文章编号:1674-2974(2025)12-0147-07 DOI:10.16339/j.cnki.hdxbzkb.2025234

基于区块链的所有权转移与追踪方案

黄梦桥[1,2],马昌社[1†]
(1. 华南师范大学 计算机科学学院,广东 广州 510631;
2. 湖南涉外经济学院 商学院,湖南 长沙 210205)

摘 要:现代信息技术虽然为商品供应链提供了实时、可视化的管理便利,但是数字化的信息流通带来了隐私安全问题.针对这一问题,利用RFID技术、区块链和现代密码技术,提出了一个商品所有权转移与追踪方案.首先建立所有权转移与追踪方案的模型;然后从不可伪造性和隐私性两个方面定义所有权转移与追踪方案的安全性;最后设计了有序聚合签名技术,并结合区块链设计了一个高效、安全且带隐私保护的所有权转移与追踪(OTT,ownership transfer and tracking)方案.在OTT中,仅要求标签具有基础的计算和存储能力,因此OTT方案可以适用于轻量级的标签;有序聚合签名不但压缩了区块链上的数字签名数据,而且提供了一种刻画商品流通路径的方法.

关键词:区块链;所有权转移;所有权追踪;隐私性;不可伪造性
中图分类号:TP309 **文献标志码**:A

Blockchain-based Ownership Transfer and Tracking Scheme

HUANG Mengqiao[1,2],MA Changshe[1†]
(1. School of Computer Science, South China Normal University, Guangzhou 510631, China;
2. College of Business, Hunan International Economics University, Changsha 210205, Chian)

Abstract: Although modern information technology provides real-time and visual management convenience for commodity supply chains, digital information circulation brings privacy security issues. To address this problem, an ownership transfer and tracking scheme is proposed through using RFID, blockchain and modern cryptography technology. Specifically, we first establish a formal model of the ownership transfer and tracking scheme. Then, we define the security of the ownership transfer and tracking scheme from two aspects: unforgeability and privacy. Finally, we design ordered aggregate signature based on which an efficient, secure and privacy-protected ownership transfer and tracking scheme (OTT) is presented. The tags of OTT are only required to have basic computing and storage capabilities, so the OTT scheme can be applied to lightweight tags. The ordered aggregate signature not only compresses the data of blockchain but also provides a way to characterize the circulation path.

Key words: blockchain; ownership transfer; ownership tracking; privacy; unforgeability

---

* **收稿日期**:2025-03-04
基金项目:国家自然科学基金资助项目(61070217), National Natural Science Foundation of China(61070217);湖南省“十四五”特色学科应用经济学项目(湘教通[2022]351), The Featured Discipline of Hunan Province During the 14th Five-Year Plan period-Applied Economics(Xiangjiaotong[2022]351)
作者简介:黄梦桥(1970—),男,湖南益阳人,华南师范大学教授
† 通信联系人,E-mail: changshema@gmail.com

区块链[1]和物联网的发展给商品流通带来了极大的便利，现代商品供应链中包括信息流、物流和资金流，这些信息的泄露给用户带来了安全隐私威胁问题. 为了有效解决这一问题，工业界与学术界对基于RFID的认证技术、隐私保护技术以及区块链隐私保护技术进行了深入的探讨和研究，取得了丰富的研究成果[2-4]，并形成了一系列切实可行的解决方案[5-7]. 然而，目前尚无研究专门同时针对商品所有权转移及其追踪进行探讨.

RFID系统中的标签计算和存储能力受限，因此对其进行安全隐私保护是一项具有挑战性的任务，虽然学术界出现了众多保护隐私的RFID认证协议，但这些协议对标签的计算要求高，不适用于受限的RFID标签，尤其是所有权转移和追踪，其设计需要一定的知识证明协议，众所周知知识证明协议是计算密集型协议，所以其难以在RFID系统中高效安全地实现. 随着区块链技术的兴起，其可以作为全局信任锚的功能使得设计高效安全的所有权转移和追踪方案变得可能. 区块链具有去中心化、安全可信、无法改写、集体维护等特点，在被提出之后就成为人们的研究热点，被广泛应用到金融、信息、物联网等领域. 虽然文献[8]提出了RFID所有权转移方案，但是这些方案均不支持所有权追踪功能[8]. 实际上，所有权追踪是商品供应链必备的功能之一，它是一种数字金融的基础构件.

