doi:10.14132/j.cnki.1673-5439.2022.05.013

# 联盟链中基于 CL 加密的安全审计协议

王 诚[1],王志伟[1,2,3]

(1.南京邮电大学 计算机学院,江苏 南京 210023
2.江苏省大数据安全与智能处理重点实验室,江苏 南京 210023
3.江苏省计算机网络技术重点实验室,江苏 南京 210096)

**摘要**:联盟链作为一个只针对特定群体和有限第三方的分布式账本,适合利益相关的金融部门之间的交互。审计作为一种经济监督活动,可以对交易的合规性和有效性进行检查。目前联盟链审计中私钥由审计者选取,因此审计者必须绝对可信,否则半可信的审计者可以随时随地恢复交易的私密信息。文中提出一种基于 CL 加密的安全审计协议,通过零知识证明,使半可信的审计者完成对交易审计的同时,不泄漏交易的细节,保证了用户交易隐私。

**关键词**:联盟链;隐私保护;安全审计;零知识证明
**中图分类号**:TP309 **文献标志码**:A **文章编号**:1673-5439(2022)05-0101-08

# A security audit protocol based on CL encryption in the consortium blockchain

WANG Cheng[1], WANG Zhiwei[1,2,3]

(1.School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
2.Jiangsu Key Laboratory of Big Data Security and Intelligent Processing, Nanjing 210023, China
3.Jiangsu Key Laboratory of Computer Networking Technology, Nanjing 210096, China)

**Abstract**: As a distributed ledger only for specific groups and limited third parties, the consortium blockchain is suitable for the interaction between financial sectors. As an economic supervision activity, audit can check the compliance and effectiveness of transactions. At present, the private key in the current audit of the consortium blockchain is selected by the auditor, so the auditor must be absolutely trusted, otherwise the semi trusted auditor can recover the private information of the transaction anytime and anywhere. This paper proposes a security audit protocol based on CL encryption. Through zero-knowledge proof, the semi trusted auditor can complete the audit of the transaction without disclosing the details of the transaction. This protocol can ensure the transaction privacy of users.

**Keywords**: consortium blockchain; privacy protection; security audit; zero-knowledge proof

联盟链[1]具有可控性强、半去中心化、高效率(每秒超过 1 万笔交易)、数据隐私性好等优点,相较于传统公有链的全网公开特性,其只针对特定群体和有限第三方,更加适用于利益相关组织之间的交互,如金融部门,通常需要将资金从一方转移到另一方,其交易隐私问题尤为重要,区块链主要通过加密算法、零知识证明等技术来实现隐私保护。审计是一种经济监督活动,指授权监管机构或审计人员,依照国家法规和审计准则,查明被审组织相关经济活动的合规性及有效性。可审计性对于金融区块链应用程序至关重要,金融机构必须根据政府的规定进行内部和外部审计,以检查是否存在洗钱或与恐

**收稿日期**:2021-11-02;**修回日期**:2022-02-21 **本刊网址**:http://nyzr.njupt.edu.cn
**基金项目**:江苏省六大人才高峰项目(RJFW-010)资助项目
**作者简介**:王诚,男,硕士研究生;王志伟(通信作者),男,博士, 教授,zhwwang@njupt.edu.cn
**引用本文**:王诚,王志伟.联盟链中基于 CL 加密的安全审计协议[J].南京邮电大学学报(自然科学版),2022,42(5):101-108.

怖主义相关的活动,简单起见,将合法进行审计的一方统称为审计者。

区块链交易是基于 UTXO[2] (Unspent Transaction Outputs)交易模型的,UTXO 指未花费交易输出,交易构成了一组链式结构,所有合法的比特币交易都可以追溯到前一个或多个交易的输出,源头都是挖矿奖励,末尾则是未花费交易输出,未花费交易输出可以作为下一笔交易的输入。区块链中的交易规定,任何一笔交易的输入总量必须等于交易输出总量,并且输入输出都在有效范围内,通过对每一笔交易进行签名,使得交易的验证者可以验证同一个事务中是否存在一笔资产被花费了两次,即防止双花攻击或重放攻击[3],Yuen[4-5]提出了一种基于零知识证明、加性同态加密、匿名证书的交易隐私保护协议,被证明在联盟链中具有良好的安全性和效率。半可信模型(the Semi-Trusted Model)是指协议中存在半可信的参与者,其遵循协议的执行,但同时会保存协议的中间状态,即诚实并好奇(Honest but Curious)。Yuen 的方案中,由于审计密钥由审计者选取,要求审计者绝对可信,但在现实中,绝对可信的审计者是不存在的。半可信的审计者可能在审计过程中保存用户的交易信息,进而通过大数据推测等方法知晓用户的真实身份或其他敏感信息[6]。

使用同态加密方案可以避免审计者了解细粒度的交易隐私。同态加密技术始于第一个概率加密方案,由 Goldwasser 和 Micali 提出[7],并由其他密码学者做出改进,其中最成功的同态加密系统是由 Paillier[8]设计的,它的语义安全性依赖于 DCR (Decisional Composite Residuosity Assumption)假设。Paillier 的方案随后被 Damgård 和 Jurik[9]推广,允许加密更大的消息,随着时间推进,这一线性同态加密技术的家族仍在增长,这些方案的安全性都是基于 RSA 的大整数分解困难问题。设计一个基于离散对数问题(DL)的通用解决方案是使用 Elgamal 算法对消息进行加密,即将消息 $m$ 加密为密文 $(g^r, h^r g^m)$ 的形式,其中 $g$ 为循环群 $G = \langle g \rangle$ 的生成元,$h = g^x$ 为公钥,然而,解密必须要从 $g^m$ 中恢复 $m$,由于 $G$ 中 DL 问题是困难的,$m$ 必须足够小以确保能够快速解密,或者提前计算一张包含 $g^i$ 的预计算表,但在不确定 $i$ 范围的情况下是不可行的。基于 DL 问题,有两种尝试以达到完全同态加密,Elgamal 模 $p^2$ [10]或将消息编码为小光滑数[11],但两种方案仍存在部分同态。Bresson 等[12]提出了一个完整的解决方案,但他们的方案不仅基于 DL 问题,还基于分解问题。Castagnos 和 Laguillaumie[13]提出了一种基于 DDH 问题的线性同态加密方案,并在随后进行了扩展,提供了一个通用加密方案[14],该方案的安全性不依赖于整数分解的困难性,并在特定的群内提供了实现,该方案由 Yuen 等[15]进行了改进并推广。

