软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.000000]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

带用户感知的可审计密码货币*

姜轶涵[1], 李 勇[1,2], 朱 岩[3]

[1](北京交通大学 电子信息工程学院, 北京 100044)

[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](北京科技大学 计算机与通信工程学院, 北京 100083)

通讯作者: 李勇, E-mail: liyong@bjtu.edu.cn

摘 要: 随着区块链的发展,越来越多的的分布式密码货币不断产生,这类货币大多采用密码技术(如: 零知识证明、环签名等)来增强隐私保护,但与此同时监管部门也失去了对交易的审计权.现有的审计方案大多基于中心化系统,不能直接应用于分布式密码货币.本文提出一种用户可感知审计的密码货币(Auditable Cryptocurrency with User Awareness,ACUA)新模型.针对需要保证审计方可以审计密码货币交易,定义了可审计性;同时为防止其滥用职权的问题,提出并定义了新的安全性质: 用户可感知审计性;考虑交易隐私问题,定义了审计信息不可区分性.基于Zerocoin,本文构造了一个用户可感知审计的密码货币方案.新方案通过加密机制实现审计方对交易的审计,引入承诺机制来保证审计方的诚实,利用随机化公钥确保用户可感知到自己是否被审计.最后,通过安全性分析,证明本方案可以同时满足可审计性、用户可感知审计性和审计信息不可区分性.

关键词: 审计;用户感知;Zerocoin;承诺机制;随机化公钥

中图法分类号: TP311

中文引用格式: 姜轶涵,李勇,朱岩.带用户感知的可审计密码货币.软件学报. http://www.jos.org.cn/1000-9825/ 0000.htm

英文引用格式: Jiang YH, Li Y, Zhu Y. Auditable Cryptocurrency with User Awareness. Ruan Jian Xue Bao/Journal of Software, 2018 (in Chinese). http://www.jos.org.cn/1000-9825/0000.htm

Auditable Cryptocurrency with User Awareness

Jiang Yihan[1], Li Yong[1,2], Zhu Yan[3]

[1](School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China)

[2](Guangxi Key Laboratory of Cryptography and Information Security (Guilin University of Electronic Technology), Guilin 541004, China)

[3](School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)

Abstract: With the development of Blockchain, more and more distributed cryptocurrencies continue to emerge. Most of these currencies use cryptographic techniques (such as zero-knowledge proofs , ring signatures, etc.) to enhance privacy protection, but at the same time the regulatory authorities cannot access to audit transactions. Most existing auditing schemes are based on a centralized system and cannot be directly applied to distributed cryptocurrencies. We propose a new Auditable Cryptocurrency with User Awareness (ACUA) model in this paper. Aiming to ensure that auditors can audit cryptocurrency's transactions, *auditability* was defined. Meanwhile, in order to prevent auditors from abusing their power, a new security property: *user awareness auditing* was proposed. And taking transaction privacy issues into consideration, we defines *indistinguishability of audit information*. Based on Zerocoin, an auditable cryptocurrency scheme with user awareness was constructed.The new scheme achieves the transaction auditing from auditors through the encryption scheme, ensures the honesty of the auditor by introducing a commitment mechanism, and ensures that the user can be aware of whether they have been audited or not by randomized public keys. Finally, the

*基金项目: 国家自然科学基金面上项目(61472032); 广西密码学与信息安全重点实验室研究课题(GCIS201609)

Foundation item: National Natural Science Foundation of China (61472032), Guangxi Key Laboratory of Cryptography and Information Security(GCIS201609) 研究课题(GCIS201609)

收稿时间: 0000-00-00; 修改时间: 0000-00-00; 采用时间: 0000-00-00; jos 在线出版时间: 0000-00-00

CNKI 在线出版时间: 0000-00-00

scheme can be proved that it satisfies auditability, user awareness auditing and indistinguishability of audit information simultaneously.

Key words: audit; user awareness; Zerocoin; commitment mechanism; randomized public key

比特币是中本聪在 2009 年提出的分布式密码货币[1],其经过共识将交易信息(发送方、接收方、交易金额)打包公开存储在区块链上,因此可以不需要第三方中介而确认交易.在现代电子支付系统当中,用户必须信任银行不会篡改系统、不会滥用用户的隐私,而比特币采用化名地址给用户提供了隐私保护.由于交易是公开存储的,任何人都可以查看交易路径,并可以向前追溯到该比特币的起源,若交易与真实世界有关,则可能会追踪到用户真实身份.因此,关于密码货币的隐私保护研究应运而生,典型的有 Zerocoin[2]、Zerocash[3]和 Monero[4].Zerocoin 通过非交互式零知识证明(Non-Interactive Zero Knowledge,NIZK)[5]提供了发送方和接收方的不可关联性,Zerocash 运用 ZK-SNARKs[6]提供了当前匿名性程度最高的密码货币隐私保护方案[7],Monero 基于 Crypto Note 协议、环状保密交易 Ring CT 来隐藏交易金额和交易双方地址.