本文利用区块链作为全局信任锚，设计了一个用RFID标签标识的商品的所有权转移和追踪(ownership transfer and tracking，OTT)方案. 首先，定义了商品的所有权转移和追踪方案的模型以及其安全性，包括所有权转移的正确性、所有权转移路径的隐私性和所有权转移路径的不可伪造性，从而保证了所有权的可追踪性；然后，基于BLS数字签名技术[8]设计了一个有序聚合签名技术，并结合区块链设计了所有权转移和追踪方案，有序聚合签名不仅压缩了数字签名的长度，也降低了区块链的存储压力，而且提供了一种流通路径的刻画方法；最后，在随机预言机模型下证明了所有权转移和追踪方案的正确性、所有权转移路径的隐私性和所有权转移路径的不可伪造性.

本文剩余部分组织如下：第1节介绍相关研究工作，第2节介绍本文方案设计的相关预备知识，第3节给出本文方案的模型和安全定义，第4节给出本文设计的OTT方案和它的安全证明，第5节总结全文.

1 相关研究

RFID认证协议的设计方法众多，包括基于硬件的方法，比如Kill命令法[9]、主动干扰法[10]、阻塞标签法[11]和法拉第网罩法[12]等；也包括基于对称密码算法的方法，比如：基于密码哈希函数的方法[13]、基于伪随机函数的方法[14]和基于伪随机发生器的方法[6]等，文献[15]证明了RFID认证协议的隐私安全性等价于标签具有计算伪随机函数的能力，因此，所有安全的RFID认证协议都要求标签配备计算伪随机函数的能力；包括基于公钥密码的方法，比如：基于椭圆曲线的方法、基于格密码的方法等. 近年来，随着区块链的发展，出现了一批基于区块链的RFID隐私认证技术设计方法.

关于所有权转移，最早由Molnar等[16]提出了一个针对RFID标签所有权转移协议，该协议的缺点是需要一个可信第三方来协助完成两方的所有权转移，这容易造成信息泄露而损害用户的隐私安全. 随后，文献[10，12]分别提出了所有权转移协议，这些协议普遍效率低下，且具有各种安全漏洞. 随着云计算的兴起，Cao等[17]提出了一个基于云服务器的所有权转移方案，该方案虽然可以保护云环境下的数据隐私，但不能抵御位置隐私攻击. 沈金伟等[18]设计了一种线性无关性循环分组函数，并基于此函数设计了一个轻量级的RFID标签所有权转移协议. 最近，文献[19]提出了基于区块链的所有权转移协议，但是该协议采用了大量的高精度数学运算，因此其性能不理想.

实际上，目前所有的所有权转移方案的设计只关注所有权的转移，并没有涉及所有权转移的追踪. 实际上，所有权转移的追踪对于商品供应链是至关重要的，因此有必要同时研究所有权转移和追踪.

2 预备知识

为了描述方便，本节首先介绍常用的符号，然后介绍区块链、RFID系统和BLS签名方案[20].

2.1 符号描述

设A是一个概率多项式时间算法，那么$v \leftarrow A^{O_1,O_2,\cdots,O_n}(x_1,x_2,\cdots,x_m)$表示算法$A$的输入是$x_1,x_2,\cdots,x_m$，并且算法$A$可以查询预言机$O_1,O_2,\cdots,O_n$，其输出赋值给变量$v$；设$S$表示一个集

合,则$e \in_R S$表示从S中根据均匀分布抽样一个样本e;$\{0,1\}^l$表示所有比特长度为l的二进制比特串的集合;设x,y是两个比特串,则$x\|y$表示把它们拼接成一个比特串,$|x|$表示比特串x的比特长度;$\Pr[E]$表示事件E发生的概率.

定义1:称函数$\mathrm{neg}:\{0,1\}^l \to \mathbf{R}$是可忽略的,如果它满足对任意一个多项式$p(n)$,当$n$充分大时有$\mathrm{neg}(n) < 1/p(n)$,$\mathbf{R}$表示实数集.

2.2 区块链

本文采用区块链[1]存储数据.区块链通常是一种链式数据结构,它的基本数据单元是区块.每一个区块$B_i =< \mathrm{hd}_i, \mathrm{bd}_i, \mathrm{crt}_i >, i \in \mathbf{N}$,其中,$\mathrm{hd}_i$为前一区块的哈希值,也称为父哈希,通过父哈希可以使当前区块和前一个区块链接到一起,bd_i为区块体的消息内容,它可以包含任意长度的二进制消息,crt_i为生成该区块的工作量证明.区块B_0称为创世区块,各个区块按照创建的时间,利用父哈希依次将多个区块进行排序链接,从而形成一个长链,因此被称为区块链.

