effectively and improves the efficiency of transferring product for about 12 times compared with the existing product ownership transfer schemes. Finally, the BPOTS scheme is implemented on ChainMaker platform and made available as open-source on Github. The testing result

收稿日期:2024-01-18;修回日期:2024-10-20;责任编辑:李勇锋
*通讯作者:刘亚丽

indicates that the efficiency of transferring product in BPOTS scheme is about 70.4% higher than that of transferring products in series. Moreover, BPOTS scheme reduces the costs of supply chain nodes effectively.

Key words: blockchain; RFID-enabled supply chain; ownership transfer; Chinese remainder theorem; Pedersen commitment

Foundation Item(s): National Natural Science Foundation of China (No.61702237, No.61972094, No. 62032005); Science and Technology Planning Foundation of Xuzhou City (No.KC22052); Opening Foundation of Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology (No.GCIS202114); Opening Foundation of Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund, Fujian Normal University (No. NSCL-KF202104); Postgraduate Research & Practice Innovation Program of Jiangsu Normal University (No.2021XKT1382, No.2022XKT1488, No.2022XKT1545); Opening Foundation of Henan Key Laboratory of Network Cryptography Technology (No. LNCT2021-A07); University-Industry Collaborative Education Program of the Ministry of Education (No.202101374001)

1 引言

供应链管理(Supply Chain Management,SCM)需要记录产品从原材料到消费者的整个生命周期内发生的一系列状态与事件,如产品数据、产品转移路径等[1]. 在供应链管理中,将产品转移给不被供应链信任的实体是风险行为[2]. 非信任实体获取产品后可能会实施仿制、伪造等恶意行为,将会造成产品伪造、窜货和隐私泄露等后果. 甚至会危害国家安全. 因此,研究指定新所有者集合的产品所有权转移方案具有重要的研究意义和实践价值.

产品所有权管理是供应链管理的关键模块之一[3]. 传统供应链管理方案以中心化数据库为基础,通常由管理员对外提供信息化服务[4]. 但基于中心化数据库的供应链管理方案存在数据篡改,透明性差等问题,已无法满足应用需求. 区块链是一种分布式账本技术,交易一旦达成共识就无法被修改[5]. 因此,区块链技术可保证数据透明性. 但区块链存在隐私数据泄露风险[6],隐私数据泄露可能导致企业利益受损[7]. 因此,在基于区块链的供应链管理方案中,应考虑隐私性与透明性的平衡.

近年来,学术界对供应链安全的重视程度越来越高. Qi等人[8]利用承诺完成所有者的身份认证,并通过同态性质将多个标签聚合. 基于区块链的供应链管理方案最早由Toyoda等人[9]提出,通过验证账户地址的方法保证交易合法性,但产品信息以及所有者身份均公开在链上. Qi等人[10]提出的CPDS方案利用属性加密保护对称加密密钥,并使用对称加密算法保护供应链数据,但密钥在产品流转的全过程保持不变,存在泄露的风险. Uesugi等人[11]利用零知识证明技术验证新所有者身份,保护了新所有者的隐私,但仍需要在链下建立安全信道传递秘密值. Vijayalakshmi等人[12]利用ZKSNARK算法实现了标签所有权的安全转移. 但产品转移效率较低. Munoz-ausecha等人[13]提出了一种基于以太坊代币的资产管理方案. 但是虚拟货币市场存在金融风险与法律风险,因此该方案风险程度较高.

因此,本文提出了一种基于区块链的RFID供应链产品所有权转移方案BPOTS,主要贡献如下:

(1)提出了一种基于中国剩余定理与Pedersen承诺的秘密值共享与验证方法,解决了RFID供应链场景下指定新所有者集合转移的问题.

(2)提出了一种基于对称加密的伪ID生成算法,平衡了RFID供应链的透明性与隐私性. 仅有管理员能够获取产品的完全转移路径,普通用户可以通过区块链验证产品转移的合法性.

(3)基于Pedersen承诺的同态性质实现了产品批量转移,BPOTS一次交易可以转移一组产品,提高了产品转移的效率.

(4)本文在长安链平台实现了BPOTS,并在Github上开源(https://github.com/mate-jc/BPOTS).

2 准备工作

2.1 理论基础

(1)中国剩余定理

假设有明文s,密钥$\mu=\sum_{i=1}^{n}x_i y_i \bmod M$,其中$M=\prod_{i=1}^{n}k_i$且$k_1,k_2,\cdots,k_n$两两互质. 密文$\gamma=\mu s=\sum_{i=1}^{n}sx_i y_i \bmod M$.

据中国剩余定理[14]密文$X=\gamma$是式(1)所示方程组的解. 故明文s可用k_1~k_n的任意值解出.

$$\begin{cases} X\equiv s\left(\bmod k_1\right) \\ X\equiv s\left(\bmod k_2\right) \\ \quad\vdots \\ X\equiv s\left(\bmod k_n\right) \end{cases} \tag{1}$$

(2)Pedersen承诺

Pedersen承诺[15]构造如式(2)所示:

$$c=sG+rH \tag{2}$$

其中,s是秘密值,r是随机数,G和H是椭圆曲线上的点. Pedersen承诺具有加同态的性质:

$$\begin{cases} c_1 = s_1 G + r_1 H \\ c_2 = s_2 G + r_2 H \\ c_1 + c_2 = (s_1 + s_2) G + (r_1 + r_2) H \end{cases} \tag{3}$$

2.2 系统模型

BPOTS面向RFID供应链产品所有权转移的场景，系统模型由以下实体构成.