本文的贡献如下:(1) 基于 CL 加密方案[13]和 Yuen 等[15]提出的零知识证明协议,提出了一种基于 CL 加密的安全审计协议;(2) 将所提出的安全审计协议应用于联盟链中的实际审计场景,通过零知识证明子协议对金额的有效性和合规性进行了审计;(3) 对所提出的安全审计协议的安全性和性能进行了分析。

## 1 预备知识

### 1.1 交互式零知识证明

零知识证明是指证明者 $P$ 能够在不向验证者提供任何有用信息的情况下,使验证者 $V$ 相信某个论断是正确的,区块链中,零知识证明被用来隐藏发送方、接收方以及交易金额等其他细节的情况下保证交易有效。

交互式零知识证明系统主要分为如下 4 个阶段:

(1) 承诺阶段。证明者提前提供承诺等待验证者发起挑战。

(2) 挑战阶段。验证者发起挑战,向证明者发送随机值。

(3) 回应阶段。证明者根据挑战中的随机值回应挑战,如果证明者确实能够证明命题的正确性,他能够通过每轮挑战,否则只能以一定概率通过。

(4) 验证阶段。验证者通过进行多轮挑战,直到认为证明者证明正确的概率足够大,则接受。

一个零知识证明系统由 3 个多项式时间算法 Setup,$P$,$V$ 组成。

Setup:输入一个安全参数 $\lambda$,输出一个通用的引用字符串 crs。

$P$:输入 crs,一个命题 $x \in X$ 和证据 $\omega \in W$。

$V$:输入 crs 和 $x$,与 P 交互后输出 0 或 1。

一个正确论点的零知识证明系统应该满足两个属性:

(1) 可靠性:不诚实的证明者难以用一个错误的命题欺骗验证者,分为计算正确性和完美正确性,满足计算正确性的零知识证明方案能够防止多项式时间的恶意证明者,而满足完美正确性的零知识证

明方案能够防止拥有任意计算资源的恶意证明者。

**定义 1**　可靠性。存在一个多项式时间的提取器 $\varepsilon$ 可以以一个不可忽略的概率输出一个命题的证据,如果对于任意两个多项式时间的敌手 $(A_0,A_1)$,满足如下两个条件,则是可靠的。

$$\Pr\left[\begin{array}{l}\langle V(\mathrm{crs},x),A_1(\mathrm{crs},x,\mathrm{state})\rangle = 1\\ \exists\omega \text{ s.t. } (x,\omega)\in R\\ (x,\mathrm{state})\leftarrow A_0(\mathrm{crs})\end{array}\middle|\,\mathrm{crs},\right] = \mathrm{negl}(\lambda)$$

$$\Pr\left[\begin{array}{l}\langle V(\mathrm{crs},x),A_1(\mathrm{crs},x,\mathrm{state})\rangle = 1\\ (x,\omega')\notin R\\ (x,\mathrm{state})\leftarrow A_0(\mathrm{crs})\\ \omega'\leftarrow\varepsilon(\mathrm{crs},x,\mathrm{state})\end{array}\middle|\,\mathrm{crs},\right] = \mathrm{negl}(\lambda)$$

(2) 零知识性:验证者无法获取除命题外的任何信息。

**定义 2**　零知识性。存在一个多项式时间的模拟器 $S$,在不知道证据的情况下输出一个模拟的文本,该文本与真实文本在计算上是不可区分的。即对于所有 $(x,\omega)\in R$ 和 $\mathrm{crs}\leftarrow\mathrm{Setup}(1^\lambda)$,$\langle V(\mathrm{crs},x),P(\mathrm{crs},x,\omega)\rangle$ 与 $\langle V(\mathrm{crs},x),S(\mathrm{crs},x)\rangle$ 在计算上是不可区分的。

### 1.2　同态加密

同态加密是基于数学难题的计算复杂性理论的密码学技术。对经过同态加密的数据进行处理得到一个输出,将这一输出解密,其结果与用同一方法处理未加密的原始数据得到输出结果是一致的。区别于典型加密算法,同态加密提供了无需密钥直接计算加密数据的能力,计算结果保留加密形式,可由密钥持有者解密。同态加密是指存在一种有效算法"$\oplus$",满足:$\mathrm{Enc}(m_1)\oplus\mathrm{Enc}(m_2)\oplus\cdots\oplus\mathrm{Enc}(m_k)=\mathrm{Enc}(m_1+m_2+\cdots+m_k)$,或者指数化的密文也是消息的一个有效加密,即 $\mathrm{Enc}(m)^\alpha$ 是消息 $\alpha m$ 的一个有效加密。

### 1.3　决策 Diffie-Hellman(DDH)假设

Diffie-Hellman 密钥协商算法主要用来解决密钥配送问题,让通信双方交换彼此信息来共同计算出相同的密钥,具体步骤是 Alice 和 Bob 分别随机选择 $a,b\in Z_q$,计算 $g^a$ 和 $g^b$ 发送给对方,然后双方根据对方发送的信息,生成密钥 $g^{ab}=g^{ba}\bmod q$,即使敌手截获了传递的信息,基于离散对数问题(DL)的困难性,恢复出双方的私钥在计算上是困难的。