2.3 RFID系统

不失一般性,假设RFID系统[6]由标签、阅读器和后端数据库系统组成.每一个标签由一个唯一的身份标识符TID所标识,阅读器有一个或者多个射频收发器,后端数据库系统维护认证标签所需要的所有数据,比如标签的TID、状态信息、TID在区块链中的区块地址信息等.一般地,阅读器R和标签T之间通过认证协议可以进行双向认证,通过所有权转移协议进行所有权的转移.标签阅读器和标签之间通过图1所示的协议进行通信.

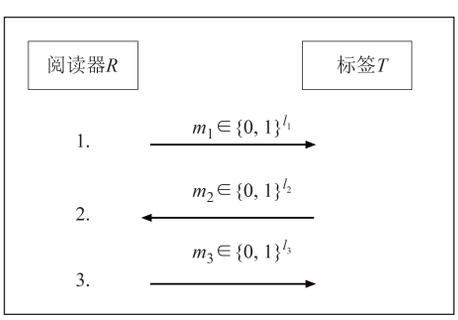

图1　RFID系统图

Fig.1　RFID System Diagram

定义2:认证协议$\mathrm{AP}(R,T)$是阅读器R和标签T之间的协议,协议执行完毕后,如果阅读器R和标签T互相接受对方,则输出1;否则,输出0.

定义3:所有权转移$\mathrm{OT}(A,B,T,\mathrm{BC})$协议是假设销售方$A$把由标签$T$标识的商品转让给销售方$B$,这是一个由$A$、$B$、$T$和区块链BC参与的四方协议,通过该协议,$B$拥有$T$的所有权,而$A$不再拥有$T$的所有权,并且$T$从$A$流通到了$B$.

2.4 BLS签名方案

BLS签名方案是由Boneh等[20]提出的一个短签名方案,其可以支持门限签名、多重签名和聚合签名等功能性签名.

假设G_1和G_2是两个阶为大素数p的乘法循环群,G_1的生成元是g,用$e()$表示.$G_1 \times G_2 \to G_T$是一个双线性映射,如果它满足:

1)双线性:任给$g \in G_1$、$h \in G_2$和$x,y \in Z_p$,均有$e(g^x,h^y) = e(g,h)^{xy}$.

2)非退化:存在$g \in G_1$、$h \in G_2$使得$e(g,h) \neq 1 \in G_T$.

BLS签名方案由三个算法组成,分别描述如下:

$\mathrm{KG}(1^\lambda)$:密钥生成算法,每一个签名用户u_i选择签名私钥$x_i \in_R Z_p^*$,并计算其签名验证公钥为$y_i = g^{x_i} \in G_1$.

$\mathrm{Sign}(x_i,m)$:签名生成算法,假设用户u_i对消息m进行签名,其生成的签名为$\sigma = H(m)^{x_i} \in G_2$,这里$H$是一个把消息哈希到$G_2$的密码哈希函数.

$\mathrm{Verify}(m,\sigma,y_i)$:密钥验证算法,如果$e(\sigma,H(m)) = e(g,y_i)$,则输出1;否则输出0.

2.5 El Gamal公钥加密

假设群G_1是一个乘法循环群,其阶为大素数q,g_1是群G_1的生成元.El Gamal公钥加密方案[21]$\mathrm{PKE} = (\mathrm{KG},\mathrm{Enc},\mathrm{Dec})$由三个算法组成,分别是密钥生成算法KG、加密算法Enc和解密算法Dec,其描述如下:

1)密钥生成算法KG:输入安全参数,首先在群Z_q上根据均匀分布抽样一个样本x,然后计算$y = g_1^x$,输出加密公钥为y,解密私钥为x.

2)加密算法Enc:输入公钥y和消息$m \in G_1$,首先在群Z_q上根据均匀分布抽样一个样本k,然后计算$u = g_1^k$和$v = y^k \times m$,输出密文为$c = (u,v)$.

3)解密算法Dec:输入私钥x和密文$c = (u,v)$,计算明文$m = v/u^x$.

2.6 伪随机函数

设有一个函数$\mathrm{PRF}: K \times D \to \mathrm{Rng}$,这里$K$是密钥的集合,$D$是定义域,Rng是值域.我们说PRF是一个安全的伪随机函数,如果它满足:对任意概率

多项式时间算法A，其区分PRF与从$D \to \mathrm{Rng}$的随机函数的优势是可以忽略不计的[22].