然而,隐私保护程度的加强会带来另一个问题:缺乏和难以审计,可能会让地下钱庄洗钱、敲诈勒索等非法行为更加泛滥.Ken Naganuma 等人提出了可审计的 Zerocoin 方案[8],审计方可关联到交易双方,而其他用户对其关联性依然毫不知情.由于审计方可打开所有信息,该方案需要建立在对审计方保持完全信任的前提下.但实际中需要考虑可能会出现审计方滥用职权超出调查范围审计、获取用户敏感信息等问题.约束审计方权力的方法有多种,比如内部监督等.而让用户对自己的审计情况保持可感知性(如审计方事先预告,用户可在审计期间进行事中查询,或审计方事后告知)以维护自身利益是其中一种解决方案.且用户的可感知性(User Awareness)也是信息安全的重要组成部分,用户需要对自己何时被审计、被何方审计、以及哪些交易被审计保证知情.若由于审计工作导致自身利益受侵害时可以追溯根源,依此可以监督审计方审计行为,促进审计方维护自身信誉和公信力.因此需要研究保证用户对审计可感知的密码货币方案.

就作者所知,目前在分布式密码货币方面对审计可感知性的研究较少.针对如何保证审计方对密码货币审计的同时,防止其滥用审计职权(比如可以确保被审计方的知情权)的问题,本文提出用户可感知审计的密码货币(Auditable Cryptocurrency with User Awareness,简称 ACUA)模型,并基于 Zerocoin 给出了具体构造.

1 相关工作

自比特币提出以来,密码货币越来越受到人们的关注,对密码货币隐私保护的研究也更加深入.Zerocoin[2]是具有隐私保护的去中心化电子现金方案,能够提供交易的不可关联性,主要包括 Mint(铸币)和 spend(花费币)操作.铸币时,将对序列号的承诺值和一个比特币发送到区块链网络上即可将一个 bitcoin 转化成一个 Zerocoin.花费币时,需要提供序列号,然后利用 NIZK 向矿工证明自己的 Zerocoin 存在于系统中且未花费过,序列号的唯一性防止了双花.有了 NIZK 的"Zerocoin 花销"证明,就可以产生一个完全没有历史交易记录的新 Zerocoin.Zerocash[3]使用承诺方案将交易双方地址、金额封装,同时使用 zk-SNARKs 技术来证明交易,证明过程中不会泄露相关信息,因此保障了交易的不可关联以及金额保密.Monero[4]利用隐身地址[9]和环签名[10]来隐藏发送双方地址,利用具有同态性质的 Pedersen 承诺[11]隐藏交易金额.隐身地址是由接收方的公钥和发送方产生的随机数加密后生成的一次性地址,由于随机数只有发送方掌握,观察者无法发现新地址信息和接收方之间的关系.环签名 MLSAG 可模糊交易的输入地址,增加攻击者分析资金来源的难度,签名中引入了密钥映像来提供身份的证明[12].

目前,对审计功能的研究大多针对中心化系统,例如 Kügler[13]提出的币追踪系统可以对任何非法应用的币予以追踪,而对未支付的硬币仍然是无条件匿名的,其还提出了第一个具有审计追踪功能的离线支付系统[14].然而,可审计的去中心化密码货币系统相关研究较少.Ken Naganuma 等人基于 Zerocoin 增加了审计功能[8],该方案允许指定的审计方提取出交易中的关联信息同时防止其他用户获得该信息.币发送者产生交易时会嵌入审计信息与 NIZK,NIZK 可防止恶意用户嵌入非法审计信息.Garman[15]等人提出了去中心化匿名支付的审计功能,修改并扩展了 Zerocash 协议,允许追踪币的交易历史.Neha Narula 等人提出了 zkLedger[16],通过 Schnorr 型 NIZK[17]提供快速、完善的审计,与 zk-SNARKs 不同,该方案不依赖可信的第三方进行参数设置,只依赖 DDH 等密码学假设,且采用多栏

式总分类账结构,以便银行不能向审计方隐藏交易,保证了系统的完备性,是第一个保护账本参与者隐私并提供快速审计的系统.