决策 Diffie-Hellman 假设是基于循环群的。设 $G$ 是一个 $q$ 阶循环群,生成元为 $g$,记作 $G=\langle g\rangle$。独立均匀地选择 $a,b\in Z_q$,得到 $g^a$ 和 $g^b$,敌手区分 $(g^a,g^b,g^{ab})$ 和 $(g^a,g^b,g^c)$ 在多项式时间内是困难的,即敌手无法从 $G$、$g^a$ 和 $g^b$ 中得到关于 $g^{ab}$ 的任何信息。

### 1.4　HSM-CL 加密

#### 1.4.1　HSM 群

困难子群成员(HSM)群是 Castagnos 和 Laguillaumie 等[14]在所提出的具有简单 DL 子群的 DDH 群的基础上,使用虚二次域中的类群进行实例化[16-17],从而以 $Z/Z_q$ 作为消息空间,证明不需要依赖于分解问题。随后 Yuen 等[15]在此基础上,稍作了修改,其定义如下:

以一个安全参数 $1^\lambda$ 和一个素数 $q$ 作为输入,HSM 群生成算法 Gen 输出 $\mathrm{param}=(\tilde{s},g,f,g_q,\hat{G},G,F,G^q)$,其中 $(\hat{G},\cdot)$ 为阶为 $q\cdot\hat{s}$ 的有限阿贝尔群,$\hat{s}$ 是长度为 $\lambda$ 比特的整数,并且 $\gcd(q,\hat{s})=1$。$\tilde{s}$ 表示 $\hat{s}$ 值的上界,可以有效地判定一个元素在多项式时间内是否在 $\hat{G}$ 中。$(F,\cdot)$ 是 $\hat{G}$ 的阶为 $q$ 的唯一循环子群,$(G,\cdot)$ 是 $\hat{G}$ 的阶为 $q\cdot s$ 的唯一循环子群,其中 $s$ 整除 $\hat{s}$。$G^q:=\{x^q,x\in G\}$ 是 $G$ 的阶为 $s$ 的子群。

由 $F\subset G$ 可得 $G=F\times G^q$,$g$、$f$、$g_q$ 分别为 $G$、$F$、$G^q$ 的生成元,因此 $g:=f\cdot g_q$。Solve 算法输入 $f^x$,$x\xleftarrow{\$}Z/Z_q$,输出 $x$。DL(离散对数)问题在 $F$ 中是简单的,说明算法 Solve 是一种确定性多项式时间算法。

$$\Pr[x:(\tilde{s},g,f,g_q,\tilde{G},G,F,G^q)\leftarrow\mathrm{Gen}(1^\lambda,q),\ x\xleftarrow{\$}Z/Z_q,x\leftarrow\mathrm{Solve}(f^x)]=1$$

相较于 Castagnos 和 Laguillaumie 等[14]的方案,在 Yuen 等[15]的定义中,$q$ 是算法输入的而非 Gen 算法生成的,并且输出 $\hat{G}$,从中生成具有简单 DL 子群 $F$ 的群 $G$。

**定义 3**　困难子群成员假设。定义 $D$ 是整数分布,这样分布 $\{g^x,x\xleftarrow{\$}D\}$ 与 $G$ 中的均匀分布距离小于 $2^\lambda$。困难子群成员假设指很难区分 $G$ 群中属于 $G^q$ 的元素,即对于多项式时间的敌手 $A$,有

$$\left|\Pr\left[b=b*\left|\begin{array}{l}G_{\mathrm{HSM}}=(\tilde{s},g,f,g_q,\hat{G},G,\\ \quad F,G^q)\leftarrow\mathrm{Gen}_{\mathrm{HSM}}(1^\lambda,q),\\ \quad x\leftarrow D,x'\in D_q,\\ b\leftarrow\{0,1\},Z_0=g^x,\\ \quad Z_1=g_q^{x'},\\ b*\leftarrow A(G_{\mathrm{HSM}},Z_b,\mathrm{Solve}(\cdot))\end{array}\right.\right]-\frac{1}{2}\right|\leqslant$$

$$\mathrm{negl}(\lambda)$$

$\mathrm{negl}(\lambda)$ 表示可以忽略不计的值。

1.4.2 CL 加密

系统参数生成: $\mathrm{param}=(\tilde{s},g,f,g_q,\hat{G},G,F,G^q)\leftarrow \mathrm{Gen}_{\mathrm{HSM}}(1^\lambda,q)$。定义 $S=\tilde{s}\cdot 2^{\mu_d},\mu_d$ 为统计距离。

密钥生成:随机选取私钥 $\mathrm{sk}\xleftarrow{\$}[0,S]$,计算公钥 $\mathrm{pk}=g_q^{\mathrm{sk}}$,输出密钥对(pk,sk)。

加密:输入公钥 pk 和消息 $m$,随机选取 $r\xleftarrow{\$}[0,S]$,计算 $C_1=f^m\mathrm{pk}^r, C_2=g_q^r$,输出 $C=(C_1,C_2)$。

解密:输入私钥 sk 和密文 $C=(C_1,C_2)$,计算 $M=C_1/C_2^{\mathrm{sk}}$,输出 $m\leftarrow \mathrm{Solve}(M)$。

标量乘:输入公钥 pk,一对密文 $C=(C_1,C_2)$ 和一个标量 $\varepsilon$,输出 $C'=(C_1'=C_1^{\varepsilon},C_2'=C_2^{\varepsilon})$。