3 所有权转移与追踪模型

3.1 系统模型

在商品供应链中，每一件商品由一个RFID标签来标识，一个商品供应链包含三类实体：商品发布方I、商品销售方S和注册机构R，他们都拥有RFID阅读器和标签，并共享一个公开的区块链BC. 假设所有参与方之间存在安全的认证信道，商品发布方I和商品销售方S均需向注册机构R它们的公私钥对. 一般地，一个商品供应链是一个有向图$GH = (V, E)$，其中V表示顶点集，它可以是商品发布方I或者商品销售方S，每一个顶点表示供应链中的一次流通，每一个顶点都配备有一台RFID阅读器；E表示边的集合，对每一条边$v_i v_j \in E$表示某个商品从v_i流通到v_j.

定义4(流通路径)：一个商品从顶点v_{i_1}开始，通过顶点$v_{i_2}, \cdots, v_{i_{k-1}}$，到达顶点$v_{i_k}$，则称$(v_{i_1}, v_{i_2}, \cdots, v_{i_k})$是一条流通路径，其长度为$k$.

定义5(所有权转移与追踪系统)：一个所有权转移与追踪系统：

$\Pi = (\mathrm{Init}, \mathrm{AP}, \mathrm{OT}, \mathrm{FindPath}, \mathrm{Track})$

其中：

$\mathrm{Init}(I^{\lambda})$：系统初始化算法，输入安全参数$\lambda$，系统初始化商品发布方$I$、商品销售方$v_i$、区块链BC和路径验证方$V$.

$\mathrm{AP}(R, T)$：定义2所描述的阅读器与标签之间的双向认证协议.

$\mathrm{OT}(v_i, v_j, \mathrm{BC}, T)$：定义3所描述的所有权转移协议.

$\mathrm{FindPath}(\mathrm{TID})$：输入标签身份TID，在区块链中回溯该TID的流通路径.

$\mathrm{Track}(\mathrm{TID}, \mathrm{path})$：追踪算法，验证标签TID的流通路径是否为path. 如果标签TID通过路径path，则输出1，否则，输出0.

3.2 安全定义

所有权转移与追踪方案的安全要求包括：所有权转移的正确性、流通路径的隐私性和流通路径的不可伪造性，分别描述如下.

定义6(所有权转移的正确性)：如果协议的各个参与方诚实地执行协议，则标签的所有权从转让方转移到受让方. 具体地说，对任意概率多项式时间算法A，以下概率是可以忽略的，即

$\Pr\left[\mathrm{AP}(B, T) = 0 | \mathrm{OT}(A, B, \mathrm{BC}, T)\right] < \mathrm{neg}(\lambda)$，$\lambda$是安全参数.

定义7(流通路径的隐私性)简单地说，敌手不能通过流通路径来识别流通的标签，也就是说如果两个标签的流通路径长度一致，那么它们的流通路径是计算不可区分的. 考虑如下隐私游戏：假设A是任意一个概率多项式时间算法，其既可以查询标签的所有权转移协议、路径生成算法、追踪算法，也可以查看区块链上的数据，然后选择两个新的标签T_0与T_1和一个路径长度l，游戏从这两个标签中随机选择一个$T_b (b \in_R \{0, 1\})$，为标签T_b产生一条长度为l的流通路径path_b，并把path_b交给敌手A，此后敌手A可以继续进行前述查询，但不能进行与标签T_0与T_1有关的查询，最后敌手A输出一个比特b'来表示其对T_b的猜测. 我们说流通路径具有隐私性如果以下概率是可以忽略的，即

$$\left|\Pr[b' = b] - \frac{1}{2}\right| < \mathrm{neg}(\lambda)$$

定义8(流通路径的不可伪造性)：简单地说，商品流通路径的不可伪造性指的是，只要伪造的流通路径上有一个诚实的参与方，敌手伪造一条流通路径是困难的. 考虑如下不可伪造游戏：假设F是任意一个概率多项式时间算法，首先，F以自适应的方式进行多项式个查询，包括查询标签的所有权转移协议、路径生成算法、追踪算法和区块链上的数据，最后敌手F输出一条路径path_F和一个身份标识为TID_F的标签T_F，这里要求path_F中至少有一个诚实的参与方H且F没有查询过以H和T_F为输入的所有权转移协议. 我们说流通路径具有不可伪造性，如果以下概率是可以忽略的，即

$\Pr[\mathrm{Track}(\mathrm{TID}_F, \mathrm{path}_F) = 1] < \mathrm{neg}(\lambda)$，$\lambda$是安全参数.

4 所有权转移与追踪方案OTT

首先设计一个有序聚合签名方案，然后描述所有权转移与追踪方案，最后给出其安全证明.

