·网络空间安全·　　文章编号：1000-3428(2022)10-0158-11　　文献标志码：A　　中图分类号：TP309

一种基于LWE-CPABE的区块链数据共享方案

张晓东[1]，陈韬伟[1]，余益民[1,2]

（1.云南财经大学 信息学院，昆明 650221；2.云南财经大学 智能应用研究院，昆明 650221）

摘　要：为应对量子计算对区块链上基于数论的隐私保护技术所带来的威胁，将区块链技术与格属性基加密算法有效融合，提出一种基于格的后量子CPABE区块链数据共享方案。将容错学习(LWE)作为方案的困难问题假设，构造一种基于格的密文策略属性基加密算法LWE-CPABE，抵御量子计算对公钥密码安全的攻击，实现数据的安全共享。设计算法参数的标准格式化交易结构，以满足LWE-CPABE算法的可追责性。在此基础上，给出交易生成与交易验证智能合约，以实现交易的自动验证与共识。功能性分析与仿真实验结果表明，该方案在算法初始化、加解密以及密钥生成的计算效率方面均优于传统的基于双线性映射理论的CPABE方案，可实现区块链上数据的高效、安全、动态共享与隐私保护，明显提高区块链数据共享安全性。

关键词：后量子密码；区块链；属性基加密；数据共享；隐私保护

开放科学（资源服务）标志码（OSID）：

中文引用格式：张晓东，陈韬伟，余益民.一种基于LWE-CPABE的区块链数据共享方案[J].计算机工程，2022，48(10)：158-168，175.

英文引用格式：ZHANG X D，CHEN T W，YU Y M.A blockchain data sharing scheme based on LWE-CPABE[J].Computer Engineering，2022，48(10)：158-168，175.

A Blockchain Data Sharing Scheme Based on LWE-CPABE

ZHANG Xiaodong[1]，CHEN Taowei[1]，YU Yimin[1,2]

（1.School of Information，Yunnan University of Finance and Economics，Kunming 650221，China；
2.Intelligent Application Research Institute，Yunnan University of Finance and Economics，Kunming 650221，China）

【Abstract】To solve the threat that quantum computing poses to the privacy protection technology using number theory applied to blockchains，a post-quantum Ciphertext-Policy Attribute-Based Encryption（CPABE）blockchain data sharing scheme based on lattice theory is proposed in this paper by effectively integrating blockchain technology and a lattice-based attribute-based encryption algorithm.First，using the Learning With Errors（LWE）problem，a lattice-based LWE-CPABE algorithm is constructed，which can effectively resist quantum computing attacks on public key cryptography to realize secure data sharing.Second，the standard formatted transaction structure of the algorithm parameters is designed to satisfy the accountability requirements associated with the LWE-CPABE algorithm.Finally，an intelligent contract for transaction generation and transaction verification is designed to realize the automatic verification and consensus of a transaction.Functional analysis and simulation results demonstrate that the initialized encryption as well as the key generation efficiency using the proposed algorithm is superior to the traditional CPABE scheme based on bilinear mapping theory.The proposed LWE-CPABE achieves higher efficiency and improves privacy protection in blockchain dynamic data sharing scenarios.

【Key words】post-quantum cryptography；blockchain；Attribute-Based Encryption（ABE）；data sharing；privacy protection

DOI：10.19678/j.issn.1000-3428.0062803

0　概述

随着区块链技术的不断普及，使用区块链在弱信任或无信任网络中进行数据共享已经非常普遍。但是由于区块链的“不可篡改”和“公开透明”的特点，使得区块链上的隐私数据保护成为一个挑战。近年来，研究人员针对区块链上的隐私保护和数据共享提出了新的解决方案[1-3]。其中，基于属性的加密算法由于其“一对多”加密和可以实现细粒度访问控制等优点，被广泛应用在数据溯

基金项目：国家自然科学基金（71964037）；中央引导地方科技发展专项资金（202007AD110001）；电子政务建模仿真国家工程实验室开放课题项目（MEL-18-03）。

作者简介：张晓东（1995—），男，硕士研究生，主研方向为属性基加密、区块链技术；陈韬伟（通信作者）、余益民，教授、博士。

收稿日期：2021-09-26　　**修回日期：**2021-11-29　　**E-mail：**twchen@ynufe.edu.cn

源[4]、云存储[5]、医疗数据共享[6]、物联网[7]等区块链的各种方案中。

属性基加密(Attribute-Based Encryption,ABE)来源于SAHAI等[9]于2005年提出的基于模糊身份加密,后来演变为基于属性的加密。其中,在密钥策略属性基加密(Key Policy-Attribute Based Encryption,KP-ABE)中,密文与属性关联,密钥与访问策略关联;而在密文策略属性基加密[10](Ciphertext Policy Attribute Based Encryption,CP-ABE)中,密钥与属性关联,密文与访问策略关联,允许数据拥有者自由制定访问控制策略,适用于分布式存储和解密方不确定的环境[11]。近年来,关于ABE的研究主要集中于计算效率[12-13]、访问策略及属性隐藏[14]和身份管理[15]。2007年,BETHENCOURT等[16]描述了密文策略属性基加密算法,针对一个解密的对象群体,利用用户相关属性及其用户对象间的相互信任关系作为授权依据,设计访问控制结构,通过一个中心权威构建加解密原语,只有当属性满足访问结构时,用户才能成功解密密文,从而实现一对多加密以及细粒度的访问控制。2011年,WATERS[10]在标准模型下证明了CP-ABE的安全性,并提出一个采用线性秘密共享方案实现秘密共享的CP-ABE,在效率上有了明显提升。2012年,OKAMOTO等[17]提出一个无界内积属性基加密方案,解除了以往属性基加密方案对谓词和属性大小的限制。2013年,GORBUBOV[18]提出基于多项式逻辑电路的属性基加密方案,其公开参数和密文大小随着电路深度线性增长,实现了由基于布尔公式向基于电路的转变,可有效抵御合谋攻击。2014年,WATERS[19]受ROUSELAKIS等[20]提出的属性基加密方案启发,提出Online-Offline属性基加密方案,将所有配对操作进行离线处理,减少了在线阶段的计算开销。

随着量子计算的不断发展,基于数论问题的困难性将会极大降低,以数论为基础的传统公钥密码体系面临着被破解的风险。格密码采用格困难问题作为格密码构造的安全性基础,拥有最困难情况假设下无法求解的安全性,可以很好地抵抗量子攻击。目前,被证明安全的格困难问题主要由小整数解[21](Small Integer Solution,SIS)问题和容错学习问题[22](Learning With Errors,LWE)问题。两种困难问题均从最坏情况理想格问题向一般变种问题归约,且计算效率高,易存储。目前,基于格的加密方案相继被提出,但主要集中于基于身份加密[23]、数字签名[24]和零知识证明[25]等。2021年5月,DATTA等[26]基于LWE困难问题,构造一种基于密文策略的属性基加密算法,实现了可抵抗量子攻击的CPABE方案。

本文通过改进CPABE方案,提出适用于区块链的抗量子攻击LWE-CPABE算法,并给出支持策略更新的密文策略属性基加密算法,以实现数据的动态访问控制。在此基础上,定义适用于LWE-CPABE算法的可公开验证数据的格式化交易结构,设计交易生成算法和交易验证合约。

1 预备知识

1.1 相关参数定义

本文设λ为安全参数,$\mathrm{negl}:\mathbb{N}\to\mathbb{R}$表示可忽略函数,若该函数渐进地小于任意反多项式函数,则该函数可忽略,即对于任意常数$c>0$存在一个整数N_c,对于所有$\lambda>N_c$都有$\mathrm{negl}(\lambda)\leqslant\lambda^{-c}$,$[n]=\{1,2,\cdots,n\}$。

令PPT(Probability Polynomial-Time)为概率多项式时间,对于某一分布$\mathcal{X}$,令$x\leftarrow\mathcal{X}$为$\mathcal{X}$分布随机抽样值;对于集合X,令$x\leftarrow X$为集合X中元素均匀采样值。在默认情况下,文中向量即为行向量;在矩阵中,第j行记为$\boldsymbol{M}_j$,$\boldsymbol{M}_J$记为$\boldsymbol{M}$的子矩阵,由所有$\boldsymbol{M}_j$的行组成$(j\in J)$,J为矩阵的一组行索引;对于向量$\boldsymbol{v}$,令$\|\boldsymbol{v}\|$为该向量的ℓ_2范数,$\|\boldsymbol{v}\|_\infty$为该项量的$\ell_\infty$范数。