2 系统模型框架

ACUA 系统由三类实体组成:用户、矿工、审计方.

（1）用户：产生交易(比如 mint 和 spend 交易)发送至区块链网络,等待确认.

（2）矿工：验证用户发来的交易,将交易打包存储在区块链中,维护区块链系统的运行.

（3）审计方：审计区块中用户的交易,打破其不可关联性(因区块链的不可窜改性,本文假设审计功能仅为打破交易的不可关联,不能进行交易撤销、账户冻结等).

下面以三个用户 A、B、C 和一个审计方 Auditor 为例,Auditor 审计区块链上 A 向 B 发出的交易,ACUA 系统框架如图 1 所示：

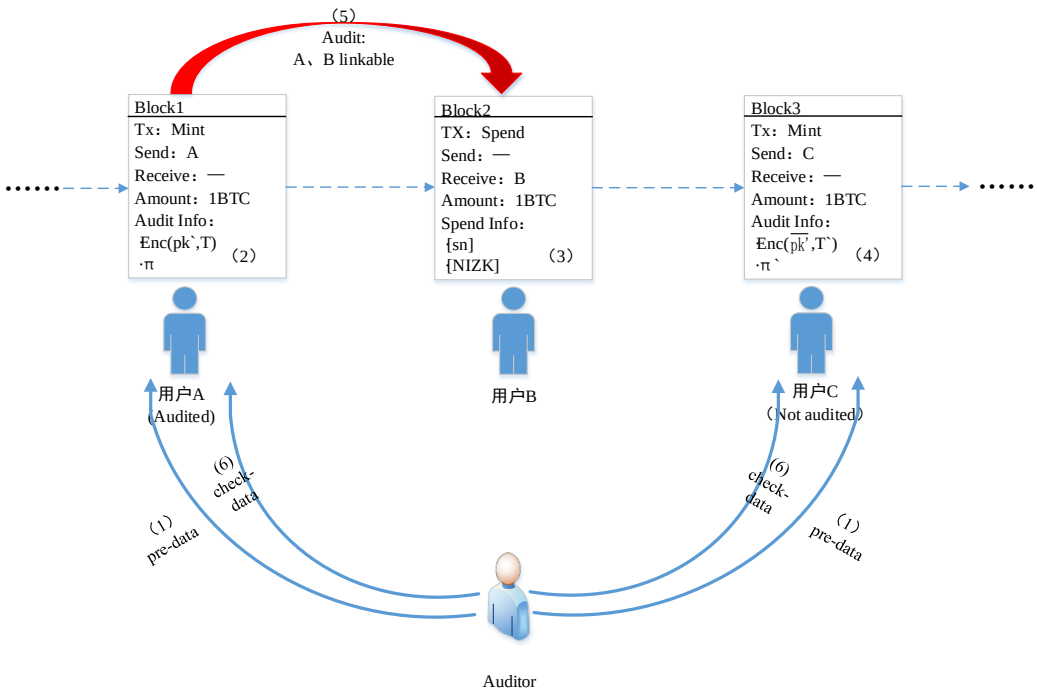

Fig.1 System Frame of ACUA

图 1 ACUA 系统框架

(1) 审计方 Auditor 将 pre-data 发给用户 A、C,pre-data 包含公钥 pk、发送给 A 的随机化公钥 pk'、发送给 C 的伪公钥 $\overline{\text{pk}'}$,以及用于构建随机化公钥的随机数的承诺值 com,保证公钥、审计方、交易用户之间的唯一对应性;

(2) 用户 A 产生包含审计信息的 mint 交易,审计信息包括在审计方所发公钥下加密的币承诺信息 Enc(pk', T)以及零知识证明 π, 随后 A 秘密地将陷门(币的序列号)给 B;

(3) 用户 B 利用序列号产生 spend 交易取出 A 的币;

(4) 用户 C 也产生包含审计信息 $\left(\text{Enc}\left(\overline{\text{pk}'}, \text{T}'\right), \pi'\right)$ 的 mint 交易;

(5) B 的交易被矿工放到区块链之后,审计方用私钥解密 A、C 的审计信息,发现 A 可以关联到 B 交易的序列号,而 C 的审计信息无法解密;

(6) 审计方将 check-data 发送给用户 A 和 C,check-data 为打开(1)中承诺的秘密值以及随机数.