4.1 有序聚合签名

假设H_2是一个密码哈希函数，用户$v_1, v_2, \cdots, v_n$的BLS签名公私钥对分别为：$(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$，他们按照$v_1, v_2, \cdots, v_n$这种顺序来产生对消

息m的聚合签名.产生聚合签名的算法如下:

$$\mathrm{OAgg}\left(\left(x_1,y_1\right),\left(x_2,y_2\right),\cdots,\left(x_n,y_n\right),m\right)$$

1)用户v_1计算$\Omega_1=H(m)^{H_2\left(y_1\|y_1\right)x_1}$,把$\Omega_1$发送给$v_2$.

2)每一个用户v_i计算$\Omega_i=\Omega_{i-1}H(m)^{H_2\left(y_{i-1}\|y_i\right)x_i}$,把$\Omega_i$发送给$v_{i+1}$,$i=2,\cdots,n-1$.

3)用户v_n计算$\Omega_n=\Omega_{n-1}H(m)^{H_2\left(y_{n-1}\|y_n\right)x_n}$;输出聚合签名$\Omega_n$.

聚合签名$\mathrm{VOAgg}(y_1,y_2,\cdots,y_n,\Omega,m)$验证算法:

如果等式

$$e\left(\Omega,H(\mathrm{TID})\right)=e\left(g,\left(y_1\right)^{H_2\left(y_1\|y_1\right)}\times\left(y_2\right)^{H_2\left(y_n\|y_2\right)}\times\cdots\times\left(y_n\right)^{H_2\left(y_{n-1}\|y_n\right)}\right)$$

成立,则输出1;否则,输出0.

4.2 OTT方案

假设$\mathrm{PKE}=(\mathrm{KG},\mathrm{Enc},\mathrm{Dec})$是群$G_1$上的El Gamal公钥加密算法[21],$\mathrm{SKE}=(\mathrm{SKG},\mathrm{SE},\mathrm{SD})$是一个对称密码算法,PRF是一个安全的伪随机函数[22].OTT方案的五个部件Init、AP、OT、FindPath和Track分别描述如下:

1)$\mathrm{Init}(I^\lambda)$:输入安全参数λ,每一个参与方v_i(包括商品发布方I和商品销售方S)随机选择一个BLS签名私钥$x_i\in_R Z_p^*$,计算其签名验证$y_i=g^{x_i}\in G_1$,然后把其身份信息ID_i和公钥y_i发送给注册机构Rst进行登记注册.商品发布方v_i初始化每一个标签T_j:把标签标识TID_j和认证密钥k_j写入到标签T_j,把消息$(y_i,y_i,\Omega_{ij},\mathrm{eidx})$写入区块链中地址为$\mathrm{idx}_j$的区块,这里$\sigma_{ij}=\mathrm{Sign}\left(x_i,\mathrm{TID}_j\right)$,$\Omega_{ij}=(\sigma_{ij})^{H_2(y_i\|y_i)}$,eidx是一个空字符串$\perp$,并把$(\mathrm{TID}_j,k_j,\mathrm{idx}_j)$写入到本地数据库中.

2)$\mathrm{AP}(R,T)$:假设R和T之间共享的认证密钥为k.

(a)首先,阅读器R选择一个随机数$n_R\in_R\{0,1\}^\lambda$,发送n_R给标签T.

(b)收到n_R后,标签T计算$n_T=\mathrm{PRF}(k,n_R)$,发送其身份信息TID和n_T给阅读器R.

(c)收到TID和n_T后,阅读器以TID为索引检索后端数据库,得到其对应的认证密钥k',如果$\mathrm{PRF}(k',n_R)=n_T$,则接受标签T且发送$f_R=\mathrm{PRF}(k',n_T)$给标签T,否则发送一个随机消息给标签T.

(d)收到f_R后,标签验证$\mathrm{PRF}(k,n_T)=f_R$,如果成立,则接受阅读器R,否则就拒绝阅读器R.

3)$\mathrm{OT}(v_i,v_j,\mathrm{BC},T)$:假设节点$v_i$和$v_j$的BLS签名公私钥对分别为$(x_i,y_i)$和$(x_j,y_j)$,标签$T$的认证密钥为$k$.协议执行如下:

(a)v_j发送其公钥y_j给v_i发起关于标签T的所有权转移.

(b)v_i从自己的后端数据库里检索得到标签T的信息TID、k和idx_i,然后将密文数据$c_i=\mathrm{Enc}(y_j,k\|\mathrm{TID}\|\mathrm{idx}_i)$发送给$v_j$.

(c)v_j利用其私钥x_j解密c_i得到TID、k和idx_i,然后发送随机数n_R给标签T.