同态加:输入公钥 pk 和两对密文 $C=(C_1,C_2)$ 与 $C'=(C_1',C_2')$,输出 $\hat{C}=(\hat{C}_1=C_1C_1',\hat{C}_2=C_2C_2')$。

### 1.5 联盟链系统模型

联盟链系统模型如图 1 所示,其中一共有 7 种节点类型。

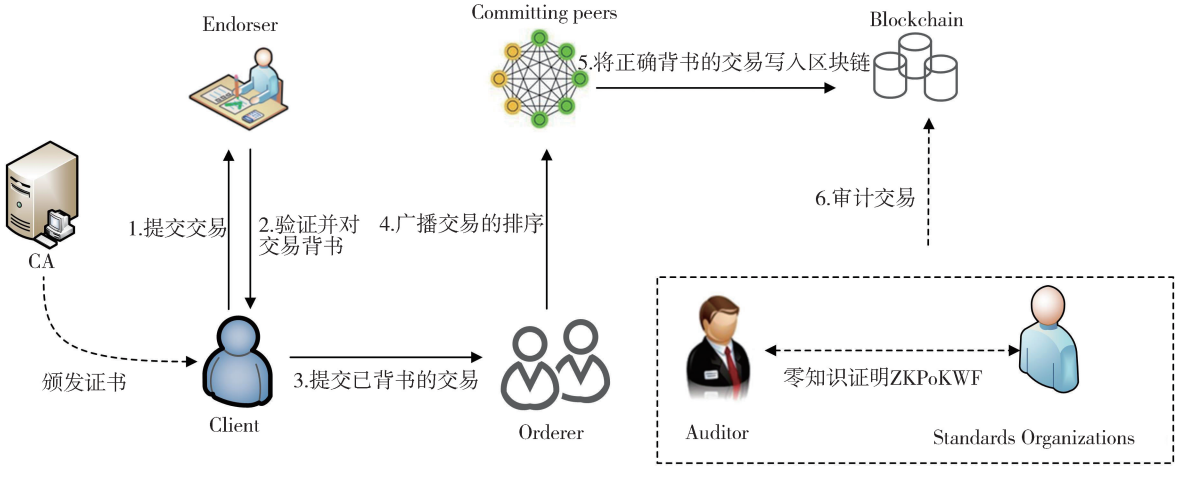


**图 1 联盟链节点和工作流**

(1) Client:代表由用户操作的实体,向 Endorser 节点提交交易,并将交易广播给 Orderer 节点。

(2) Endorser:验证 Client 节点提交的交易。

(3) Orderer:对交易进行排序并且运行共识算法。

(4) Committing Peer:提交交易并且维护分类账。

(5) Auditor:审计者可以对任何交易进行审计。

(6) CA:为客户端的公钥颁发证书,只有被授权的一方才能参与到交易中。

(7) Standards Organizations:联盟链中的可信第三方,下文统一译为标准化组织。

## 2 安全审计协议

假设联盟链系统中,用户从 CA 获得了一个证书,交易的工作流如下。

Step 1:Client 将一个已签名的交易发送给其选择的 Endorser。

Step 2:该 Endorser 验证交易,并将背书证书退还给 Client。

Step 3:Client 将已被背书的交易广播给所有 Orderer。

Step 4:Orderer 将有序的交易块传输给所有 Committing Peer。

Step 5:Comminting Peer 验证是否所有交易已被正确背书,然后将其提交到区块链中,并维护一个分类账的副本。

Step 6:Auditor 在必要的时候可以对交易进行审计。

在本节中,所提出的安全审计协议使用加法同态 CL 加密和零知识证明完成审计,大致执行流程为:首先,Client 在 Step 1 中利用标准化组织选取的公钥对交易进行 CL 加密,随后经过 Step 2~Step 5,交易以密文的形式被提交到联盟链中,最后,在 Step 6 中,标准化组织与审计者执行零知识证明完成审计。

联盟链中对交易的审计一般要保证两个方面:(1) 总的承诺输入金额等于总的承诺输出金额;(2) 所有提交的金额都在有效范围内。联盟链采用

UTXO 交易模型,交易构成了一组链式结构,所有合法的交易都可以追溯到前向一个或多个交易输出,因此同态加密可以在保证交易隐私的前提下,完成金额的累加。同时,在 CL 密文良好性的零知识证明中,证明者可以在不泄露消息的任何有效信息的情况下,使验证者相信密文的良好性。本协议基于 HSM-CL 加密方案,将其应用于联盟链的审计领域,在不泄露交易隐私的情况下,实现对交易金额有效范围和收支平衡的审计,主要分为准备阶段、零知识证明阶段和审计阶段。具体过程如图 2 所示。

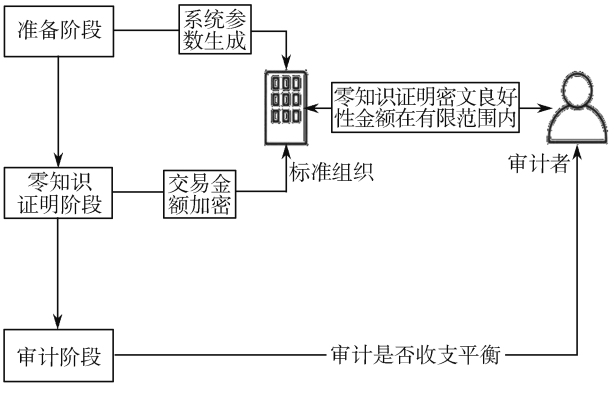


**图 2　协议过程**

### 2.1　准备阶段

系统参数: $\text{param}=(\tilde{s},g,f,g_q,\hat{G},G,F,G^q)\leftarrow \text{Gen}_{\text{HSM}}(1^\lambda,q)$。定义 $B=\tilde{s}\cdot 2^{\lambda+\mu_d+2}$,$\mu_d$ 取值 80。输入一个范围参数 $u$。