A、C 结合(1)中的 pre-data 和(6)中 check-data 判断审计方是否欺诈。若审计方欺诈,则该用户可广播至区块链网络告知其余用户审计方不诚实;若诚实,用户再继续计算(1)和(6)中收到的数据是否匹配,判断自己是否被审计.图中所示,A 的 pre-data 与 check-data 计算相匹配,则 A 可感知自己被审计,而 C 计算结果不匹配,因此 C 可知自己未被审计.

3 方案和安全模型定义

3.1 ACUA方案定义

ACUA 方案由(Setup, KeyGen, Mint, Mint-Verify, Spend, Spend-Verify, AuditFunc, Comm, Comm-Verify, UserAwareness) 10 个算法组成,定义如下:

(1) $Setup(1^{\lambda}) \to (para, AC)$:参数设置算法,输入安全参数 λ,输出公共参数集合 para 以及可允许的币值集合 AC.

(2) $KeyGen(para) \to (pk, sk, pk', r)$:密钥产生算法,由审计方执行,输入公共参数 para,输出公钥 pk,私钥 sk、随机数 r 以及由 pk 和 r 随机化产生的 pk’.

(3) $Mint(para) \to (Com, Skc, Audit)$:铸币算法,由用户执行,输入公共参数 para,输出币承诺 Com∈AC,陷门 Skc,审计信息 Audit,则可审计的铸币交易为 mint=(Com,Skc,Audit).

(4) $Mint\text{-}Verify(para, Com, Audit) \to \{0,1\}$:铸币验证算法,由矿工执行,输入公共参数 para,可审计的币承诺 Com,审计信息 Audit,如果验证为有效则输出 1,否则输出 0.

(5) $Spend(para, Com, Skc, subAC) \to (sn, w)$:花费算法,由用户执行,输入公共参数 para,可审计的币承诺 Com,陷门 Skc,AC 的任意子集 subAC（包含 Com）,输出序列号 sn 和零知识证明 w.

(6) $Spend\text{-}Verify(para, subAC, sn, w) \to \{0,1\}$:花费验证算法,由矿工执行,输入公共参数 para,子集 subAC,序列号 sn,证明 w,若验证为有效则输出 1,否则输出 0.

(7) $AuditFunc(para, sk, sn, Audit) \to \{0,1\}$:审计功能算法,由审计方执行,输入公共参数 para,私钥 sk,序列号 sn,审计信息 Audit,若存在 (Com,Skc,subAC) 使得 Mint 算法输出为 (Com,Skc,Audit) 且 sn 是 $Spend(para, Com, Skc, subAC)$ 的输出,则输出 1,否则输出 0.

(8) $Comm(para, trap) \to com$:承诺算法,由审计方执行,输入公共参数 para,承诺陷门 trap,输出承诺值 com.

(9) $Comm\text{-}Verify(para, trap, com) \to \{0,1\}$:承诺验证算法由用户执行,输入公共参数 para,承诺的陷门 trap,若承诺匹配则输出 1,否则输出 0.1 代表审计方诚实,没有欺骗用户,0 代表审计方欺诈.

(10) $UserAwareness(trap, pk', pk) \to \{0,1\}$:用户感知算法,由用户输入承诺的陷门 trap,审计方随机公钥 pk’,审计方公钥 pk,输出判断结果 1 或 0,1 代表用户感知到自己被审计,0 代表用户感知到未被审计.

3.2 安全模型定义

定义 1. 可审计性.对于所有上述算法使用的币,如果满足以下条件,则该方案具有审计性:

$$\Pr\left[\begin{array}{c} Setup(1^{\lambda}) \to (para,\ AC) \\ KeyGen(para) \to (pk, sk,\ pk') \\ Mint(para) \to (Com,\ Skc,\ Audit) \\ Spend(para,\ Com,\ Skc,\ subAC) \to (sn, w) \end{array} : AuditFunc(para,\ sk,\ sn,\ Audit) = 1\right] \geq 1 - v(\lambda)\left(v(\lambda)\text{为可忽略函数}\right)$$

即对于收到随机化公钥 pk'的用户产生的交易,审计方能够根据审计信息关联到交易双方的概率接近 1.