(1)管理员:管理供应链节点的实体;

(2)原所有者:当前持有产品的供应链节点;

(3)新所有者集合:合法新所有者节点集合;

(4)新所有者:即将持有产品的供应链节点;

(5)区块链:BPOTS中的区块链为联盟链，由供应链联盟中的成员共同维护.

图1描述了BPOTS的系统模型，管理员向新所有者集合中的节点共享β，原所有者S_0向实际新所有者S_i共享α. 最后新所有者将α,β以及自己的PID提交到区块链上完成产品转移过程.

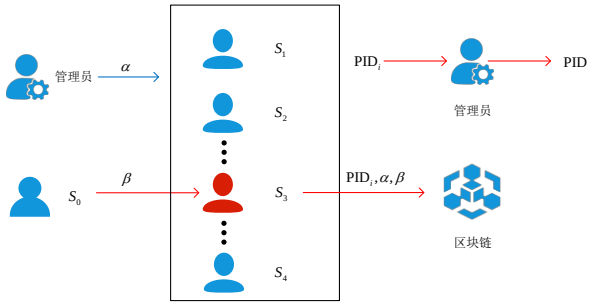


图1　系统模型图

3 秘密值共享与验证算法

本文提出了一种基于中国剩余定理和Pedersen承诺的秘密值共享与验证算法，包括加密密钥生成算法、秘密值加密算法和秘密值解密与验证算法.

算法1描述了加密密钥生成算法，输入素数集合P，输出加密密钥μ.

算法2描述了秘密值加密算法，输入秘密值s，加密密钥μ，输出密文γ和承诺c.

算法3描述了秘密值解密与验证算法. 输入密文γ，承诺值c和原所有者持有的解密密钥k，输出秘密值s. 若输出的$s=\perp$，说明验证失败.

4 BPOTS方案

本文提出了BPOTS方案，实现了指定新所有者集合转移，包括系统初始化、交易初始化和所有权转移等三个阶段.

4.1 系统初始化阶段

系统初始化阶段初始化BPOTS运行环境.

算法1　加密密钥生成算法

输入:$P=\{k_1,k_2,\cdots,k_n\}$

输出:μ

Gen_Key:

$\delta \leftarrow \prod_{i=1}^{n} k_i$

FOR k_i IN P

$x_i \leftarrow \frac{\delta}{sk_i}$

$y_i \leftarrow x_i^{-1} (\mathrm{mod}\ k_i)$

$\mu \leftarrow \sum_{i=1}^{n} x_i y_i$

算法2　秘密值加密算法

输入:s,μ

输出:γ,c

Encrypt:

$k,r \leftarrow$ random

$\gamma_1 \leftarrow \mu k, \gamma_2 \leftarrow \mathrm{aes\_enc}(k, r \| s)$

$\gamma \leftarrow \gamma_1 \| \gamma_2$

$c \leftarrow \mathrm{commit}(s,r)$

算法3　秘密值解密与验证算法

输入:γ,c,sk

输出:s

Decrypt:

$K \leftarrow \gamma_1 \bmod k$

$r \| s \leftarrow \mathrm{aes\_dec}(K, \gamma_2)$

$f \leftarrow \mathrm{verify\_commit}(c,s,r)$

IF f THEN

　RETURN s

ELSE THEN

　RETURN $\perp$

(1)管理员系统初始化

管理员选择大素数k_{n+1}作为解密秘密值的密钥;管理员在链下生成签名公私钥对$\mathrm{sk}_{\mathrm{admin}}^{\mathrm{sig}}, \mathrm{pk}_{\mathrm{admin}}^{\mathrm{sig}}$，并将$\mathrm{pk}_{\mathrm{admin}}^{\mathrm{sig}}$公开在区块链上.

(2)解密密钥的生成与分发

管理员随机选择大素数k作为供应链节点的解密密钥，并通过安全信道分发给供应链节点.

(3)部署智能合约

管理员在区块链部署智能合约. 产品以TID作为索引，每一个产品都有对应的六元组$(\mathrm{owner}_{\mathrm{TID}}, \gamma_\alpha, c_\alpha, \gamma_\beta, c_\beta, \mathrm{path}_{\mathrm{TID}})$记录产品状态. 其中，$\mathrm{owner}_{\mathrm{TID}}$是产品当前所有者的PID;$\gamma_\alpha, c_\alpha$是$\alpha$的密文与承诺;$\gamma_\beta, c_\beta$是$\beta$的密文与承诺;$\mathrm{path}_{\mathrm{TID}}$记录产品流转路径上所有供应链节点的PID.