对于整数$q\geqslant 2$,设$\mathbb{Z}_q$为模q的环,$\mathbb{Z}_q$表示$(-q/2,q/2]$范围内的整数。

1.2 B边界

对于整数上的一组分布$\mathcal{D}=\{\mathcal{D}_\lambda\}_{\lambda\in\mathbb{N}}$并且存在边界$B=B(\lambda)>0$,若对于每个$\lambda\in\mathbb{N}$都有:

$$\Pr_{x\leftarrow\mathcal{D}_\lambda}[|x|\leqslant B(\lambda)]=1$$

则认为$\mathcal{D}$是有B边界的。

引理1 设$B_1=B_1(\lambda)$和$B_2=B_2(\lambda)$为正,令$\mathcal{D}=\{\mathcal{D}_\lambda\}_\lambda$为$B_1$的有界分布族,$\mathcal{U}=\{\mathcal{U}_\lambda\}_\lambda$为$[-B_2(\lambda),B_2(\lambda)]$上的均匀分布。若存在一个可忽略函数$\mathrm{negl}(\cdot)$使得对于所有$\lambda\in\mathbb{N}$都有:

$$B_1(\lambda)/B_2(\lambda)\leqslant\mathrm{negl}(\lambda)$$

则认为分布族$\mathcal{D}+\mathcal{U}$和$\mathcal{U}$在统计上是不可区分的。

1.3 剩余哈希

定理1(剩余哈希定理) 令$n:\mathbb{N}\to\mathbb{N}$,$q:\mathbb{N}\to\mathbb{N}$,$m>(n+1)\log_a q+\omega(\log_a n)$并且$k=k(n)$为多项式,则以下两个分布在统计上是不可区分的:

$$\mathcal{D}_1\equiv\{(\boldsymbol{A},\boldsymbol{AR})\,|\,\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m},\boldsymbol{R}\leftarrow\{-1,1\}^{m\times k}\}$$

$$\mathcal{D}_2\equiv\{(\boldsymbol{A},\boldsymbol{S})\,|\,\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m},\boldsymbol{S}\leftarrow\mathbb{Z}_q^{n\times k}\}$$

1.4 格

定义格$\mathcal{L}$为$\mathbb{R}^m$中一个维度为m的离散加法子群,定义正整数n、m、q和矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,令$\lambda_q^\perp(\boldsymbol{A})$表示格$\{\boldsymbol{x}\in\mathbb{Z}^m\,|\,\boldsymbol{Ax}^\perp=\boldsymbol{0}^\perp \bmod q\}$。对于$\boldsymbol{u}\in\mathbb{Z}_q^n$,令$\lambda_q^{\boldsymbol{u}}(\boldsymbol{A})$表示陪集$\{\boldsymbol{x}\in\mathbb{Z}^m\,|\,\boldsymbol{Ax}^\perp=\boldsymbol{u}^\perp \bmod q\}$。

1)离散高斯分布

令σ为任意正实数,由函数$\rho_\sigma(\boldsymbol{x})=\exp\left(-\pi\|\boldsymbol{x}\|^2/\sigma^2\right)$生成一个高斯分布$\mathcal{D}_\sigma$,对于任意离散集合$\mathcal{L}\in\mathbb{R}^m$,定义$\rho_\sigma(\mathcal{L})=\sum_{\boldsymbol{x}\in\mathcal{L}}\rho_\sigma(\boldsymbol{x})$,包含参数$\sigma$的格$\mathcal{L}$上的离散高斯分布$\mathcal{D}_{\mathcal{L},\sigma}$由概率分布$\rho_{\mathcal{L},\sigma}(\boldsymbol{x})$定义:

$$\rho_{\mathcal{L},\sigma}(\boldsymbol{x})=\rho_\sigma(\boldsymbol{x})/\rho_\sigma(\mathcal{L})$$

引理2 若离散高斯分布的参数σ较小，则从该分布提取的任何向量大概率将较短。

引理3 令m、n、q为正整数且满足$m>n$，$q>2$。定义矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，$\sigma=\tilde{\Omega}(n)$和$\mathcal{L}=\lambda_q^{\perp}(\boldsymbol{A})$，则存在可忽略函数$\mathrm{negl}(\cdot)$，使得：

$$\Pr_{x\leftarrow\mathcal{D}_{\mathcal{L},\sigma}}\left[\|\boldsymbol{x}\|>\sqrt{m}\,\sigma\right]\leqslant\mathrm{negl}(n)$$

其中：$\|\boldsymbol{x}\|$为$\boldsymbol{x}$的ℓ_2范数。

2）截断离散高斯

$\mathbb{Z}^m$上参数为σ的截断离散高斯分布$\tilde{\mathcal{D}}_{\mathbb{Z}^m,\sigma}$与离散高斯分布$\mathcal{D}_{\mathbb{Z}^m,\sigma}$相同，但当$\ell_\infty$范数大于$\sqrt{m}\,\sigma$时，则输出0。另外，从引理2可知，$\tilde{\mathcal{D}}_{\mathbb{Z}^m,\sigma}$和$\mathcal{D}_{\mathbb{Z}^m,\sigma}$在统计学角度上是无法区分的。

3）格中陷门

格陷门函数包括以下两个算法：

（1）$\mathrm{TrapGen}(1^n,1^m,q)\mapsto(\boldsymbol{A},T_{\boldsymbol{A}})$：格初始化算法是一个随机化算法，输入矩阵的维度$n$、$m$和模$q$，输出一个矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$和一个格陷门函数$T_{\boldsymbol{A}}$。

（2）$\mathrm{SamplePre}(\boldsymbol{A},T_{\boldsymbol{A}},\sigma,\boldsymbol{u})\mapsto\boldsymbol{s}$：预采样算法将矩阵$\boldsymbol{A}$、格陷门函数$T_{\boldsymbol{A}}$、向量$\boldsymbol{u}\in\mathbb{Z}_q^n$和参数$\sigma\in\mathbb{R}$作为输入，输出向量$\boldsymbol{s}\in\mathbb{Z}_q^n$。向量$\boldsymbol{s}$满足$\boldsymbol{A}\cdot\boldsymbol{s}^{\mathrm{T}}=\boldsymbol{u}^{\mathrm{T}}$并且$\|\boldsymbol{s}\|\leqslant\sqrt{m}\cdot\sigma$。

1.5 LWE困难问题假设

对于安全参数$\lambda\in\mathbb{N}$，假设$n:\mathbb{N}\to\mathbb{N}$，$q:\mathbb{N}\to\mathbb{N}$，$\sigma:\mathbb{N}\to\mathbb{R}^+$是$\lambda$的函数。定义$\mathrm{LWE}_{n,q,\sigma}$为由$n=n(\lambda)$、$q=q(\lambda)$和$\sigma=\sigma(\lambda)$参数化的LWE困难问题假设。对于任意PPT敌手$\mathcal{A}$，存在一个可忽略函数$\mathrm{negl}(\cdot)$，对于任意$\lambda\in\mathbb{N}$：

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{LWE}_{n,q,\sigma}}(\lambda)\triangleq\left|\begin{matrix}\Pr\left[\begin{matrix}1\leftarrow\mathcal{A}^{\mathcal{O}_1^s(\cdot)}(1^\lambda)\\ \boldsymbol{s}\leftarrow\mathbb{Z}_q^n\end{matrix}\right]\\ -\Pr\left[1\leftarrow\mathcal{A}^{\mathcal{O}_2(\cdot)}(1^\lambda)\right]\end{matrix}\right|\leqslant\mathrm{negl}(\lambda)$$

谕言机$\mathcal{O}_1^s(\cdot)$、$\mathcal{O}_2(\cdot)$定义如下：

$\mathcal{O}_1^s(\cdot)$与$\boldsymbol{s}\in\mathbb{Z}_q^n$强连接，在面对每次询问时选择$\boldsymbol{a}\leftarrow\mathbb{Z}_q^n$和$e\leftarrow\mathcal{D}_{\mathbb{Z},\sigma}$并输出$(\boldsymbol{a},\boldsymbol{s}\boldsymbol{a}^{\mathrm{T}}+e\bmod q)$。$\mathcal{O}_2(\cdot)$在每次询问过程中选择$\boldsymbol{a}\leftarrow\mathbb{Z}_q^n$和$u\leftarrow\mathbb{Z}_q$并输出$(\boldsymbol{a},u)$。