(d)收到n_R后,标签T计算$n_T=\mathrm{PRF}(k,n_R)$,发送其身份信息TID′和n_T给v_j.

(e)收到TID′和n_T后,v_j验证TID′=TID和$\mathrm{PRF}(k,n_R)=n_T$,如果都成立,则发送$f_R=\mathrm{PRF}(k,n_T)$和$\mathrm{ek}=\mathrm{PRF}(k,f_R)\oplus k_{new}$给标签$T$;否则所有权转移失败且终止协议执行.

(f)收到f_R和ek后,标签T先验证$\mathrm{PRF}(k,n_T)=f_R$,如果成立,则解密ek得到k_{new},即$k_{new}=\mathrm{ek}\oplus\mathrm{PRF}(k,f_R)$,然后替换其认证密钥$k=k_{new}$,并返回$f_T=\mathrm{PRF}(k_{new},f_R)$给$v_j$.

(g)收到f_T后,v_j验证$f_T=\mathrm{PRF}(k_{new},f_R)$,如果成立则向区块链请求地址为$\mathrm{idx}_i$的区块内容,获得聚合签名$\Omega_i$.

(h)v_j计算其对TID的签名$\sigma_j=\mathrm{Sign}(x_j,\mathrm{TID})$,然后计算聚合签名$\Omega_j=\Omega_i\times(\sigma_j)^{H_2\left(y_i\|y_j\right)}$,把消息$(y_i,y_j,\Omega_j,\mathrm{ept})$写入区块链中地址为$\mathrm{idx}_j$的区块,这里$\mathrm{ept}=\mathrm{SE}(\mathrm{idx}_j,\mathrm{idx}_i)$,并把$(\mathrm{TID},k_{new},\mathrm{idx}_j)$写入自己的后端数据库.

4)FindPath(TID):为了得到TID的流通路径,节点v_i首先从自己的后端数据库中检索TID对应的区块链地址idx,并从区块链中获取地址为idx的区块B_1,假设区块B_1的消息内容为$(y_2,y_1,\Omega_1,\mathrm{eidx}_1)$,解密该区块中的字段$\mathrm{eidx}_1$,即$\mathrm{idx}_1=\mathrm{SD}(\mathrm{idx},\mathrm{eidx}_1)$;然后从区块链中获取地址为$\mathrm{idx}_1$的区块$B_2$,假设区块$B_2$的消息内容为$(y_3,y_2,\Omega_2,\mathrm{eidx}_2)$,解密该区块中的字段$\mathrm{eidx}_2$,即$\mathrm{idx}_2=\mathrm{SD}(\mathrm{idx}_1,\mathrm{edix}_2)$;以此类推,直到取出的区块中的eidx字段为空而结束.假设取出的最后一个区块为B_n,其消息内容为$(y_n,y_n,\Omega_n,\perp)$.令$y_i'=y_{n-i+1}$,这里$i=1,2,\cdots,n$.最后,输出TID的流通路径:

$\text{path} = (y_1', y_2', \cdots, y_n', \Omega_1)$

实际上，Ω_1是公钥为$y_1', y_2', \cdots, y_n'$的节点对TID的有序聚合签名，即：

$$\Omega_1 = \text{OAgg}\left(\left(x_1, y_1'\right), \left(x_2, y_2'\right), \cdots, \left(x_n, y_n'\right), \text{TID}\right).$$

5) $\text{Track}\left(\text{TID}, \text{path}\right)$：如果 $\text{VOAgg}\left(y_1', y_2', \cdots, y_n', \right)\left(\Omega_1, \text{TID}\right) = 1$则输出1；否则，输出0.

4.3 安全证明

接下来证明所有权转移协议与追踪方案的正确性、流通路径隐私性和流通路径不可伪造性，分别由如下定理1、2和3所描述.

定理1：如果PRF是一个安全的伪随机函数，各参与方都诚实地执行所有权转移与追踪协议，且协议执行没有失败，那么所有权转移协议与追踪方案是正确的.

证明：根据协议 $\text{OT}\left(v_i, v_j, \text{BC}, T\right)$执行过程，在没有失败的前提条件下，协议执行完毕后，参与方v_j拥有了和标签T共享的认证新密钥k_{new}；根据阅读器与标签之间的认证协议AP，利用该新密钥参与方v_j可以和标签T实现互相认证. 根据基于伪随机函数的RFID认证协议的构造方法和理论，如果PRF是一个安全的伪随机函数，那么不具有新密钥k_{new}的参与方v_i通过标签T的认证的概率是可以忽略的，因此，参与方v_i不能与标签T实现互相认证. 所以，所有权转移协议与追踪方案是正确的.