(4)伪ID的生成与分发

管理员首先随机选择二元组(v,k). 管理员可以初始化多个二元组(v,k). 当供应链节点向管理员申请PID时,管理员随机选择一个二元组(v,k)输入算法4生成PID,并随机选择其对应的签名密钥对$\left(\mathrm{sk}_{\mathrm{PID}}^{\mathrm{sig}},\mathrm{pk}_{\mathrm{PID}}^{\mathrm{sig}}\right)$. 管理员将三元组$\left(\mathrm{PID},\mathrm{sk}_{\mathrm{PID}}^{\mathrm{sig}},\mathrm{pk}_{\mathrm{PID}}^{\mathrm{sig}}\right)$通过安全信道返回给供应链节点,并在区块链上公开$\left(\mathrm{PID},\mathrm{pk}_{\mathrm{PID}}^{\mathrm{sig}}\right)$. 供应链节点可以获得多个PID.

算法4 PID生成算法

输入: ID, v, k, Δt

输出: PID

Gen_PID:

select random number r

get current timestamp t

$T\leftarrow t+\Delta t$

$ct\leftarrow \mathrm{aes\_enc}\left(k,r\|\mathrm{ID}\|T\right)$

$\mathrm{PID}\leftarrow v\parallel T\parallel ct$

4.2 交易初始化阶段

交易初始化阶段完成加密密钥的生成与分发.

(1)加密密钥生成

假设原所有者持有的解密密钥为k_0,管理员持有的解密密钥为k_{n+1},新所有者集合中的成员持有的解密密钥集合为$\{k_1,k_2,\cdots,k_n\}$. 如式(4)所示,管理员计算$n+1$个加密密钥:

$$\mu_i=\begin{cases}\mathrm{Gen\_Key}\left(\{k_1,k_2,\cdots,k_{n+1}\}\right), & i=0\\ \mathrm{Gen\_Key}\left(\{k_0,k_i,k_{n+1}\}\right), & 1\leqslant i\leqslant n\end{cases}\tag{4}$$

(2)加密密钥分发

管理员选择n个随机数$r_1\sim r_n$,并用μ_i加密r_i:

$$\tau_i=r_i\cdot\mu_i\tag{5}$$

利用式(5)得到加密密钥的密文$\tau_1\sim\tau_n$后,原所有者计算签名σ,将$\tau_1\sim\tau_n$以及σ发送给原所有者. 原所有者验证签名之后,解密获得$\mu_1\sim\mu_n$:

$$\begin{cases}r_i=\tau_i \bmod k_0\\ \mu_i=\tau_i/r_i\end{cases}\tag{6}$$

4.3 所有权转移阶段

图2描述了BPOTS所有权转移阶段. 假设新所有者集合为S,原所有者S_0选择S_i为新所有者.

(1)原所有者选择随机数α,并用式(7)加密. 计算签名后,发送$\mathrm{TID}\parallel\mathrm{PID}_0\|\gamma_\alpha\|c_\alpha\|\sigma_\alpha$到区块链. 区块链检查$\mathrm{owner}_{\mathrm{TID}}=\mathrm{PID}_0$,并利用$\mathrm{PID}_0$验证签名,若签名验证成功,则保存$\left(\mathrm{TID},\gamma_\alpha,c_\alpha\right)$.

$$\begin{cases}\gamma_\alpha,c_\alpha\leftarrow\mathrm{Encrypt}\left(\alpha,\mu_i\right)\\ \sigma_\alpha\leftarrow\mathrm{sign}\left(\mathrm{sk}_{\mathrm{PID}_0}^{\mathrm{sig}},\gamma_\alpha\|c_\alpha\right)\end{cases}\tag{7}$$

(2)管理员选择随机数β,并用式(8)加密. 计算签名后,发送$\mathrm{TID}\parallel\gamma_\beta\|c_\beta\|\sigma_\beta$到区块链. 区块链验证签名,若签名验证成功,则保存$\left(\mathrm{TID},\gamma_\beta,c_\beta\right)$.

$$\begin{cases}\gamma_\beta,c_\beta\leftarrow\mathrm{Encrypt}\left(\beta,\mu_i\right)\\ \sigma_\beta\leftarrow\mathrm{sign}\left(\mathrm{sk}_{\mathrm{PID}_0}^{\mathrm{sig}},\gamma_\beta\|c_\beta\right)\end{cases}\tag{8}$$

(3)新所有者在收到产品后,在区块链中获取$\gamma_\alpha,\gamma_\beta$,解密得到秘密值$\alpha,\beta$以及随机数$r_\alpha,r_\beta$.

$$\begin{cases}\alpha,r_\alpha\leftarrow\mathrm{Decrypt}\left(k,\gamma_\alpha\right)\\ \beta,r_\beta\leftarrow\mathrm{Decrypt}\left(k,\gamma_\beta\right)\end{cases}\tag{9}$$

(4)如式(10)所示,新所有者将α,β相加,计算签名σ后,向区块链发送交易$\mathrm{TID}\parallel\mathrm{PID}_i\|p\parallel\sigma$.

$$\begin{cases}p\leftarrow\alpha+\beta\\ r\leftarrow r_\alpha+r_\beta\\ \sigma\leftarrow\mathrm{sign}\left(\mathrm{sk}_{\mathrm{PID}_i}^{\mathrm{sig}},\mathrm{TID}\parallel p\parallel r\right)\end{cases}\tag{10}$$

$$\begin{cases}p\leftarrow\sum_{k=1}^{m}\alpha_k+\beta_k\\ r\leftarrow\sum_{k=1}^{m}r_{\alpha_k}+r_{\beta_k}\\ \sigma\leftarrow\mathrm{sign}\left(\mathrm{sk}_{\mathrm{PID}_i}^{\mathrm{sig}},\mathrm{TID}_1\|\cdots\|\mathrm{TID}_m\|p\parallel r\right)\end{cases}\tag{11}$$