定义1 若存在一个PPT敌手可以解决LWE困难问题假设，那么存在一个PPT量子算法可以在最高困难下解决格困难问题。

鉴于目前有关格困难问题的技术方案，当所有$\lambda\in\mathbb{N}$，$n=n(\lambda)$，$q=q(\lambda)$，$\sigma=\sigma(\lambda)$满足以下条件时：

$$2\sqrt{n}<\sigma<q<2^n,\ n\cdot q/\sigma<2^n,\ 0<\epsilon<1/2$$

LWE困难问题假设对于任意多项式$n(\cdot)$和任意函数$q(\cdot)$、$\sigma(\cdot)$都成立。

2 LWE-CPABE算法

2.1 算法描述

如图1所示，LWE-CPABE算法主要由系统初始化、用户属性私钥生成、明文加密、密文解密、密文策略生成以及密文策略更新6个部分组成。

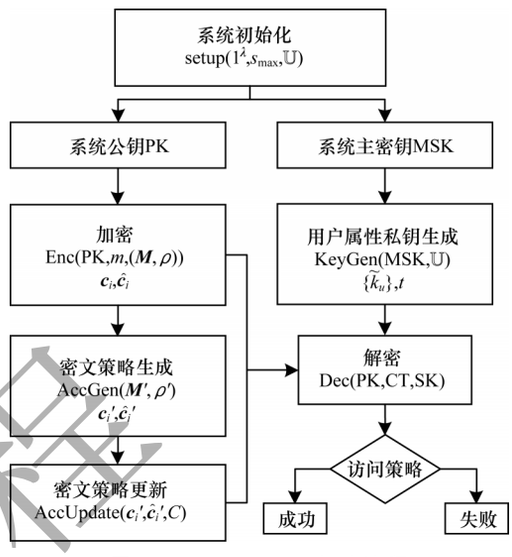

图1 LWE-CPABE算法流程

Fig.1 Procedure of LWE-CPABE algorithm

LWE-CPABE算法流程如下：

1）$\mathrm{Setup}(1^\lambda,s_{\max},\mathbb{U})\to(\mathrm{PK},\mathrm{MSK})$。系统初始化算法通过输入安全参数$\lambda$，LSSS矩阵所支持的最大宽度$s_{\max}=s_{\max}(\lambda)$和用户属性集合$\mathbb{U}$，输出系统公私钥对$(\mathrm{PK},\mathrm{MSK})$。

对于系统中的每个属性$\boldsymbol{u}$，选择$\boldsymbol{A}_{\boldsymbol{u}}\in\mathbb{Z}_q^{n\times m}$生成陷门函数$\boldsymbol{T}_{\boldsymbol{A}_{\boldsymbol{u}}}$、均匀分布的随机矩阵$\boldsymbol{H}_{\boldsymbol{u}}\in\mathbb{Z}_q^{n\times m}$和随机向量$\boldsymbol{y}\leftarrow\mathbb{Z}_q^n$，输出：

$$\mathrm{PK}=(\boldsymbol{y}\{\boldsymbol{A}_{\boldsymbol{u}}\},\{\boldsymbol{H}_{\boldsymbol{u}}\}),\ \mathrm{MSK}=\{\boldsymbol{T}_{\boldsymbol{A}_{\boldsymbol{u}}}\}$$

2）$\mathrm{KeyGen}(\mathrm{MSK},\mathbb{U})\to\mathrm{SK}$。用户属性私钥生成算法通过输入主密钥MSK和用户属性集合$\mathbb{U}$，输出该用户的用户属性私钥SK。

令$\hat{\boldsymbol{t}}\leftarrow\mathrm{noise}^{m-1}$，$\boldsymbol{t}=(1,\hat{\boldsymbol{t}})\in\mathbb{Z}^m$。向量$\boldsymbol{t}$为用户属性私钥的一部分，每个用户所持有的$\boldsymbol{t}$不同，可防止合谋攻击。对于每个属性$\boldsymbol{u}\in\mathbb{U}$，利用陷门$\boldsymbol{T}_{\boldsymbol{A}_{\boldsymbol{u}}}$生成一个短向量$\tilde{\boldsymbol{k}}_{\boldsymbol{u}}$，并且满足$\boldsymbol{A}_{\boldsymbol{u}}\tilde{\boldsymbol{k}}_{\boldsymbol{u}}^{\mathrm{T}}=\boldsymbol{H}_{\boldsymbol{u}}\boldsymbol{t}^{\mathrm{T}}$，输出：

$$\mathrm{SK}=\left(\left\{\tilde{\boldsymbol{k}}_{\boldsymbol{u}}\right\},t\right)$$

3）$\mathrm{Enc}(\mathrm{PK},m,(\boldsymbol{M},\rho))\to\mathrm{CT}$。明文加密算法通过输入公钥PK、明文$m$和访问控制策略，输出密文CT。

设ρ是一个将属性映射到矩阵$\boldsymbol{M}$行向量的映射函数，即$\rho(i)$为矩阵$\boldsymbol{M}$中第i行相关联的属性。随机选择$\boldsymbol{s}\leftarrow\mathbb{Z}_n^q$和$\boldsymbol{v}_2,\boldsymbol{v}_3,\cdots,\boldsymbol{v}_{s_{\max}}\leftarrow\mathbb{Z}_q^m$，并计算：

$$\boldsymbol{c}_i=\boldsymbol{s}\boldsymbol{A}_{\rho(i)}+\mathrm{noise}$$

$$\hat{\boldsymbol{c}}_i=M_{i,1}\left(\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}},\overbrace{0,\cdots,0}^{m-1}\right)+\left[\sum_{j\in\{2,3,\cdots,s_{\max}\}}M_{i,j}\boldsymbol{v}_j\right]-\boldsymbol{s}\boldsymbol{H}_{\rho(i)}+\mathrm{noise}$$

输出密文CT：

$$\mathrm{CT}=(\{\boldsymbol{c}_i\}_{i\in[\ell]},\{\hat{\boldsymbol{c}}_i\}_{i\in[\ell]},C=\mathrm{MSB}(\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}))\oplus m)$$

4）$\mathrm{Dec}(\mathrm{PK},\mathrm{CT},\mathrm{SK})\to m$。密文解密算法输入公钥PK、密文CT和用户属性私钥SK，输出明文m。

设用户所拥有的属性满足访问控制策略。令$\boldsymbol{I}$为对应于属性的行向量集合，令$\{\omega_i\}_{i\in\boldsymbol{I}}\in\{0,1\}\subset\mathbb{Z}_q$为重构系数。对于任意$i\in\boldsymbol{I}$，令$\rho(i)$为行关联属性，计算：

$$K=\sum_{i\in\boldsymbol{I}}\omega_i\left(\boldsymbol{c}_i\tilde{\boldsymbol{k}}_{\rho(i)}^{\mathrm{T}}+\hat{\boldsymbol{c}}_i\boldsymbol{t}^{\mathrm{T}}\right)$$

输出$m=C\oplus\mathrm{MSB}(K)$。

5）$\mathrm{AccGen}(\boldsymbol{M}',\rho')\rightarrow(\boldsymbol{c}_i'\hat{\boldsymbol{c}}_i')$。密文策略生成算法将新的访问控制策略作为输入，输出更新后的策略密文。

6）$\mathrm{AccUpdate}(\boldsymbol{c}_i',\hat{\boldsymbol{c}}_i',C)\rightarrow\mathrm{CT}'$。密文策略更新算法将策略生成算法生成的策略密文作为输入，输出新的密文CT′。

2.2　安全模型

LWE-CPABE安全游戏中包含一个挑战者和一个敌手，挑战者模拟系统运行并回答敌手询问。具体游戏如下：

1）系统建立。敌手接收安全参数1^{λ}并提交一个访问控制策略$(\boldsymbol{M},\rho)$，挑战者运行Setup算法生成系统公钥PK发送给敌手。

2）私钥询问。敌手对挑战者进行多项式时间的私钥询问，对于每次密钥查询，敌手发送一组属性$\boldsymbol{U}\in\mathbb{U}$，但是这些属性不满足访问控制策略$(\boldsymbol{M},\rho)$。挑战者运行KeyGen算法并将生成的用户属性私钥SK发送给敌手。

3）挑战阶段。挑战者选择一个随机消息$b\leftarrow\{0,1\}$并使用敌手提供的访问控制策略$(\boldsymbol{M},\rho)$运行Enc算法对消息进行加密。此后，将密文CT发送给敌手。

4）重复步骤2）。

5）猜测阶段。敌手输出对b的猜想$b'\leftarrow\{0,1\}$。

敌手$\mathcal{A}$在该游戏中的优势为：

$$\mathrm{Adv}_{\mathcal{A}}^{\text{LWE-CPABE, SEL-CPA}}(\lambda)\triangleq|\Pr[b=b']-1/2|$$

定义2　若对于任何PPT敌手$\mathcal{A}$，存在一个可忽略函数$\mathrm{negl}(\cdot)$，使得对于所有的$\lambda\in\mathbb{N}$，都有$\mathrm{Adv}_{\mathcal{A}}^{\text{LWE-CPABE, SEL-CPA}}(\lambda)\leqslant\mathrm{negl}(\lambda)$，则本文所提出的LWE-CPABE方案是选择性安全的。

3　LWE-CPABE区块链数据共享方案

3.1　方案架构

为实现区块链中的数据高效流转与策略更新，数据的上传、共享、修改及策略更新都通过交易的形式写入区块链中。用户可通过所持有的与自身属性相匹配的用户属性私钥访问链上的授权信息，完成安全可控的数据共享。LWE-CPABE区块链数据共享方案架构如图2所示，其中，实线为交易过程，虚线为相关参数传递过程。