密钥生成:标准化组织 $S$ 随机选取私钥 $\text{sk}\xleftarrow{\$}[0,B]$,计算公钥 $\text{pk}=g_q^{\text{sk}}$,输出密钥对(pk,sk)。

### 2.2　零知识证明阶段

加密:对于一段时间内的 $l$ 笔交易 $M_i,i=1,2,\cdots,l$,总的交易金额为 $M=\sum_{i=1}^{l}M_i$。随机选取 $r\xleftarrow{\$}[0,B]$,计算 CL 加密密文 $C_{1,i}=f^{M_i}\text{pk}^r,C_{2,i}=g_q^r$,输出 $C_i=(C_{1,i},C_{2,i})$。对于所有的密文 $C_i$,$S$ 与审计者执行如下零知识协议证明了 CL 加密密文的良好性。

零知识证明 ZKPoKWF:零知识证明过程如图 3 所示。

(1) 输入 $C_i=(C_{1,i},C_{2,i})$ 和 $\text{pk}=g_q^{\text{sk}}$,$S$ 即为证明者,审计者为验证者。

(2) $S$ 随机选择 $\alpha\xleftarrow{\$}[-B,B],\beta\xleftarrow{\$}Z_q$,计算 $S_1=\text{pk}^\alpha f^\beta,S_2=g_q^\alpha$,将 $(S_1,S_2)$ 发送给审计者。

(3) 审计者选取 $\gamma\xleftarrow{\$}[0,q-1]$ 并发送给 $S$。

(4) $S$ 计算 $u_r=\alpha+\gamma r,u_M=\beta+\gamma M_i \bmod q$。$S$ 选取 $\mu\in Z_q$ 和 $\nu\in[0,q-1]$ 使得 $u_r=\mu q+\nu$,其中 $Z_q$ 为整数乘法群,计算 $D_1=\text{pk}^\mu,D_2=g_q^\mu,E=\beta+\gamma u$ 将 $(u_M,D_1,D_2,\nu,E)$ 发送给审计者。

(5) 审计者验证是否:

$$\nu\in[0,q-1],D_1^q\text{pk}^\nu f^{u_M}=S_1C_{1,i}^\gamma,D_2^q g_q^\nu=S_2C_{2,i}^\gamma$$

如果是,审计者选取 $\tau\xleftarrow{\$}\text{Prime}(\lambda)$ 发送给 $S$。其中 $\text{Prime}(\lambda)$ 为小于 $2^\lambda$ 的奇质数集。

(6) $S$ 选取 $\rho\in Z_q$ 和 $\sigma\in[0,\tau-1]$ 使得 $u_r=\rho\tau+\sigma$,计算 $Q_1=\text{pk}^\rho,Q_2=g_q^\rho$,将 $(Q_1,Q_2,\sigma)$ 发送给审计者。

(7) 审计者验证是否:

$$\sigma\in[0,\tau-1],Q_1^\tau\text{pk}^\sigma f^{u_M}=S_1C_{1,i}^\gamma,Q_2^\tau g_q^\nu=S_2C_{2,i}^\gamma。$$

如果是,则证明 CL 加密密文的良好性。

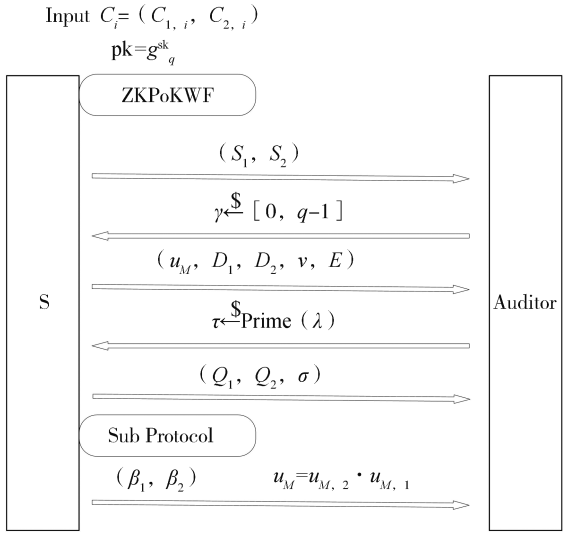


**图 3　零知识证明过程**

为了证明交易金额在有效范围内,$S$ 和审计者执行如下交互子协议[18]:

(1) $S$ 将 $\beta$ 表示为两个整数相乘的形式,即 $\beta=\beta_2\cdot\beta_1$,计算 $a=g_q^{\beta_1},b=g_q^{\beta_2}$,并将 $(a,b)$ 发送给审计者。

(2) 审计者将 $u_M$ 表示为两个整数相乘的形式,即 $u_M=u_{M,2}\cdot u_{M,1}$。

(3) 审计者计算 $n_1=\dfrac{ab\cdot g_q^{u_{M,2}+1}}{b^{2u_{M,2}}\cdot g_q^{u_{M,1}}}=g_q^{\beta_1-u_{M,1}+1+\beta_2+u_{M,2}-2\cdot\beta_2\cdot u_{M,2}},n_2=\dfrac{b\cdot g_q}{g_q^{u_{M,2}}}=g_q^{\beta_2-u_{M,2}+1}$。