(5)区块链在收到交易$\mathrm{TID}\parallel\mathrm{PID}_i\|p\parallel\sigma$后,首先验证签名,验证通过之后,区块链根据TID获取c_α、c_β,计算p的承诺c'以及利用同态性质计算两个承诺的和c,并验证c、p、r是否存在Pedersen承诺的绑定关系. 若验证成功,则修改变量$\mathrm{owner}_{\mathrm{TID}}=\mathrm{PID}_i$. BPOTS设计了一种产品批量所有权转移方法. 如式(11)所示,新所有者首先计算秘密值的和p以及所有r_α和r_β的和r,计算签名σ后,将$\mathrm{PID}_i\|p\parallel r\parallel\sigma\parallel\mathrm{TID}_1\|\cdots\|\mathrm{TID}_m$发送到区块链. 区块链根据输入的TID依次获取所有产品的承诺值之和c,将p、c、r输入承诺的验证方法中,若验证成功,则修改所有产品的所有者.

5 BAN逻辑分析与证明

本节使用BAN逻辑[16]对本文提出的BPOTS进行安全性形式化分析与证明.

设M代表管理员,O代表原所有者,N代表新所有者,α和β是方案需要传递的秘密值. BPOTS的初始化假设如下:

A_1: $N|\equiv\#\{\alpha\}$; A_2: $N|\equiv\#\{\beta\}$;

A_3: $N|\equiv N\xleftrightarrow[X]{}O$; A_4: $N|\equiv N\xleftrightarrow[Y]{}M$;

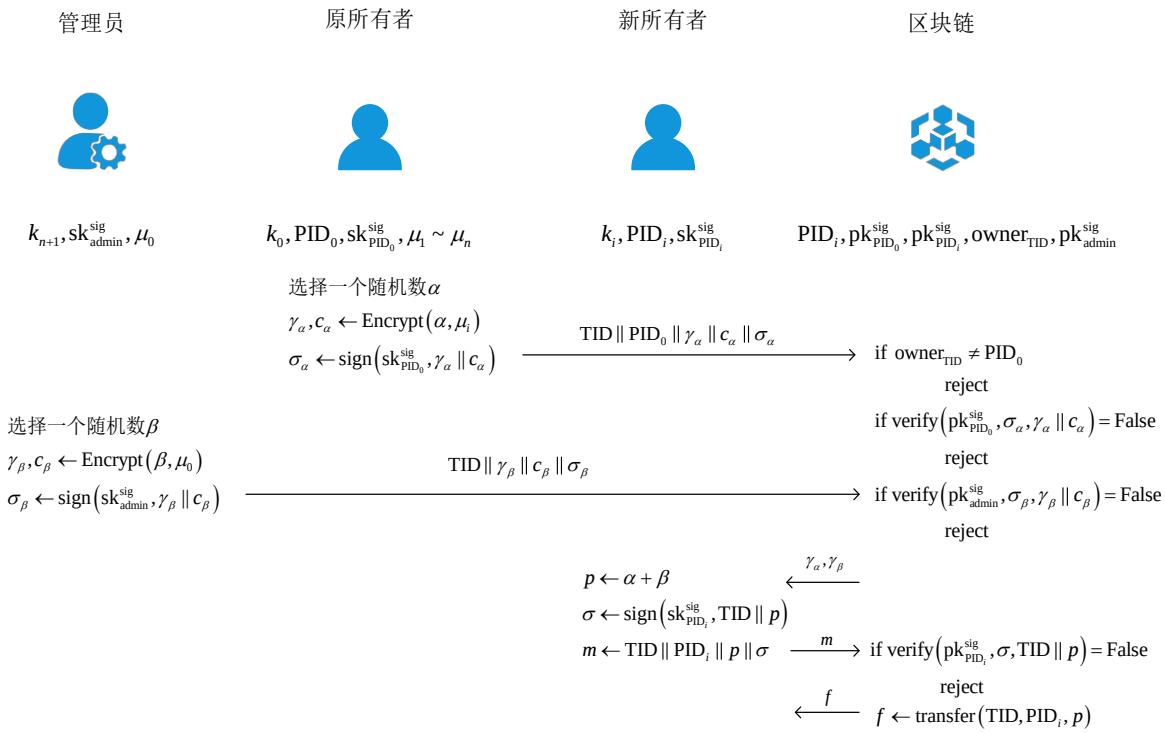


图2　产品转移流程图

A_5: $N \triangleleft \{\alpha\}_X$; A_6: $N \triangleleft \{\beta\}_Y$;

A_7: $N| \equiv O| \Rightarrow \alpha$; A_8: $N| \equiv M| \Rightarrow \beta$.

BPOTS的安全目标如下:

G_1: $N| \equiv \alpha$, N信任消息α;

G_2: $N| \equiv \beta$, N信任消息β.