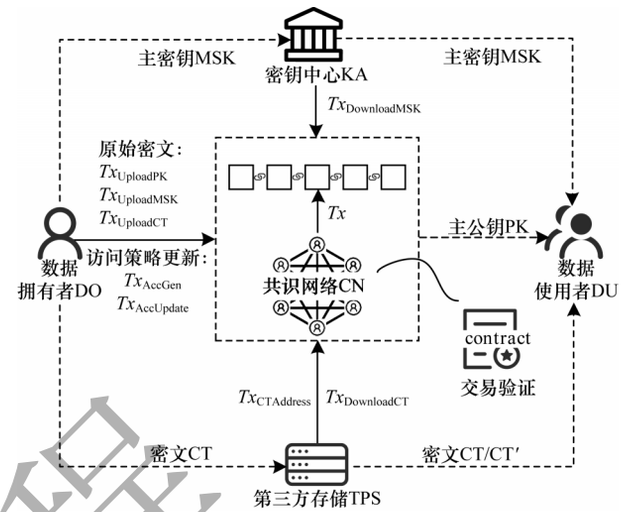

图2　数据共享方案的架构

Fig.2　Architecture of data sharing scheme

3.2　格式化交易结构

格式化交易结构如下：

1）用户（DO、DU）。包括数据拥有者和数据使用者。数据拥有者DO制定访问控制策略，并生成相对应的密文，将密文上传至第三方存储并将地址上传至区块链，同时，将主密钥MSK委托密钥中心保管；数据使用者DU从密钥中心获取主密钥，之后利用自己的属性集合生成用户属性私钥SK，从区块链获取密文并解密。

2）第三方存储（TPS）。提供加密数据的存储服务，并将加密数据地址存入区块链中。

3）共识网络（CN）。由区块链中各记账节点组成，负责LWE-CPABE区块链加密协议中所涉及的交易的共识与记账更新。

4）密钥中心（KA）。存储LWE-CPABE加密算法中的主密钥MSK，各用户通过密钥中心获取主密钥。

5）智能合约（SC）。为协议各参与方提供交互接口。

LWE-CPABE区块链数据共享方案以区块链中的交易为载体实现数据的加密存储与细粒度访问控制。加密数据的访问控制权限由数据拥有者制定，数据被发布至链上后可以任意次数更新访问控制策略，直至加密数据被撤销，结束本次加密数据共享的生命周期。为使各参与方更高效地获取所需数据，便于审计和掌握访问控制动态，加密协议中定义了适用于该协议的交易格式：

Tx={From，To，TxType，OpType，Timestamp，Data，CheckText，Sign}

其中：From表示交易发起方；To表示交易接收方；TxType表示交易类型，A表示访问控制策略类消息，D表示数据类消息；OpType表示操作类型，P表示发布，U表示更新，R表示撤销；Timestamp表示交易发布的时间戳；Data表示交易包含的数据体；

CheckText表示数据域Data的哈希值；Sign表示交易发起方的签名。

3.3 交易发布与验证合约

在LWE-CPABE区块链数据共享方案中，各参与方通过交易的方式进行相关数据的流转。为保证交易的正确性、完整性和可追溯性，在交易生成后需共识网络中各节点进行共识验证。

参与数据共享的各参与方和全网节点通过智能合约的方式进行交易的生成与验证。交易生成合约如算法1所示。

算法1 交易生成算法

输入 格式化交易中各参数From、To、TxType、OpType、Timestamp、Data、CheckText、Sign；共识网络中交易发起方的区块链私钥BSK

输出 某特定交易 Tx

1.CheckText=H(Data);/*计算数据中与相关数据的数字摘要*/

2.MD=H(From, To, TxType, OpType, Timestamp, Data, CheckText);/*计算交易数字摘要(除签名字段)*/

3.Sign = $\mathrm{Sign}_{\mathrm{BSK}}$(MD) /*使用交易方的区块链私钥对该交易进行数字签名*/

4. Tx={From, To, TxType, OpType, Timestamp, Data, CheckText, Sign};/*生成交易*/

5.Return Tx;

交易生成后，将被广播至共识网络被其他节点验证。区块链中的节点可通过CheckText和签名Sign对该交易进行快速验证。

交易验证合约如算法2所示。

算法2 交易验证合约算法

输入 交易Tx，共识网络中交易发起方的区块链公钥BPK

输出 交易验证结果True或False

1.MD′= H(From, To, TxType, OpType, Timestamp, Data, CheckText);/*统计交易数字摘要(除签名字段)*/

2.MD=$\mathrm{Compute}_{\mathrm{BPK}}$Sign;/*验证签名*/

3.if MD′= MD then

4. Obtain Data From Tx;/*从交易中获取数据域数据Data*/

5. CheckText′=H(Data);

6. if CheckText′=CheckText then

7. Return True;

8.Return False;

当该交易获得节点验证成功并全网共识后，挖矿节点会打包交易、出块并全网广播，最终由本地节点接收并同步区块。

3.4 方案构造

本节将详细阐述基于LWE-CPABE方案的区块链数据共享过程。

DO选择正确性证明所需的参数约束。对于任意 $B \in \mathbb{N}$，令 $\mathcal{U}_B$ 表示 $\mathbb{Z} \cap [-B, B]$ 上的均匀分布。系统初始化算法选择参数 n、m、σ、q 和噪声分布 $\mathcal{X}_{lwe}$、$\mathcal{X}_1$、$\mathcal{X}_2$、$\mathcal{X}_{big}$：

- $n = \mathrm{ploy}(\lambda), \sigma < q, n \cdot q/\sigma < 2^{n^\epsilon}, \mathcal{X}_{lwe} = \tilde{\mathcal{D}}_{\mathbb{Z}^m, \sigma}$
- $m > 2s_{\max} n \log_a q + \omega \log_a n + 2\lambda$
- $\sigma > \sqrt{s_{\max} n \log_a q \log_a m} - \lambda$
- $\mathcal{X}_1 = \tilde{\mathcal{D}}_{\mathbb{Z}^{m-1}, \sigma}, \mathcal{X}_2 = \tilde{\mathcal{D}}_{\mathbb{Z}^m, \sigma}$
- $\mathcal{X}_{big} = \mathcal{U}_{\hat{B}}, \hat{B} > (m^{3/2}\sigma + 1)2^\lambda$
- $|\mathbb{U}| \cdot 3m^{3/2}\sigma\hat{B} < q/4$

1)系统初始化。数据拥有者DO选取安全参数 λ，LSSS矩阵支持的最大宽度 $s_{\max}$ 和用户属性集合 $\mathbb{U}$，运行Setup算法生成公钥PK和主密钥MSK。

系统初始化算法如算法3所示。

算法3 系统初始化算法

输入 安全参数 λ，LSSS矩阵支持的最大宽度 $s_{\max}$，用户属性集合

输出 公钥PK，主密钥MSK

1. Choose an LWE modulus q, dimensions n, m and distributions $\mathcal{X}_{\mathrm{lwe}}, \mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_{\mathrm{big}}$;

2. Choose a vector $y \leftarrow \mathbb{Z}_q^n$ and a matrices $\{H_u\}_{u \in \mathbb{U}} \leftarrow \mathbb{Z}_q^{n \times m}$;

3. $\mathrm{EnTrapGen}(1^n, 1^m, q) \rightarrow \{(A_u, T_{A_u})\}$ /*进行陷门计算*/

$$PK = \left(n, m, q, \mathcal{X}_{\mathrm{lwe}}, \mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_{\mathrm{big}}, y\{A_u\}_{u \in \mathbb{U}}, \{H_u\}_{u \in \mathbb{U}}\right)$$

$$MSK = \{T_{A_u}\}_{u \in \mathbb{U}}$$

DO生成交易 $\mathrm{Tx}_{\mathrm{UploadPK}}$={DO, BC, A, P, Timestamp, PK, CheckText, $\mathrm{Sig}_{\mathrm{DO}}$}将公钥上链。然后使用KA公钥对主密钥加密得到 $\mathrm{CT}_{\mathrm{MSK}}$，并生成交易 $\mathrm{Tx}_{\mathrm{UploadMSK}}$={DO, KA, A, P, Timestamp, $\mathrm{CT}_{\mathrm{MSK}}$, CheckText, $\mathrm{Sig}_{\mathrm{DO}}$}，将主密钥MSK委托KA保管。

2)数据加密。数据拥有者DO制定访问控制策略 $(\boldsymbol{M}, \rho)$，$(\boldsymbol{M}, \rho)$ 为LSSS访问控制策略，其中 $\boldsymbol{M} = (M_{i,j})_{\ell \times s_{\max}} \in \{-1, 0, 1\}^{\ell \times s_{\max}} \subset \mathbb{Z}_q^{\ell \times s_{\max}}$，$\rho$ 为属性映射(单射)函数 $\rho: [\ell] \rightarrow \mathbb{U}$，将访问控制矩阵 $\boldsymbol{M}_i$ 映射到属性集合 $\mathbb{U}$。之后，运行Enc算法，输入公钥PK、明文 m 和访问控制策略 $(\boldsymbol{M}, \rho)$ 后得到密文CT。