定义 2. 用户可感知审计性.对于所有上述算法使用的币,如果满足以下条件,则该方案具有用户可感知审计性:

$$\Pr\left[\begin{array}{c} Setup(1^{\lambda}) \to (para,\ AC) \\ KeyGen(para) \to (pk, sk,\ pk') \\ Comm(para, trap) \to com \\ AuditFunc(para, sk, sn, Audit) = 1 \\ Comm\text{-}Verify(para, trap, com) = 1 \end{array} : UserAwareness(trap,\ pk',\ pk) = 1\right] \geq 1 - v(\lambda)\left(v(\lambda)\text{为可忽略函数}\right)$$

或

$$\Pr\left[\begin{array}{c} Setup(1^{\lambda}) \to (para,\ AC) \\ KeyGen(para) \to (pk, sk,\ pk') \\ Comm(para, trap) \to com \\ AuditFunc(para, sk, sn, Audit) = 0 \\ Comm\text{-}Verify(para, trap, com) = 1 \end{array} : UserAwareness(trap,\ pk',\ pk) = 0\right] \geq 1 - v(\lambda)\left(v(\lambda)\text{为可忽略函数}\right)$$

即只要审计方审计了用户,则用户可感知到自己被审计的概率接近 1,未被审计的用户感知到自己没有被审计的概率同样接近 1.

定义 3. 审计信息不可区分性.对于任意多项式时间敌手 A=(A_0,A_1),如果 A 在如下实验中成功的优势是可忽略的,即 A 得到交易关联性的信息的优势可忽略,则 ACUA 方案具有审计信息不可区分性.

$Expt_{\Pi,A(\cdot)}^{Audit\text{-}Ind}$:

b←{0，1}

(para)←$Setup(1^{\lambda})$

(pk，pk')←*KeyGen(para)*

(m_0，m_1，*h*)←A_0(para，pk')

Audit←(*Enc*(pk'，m_b)，π_b)

b'←A_1(*Audit*，*h*)

return (*b'*=*b*)

上述实验中Π为 ACUA 方案,A 的优势为:

$$Adv_{A,\Pi}^{Audit\text{-}Ind} = \left|\Pr[Expt_{\Pi,A(\cdot)}^{Audit\text{-}Ind}(1^{\lambda}) = 1] - 1/2\right| = \left|\Pr[b' = b] - 1/2\right|$$

.

即只有审计方可审计交易,对于其他用户或矿工,交易仍不可关联.

4 方案设计

本节首先给出方案概述,然后给出各个算法的具体实现过程.

4.1 方案概述

本文借鉴了 Markulf Kohlweiss[18]中的 EIKO 方法产生随机化公钥.审计方将 pre-data(公钥 pk、随机化公钥 pk'(或随机选取的伪公钥 $\overline{\text{pk'}}$)、对随机数 r 的承诺 com)发给用户,发送方产生 mint 交易时要附带审计信息,接收方利用序列号产生的 spend 交易被矿工放到区块链之后,审计方用私钥解密审计信息,根据序列号关联到收发双方.一段时间之后,审计方将 check-data(随机数 r 和盲化因子 x)揭露给用户,用户计算承诺值判断与 com 是否匹配,若不匹配则审计方欺诈,用户可广播告知其余用户、矿工;若匹配,再计算 pk^r 是否等于 pk'判断自己是否被审计.

4.2 ACUA方案的具体构建

本方案由十个算法构成,算法如下:

① $Setup(1^{\lambda}) \to ((q,g,h),G)$:参数生成算法,输入安全参数 λ,产生阶数 q,随机生成元 g,h,使得 G=<g>=<h>,输出 para=(q,g,h),可允许的币值集合 AC=G.

② $KeyGen(para) \to (pk,sk,pk',r)$:密钥产生算法,由审计方执行,取 t,γ←Zq,令私钥为 γ,计算 $A=g^t \bmod q$,$B=(g^{\gamma})^t \bmod q$,输出公钥为 pk=(A,B).取 r←Zq,输出随机化公钥 pk' =(A', B')=($A^r \bmod q$,$B^r \bmod q$).

③ $Comm(para,r,x) \to com$:承诺算法,由审计方执行,输入公共参数 para, 产生 pk'的随机数 r, 取盲化因子 x←Zq,输出 $com=g^rh^x$.

④ $Mint(para) \to (g^{sn}h^z,(sn,z),Enc(pk',g^{sn}),\pi)$:铸币算法,由用户执行,输入公共参数 para,取 sn,z←Zq,计算 Pedersen 承诺 $g^{sn}h^z$.在审计方所发公钥下进行加密,取 s←Zq,计算 C=(A')^s mod q,D=(B')^s • g^{sn} mod q,Enc(pk',g^{sn})→(C,D).计算 NIZK-π,π 证明以下知识:

π= NIZK{Enc(pk',g^{sn})是由正确的步骤产生}

= NIZK{Enc(pk',g^{sn})由审计方所发公钥加密产生∧明文为 g^{sn}}

最终,输出 Com = $g^{sn}h^z$,陷门 Skc = (sn,z),Audit =(Enc(pk',g^{sn}),π).