如果 $n_1$ 和 $n_2$ 有一个等于 1,则 $\beta<u_M$,否则 $\beta\geqslant u_M$。

审计者同时验证是否 $u_M \leqslant E$, 当且仅当 $u_M \in (\beta, E]$, 输出 1,否则输出 0。

当且仅当上述子协议输出为 1,证明交易金额在有效范围内,审计者接受,否则拒绝。

### 2.3 审计阶段

为避免审计者了解细粒度的交易细节,使用 CL 加法同态加密。对于所有交易的密文 $C_i = (C_{1,i}, C_{2,i})$, 经过上述零知识证明,证明了交易金额的有效性和加密密文的良好性,可以计算同态加密的密文 $C_1 = \prod_{i=1}^{l} C_{1,i}, C_2 = \prod_{i=1}^{l} C_{2,i}$, 输出 $C = (C_1, C_2)$。在一次审计过程中,对于总输入金额为 $M_{\text{in}}$ 的 $n$ 笔交易输入和总输出金额为 $M_{\text{out}}$ 的 $n'$ 笔交易输出,分别可以输出同态加密密文: $C_{\text{out}} = (\prod_{j=1}^{n'} C_{1,j}, \prod_{j=1}^{n'} C_{2,j}) = (f^{M_{\text{out}}} \text{pk}^{\sum_{j=1}^{n'} r_{\text{out},j}}, g_q^{\sum_{j=1}^{n'} r_{\text{out},j}}) C_{\text{in}} = (\prod_{i=1}^{n} C_{1,i}, \prod_{i=1}^{n} C_{2,i}) = (f^{M_{\text{in}}} \text{pk}^{\sum_{i=1}^{n} r_{\text{in},i}}, g_q^{\sum_{i=1}^{n} r_{\text{in},i}})$。

因此,要证明总的输入金额等于总的输出金额,等同于证明:

$$\prod_{j=1}^{n'} C_{1,j} / \prod_{i=1}^{n} C_{1,i} = \text{pk}^{\sum_{j=1}^{n'} r_{\text{out},j} - \sum_{i=1}^{n} r_{\text{in},i}}$$

定义 $x_s = \sum_{j=1}^{n'} r_{\text{out},j} - \sum_{i=1}^{n} r_{\text{in},i}$。

标准化组织 $S$ 随机选取 $r_s \xleftarrow{\$} [0, B]$, 计算 $R = \text{pk}^{r_s}, \tilde{R} = g_q^{r_s}$。

定义 $H: \{0,1\}^* \to Z_p$ 是一个抗碰撞的哈希函数,计算 $\tilde{c} = H(\text{param}, R, \tilde{R}, C_{\text{out}}, C_{\text{in}}), z_s = r_s + \tilde{c} x_s$。将 $(\tilde{c}, z_s)$ 发送给审计者。审计者接收到后,计算

$$R' = \text{pk}^{z_s} (\prod_{i=1}^{n} C_{1,i} / \prod_{j=1}^{n'} C_{1,j})^{\tilde{c}} \tilde{R}' = g_q^{z_s} (\prod_{i=1}^{n} C_{1,i} / \prod_{j=1}^{n'} C_{1,j})^{\tilde{c}}$$

当且仅当 $\tilde{c} = H(\text{param}, R', \tilde{R}', C_{\text{out}}, C_{\text{in}})$, 输出 1,证明交易金额收支平衡,否则输出 0。

## 3 安全性分析及性能分析

### 3.1 安全性分析

CL 加密已被证明在 DDH 假设下是 IND-CPA 安全的。本协议的安全性是基于 CL 密文良好性的零知识证明,该方案已被证明是多项式安全的,在交互过程中不会泄露任何有效信息。本协议将其应用于联盟链审计场景,增加了对单笔交易金额有效范围和总的交易输入输出收支平衡的审计,金额有效范围的证明是通过子协议实现,该子协议的安全性是基于离散对数问题的困难性,假设敌手窃听了 $(a, b)$, 在多项式时间内恢复出 $(\beta_2, \beta_1)$ 在计算上是困难的。传统的联盟链交易审计协议中,私钥由审计者选取,因此不诚实的审计者可以随时随地披露交易的完整细节,损害交易双方的利益。本协议基于交互式零知识证明,交易金额以 $u_M = \beta + \gamma M \bmod q$ 的形式发送给审计者,其中 $\beta$ 的标准化组织是 $S$ 选取的, $\gamma$ 是审计者第一次挑战过程中发送的,由于没有关于 $\beta$ 的信息,审计者得不到关于 $M$ 的任何有效信息。

**定理 1** 零知识证明 ZKPoKWF 是可靠的。

证明:使用倒带技术回顾敌手的每一次新的挑战 $\tau$, 可以输出 $(\sigma, \tau)$, 有极大的概率使 $u_r \equiv \sigma \bmod \tau$。如果 $\text{pk}^{u_r} \neq S_1 C_{1,i} f^{u_M}$ 并且 $(\text{pk}^{u_r})^q \neq (S_1 C_{1,i} f^{u_M})^q$, 则 $\text{pk}^{u_r} \neq S_1 C_{1,i} f^{u_M} = Q_1^{\tau} \text{pk}^{\sigma} = D_1^q \text{pk}^{\nu}$。令 $\chi = \dfrac{u_r - \sigma}{\tau}$, 则 $Q_1 \text{pk}^{\chi}$ 是 $S_1 C_{1,i} f^{u_M} / \text{pk}^{u_r} \neq 1$ 的第 $\tau$ 个根,这将打破自适应根子群假设,因此有极大的概率使 $\text{pk}^{u_r} = S_1 C_{1,i} f^{u_M} = Q_1^{\tau} \text{pk}^{\sigma}$。提取器从协议输出副本中提取 $(u_r, u_M, \gamma)$ 和 $(u'_r, u'_M, \gamma')$, 计算 $\Delta u_r = u_r - u'_r, \Delta u_M = u_M - u'_M$ 和 $\Delta\gamma = \gamma - \gamma' \bmod q$, 表示 $r = \dfrac{\Delta u_r}{\Delta\gamma}, M_i = \dfrac{\Delta u_M}{\Delta\gamma}$, 则 $C_1^{\Delta\gamma} = (\text{pk}^r f^{M_i})^{\Delta\gamma}$, 如果 $C_1 \neq \text{pk}^r f^{M_i}$, 定义 $\varphi = \text{pk}^r f^{M_i} / C_1 \neq 1, \varphi^{\Delta\gamma} = 1 (\Delta\gamma < q)$, 则 $\varphi$ 是一个非平凡的元素,因此有极大的概率使 $C_1 = \text{pk}^r f^{M_i}$。综上,零知识证明 ZKPoKWF 是可靠的。