数据加密算法如算法4所示。

算法4 数据加密算法

输入 公钥PK，明文 m，访问控制策略 $(\boldsymbol{M}, \rho)$

输出 密文CT

1.Generate Access Policy (M, ρ);

2.Select a random vector $s \leftarrow \mathbb{Z}_q^n$;/*秘密共享密钥*/

3.Sample a vector $\{v_j\}_{j \in \{2, 3, \cdots, s_{\max}\}} \leftarrow \mathbb{Z}_q^n$;

4.for each $i \in [\ell]$

Select random noise $\{e_i\}_{i \in [\ell]} \leftarrow \mathcal{X}_{\mathrm{lwe}}^m$ and $\{\hat{e}_i\}_{i \in [\ell]} \leftarrow \mathcal{X}_{\mathrm{big}}^m$;

Compute $c_i, \hat{c}_i \in \mathbb{Z}_q^m$

$$c_i = sA_{\rho(i)} + e_i$$

$$\hat{c}_i = M_{i,1}\left(sy^{\mathrm{T}}, \overbrace{0, \cdots, 0}^{m-1}\right) + \left[\sum_{j \in \{2, 3, \cdots, s_{\max}\}} M_{i,j} v_j\right] - sH_{\rho(i)} + \hat{e}_i$$

$$CT = (\{M, \rho\}\{c_i\}_{i \in [\ell]}, \{\hat{c}_i\}_{i \in [\ell]}, C = \mathrm{MSB}(sy^{\mathrm{T}})) \oplus m)$$

DO生成交易 $\mathrm{Tx}_{\mathrm{UploadCT}}$={DO, TPS, A, P, Timestamp, $\mathrm{CT}_{\mathrm{MSK}}$, CheckText, $\mathrm{Sig}_{\mathrm{DO}}$}，将密文上传至第三方存储TPS，TPS生成交易 $\mathrm{Tx}_{\mathrm{CTAddress}}$={TPS, BC, A, D, Timestamp, $\mathrm{CT}_{\mathrm{Address}}$, CheckText, $\mathrm{Sig}_{\mathrm{TPS}}$}，将密文地址上链。

3）用户属性私钥生成。各数据使用者DU从密钥中心KA处申请获得主密钥，KA使用各用户区块链公钥对MSK加密后生成交易 $Tx_{DownloadMSK=}$｛KA，DU，A，P，Timestamp，CT_{MSK}，CheckText，Sig_{DO}｝。之后DU输入自身属性信息 $\boldsymbol{U}$ 和主密钥MSK，运行KeyGen算法输出与自身属性对应的用户属性私钥SK。

用户属性私钥生成算法如算法5所示。

算法5　用户属性私钥生成算法

输入　主密钥MSK，自身属性信息 $\boldsymbol{U}$

输出　用户属性私钥SK

1. Select a random vector $\hat{\mathrm{t}} \leftarrow \mathcal{X}_1$;

2. Let $\mathrm{t}=(1,\hat{\mathrm{t}}) \in \mathbb{Z}^{\mathrm{m}}$;

3. for each $\mathrm{u} \in \mathrm{U}$

Select $\hat{\mathrm{k}}_{\mathrm{u}} \leftarrow \mathcal{X}_{\mathrm{big}}$;

$\hat{\mathrm{k}}_{\mathrm{u}} \leftarrow$ EnSamplePre

Compute $(\mathrm{A}_{\mathrm{u}}, \mathrm{T}_{\mathrm{A}_{\mathrm{u}}}, \sigma, \mathrm{tH}_{\mathrm{u}}^{\mathrm{T}} - \hat{\mathrm{k}}_{\mathrm{u}}\mathrm{A}_{\mathrm{u}}^{\mathrm{T}})$

then Compute $\mathrm{k}_{\mathrm{u}} = \hat{\mathrm{k}}_{\mathrm{u}} + \tilde{\mathrm{k}}_{\mathrm{u}}$;

$\mathrm{SK} = (\{\mathrm{k}_{\mathrm{u}}\}_{\mathrm{u} \in \mathbb{U}}, \mathrm{t})$

4）密文解密。DU从区块链BC检索密文地址，通过密文地址 $CT_{Address}$ 从TPS搜索到相对应密文CT并下载至本地，TPS生成交易 $Tx_{DownloadCT}$=｛TPS，DU，D，P，Timestamp，CT，CheckText，Sig_{TPS}｝进行密文下载记录。DU使用SK对密文CT进行解密，获取明文。

在密文解密过程中，SK对应于属性集合 $\mathbb{U}$ 的某个子集 $\boldsymbol{U} \in \mathbb{U}$，若 $(1,0,\cdots,0)$ 不在与 $\boldsymbol{U}$ 关联的矩阵 $\boldsymbol{M}$ 的行空间中，则解密失败；否则，设 $\boldsymbol{I}$ 为矩阵 $\boldsymbol{M}$ 的一组行索引并满足 $\forall i \in \boldsymbol{I}$: $\rho(i) \in \boldsymbol{U}$，设标量 $\{\omega_i\}_{i \in \boldsymbol{I}} \in \{0,1\} \subset \mathbb{Z}_q$，且 $\sum_{i \in \boldsymbol{I}} \omega_i M_i = (1,0,\cdots,0)$，其中 M_i 为矩阵 $\boldsymbol{M}$ 的第 i 行。

解密算法如算法6所示。

算法6　解密算法

输入　密文CT，用户属性私钥SK

输出　明文数据 m

1. Compute $\mathrm{K} = \sum_{\mathrm{i} \in \mathrm{I}} \omega_{\mathrm{i}} (\mathrm{c}_{\mathrm{i}} \mathrm{k}_{\rho(\mathrm{i})}^{\mathrm{T}} + \hat{\mathrm{c}}_{\mathrm{i}} \mathrm{t}^{\mathrm{T}})$;

2. Compute $\mathrm{m} = \mathrm{C} \oplus \mathrm{MSB}(\mathrm{K})$;

5）密文策略生成。当访问控制策略发生变更时，重新加密需要耗费更多密钥空间成本和密文加密时间成本。在LWE-CPABE区块链加密协议中，数据使用者可进行原始密文保留的访问控制策略更新。在进行策略更新时，DO生成新的访问控制策略 $(\boldsymbol{M}', \rho')$，之后运行AccGen算法得到更新后的策略密文 $\mathrm{Update}_{\mathrm{CT}} = (\boldsymbol{c}_i', \hat{\boldsymbol{c}}_i')$：

$$\boldsymbol{c}_i' = \boldsymbol{s}\boldsymbol{A}_{\rho'(i)} + \boldsymbol{e}_i$$

$$\hat{\boldsymbol{c}}_i' = M_{i,1}' \left(\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}, \overbrace{0,\cdots,0}^{m-1} \right) + \left[\sum_{j \in \{2,3,\cdots,s_{\max}\}} M_{i,j}' \boldsymbol{v}_j \right] - \boldsymbol{s}\boldsymbol{H}_{\rho(i)} + \hat{\boldsymbol{e}}_i$$

随后生成策略更新交易 Tx_{AccGen}=｛DO，TPS，A，U，Timestamp，$Update_{CT}$，CheckText，Sig_{DO}｝发送给第三方存储TPS。同时，生成原密文撤销交易发送至区块链以更新密文信息 $Tx_{AccUpdate}$=｛DO，BC，A，R，Timestamp，CT，CheckText，Sig_{DO}｝告知各数据使用者DU。

6）密文策略更新。TPS获取更新后的策略密文后，从原CT中获取密文 C，输入更新的访问控制策略密文 $(\boldsymbol{c}_i', \hat{\boldsymbol{c}}_i')$，运行AccUpdate算法生成更新后密文CT′。

$$\mathrm{CT}' = \left((\boldsymbol{M}', \rho'), \{\boldsymbol{c}_i'\}_{i \in [\ell]}, \{\hat{\boldsymbol{c}}_i'\}_{i \in [\ell]}, C = \mathrm{MSB}(\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}) \right) \oplus m$$

更新后密文仍使用原密文地址，各数据使用者仍可通过上述步骤获取密文并进行解密。

在基于LWE-CPABE的区块链加密协议中，各用户利用格式化的交易结构可快速高效地检索到各自所需信息，同时，整个数据流转周期内实现了各节点行为全过程链上监管，可以更好地进行审计和掌握访问控制动态。

4　方案分析

4.1　正确性分析

假设某数据使用者拥有的属性 $\boldsymbol{U} \in \mathbb{U}$，并且满足LSSS访问控制策略 $(\boldsymbol{M}, \rho)$，则由密文解密算法可得：

$$K = \sum_{i \in \boldsymbol{I}} \omega_i \left(\boldsymbol{c}_i \boldsymbol{k}_{\rho(i)}^{\mathrm{T}} + \hat{\boldsymbol{c}}_i \boldsymbol{t}^{\mathrm{T}} \right)$$