定理2：如果对称加密方案SKE是语义安全的，那么在随机预言机模型下，所有权转移协议与追踪方案OTT是流通路径隐私安全的.

证明：这里我们假定哈希函数H_2是一个随机预言机. 证明这个定理只需要证明任意两个相同长度的流通路径的分布是计算不可区分的. 假设 $\text{path}_0 = (y_1', y_2', \cdots, y_n', \Omega)$和$\text{path}_1 = (y_1'', y_2'', \cdots, y_n'', \Omega')$是两条长度为$n$的路径. 首先，$(y_1', y_2', \cdots, y_n')$与$(y_1'', y_2'', \cdots, y_n'')$的分布计算不可区分，这是因为BLS签名方案的公钥的分布与G_1上的均匀分布是计算不可区分的，且任意两个签名公钥的分布是独立的. 其次，Ω与Ω'的分布是计算不可区分的，这是因为H_2是一个随机预言机，导致了签名聚合Ω中的每一个参与方v_i的贡献$\left(\sigma_i\right)^{H_2(y_j \| y_i)}$服从$G_2$中的均匀分布，所以$\Omega$的分布与$G_2$中的均匀分布计算不可区分，从而$\Omega$与$\Omega'$的分布是计算不可区分的. 综上所述，路径$\text{path}_0$与$\text{path}_1$的分布是计算不可区分的.

定理3：如果BLS数字签名是不可伪造的，那么在随机预言机模型下，所有权转移协议与追踪方案OTT具有流通路径不可伪造安全性.

证明：假设存在一个伪造者F，其可以为身份为TID^*的标签T^*伪造一条可以通过验证的流通路径path^*，接下来我们可以构造一个算法B，其可以伪造一个BLS数字签名. 算法B的设计如下：

假设流通路径path^*中没有被伪造者F腐化的节点为v_k，算法B的输入是BLS的签名公钥y. 首先，算法B初始化OTT方案，设置节点为v_k的签名公钥为y，并按照OTT方案来设置其他参与节点. 在接下来的查询中，如果涉及需要节点v_k关于TID的签名的查询(比如：所有权转移查询含有节点v_k)，算法B先对BLS签名方案发起对消息TID的签名查询，然后利用得到的签名来回答F的查询. 当伪造者F输出身份为TID^*的标签T^*的流通路径path^*后，假设$\text{path}^* = (y_n^*, y_{n-1}^*, \cdots, y_{k+1}^*, y, y_{k-1}^* \cdots, y_1^*, \Omega^*)$，利用算法$B$计算：

$$h_n = H_2(y_n^* \| y_n^*)x_n^*$$

$$h_k = H_2(y_{k+1}^* \| y)$$

$$h_i = H_2(y_{i+1}^* \| y_i^*)x_i^*, \quad i = n-1, \cdots, k+1, k-1, \cdots, 1$$

$$h = (h_n + \cdots + h_{k+1} + h_{k-1} + \cdots + h_1) \bmod p$$

$$\sigma^* = \left(\frac{\Omega^*}{H\left(\text{TID}^*\right)^h}\right)^{1/h_k} \in G_2$$

最后，算法B输出对消息TID^*的伪造的BLS签名σ^*. 因为BLS签名方案被证明是不可伪造的，所以所有权转移协议与追踪方案OTT具有流通路径不可伪造安全性.

5 结束语

本文针对所有权转移与追踪问题，利用RFID技术、区块链和现代密码技术，提出了一个商品所有权转移与追踪方案. 具体地，首先建立所有权转移与追踪方案的模型；然后从不可伪造性和隐私性两个方面定义所有权转移与追踪方案的安全性；最后设计了有序聚合签名技术，并结合区块链设计了一个高效、安全且带隐私保护的所有权转移与追踪方案. 在OTT中，仅要求标签具有基础的计算和存储能力，因此OTT方案可以适用于轻量级的标签；

有序聚合签名不但压缩了区块链上的数字签名数据,而且提供了一种刻画商品流通路径的方法.

参考文献

[1] REBELLO G A F, CAMILO G F, DE SOUZA L A C, et al. A survey on blockchain scalability: from hardware to layer-two protocols[J]. IEEE Communications Surveys & Tutorials, 2024, 26(4): 2411-2458.

[2] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述:原理、进展与应用[J]. 通信学报, 2020, 41(1):134-151.
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: principle, progress and application [J]. Journal on Communications, 2020, 41(1):134-151.(in Chinese)

[3] FAN K, LUO Q, ZHANG K, et al. Cloud-based lightweight secure RFID mutual authentication protocol in IoT[J]. Information Sciences, 2020, 527:329-340.