BPOTS安全目标进行形式化证明如下:

(1)首先由假设A_3, A_5和消息含义规则R_1可以推得: F_1: $N| \equiv O| \sim \alpha$;再由F_1和假设A_1,应用随机数验证规则R_2可以推得: F_2: $N| \equiv O| \equiv \alpha$;最后由$F_2$和假设$A_7$,应用管辖权法则$R_3$可以推得: G_1: $N| \equiv \alpha$. 综上所述,安全目标G_1得证.

(2)首先由假设A_4, A_6和消息含义规则R_1可以推得: F_3: $N| \equiv M| \sim \beta$;再由F_3和假设A_2,应用随机数验证规则R_2可以推得: F_4: $N| \equiv M| \equiv \beta$;最后由$F_4$和假设$A_8$,应用管辖权法则$R_3$可以推得: G_2: $N| \equiv \beta$. 综上所述,安全目标G_2得证.

综上,BPOTS能够达到期望的安全目标.

6　BPOTS安全性分析

本节分析BPOTS抵抗数据篡改攻击、冒充攻击以及相关安全属性.

(1)抵抗数据篡改攻击

BPOTS能够抵抗针对区块链中交易数据的篡改攻击. 原所有者提交α时的PID需与$\mathrm{owner}_{\mathrm{TID}}$一致,且交易数据使用$\mathrm{sk}^{\mathrm{sig}}_{\mathrm{PID}}$签名,当恶意节点试图通过篡改交易数据非法获取产品转移所有权时,必须使用$\mathrm{sk}^{\mathrm{sig}}_{\mathrm{PID}}$对交易重新签名,才能通过区块链的验证. 因此,攻击者无法通过篡改用户交易数据实现产品非法转移,BPOTS能够拒绝执行被攻击者篡改后的交易. 因此,BPOTS能够抵抗数据篡改攻击.

(2)抵抗冒充攻击

为了逃避责任,供应链节点可能会使用不属于自己的PID或者使用一个伪造的PID进行产品转移操作. 合法的供应链节点向管理员申请一个PID,管理员将合法节点的PID及其公钥$\mathrm{pk}^{\mathrm{sig}}_{\mathrm{PID}}$上传至区块链. 若非法的供应链节点试图通过伪造的PID提交交易,由于缺少合法PID所对应的签名私钥$\mathrm{sk}^{\mathrm{sig}}_{\mathrm{PID}}$,无法对数据进行合法签名,进而非法的供应链节点所提交的交易无法通过区块链的认证. 因此,供应链节点无法使用一个未经管理员认证的PID提交交易,BPOTS方案能够抵抗冒充攻击. 因此,BPOTS能够有效抵抗冒充攻击.

(3)指定新所有者集合转移

BPOTS实现了指定新所有者集合的产品转移功能. 指定新所有者集合转移是指管理员给原所有者一个合法的新所有者集合,原所有者仅在该集合中任意选择一个作为新所有者,原所有者向自己选择的新所有者共享α,且管理员向整个合法的新所有者集合共享β. 若原所有者选择的新所有者不属于新所有者集合,由于其没有秘密值β,则无法通过区块链的验证;若新所有者属于管理员所规定的新所有者集合,但该新所

有者没有被原所有者选择，由于无法解密获取α，被选择的新所有者无法计算承诺值c_α. 因此，如果被选择的新所有者不是合法的新所有者集合中的成员，则无法通过区块链的验证. 综上所述，仅有既属于合法的新所有者集合且是原所有者选择成为供应链节点才能成为合法的新所有者，完成产品转移的操作. BPTOS方案成功实现了指定新所有者集合转移功能.

(4)供应链隐私性与透明性平衡

BPOTS通过对称加密保证供应链隐私性. 除管理员节点以外，供应链节点无法将伪ID映射到真实ID. 由于用户可使用不同的PID提交交易，即使少量PID与ID的对应关系泄露，仍不会暴露用户的全部隐私. 因此，BPOTS保证了供应链的隐私性.

BPOTS通过区块链保证了供应链透明性. 普通用户可通过链上转移信息验证转移过程合法性. 仅有管理员拥有PID与真实ID的对应关系. 当产品出现问题时，可根据产品真实转移路径对产品进行追踪溯源. 若恶意用户实施破坏供应链系统安全的行为，管理员能够通过伪ID追踪其真实身份. 因此，BPOTS保证了供应链的透明性.

综上所述，在BPOTS中，供应链产品转移的完整路径等隐私信息只有管理员能够获取，而普通用户可以验证产品转移操作的合法性. 因此，BPOTS平衡了供应链的隐私性和透明性.

7 性能分析

本节分析BPOTS扩展性、性能以及计算代价.

7.1 可扩展性分析

(1)降低新所有者集合成员增多的存储代价

以256位解密密钥为例，集合中每增加一个成员，解密密钥将增加128 B，生成的密文也将增加32 B，当集合中成员过多时，将导致存储代价过大.

中国剩余定理[14]的加解密复杂度均为常数时间，密钥生成为$O(n)$. 因此，每次产品转移时，管理员重新计算密钥，能够有效降低原所有者的存储代价. 此外，管理员指定新所有者集合的方式灵活. 若新所有者集合成员不断增加，管理员可以将新所有者集合拆分为多个较小的所有者子集合，原所有者在转移产品时可指定一个所有者子集合. 管理员根据子集合下发密钥，由原所有者端计算密文并上传到区块链中. 因此，BPOTS在面对新所有者集合过大情况时具有较好的可扩展性，仅需增加少量计算代价就可降低系统存储代价.