**定理 2** 零知识证明 ZKPoKWF 是零知识的。

证明:假设多项式时间内的模拟器与诚实的验证者一样随机选取一个 $\gamma' \xleftarrow{\$} [0, q-1]$ 和 $\tau' \xleftarrow{\$} \text{Prime}(\lambda)$, 在交互过程中可以找到 $\mu' \in Z_q, \nu' \in [0, q-1]$ 以及 $\rho' \in Z_q$ 和 $\sigma' \in [0, \tau'-1]$, 使得 $\mu' q + \nu' = \rho' \tau' + \sigma'$。然后,计算可得 $(D'_1, D'_2, Q'_1, Q'_2, E')$, 对于协议中的所有输出,包括协议执行期间选择的随机数, $(\mu', \nu', \rho', u'_M, D'_1, D'_2, E')$ 由 $(\gamma', \tau')$ 唯一确定,以确保验证有效。对于 $\sigma'$, 其值与 $[0, \tau'-1]$ 上的均匀分布的统计距离可以忽略不计, $(Q'_1, Q'_2)$ 的值仅与 $\sigma'$ 有关,因此模拟器产生的输出 $(\mu', \nu', \rho', \sigma', u'_M, D'_1, D'_2, Q'_1, Q'_2, E')$ 与实际证明者和验证者之间交互产生的输出 $(\mu, \nu, \rho, \sigma, u_M, D_1, D_2, Q_1, Q_2, E)$ 在统计上无法区分。综上,零知识证明 ZKPoKWF 是零知识的。

### 3.2　性能分析

为了测试本协议算法的计算消耗,在 Windows 环境配置为 Intel(R) Core(TM) i5-4200H CPU @ 2.80 GHz,RAM 16.00 GB 的平台上使用 Java 语言、JPBC 库以及 Bouncycastle 第三方库实现本协议的算法。

Yuen 等[15] 提出了一种安全审计协议,利用 Elgamal 加密的加法同态性质和非交互式零知识证明,完成对交易的审计。本文分别在 112 bit 和 128 bit 安全性下对 Yuen 等[15] 的审计协议以及本协议的通信带宽和运行时间做对比,结果是多次运行之后所取得的平均值,分别如图 4 和图 5 所示。需要注意的是,由于本地测试环境的异构性和代码编写复杂程度的不同,运行结果会有一些偏差,但总体趋势不变。本协议基于同样采用 Elgamal 形式的 CL 加密,与传统 CL 加密相比,在使用相同统计距离和可靠误差的情况下,通过紧凑零知识证明有效降低了通信带宽和运行时间,加入一个对金额有效范围进行审计的子协议,使得本协议能够适用于联盟链中的审计场景。由图 4 和图 5 可以得出,相较于 Yuen 等[15] 的审计协议,本协议在通信带宽方面开销更小,但在运行时间方面,由于本协议采用交互式零知识证明,增加了重复挑战和回应的时间,故运行成本略高,但仍在同一个数量级。本协议相较于 Yuen 等[15] 的审计协议,优势主要在于:(1) DL 问题在 $F$ 中是简单的,在解密上的计算成本更低;(2) 审计过程中不泄露任何交易信息,增加一些运行成本以获得更高的安全性是有价值的。

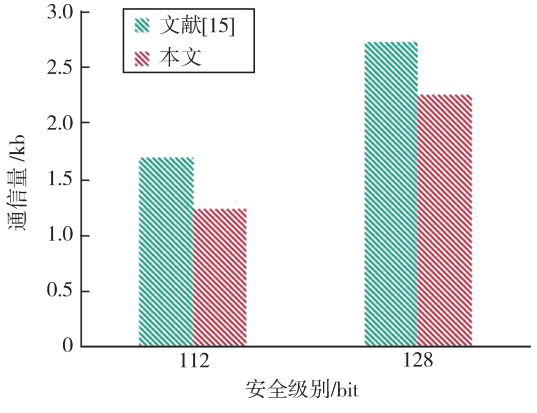


**图 4　通信带宽比较**

随后,在 Linux CentOS 7 环境中搭建了一个简单的 Hyperledger Fabric 1.4 网络,其具备完整的交易流程,包括用户初始化、正常转账和余额查询等功能,并将审计逻辑加入到智能合约中。在该网络中,创建了两个虚拟用户 Alice 和 Bob,在他们之间进行了若干交易,每一笔交易由 Alice 和 Bob 中的一方发起,首先提交给一些 Peer 节点进行背书,随后发送给 Orderer 节点进行排序,最后由 Committing Peer 节点将有效背书的交易写入联盟链。联盟链账本上会存储交易的一些信息,使用 Fabric 提供的 API 接口,可以查询交易的历史记录,本次实验的部分交易信息如表 1 所示。