⑤ $Mint\text{-}Verify(para,Com,Audit) \to \{0,1\}$:铸币验证算法,由矿工执行,若验证 NIZK 有效则输出 1,否则输出 0.

⑥ $Spend(para,g^{sn}h^z,(sn,z),subAC) \to (sn,w)$:花销算法,由用户执行,输入 para,com=$g^rh^x$,Skc =(sn,z),subAC,输出序列号 sn 和证明 w,w 包含以下知识:w= NIZK{Com∈subAC∧Com = $g^{sn}h^z$ }.

⑦ $Spend\text{-}Verify(para,subAC,sn,w) \to \{0,1\}$:花销验证算法,由矿工执行,若验证 NIZK 有效,且 sn 未出现在区块链上,输出 1,否则输出 0.

⑧ $AuditFunc(para,sk,sn,Enc(pk',g^{sn}),\pi) \to \{0,1\}$:审计功能算法,由审计方执行:输入 para,审计方私钥 sk=γ,spend 交易的序列号 sn,mint 交易的审计信息 $Enc(pk',g^{sn}),\pi) = (C,D,\pi)$,利用 EIKO.Dec(sk,(C,D))提取出明文 $g^{sn'} = D/C^{\gamma}$,若 $g^{sn'} = g^{sn}$,则输出 1,否则输出 0.

⑨ $Comm\text{-}Verify(para,(r,x),com) \to \{0,1\}$:承诺验证算法,由用户执行,输入 para,计算 g^rh^x,若 com=g^rh^x,输出 1,否则输出 0.

⑩ $UserAwareness(para, r, pk', pk) \to \{0,1\}$:用户感知算法,由用户执行,输入 pk=(A,B),pk'=(A',B'),若(A^r mod q,B^r mod q)=(A',B'),则输出 1,否则输出 0.

5 安全性分析

定理 1 在用户和审计方都是诚实的前提下,对于收到随机化公钥 pk'的用户产生的交易,审计方能够关联到交易双方,即具有可审计性.

证明:对于审计信息(C, D)=Enc(pk', g^{sn})=((A')^s mod q, (B')^s • g^{sn} mod q),解密正确性如下:

$$EIKO.Dec(sk,(C,D)) = \frac{D}{C^{\gamma}} = \frac{(B')^{s} \cdot g^{sn}}{(A')^{s\cdot\gamma}}$$

$$= \frac{(B^{r})^{s} \cdot g^{sn}}{(A^{r})^{s\cdot\gamma}} = \frac{(g^{\gamma t})^{r\cdot s} \cdot g^{sn}}{(g^{t})^{r\cdot s\cdot\gamma}} = g^{sn}$$

因此输入由 pk'加密的审计信息,AuditFunc 算法的输出为 1,审计方具有审计性,即可关联交易双方.

定理 2 如果承诺方案具有绑定性,则 ACUA 方案满足用户可感知审计性.

证明:假设存在不诚实的审计方审计用户之后,对用户欺骗其审计情况,即发送和随机化公钥不匹配的随机数而通过承诺验证的概率不可忽略,则存在 $r_0 \neq r_1$,使得

$$\Pr\left[\begin{matrix} Comm(para, r_0, x_0) = com \\ Comm(para, r_1, x_1) = com \end{matrix} : Comm\text{-}Verify(para, r_i, x_i, com) = 1, i \in \{0,1\}\right] \geq 1 - v(\lambda)$$

与承诺方案绑定性相矛盾,所以若审计方执行 AuditFunc 输出为 1,且 Comm-Verify 算法输出为 1,则 UserAwareness 算法的输入 r 满足(A^r mod q,B^r mod q)=(A',B')=pk',即 UserAwareness 输出为 1;若审计方执行 AuditFunc 输出为 0,且 Comm-Verify 算法输出为 1,则 UserAwareness 输出为 0.因此 ACUA 方案满足用户可感知审计性.

定理 3 如果 DDH 问题是困难的,且零知识证明是计算零知识的,则 ACUA 方案满足审计信息不可区分性.

证明:利用一系列游戏来证明本定理.

G1:第一个游戏是原始的 $Expt_{\prod,A(\cdot)}^{Audit-Ind}$.