(2)新所有者集合节点退出效率高

由式(12)，加密密钥可描述如下：

$$\mu=x_0y_0+x_1y_1+\cdots+x_ny_n \tag{12}$$

根据中国剩余定理，若μ的累加式中不包含x_iy_i，则k_i无法解密使用μ加密的数据. 因此，若集合中的第i个成员退出，无需通过$O(n)$时间重新计算μ，而仅需消耗常数时间计算$\mu'=\mu-x_iy_i$. 综上所述，BPOTS在新所有者集合的动态管理上具有较好可扩展性.

7.2 性能对比分析

BPOTS与现有典型的供应链产品所有权转移方案[11,13,14]的性能对比如表1所示. BPOTS实现了指定新所有者集合转移，提高了系统安全性；其次，BPOTS基于区块链实现，保证了供应链的透明性；再次，BPOTS中仅管理员能够获取所有者的真实ID，保护了供应链隐私安全；最后，BPOTS实现了产品的批量转移，提高了产品转移的效率.

表1 BPOTS方案性能分析

方案	区块链	隐私保护	批量转移	新所有者
CPDS[10]	√	×	×	固定
UESUGI[11]	√	√	×	任意
ANTS[8]	×	×	√	任意
BPOTS	√	√	√	指定集合

7.3 计算代价对比分析

现有经典供应链产品所有权转移方案[8,10,11]主要研究所有权转移过程的验证. UESUGI[11]通过对称加密共享秘密值，再通过零知识证明技术验证秘密值正确性；CPDS[10]通过属性加密技术共享秘密值和数字签名技术验证秘密值；ANTS[8]提出了一种公钥同态承诺方案，实现了产品批量转移. 本节对BPOTS与现有典型的供应链产品所有权转移方案[11,13,14]进行计算代价对比分析. 实验代码用Go语言编写，程序运行在Intel(R) Xeon(R) Gold 6133 2.50 GHz和配备4核8 G的Linux操作系统上. 实验中的椭圆曲线为Brainpool P256曲线，零知识证明基于GNARK和长安链开发框架实现.

BPOTS与ANTS[8]、CPDS[10]、UESUGI[11]等三种方案完成单一产品所有权转移的性能对比如图3所示. 结果表明：BPOTS与ANTS[8]、CPDS[10]、UESUGI[11]相比，效率分别提高了3倍、24倍和27倍.

CPDS[10]和UESUGI[11]没有产品批量转移方法，在实现时将一次转移过程运行多次以完成产品所有权批量转移任务. BPOTS与ANTS[8]、CPDS[10]、UESUGI[11]等三种方案完成批量产品所有权转移的性能对比如图4所示. 结果表明：BPOTS完成产品批量转移的效率最高，与ANTS[8]、CPDS[10]和UESUGI[11]相比分别提高了约12倍、30倍和40倍.

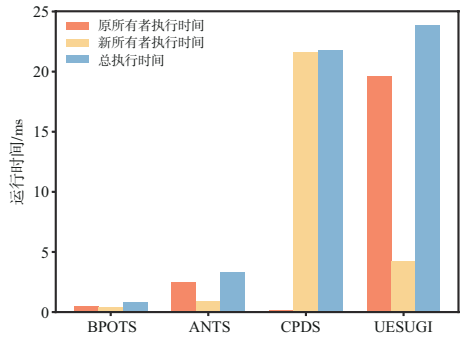


图3　转移单个产品所有权计算代价对比图

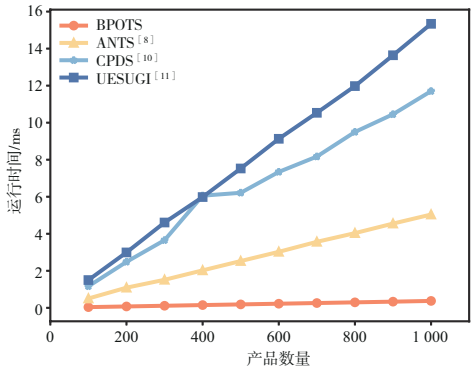


图4　产品所有权批量转移计算代价对比图

8　BPOTS实现

本文在长安链平台部署了智能合约,智能合约包括以下5种方法.

(1)AddPid $\left(\mathrm{PID}, \mathrm{pk}_{\mathrm{PID}}^{\mathrm{sig}}, \sigma\right)$:在区块链记录一对合法的$\left(\mathrm{PID}, \mathrm{pk}_{\mathrm{PID}}^{\mathrm{sig}}\right)$;

(2)CreateProduct $(\mathrm{TID}, \mathrm{PID}, \sigma)$:在区块链中创建初始所有者为PID,产品ID为TID的产品;

(3)UploadAlpha $\left(\mathrm{TID}, \gamma_{\alpha}, c_{\alpha}, \sigma\right)$:上传秘密值$\alpha$对应的密文$\gamma_{\alpha}$、承诺$c_{\alpha}$和签名$\sigma$;