展开 $\{\boldsymbol{c}_i\}_{i \in \boldsymbol{I}}$ 和 $\{\hat{\boldsymbol{c}}_i\}_{i \in \boldsymbol{I}}$ 可得：

$$K = \sum_{i \in \boldsymbol{I}} \omega_i \boldsymbol{s}\boldsymbol{A}_{\rho(i)} \boldsymbol{k}_{\rho(i)}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}} \omega_i M_{i,1} (\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}, 0, \cdots, 0) \boldsymbol{t}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}, j \in \{2,3,\cdots,s_{\max}\}} \omega_i M_{i,j} \boldsymbol{v}_j \boldsymbol{t}^{\mathrm{T}} - \sum_{i \in \boldsymbol{I}} \omega_i \boldsymbol{s}\boldsymbol{H}_{\rho(i)} \boldsymbol{t}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}} \omega_i \hat{\boldsymbol{e}}_i \boldsymbol{t}^{\mathrm{T}}$$

对于每个 $u \in \boldsymbol{U}$，有 $\boldsymbol{k}_u = \hat{\boldsymbol{k}}_u + \tilde{\boldsymbol{k}}_u$。由EnSamplePre可得：

$$\boldsymbol{A}_u \tilde{\boldsymbol{k}}_u^{\mathrm{T}} = \boldsymbol{H}_u \boldsymbol{t}^{\mathrm{T}} - \boldsymbol{A}_u \hat{\boldsymbol{k}}_u^{\mathrm{T}}$$

因此，对于每个 $i \in \boldsymbol{I}$ 有：

$$\boldsymbol{A}_{\rho(i)} \boldsymbol{k}_{\rho(i)}^{\mathrm{T}} = \boldsymbol{A}_{\rho(i)} \hat{\boldsymbol{k}}_{\rho(i)}^{\mathrm{T}} + \boldsymbol{A}_{\rho(i)} \tilde{\boldsymbol{k}}_{\rho(i)}^{\mathrm{T}} = \boldsymbol{H}_{\rho(i)} \boldsymbol{t}^{\mathrm{T}}$$

可得：

$$K = \sum_{i \in \boldsymbol{I}} \omega_i \boldsymbol{s}\boldsymbol{H}_{\rho(i)} \boldsymbol{t}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}} \omega_i M_{i,1} (\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}, 0, \cdots, 0) \boldsymbol{t}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}, j \in \{2,3,\cdots,s_{\max}\}} \omega_i M_{i,j} \boldsymbol{v}_j \boldsymbol{t}^{\mathrm{T}} - \sum_{i \in \boldsymbol{I}} \omega_i \boldsymbol{s}\boldsymbol{H}_{\rho(i)} \boldsymbol{t}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}} \omega_i \boldsymbol{e}_i \boldsymbol{k}_{\rho(i)}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}} \omega_i \hat{\boldsymbol{e}}_i \boldsymbol{t}^{\mathrm{T}} = \sum_{i \in \boldsymbol{I}} \omega_i M_{i,1} (\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}, 0, \cdots, 0) \boldsymbol{t}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}, j \in \{2,3,\cdots,s_{\max}\}} \omega_i M_{i,j} \boldsymbol{v}_j \boldsymbol{t}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}} \omega_i \boldsymbol{e}_i \boldsymbol{k}_{\rho(i)}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}} \omega_i \hat{\boldsymbol{e}}_i \boldsymbol{t}^{\mathrm{T}} = \left(\sum_{i \in \boldsymbol{I}} \omega_i M_{i,1} \right) (\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}, 0, \cdots, 0) \boldsymbol{t}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}, j \in \{2,3,\cdots,s_{\max}\}} \omega_i M_{i,j} \boldsymbol{v}_j \boldsymbol{t}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}} \omega_i \boldsymbol{e}_i \boldsymbol{k}_{\rho(i)}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}} \omega_i \hat{\boldsymbol{e}}_i \boldsymbol{t}^{\mathrm{T}}$$

当 $1 < j \leqslant s_{\max}$ 时，$\sum_{i \in \boldsymbol{I}} \omega_i M_{i,j} = 0$，否则 $\sum_{i \in \boldsymbol{I}} \omega_i M_{i,j} = 1$，由3.1节KeyGen构造 $\boldsymbol{t} = (1, \hat{\boldsymbol{t}})$，所以 $(\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}, 0, \cdots, 0) \boldsymbol{t}^{\mathrm{T}} = \boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}$，因此有：

$$K = \boldsymbol{s}\boldsymbol{y}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}} \omega_i \boldsymbol{e}_i \boldsymbol{k}_{\rho(i)}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}} \omega_i \hat{\boldsymbol{e}}_i \boldsymbol{k}_{\rho(i)}^{\mathrm{T}}$$

对于噪声部分 $\sum_{i \in \boldsymbol{I}} \omega_i \boldsymbol{e}_i \boldsymbol{k}_{\rho(i)}^{\mathrm{T}} + \sum_{i \in \boldsymbol{I}} \omega_i \hat{\boldsymbol{e}}_i \boldsymbol{k}_{\rho(i)}^{\mathrm{T}}$，存在以下约束：

1）由引理3可知，因为 $\boldsymbol{e}_i$ 中的 m 个坐标均来自于截断离散高斯分布 $\tilde{D}_{\mathbb{Z},\sigma}$，所以有 $\| \boldsymbol{e}_i \| \leqslant \sqrt{m}\, \sigma$。

2）因为 $\hat{\boldsymbol{e}}_i$ 中的 m 个坐标均来自于均匀分布 $\mathbb{Z}\cap\left[-\hat{B},\hat{B}\right]$，所以有 $\left\|\hat{\boldsymbol{e}}_i\right\|\leqslant\sqrt{m}\,\hat{B}$。

3）因为 $\hat{\boldsymbol{k}}_{\rho(i)}$ 中的 m 个坐标均来自于均匀分布 $\mathbb{Z}\cap\left[-\hat{B},\hat{B}\right]$，所以有 $\left\|\hat{\boldsymbol{k}}_{\rho(i)}\right\|\leqslant\sqrt{m}\,\hat{B}$。又因为 $\tilde{\boldsymbol{k}}_{\rho(i)}$ 中的 m 个坐标均来自于统计上接近截断离散高斯分布的 $\tilde{\mathcal{D}}_{\mathbb{Z}^m,\sigma}$，所以有 $\left\|\tilde{\boldsymbol{k}}_{\rho(i)}\right\|\leqslant m\sigma$。综上所述，对于 $\left\|\boldsymbol{k}_{\rho(i)}\right\|$，因为 $\boldsymbol{k}_{\rho(i)}=\hat{\boldsymbol{k}}_{\rho(i)}+\tilde{\boldsymbol{k}}_{\rho(i)}$，所以 $\left\|\boldsymbol{k}_{\rho(i)}\right\|$ 的上界为 $\left\|\boldsymbol{k}_{\rho(i)}\right\|\leqslant m\sigma+\sqrt{m}\,\hat{B}$。

4）因为 $\boldsymbol{t}-\left(1,\hat{\boldsymbol{t}}\right)$，其中 $\hat{\boldsymbol{t}}$ 取自截断离散高斯分布 $\tilde{\mathcal{D}}_{\mathbb{Z}^{m-1},\sigma}$，所以有 $\left\|\boldsymbol{t}\right\|\leqslant m\sigma$。

因此可得：

$$\left\|\sum_{i\in I}\omega_i\boldsymbol{e}_i\boldsymbol{k}_{\rho(i)}^{\mathrm{T}}+\sum_{i\in I}\omega_i\hat{\boldsymbol{e}}_i\boldsymbol{k}_{\rho(i)}^{\mathrm{T}}+\right\|<$$

$$|\mathbb{U}|(m^{3/2}\sigma^2+m\sigma\hat{B}+m^{3/2}\sigma\hat{B})<$$

$$|\mathbb{U}|\cdot 3m^{3/2}\sigma\hat{B}<q/4$$

因此，以 λ 中几乎可以忽略的概率，$\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}$ 的最高有效位（MSB）不受上述噪声的影响，其范围为 $q/4$，因此不影响最高有效位，即 $\mathrm{MSB}(K)=\mathrm{MSB}(\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}})$。

证毕。

4.2 安全性分析

本文基于LSSS访问控制结构的LWE-CPABE，定义了更灵活的选择性安全，即“线性独立约束下的选择性安全”。因此，将游戏中的密钥询问阶段修改如下：

在密钥询问阶段，敌手向挑战者进行多项式的密钥询问，对于每次密钥询问，攻击者发送一系列不满足访问控制策略 $(\boldsymbol{M},\rho)$ 的属性 $\boldsymbol{U}\in\mathbb{U}$。此外，访问控制矩阵 $\boldsymbol{M}$ 的行由 $\boldsymbol{U}$ 中的属性进行标记，即 $\boldsymbol{M}$ 在 $\rho^{-1}(\boldsymbol{U})$ 中的索引必须线性无关。之后，挑战者回复相应的用户属性私钥 $\mathrm{SK}\leftarrow\mathrm{KeyGen}(\mathrm{MSK},\boldsymbol{U})$。