G2:第二个游戏与 G1 类似,不同之处是零知识证明 π 是由模拟器 S 模拟的,S 调用 Sim(1^{λ})获得陷门 trap.在每次调用 Mint(para)算法时,S 计算 π←Sim（trap）而不使用任何证据,由于零知识证明至少是计算零知识的,模拟的 π 的分布和 G1 中计算的 π 是一样的,因此 $Adv_{A,\prod}^{G2} = 0$.

G3:第三个游戏与 G2 类似,不同之处是在审计信息中用随机串的加密代替密文.更精确地说,密文 C=Enc(pk',rand),rand 是加密方案中从明文空间中均匀采样的消息.通过引理 3.1 可知,$\left|Adv_{A,\prod}^{G3} - Adv_{A,\prod}^{G2}\right| \leq q_m \cdot Adv_{A,\prod}^{enc}$,通过引理 3.2 可知,$Adv_{A,\prod}^{enc} \leq v(\lambda)$.

引理 3.1 令 $Adv_{A,\prod}^{enc}$ 为在 IND-CPA 实验中 A 的优势,则 $\left|Adv_{A,\prod}^{G3} - Adv_{A,\prod}^{G2}\right| \leq q_m \cdot Adv_{A,\prod}^{enc}$.

证明:令 $\varepsilon = Adv_{A,\prod}^{G3} - Adv_{A,\prod}^{G2}$,首先,构造一个在 IND-CPA 实验中优势≥ ε /q_m 的运算器 A,q_m 为 A 询问挑战

者 C 密文的总次数.每次,A 询问 IND-CPA 挑战者获得两个明文(m_0,m_1),在响应阶段返回给 A 消息 m=m_0,然后 A 向 C 询问 m 的密文,收到 C*=Enc(pk', m_b),b 是 C 选取的 bit.A 输出 b'作为 IND-CPA 实验返回的结果.注意到当 b=0 时,A 的视图和 G2 的分布一样,b=1 时,A 的视图与 G3 分布一样,在经过 n 次询问之后,运算器 A 在 IND-CPA 实验中成功的优势$\geqslant \varepsilon / q_m$.假设 A 在 IND-CPA 实验中最大的优势为 $Adv_{A,\prod}^{enc}$,则有 $\left|Adv_{A,\prod}^{G3} - Adv_{A,\prod}^{G2}\right| \leq q_m \cdot Adv_{A,\prod}^{enc}$.

引理 3.2 令 $Adv_{A,\prod}^{enc}$ 为在 IND-CPA 实验中 A 的优势,如果 DDH 问题是困难的,则 $Adv_{A,\prod}^{enc} \leq v(\lambda)$.

证明:构建一个区分器 D:

Distinguisher D (para，X，Y，T)：
X = g^r, Y = g^γ, T = $g^{\gamma r}$
b←{0,1}
t←Zq
pk←(g^t, Y^t)
pk'←(X^t, T^t)
(m_0, m_1, h)←A_0(para, pk')
s←Zq
ct←((X^t)^s, (T^t)^s m_b)
b'←A_1(ct)
return(b=b')

上述(X,Y,T)是一个 DDH 元组,A 优势为 $Adv_{A,\prod}^{D} = |\Pr[b = b'] - 1/2|$,A 的视图与 IND-CPA 实验一样,收到 g^t,$g^{\gamma t}$,(((g^t)^s)^r,((g^t)^s)$^{\gamma r}$ m),而当 T 是随机群元素时,(T^t)^s m_b 揭露不了 m_b 的任何信息,b 完全独立于敌手 A 的视图,因此

$$\Pr[b = b' | (X,Y,T) \notin DDH] = 1/2$$

$$\begin{aligned} Adv_{A,\prod}^{enc} &= \{\Pr[b = b' | (X,Y,T) \in DDH] - 1/2)\} \\ &\quad + \{\Pr[b = b' | (X,Y,T) \notin DDH] - 1/2\} \\ &= \Pr[b = b' | (X,Y,T) \in DDH] - 1/2 \\ &= Adv_{A,\prod}^{D} \end{aligned}$$

假设存在多项式时间敌手 A 以不可忽略的优势 $Adv_{A,\prod}^{enc}$ 赢得 IND-CPA 实验,A 会以同样不可忽略的优势 $Adv_{A,\prod}^{D}$ 打破 DDH 的困难性,与 DDH 假设矛盾,因此 $Adv_{A,\prod}^{enc} \leq v(\lambda)$.