(4)UploadBeta $\left(\mathrm{TID}, \gamma_{\beta}, c_{\beta}, \sigma\right)$:上传秘密值$\beta$对应的密文$\gamma_{\beta}$、承诺$c_{\beta}$和签名$\sigma$;

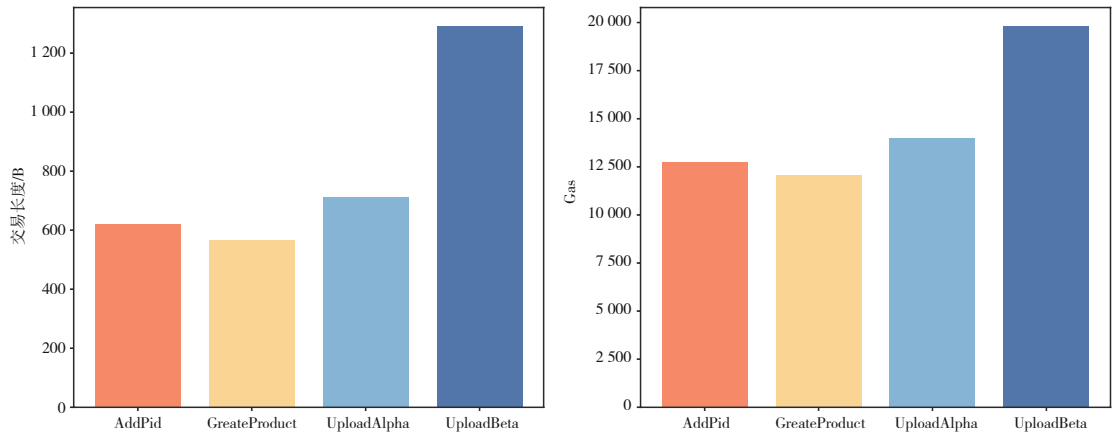
(5)BatchTransfer $(S, \mathrm{PID}, p, r, \sigma)$:将待转移产品集合$S$所有权转移至PID,提交秘密值的和$p$、随机数的和$r$以及签名$\sigma$验证新所有者身份.

表2描述了BenchMask工具分析四种智能合约方法的资源消耗情况,每种方法结果均取样100万次.由BenchMask分析结果可知,四种智能合约方法均有较高的运行效率和较少的内存消耗.

表2　BenchMask智能合约分析结果

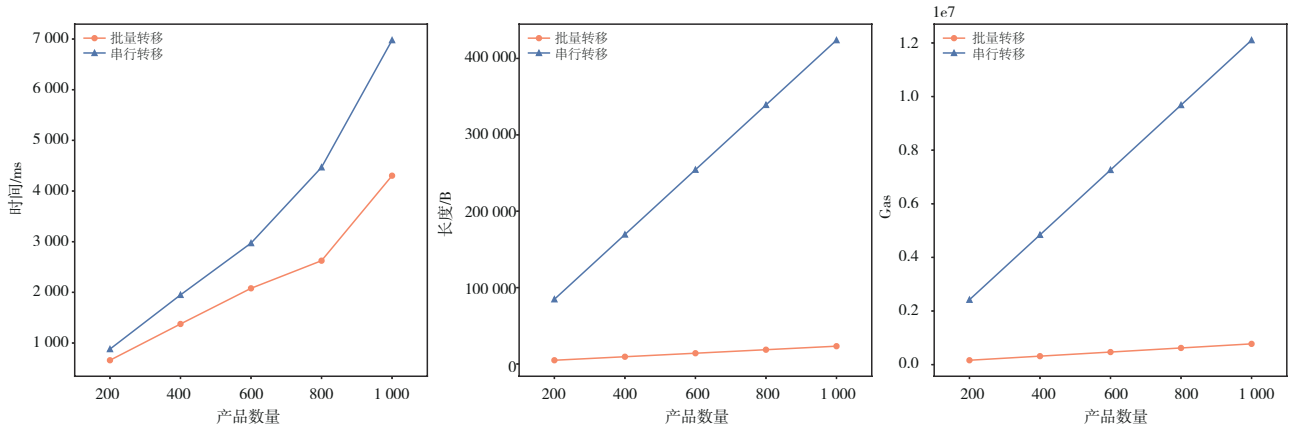
方法	迭代次数	运行时间/(ns·op^{-1})	内存使用/(B·op^{-1})	内存分配次数/(allocs·op^{-1})
Addpid	1 000 000	1 378	343	9
CreateProduct	1 000 000	1 663	336	10
UploadAlpha	1 000 000	2 250	511	11
UploadBeta	1 000 000	2 450	607	11

本文将上述五种方法的智能合约部署到长安链平台.长安链平台属于联盟链,节点需要证书才能加入区块链网络.长安链平台100 ms生成一个区块,每个区块最多含有100笔交易.经过实验测试,用户发起AddPid、CreateProduct、UploadAlpha、UploadBeta这四种类型的交易时,从交易发起到交易写入区块链的时间约为50 ms.智能合约方法资源消耗对比如图5所示,结果表明:UploadBeta的通信代价约为1 350 B,Gas消耗约为20 000.其他三种操作的通信代价约为650 B,Gas消耗约13 000.区块链执行产品批量与单一产品转移性能对比如图6所示.结果表明:相比于单一产品转移,产品批量转移的执行效率提高了70.4%,存储代价降低了约17倍,成本降低了约14倍,有效降低区块链的性能代价与成本.