敌手 $\mathcal{A}$ 在该游戏中的优势定义为：

$$\mathrm{Adv}_{\mathcal{A}}^{\text{LWE-CPABE, SEL-LI-CPA}}(\lambda)\triangleq|\Pr[b=b']-1/2|$$

定义3 若上述游戏中任意PPT敌手 $\mathcal{A}$ 的优势 $\mathrm{Adv}_{\mathcal{A}}^{\text{LWE-CPABE, SEL-LI-CPA}}(\lambda)$ 可以忽略不计，则基于LSSS访问控制结构的LWE-CPABE加密方案在线性独立约束下是选择性安全的。

定义4 若LWE困难问题假设成立，则本文所构造的LWE-CPABE满足选择性安全。

证明 为证明定义4，本文设置了一系列混合博弈游戏，该系列游戏在公共参数的生成、密文挑战和密钥询问阶段各不相同。系列游戏中的第一个游戏对应于所提出的LWE-CPABE方案在线性独立约束博弈下的选择性安全，最后一个游戏是证明敌手 $\mathcal{A}$ 的优势为0。此外，敌手 $\mathcal{A}$ 在每个连续游戏之间的变化量可忽略不计。

证毕。

以下是混合游戏的构建与归约：

Hyb_0：该混合游戏对应于ABE方案的真实弱安全选择性博弈。

Setup阶段：

1.$\boldsymbol{y}\leftarrow\mathbb{Z}_q^n$。

2.$\{(\boldsymbol{A}_u,T_{A_u})\}_{u\in\mathbb{U}}\leftarrow\mathrm{EnTrapGen}(1^n,1^m,q)$。

3.$\{(\boldsymbol{A}_u,T_{A_u})\}_{u\in\mathbb{U}}\leftarrow\mathbb{Z}_q^{n\times m}$。

4.$\mathrm{PK}=\begin{pmatrix}n,m,q,\mathcal{X}_{lwe},\mathcal{X}_1,\mathcal{X}_2,\mathcal{X}_{\mathrm{big}}\\ \boldsymbol{y},\{\boldsymbol{A}_u\}_{u\in\mathbb{U}},\{\boldsymbol{H}_u\}_{u\in\mathbb{U}}\end{pmatrix}$。

Key query阶段：

1.$\left\{\hat{\boldsymbol{k}}_u\right\}_{u\in\mathbb{U}}\leftarrow\mathcal{X}_{\mathrm{big}}^m$。

2.$\hat{\boldsymbol{t}}\leftarrow\mathcal{X}_1$。

3.$\boldsymbol{t}=\left(1,\hat{\boldsymbol{t}}\right)$。

4.$\forall u\in U$: $\hat{\boldsymbol{k}}_u\leftarrow\mathrm{EnSamplePre}(\boldsymbol{A}_u,T_{A_u},\sigma,\boldsymbol{t}\boldsymbol{H}_u^{\mathrm{T}}-\hat{\boldsymbol{k}}_u\boldsymbol{A}_u^{\mathrm{T}})$。

5.$\forall u\in U$: $\boldsymbol{k}_u=\hat{\boldsymbol{k}}_u+\tilde{\boldsymbol{k}}_u$。

6.$\mathrm{SK}=(\{\boldsymbol{k}_u\}_{u\in\mathbb{U}},\boldsymbol{t})$。

Challenge阶段：

1.$\boldsymbol{s}\leftarrow\mathbb{Z}_q^n$。

2.$\{\boldsymbol{v}_j\}_{j\in\{2,3,\cdots,s_{\max}\}}\leftarrow\mathbb{Z}_q^m$。

3.$\{\boldsymbol{e}_i\}_{i\in[\ell]}\leftarrow\mathcal{X}_{\mathrm{lwe}}^m$。

4.$\{\boldsymbol{e}_i\}_{i\in[\ell]}\leftarrow\mathcal{X}_{\mathrm{big}}^m$。

5.$\forall\boldsymbol{i}\in[\ell]$: $\boldsymbol{c}_i=\boldsymbol{s}\boldsymbol{A}_{\rho(i)}+\boldsymbol{e}_i$。

6.$\forall\boldsymbol{i}\in[\ell]$: $\boldsymbol{c}_i=M_{i,1}\left(\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}},\overbrace{0,\cdots,0}^{m-1}\right)+\left[\sum_{j\in\{2,3,\cdots,s_{\max}\}}M_{i,j}\boldsymbol{v}_j\right]-\boldsymbol{s}\boldsymbol{H}_{\rho(i)}+\hat{\boldsymbol{e}}_i$。

7.$\mathrm{CT}=(\{\boldsymbol{c}_i\}_{i\in[\ell]},\{\hat{\boldsymbol{c}}_i\}_{i\in[\ell]},\mathrm{MSB}(\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}))\oplus b)$。

Hyb_1：该游戏与Hyb_0类似，但是在Setup阶段增加了矩阵 $\{\boldsymbol{B}_j\}_{j\in\{2,3,\cdots,s_{\max}\}}\leftarrow\mathbb{Z}_q^{n\times m}$ 的生成，并在挑战阶段进行了改进。

1.将原来 $\{\boldsymbol{v}_j\}$ 转变为 $\{\hat{\boldsymbol{v}}_j\}_{j\in\{2,3,\cdots,s_{\max}\}}\leftarrow\mathbb{Z}_q^n$。

2.将原来 $\{\hat{\boldsymbol{c}}_i\}$ 转变为：

$$\forall i\in[\ell]:\ \hat{\boldsymbol{c}}_i=M_{i,1}\left(\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}},\overbrace{0,\cdots,0}^{m-1}\right)+\left[\sum_{j\in\{2,3,\cdots,s_{\max}\}}M_{i,j}\hat{\boldsymbol{v}}_j\boldsymbol{B}_j\right]-\boldsymbol{s}\boldsymbol{H}_{\rho(i)}+\hat{\boldsymbol{e}}_i$$

Hyb_1和Hyb_0之间的变化仅仅是句法上的变化，因此这两个混合游戏是无法区分的。

Hyb_2：该游戏与Hyb_1类似，区别是在Setup阶段矩阵 $\{\boldsymbol{H}_u\}$ 生成的改变。

1.$\{\boldsymbol{H}'_u\}_{u\in\rho([\ell])}\leftarrow\mathbb{Z}_q^{n\times m}$。

2.$\forall u\in\rho([\ell])$: $\boldsymbol{H}_u=M_{\rho^{-1}(u),1}\left[\boldsymbol{y},\overbrace{|0|\cdots|0}^{m-1}\right]+\sum_{j\in\{2,3,\cdots,s_{\max}\}}M_{\rho^{-1}(u)}\boldsymbol{B}_j+\boldsymbol{H}'_u$。

Hyb_2和Hyb_1之间的变化同样仅仅是句法上的变化，因此这两个混合游戏是无法区分的。

Hyb_3：该游戏与Hyb_2类似，区别是在Setup阶段矩阵 $\{\boldsymbol{H}'_u\}$ 生成的改变。

1.$\{\boldsymbol{R}_u\}_{u\in\rho([\ell])}\leftarrow\{-1,1\}^{m\times m}$。

2.$\boldsymbol{H}'_u=\boldsymbol{A}_u\boldsymbol{R}_u$。

由定理1可知，Hyb_3和Hyb_2在选择上是不可区分的。

Hyb_4：该游戏与Hyb_3类似，区别在于Setup阶段矩阵$\boldsymbol{B}_j$的改变。

1.$\boldsymbol{B}'=[\boldsymbol{B}_2^{\mathrm{T}}|\cdots|\boldsymbol{B}_{s_{\max}}^{\mathrm{T}},T_{\boldsymbol{B}'}]\leftarrow\mathrm{EnTrapGen}(1^{n(s_{\max}-1)},1^{m-1},q)$：$\{\boldsymbol{B}'_j\}_{j\in\{2,3,\cdots,s_{\max}\}}\in\mathbb{Z}_q^{n\times(m-1)}$。

2.$\{\boldsymbol{b}'_j\}_{j\in\{2,3,\cdots,s_{\max}\}}\leftarrow\mathbb{Z}_q^n$。

3.$\forall j\in\{2,3,\cdots,s_{\max}\}$：$\boldsymbol{B}_j=[\boldsymbol{b}_j^{\mathrm{T}}|\boldsymbol{B}'_j]$。

Hyb_4和Hyb_3的不可区分性源于格陷门函数$\mathrm{EnLT}=(\mathrm{EnTrapGen},\mathrm{EnSamplePre})$。