综上,

$$\begin{aligned} Adv_{\prod,A}^{Audit-Ind}(\lambda) &= \left|Adv_{A,\prod}^{G3} - Adv_{A,\prod}^{G2}\right| \\ &\leq q_m \cdot Adv_{A,\prod}^{enc} \leq v(\lambda) \end{aligned},$$

因此如果 DDH 问题是困难的,且零知识证明是计算零知识的,则 ACUA 方案满足审计信息不可区分性.

6 总结

目前对于区块链的研究大多旨在增强隐私保护,缺乏和难以审计.而在区块链环境下,传统的审计方案不能直接应用.本文提出具有用户感知性质的可审计密码货币模型 ACUA,并定义了新的安全性质:用户可感知审计性和审计信息不可区分性.基于 Zerocoin 方案,本文构造出一个带用户感知的可审计密码货币方案,在保证审计方对密码货币审计之后,用户可感知自己是否被审计,同时证明了方案的正确性和安全性.与[8]相比,本方案优势为用户可以感知到自己是否被审计,从而可约束监督审计方,在一定程度上防止其滥用职权,保障了用户权益.但由于审计方需要在开始时发送给所有节点 pre-data,结束时再发送 check-data,增加了方案的通信开销.如何优化算法,减少通信开销是下一步研究改进的方向.

References:

[1] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. 2008 [2018-05-01]. http://bitcoin.org/bitcoin.pdf

[2] Miers I, Garman C, Green M, et al. Zerocoin: Anonymous Distributed E-Cash from Bitcoin[C]// IEEE Symposium on Security and Privacy. IEEE Computer Society, 2013:397-411.

[3] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin[C]// IEEE Symposium on Security and Privacy. IEEE Computer Society,2014:459-474.

[4] Shen N, Mackenzie A, Lab T M. Ring Confidential Transactions[J]. Ledger, 2016:1-18.

[5] Camenisch J, Michels M. Proving in zero-knowledge that a number is the product of two safe primes[J]. Theory and Application of Cryptographic Techniques, 1999: 107-122.

[6] Bitansky N, Chiesa A, Ishai Y, et al. Succinct non-interactive arguments via linear interactive proofs[C]// Theory of Cryptography Springer, Berlin, Heidelberg, 2013: 315-333.

[7] Zhu Liehuang, Gao Feng, Shen Meng, et al. Survey on Privacy Preserving Techniques for Blockchain Technology[J]. Journal of Computer Research and Development, 2017, 54(10):2170-2186 (in Chinese).

[8] Naganuma K, Yoshino M, Sato H, et al. Auditable Zerocoin[C]// IEEE European Symposium on Security and Privacy Workshops. IEEE, 2017.

[9] Saberhagen, N, V. CryptoNote v 2.0[EB/OL]. 2013 [2017-12-22] https://cryptonote.org/whitepaper.pdf

[10] Liu J K, Wei V K, Wong D S. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups[C]// Australasian Conference on Information Security and Privacy (ACISP). Springer, Berlin, Heidelberg, 2004:325-335.

[11] Pedersen T P. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing[C]// International Cryptology Conference on Advances in Cryptology. Springer-Verlag, 1991:129-140.

[12] Zhang Xian, Jiang Yuzhao, Yan Ying. A Glimpse at Blockchain: From the Perspective of Privacy[J]. Journal of Information Security Research, 2017, 3(11): 981-989 (in Chinese).

[13] Kügler D, Vogt H. Auditable tracing with unconditional anonymity[EB/OL]. 2001 [2018-05-01]. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.21.6424.

[14] Kügler D, Vogt H. Offline payments with auditable tracing[C]// International Conference on Financial Cryptography. Springer-Verlag, 2002:269-281.

[15] Garman C, Green M, Miers I. Accountable Privacy for Decentralized Anonymous Payments[C]// International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016:81-98.

[16] Narula, N, Vasquez, W, Virza, M. zkLedger: Privacy-Preserving Auditing for Distributed Ledgers[EB/OL]. 2018 [2018-05-01] https://eprint.iacr.org/2018/241.

[17] Schnorr C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3):161-174.

[18] Kohlweiss M, Miers I. Accountable Tracing Signatures[EB/OL]. 2014 [2018-05-01], https://eprint.iacr.org/2014/824

附中文参考文献:

[7] 祝烈煌, 高峰, 沈蒙,等. 区块链隐私保护研究综述[J]. 计算机研究与发展, 2017, 54(10):2170-2186.

[12] 张宪, 蒋钰钊, 闫莺. 区块链隐私技术综述[J]. 信息安全研究, 2017, 3(11): 981-989.