(a) 交易长度　　(b) 交易Gas消耗

图5　智能合约方法资源消耗对比图



(*a*) 交易运行时间 (*b*) 交易通信代价 (*c*) 交易Gas消耗

图6 产品所有权转移性能对比图

9 结束语

本文针对现有RFID供应链产品所有权转移方案中存在的无法实现指定新所有者集合所有权转移、隐私泄露、转移效率低等问题,提出了一种基于区块链的RFID供应链产品所有权转移方案BPOTS. 首先,设计了一种基于中国剩余定理和Pedersen承诺的秘密值共享与验证算法,实现了指定新所有者集合的产品所有权转移;其次,提出了一种基于对称加密的伪ID生成算法,有效平衡了供应链隐私性与透明性;再次,构建了一种基于Pedersen承诺的产品所有权批量转移方法,大大提高了产品批量转移的效率,有效降低了供应链节点的成本;最后,本文在长安链平台上实现了BPOTS并将源代码开源.

参考文献

[1] DUTTA P, CHOI T M, SOMANI S, et al. Blockchain technology in supply chain operations: Applications, challenges and research opportunities[J]. Transportation Research Part E: Logistics and Transportation Review, 2020, 142(10): 102067.

[2] LINTON J D, KLASSEN R, JAYARAMAN V. Sustainable supply chains: An introduction[J]. Journal of Operations Management, 2007, 25(6): 1075-1082.

[3] SODHI M S, TANG C S. Research opportunities in supply chain transparency[J]. Production and Operations Management, 2019, 28(12): 2946-2959.

[4] OGHAZI P, FAKHRAI RAD F, KARLSSON S, et al. RFID and ERP systems in supply chain management[J]. European Journal of Management and Business Economics, 2018, 27(2): 171-182.

[5] DORRI A, KANHERE S S, JURDAK R. Towards an optimized blockchain for IoT[C]//2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). Piscataway: IEEE, 2017: 173-178.

[6] 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.(in Chinese)

[7] REIMSBACH-KOUNATZE C. Enhancing access to and sharing of data: striking the balance between openness and control over data[M]//Data Access, Consumer Interests and Public Welfare. Munich: Nomos Verlagsgesellschaft mbH &; Co. KG, 2021: 25-68.

[8] QI S Y, ZHENG Y Q, CHEN X F, et al. Ants can carry cheese: Secure and private RFID-enabled third-party distribution[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(3): 1505-1517.

[9] TOYODA K, MATHIOPOULOS P T, SASASE I, et al. A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain[J]. IEEE Access, 2017, 5: 17465-17477.

[10] QI S Y, LU Y S, ZHENG Y Q, et al. Cpds: Enabling compressed and private data sharing for industrial Internet of Things over blockchain[J]. IEEE Transactions on Industrial Informatics, 2021, 17(4): 2376-2387.

[11] UESUGI T, SHIJO Y, MURATA M. Design and evaluation of a privacy-preserving supply chain system based on public permissionless blockchain[C]//2021 International Symposium on Electrical, Electronics and Information Engineering. New York: ACM, 2021: 312-321.

[12] VIJAYALAKSHMI M, SHALINIE S M, YANG M H, et al. A blockchain-based secure radio frequency identifica-

tion ownership transfer protocol[J]. Security and Communication Networks, 2022, 2022(1): 9377818.

[13] MUNOZ-AUSECHA C, GÓMEZ J E G, RUIZ-ROSERO J, et al. Asset ownership transfer and inventory using RFID UHF tags and ethereum blockchain NFTs[J]. Electronics, 2023, 12(6): 1497.

[14] ZHANG J, CUI J, ZHONG H, et al. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(2): 722-735.

[15] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[M]//Advances in Cryptology - CRYPTO' 91. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007: 129-140.

[16] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18-36.

作者简介

陆琪鹏　男,1999年生于江苏南京,硕士研究生. 主要研究方向为RFID认证技术、物联网安全和区块链安全.
E-mail: 2020210522@jsnu.edu.cn

曾聪爱　女,1999年生于湖南衡阳,硕士研究生. 主要研究方向为位置服务隐私保护、车联网安全和数据安全.
E-mail: zengcongai@jsnu.edu.cn

刘亚丽　女,1981年生于江苏徐州,博士,教授,硕士生导师,CCF高级会员. 主要研究方向为信息安全、认证和隐私保护技术、区块链安全、车联网安全、密码算法和协议及其在物联网和移动通信中的应用.
E-mail: liuyali@jsnu.edu.cn

陈东东　男,2000年生于江苏淮安,硕士研究生. 主要研究方向为无人机认证技术、物联网安全和隐私保护技术.
E-mail: 2020220572@jsnu.edu.cn

刘长庚　男,1997年生于江苏连云港,硕士研究生. 主要研究方向为RFID认证技术、物联网安全和隐私保护技术.
E-mail: 2020200444@jsnu.edu.cn

宁建廷　男,1988年生于浙江衢州,博士,教授,博士生导师. 主要研究方向为密码学与数据安全、区块链与机器学习安全隐私、隐私保护技术.
E-mail: jtning88@gmail.com