[4] 李鹏, 郑田甜, 徐鹤, 等. 基于区块链技术的RFID安全认证协议[J]. 信息网络安全, 2021, 21(5):1-11.
LI P, ZHENG T T, XU H, et al. RFID security authentication protocol based on blockchain technology[J]. Netinfo Security, 2021, 21(5):1-11.(in Chinese)

[5] 马昌社. 前向隐私安全的低成本RFID认证协议[J]. 计算机学报, 2011, 34(8):1387-1398.
MA C S. Low cost RFID authentication protocol with forward privacy[J]. Chinese Journal of Computers, 2011, 34(8):1387-1398.(in Chinese)

[6] 唐飞, 陈云龙, 冯卓. 基于区块链和代理重加密的电子处方共享方案[J]. 计算机科学, 2021, 48(增刊1):498-503.
TANG F, CHEN Y L, FENG Z. Electronic prescription sharing scheme based on blockchain and proxy re-encryption [J]. Computer Science, 2021, 48(Sup.1):498-503.(in Chinese)

[7] JUELS A, PAPPU R, PARNO B. Unidirectional key distribution across time and space with applications to RFID security[C]//17th USENIX Security Symposium, San Jose, CA, 2008. California: USENIX Association Berkeley, 2008:75-90.

[8] BONEH D, GENTRY C, LYNN B, et al. Aggregate and verifiably encrypted signatures from bilinear maps. [M]// Advances in Cryptology — EUROCRYPT 2003. Berlin, Heidelberg:Springer, 2003:416-432.

[9] RHEE K, KWAK J, KIM S, et al. Challenge-response based RFID authentication protocol for distributed database environment [C]//Security in Pervasive Computing. Berlin, Heidelberg: Springer, 2005:70-84.

[10] ERGULER I, ANARIM E. Scalability and security conflict for RFID authentication protocols [J]. Wireless Personal Communications, 2011, 59(1):43-56.

[11] JUELS A, RIVEST R L, SZYDLO M. The blocker tag: selective blocking of RFID tags for consumer privacy [C]//Proceedings of the 10th ACM Conference on Computer and Communication Security-CCS '03. October 27-30, 2003. Washington D. C., USA. ACM, 2003:103.

[12] DIMITRIOU T. A lightweight RFID protocol to protect against traceability and cloning attacks[C]//First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05). September 5-9, 2005, Athens, Greece. IEEE, 2006: 59-66.

[13] AVOINE G, OECHSLIN P. A scalable and provably secure hash-based RFID protocol [C]//Third IEEE International Conference on Pervasive Computing and Communications Workshops. March 8-12, 2005, Kauai, HI, USA. IEEE, 2005:110-114.

[14] TSUDIK G. YA-TRAP: yet another trivial RFID authentication protocol [C]//Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06). March 13-17, 2006, Pisa, Italy. IEEE, 2006: 640-643.

[15] MA C S, LI Y J, DENG R H, et al. RFID privacy: relation between two notions, minimal condition, and efficient construction [C]//Proceedings of the 16th ACM Conference on Computer and Communications Security. Chicago Illinois USA. ACM, 2009: 54-65.

[16] MOLNAR D, SOPPERA A, WAGNER D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags [M]//Selected Areas in Cryptography. Berlin, Heidelberg:Springer, 2006:276-290.

[17] CAO T J, CHEN X Q, DOSS R, et al. RFID ownership transfer protocol based on cloud[J]. Computer Networks, 2016, 105: 47-59.

[18] 沈金伟, 赵一, 梁春林, 等. 基于循环分组的RFID群组标签所有权转移协议[J]. 信息网络安全, 2020, 20(9):102-106.
SHEN J W, ZHAO Y, LIANG C L, et al. RFID group tag ownership transfer protocol based on cyclic grouping function[J]. Netinfo Security, 2020, 20(9): 102-106.(in Chinese)

[19] QINGKAUN D, GAO W X, LI L, et al. Lightweight RFID ownership transfer protocol based on blockchain[C]//2021 IEEE Globecom Workshops (GC Wkshps). December 7-11, 2021, Madrid, Spain. IEEE, 2022:1-7.

[20] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[M]//Advances in Cryptology — ASIACRYPT 2001. Berlin, Heidelberg:Springer, 2001:514-532.

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

[22] GOLDREICH O, GOLDWASSER S, MICALI S. How to construct random functions [J]. Journal of the ACM, 1986, 33 (4): 792-807.