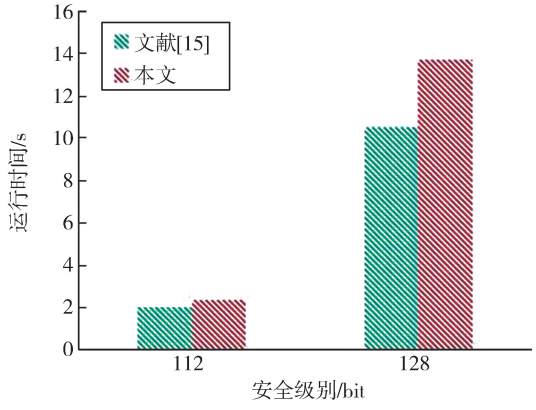


**图 5　运行效率比较**

**表 1　部分交易记录**

| Txid | Owner | Timestamp | isDelete |
|---|---|---|---|
| 307e18… | Alice | 2021-12-25 12:27:35.219 | false |
| 956f42… | Alice | 2021-12-25 12:31:45.124 | false |
| d6d933… | Bob | 2021-12-25 12:36:21.207 | false |
| … | … | … | … |

对这些交易进行审计,以分析本协议在实际联盟链审计场景下的运行效率。

如图 6 所示,本协议在不同数量的交易下都具有良好的审计效率,不过由于使用 Java 语言开发的 Fabric 链码,在效率上会比使用 Go 语言和 BN256 配对库开发的链码略微差一点。

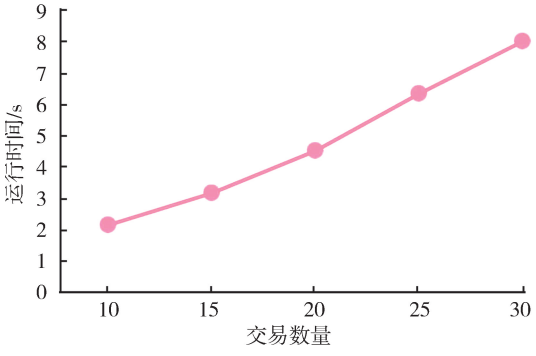


**图 6　审计效率**

## 4 结束语

本文提出了一种基于 CL 加密的安全审计协议,实现了审计过程中交易隐私保护。相较于现有的审计方案,本文提出的安全审计协议具有如下特点:(1) 审计过程中不会泄漏与交易相关的任何有效信息,避免了不诚实审计者权力过大造成的安全隐患。(2) 通过交互式零知识证明,审计者可以在不知道任何有效信息的情况下,相信交易的有效性和合规性。基于零知识证明、DDH 假设、DL 问题的困难性等数学问题,所提出的安全审计协议具有良好的安全性,通过紧凑型零知识证明,有效提高了性能,适用于联盟链中的审计场景,并有良好的扩展性。

**参考文献:**


[1] ZHANG A, BAI X Y. Decentralized authorization and authentication based on consortium blockchain[C]//Blockchain and Trustworthy Systems. 2020: 267-272.

[2] PÉREZ-SOLÀ C, DELGADO-SEGURA S, NAVARRO-ARRIBAS G, et al. Another coin bites the dust: an analysis of dust in UTXO-based cryptocurrencies[J]. Royal Society Open Science, 2019, 6(1): 180817.

[3] 孙国梓, 李芝, 肖荣宇, 等. 区块链交易安全问题研究[J]. 南京邮电大学学报(自然科学版), 2021, 41(2): 36-48.
SUN Guozi, LI Zhi, XIAO Rongyu, et al. Research on blockchain transaction security[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2021, 41(2): 36-48.(in Chinese)

[4] YUEN T H. PAChain:private, authenticated and auditable consortium blockchain[C]//CANS. 2019:214-234.

[5] YUEN T H. PAChain: private, authenticated & auditable consortium blockchain and its implementation[J]. Future Generation Computer Systems, 2020, 112: 913-929.

[6] 孙国梓,王纪涛,谷宇.区块链技术安全威胁分析[J].南京邮电大学学报(自然科学版),2019,39(5):48-62.
SUN Guozi, WANG Jitao, GU Yu. Security threat analysis of blockchain technology[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2019, 39(5): 48-62.(in Chinese)

[7] GOLDWASSER S, MICALI S. Probabilistic encryption[J]. Journal of Computer and System Sciences, 1984, 28(2): 270-299.

[8] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//Advances in Cryptology. 1999: 223-238.

[9] DAMGÅRD I, JURIK M. A generalisation, a simplification and some applications of paillier's probabilistic public-key system[C]//Public Key Cryptography.2001: 119-136.

[10] CHEVALLIER-MAMES B, PAILLIER P, POINTCHEVAL D. Encoding-free ElGamal encryption without random oracles[C]//Public Key Cryptography.2006: 91-104.

[11] CASTAGNOS G, CHEVALLIER-MAMES B. Towards a DL-based additively homomorphic encryption scheme[C]//Information Security. 2007: 362-375.

[12] BRESSON E, CATALANO D, POINTCHEVAL D. A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications[C]//Advances in Cryptology.2003: 37-54.

[13] CASTAGNOS G, LAGUILLAUMIE F. Linearly homomorphic encryption from DDH[C]//Topics in Cryptology. 2015: 487-505.

[14] CASTAGNOS G, CATALANO D, LAGUILLAUMIE F, et al. Two-party ECDSA from hash proof systems and efficient instantiations[C]//Advances in Cryptology. 2019: 191-221.

[15] YUEN T H, CUI H D, XIE X. Compact zero-knowledge proofs for threshold ECDSA with trustless setup[EB/OL]. [2021-02-24]. https://eprint.iacr.org/2021/205.

[16] BUCHMANN J, HAMDY S. A survey on IQ cryptography[C]//Proceedings of Public-Key Cryptography and Computational Number Theory. 2001: 1-16.

[17] BIASSE J F, JACOBSON M J, SILVESTER A K. Security estimates for quadratic field based cryptosystems[C]//Information Security and Privacy.2010: 233-247.

[18] BLASS E O, KERSCHBAUM F. BOREALIS: building block for sealed bid auctions on blockchains[C]// Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. 2020: 558-571.


(责任编辑:潘雪松)