Hyb_5：该游戏与Hyb_4类似，区别在于回答敌手$\mathcal{A}$的密钥询问时向量$\{\boldsymbol{k}_u\}_{u\in U\cap\rho([\ell])}$的改变。

1.$\tilde{\boldsymbol{k}}_u\leftarrow\mathrm{EnSamplePre}\left(\begin{array}{c}\boldsymbol{A}_u,T_{A_u},\sigma\\ \boldsymbol{t}\left(M_{\rho^{-1}(u),1}\left[\boldsymbol{y}^{\mathrm{T}},\overbrace{|0^{\mathrm{T}}|\cdots|0^{\mathrm{T}}|}^{m-1}\right]\right)^{\mathrm{T}}+\\ \sum_{j\in\{2,3,\cdots,s_{\max}\}}\boldsymbol{t}(M_{\rho^{-1}(u),j}\boldsymbol{B}_j)^{\mathrm{T}}-\hat{\boldsymbol{k}}_u\boldsymbol{A}_u^{\mathrm{T}}\end{array}\right)$。

2.$\boldsymbol{k}_u=\hat{\boldsymbol{k}}_u+\tilde{\boldsymbol{k}}_u+\boldsymbol{t}\boldsymbol{R}_u^{\mathrm{T}}$。

Hyb_5和Hyb_4的不可区分性见引理1。

Hyb_6：该游戏与Hyb_5类似，区别在于回答敌手$\mathcal{A}$的密钥询问时向量$\hat{\boldsymbol{t}}$的改变。

1.$\{\boldsymbol{f}_j\}_{j\in\{2,3,\cdots,s_{\max}\}}\leftarrow\mathbb{Z}_q^n$。

2.$\hat{\boldsymbol{t}}\leftarrow\mathrm{EnSamplePre}\left(\begin{array}{c}\boldsymbol{B}',T_{\boldsymbol{B}'},\sigma\\ \begin{pmatrix}d_2\boldsymbol{y}+\boldsymbol{f}_2-\boldsymbol{b}'_2,\cdots,\\ d_{s_{\max}}\boldsymbol{y}+\boldsymbol{f}_{s_{\max}}-\boldsymbol{b}'_{s_{\max}}\end{pmatrix}\end{array}\right)$。

$\boldsymbol{d}=(d_1,\cdots,d_{s_{\max}})\in\mathbb{Z}_q^{s_{\max}}$为一个向量且$d_1=1$，对于所有的$u\in\boldsymbol{U}$有$\sum_{j\in[s_{\max}]}M_{\rho^{-1}(u),j}d_j=0$。值得注意的是，由于游戏限制，索引在$\rho^{-1}(\boldsymbol{U})$中的$\boldsymbol{M}$行的集合相对于访问控制策略$(\boldsymbol{M},\rho)$必须是未授权的，由此保证向量$\boldsymbol{d}$的存在。

Hyb_6和Hyb_5的不可区分性源于格陷门函数$\mathrm{EnLT}=(\mathrm{EnTrapGen},\mathrm{EnSamplePre})$。

Hyb_7：该游戏与Hyb_6类似，区别在于回答敌手$\mathcal{A}$的密钥询问时密钥组件的改变。

1.$\{\boldsymbol{z}_u\}_{u\in U\cap\rho([\ell])}\leftarrow\mathbb{Z}_q^n$。

2.$\forall u\in U\cap\rho([\ell])$：$\sum_{j\in\{2,\cdots,s_{\max}\}}M_{\rho^{-1}(u),j}\boldsymbol{f}_j=\boldsymbol{z}_u+\hat{\boldsymbol{k}}_u\boldsymbol{A}_u^{\mathrm{T}}$。

3.$\forall u\in U\cap\rho([\ell])$：

$\tilde{\boldsymbol{k}}_u\leftarrow\mathrm{EnSamplePre}(\boldsymbol{A}_u,T_{A_u},\rho,\boldsymbol{z}_u)$。

Hyb_7和Hyb_6之间的变化同样仅仅是句法上的变化，因此这两个混合游戏是无法区分的。

Hyb_8：该游戏与Hyb_7类似，区别在于回答敌手$\mathcal{A}$的密钥询问时向量$\{\boldsymbol{k}_u\}_{u\in U\cap\rho([\ell])}$的改变。

1.$\{\tilde{\boldsymbol{k}}_u\}_{u\in U\cap\rho([\ell])}\leftarrow\mathcal{X}_2$。

2.$\forall u\in U\cap\rho([\ell])$：$\sum_{j\in\{2,3,\cdots,s_{\max}\}}M_{\rho^{-1}(u),j}\boldsymbol{f}_i=\tilde{\boldsymbol{k}}_u\boldsymbol{A}_u^{\mathrm{T}}+\hat{\boldsymbol{k}}_u\boldsymbol{A}_u^{\mathrm{T}}$。

Hyb_8和Hyb_7的不可区分性源于格陷门函数$\mathrm{EnLT}=(\mathrm{EnTrapGen},\mathrm{EnSamplePre})$。

Hyb_9：该游戏与Hyb_8类似，区别是在Setup阶段矩阵$\{\boldsymbol{A}_u\}$生成的改变。

$\{\boldsymbol{A}_u\}_{u\in U\cap\rho([\ell])}\leftarrow\mathbb{Z}_q^{n\times m}$

Hyb_9和Hyb_8的不可区分性源于格陷门函数$\mathrm{EnLT}=(\mathrm{EnTrapGen},\mathrm{EnSamplePre})$。

Hyb_{10}：该游戏与Hyb_9类似，区别是在Challenge阶段挑战密文中向量$\{\hat{\boldsymbol{c}}_i\}$的改变。

1.$\{\boldsymbol{e}'_i\}_{i\in[\ell]}\leftarrow\mathcal{X}_{\mathrm{big}}^m$。

2.$\forall i\in[\ell]$：$\hat{\boldsymbol{e}}_i=-\boldsymbol{e}_i\boldsymbol{R}_{\rho(i)}+\boldsymbol{e}'_i$。

由定理1可知，Hyb_{10}和Hyb_9在选择上是不可区分的。

Hyb_{11}：该游戏与Hyb_{10}类似，区别是在Challenge阶段挑战密文的改变。

Challenge阶段：

1.$\tau\leftarrow\mathbb{Z}_q$。

2.$\{\hat{\boldsymbol{v}}'_j\}_{j\in\{2,3,\cdots,s_{\max}\}}\leftarrow\mathbb{Z}_q^n$。

3.$\{\boldsymbol{e}'_i\}_{i\in[\ell]}\leftarrow\mathcal{X}_{\mathrm{big}}^m$。

4.$\{\boldsymbol{c}_i\}_{i\in[\ell]}\leftarrow\mathbb{Z}_q^m$。

5.$\forall u\in\rho([\ell])$：

$\hat{\boldsymbol{c}}_i=\left[\sum_{j\in\{2,3\cdots,s_{\max}\}}M_{i,j}\hat{\boldsymbol{v}}'_j\boldsymbol{B}_j\right]-\boldsymbol{c}_i\boldsymbol{R}_{\rho(i)}+\boldsymbol{e}'_i$。

6.$\mathrm{CT}=(\{\boldsymbol{c}_i\}_{i\in[\ell]},\{\hat{\boldsymbol{c}}_i\}_{i\in[\ell]},\mathrm{MSB}(\tau))$。

由LWE困难问题假设可知，Hyb_{11}和Hyb_{10}在选择上是不可区分的。

证明　对于任意敌手$\mathcal{A}$和任意$\boldsymbol{x}\in\{0,1,\cdots,11\}$。令$p_{\mathcal{A},\boldsymbol{x}}:\mathbb{N}\rightarrow[0,1]$为一个函数，对于所有$\lambda\in\mathbb{N}$，定义敌手在混合博弈游戏中胜出的概率为$p_{\mathcal{A},\boldsymbol{x}}(\lambda)$。根据$\mathrm{Hyb}_0$的定义，对于所有的$\lambda\in\mathbb{N}$，有：

$$\left|p_{\mathcal{A},x-1}(\lambda)-1/2\right|=\mathrm{Adv}_{\mathcal{A}}^{\text{LWE-CPABE, SEL-CPA}}(\lambda)$$

另外，对于所有$\lambda\in\mathbb{N}$，有$p_{\mathcal{A},11}=1/2$，因为在Hyb_{11}中的挑战密文中没有挑战者选择挑战位的信息。因此，对于所有$\lambda\in\mathbb{N}$，有：

$$\mathrm{Adv}_{\mathcal{A}}^{\text{LWE-CPABE}}(\lambda)\leqslant\sum_{x\in[11]}\left|p_{\mathcal{A},x-1}(\lambda)-p_{\mathcal{A},x}(\lambda)\right|$$

在Hyb_0与Hyb_1中，由于向量$\{\hat{\boldsymbol{v}}_j\}_{j\in\{2,3,\cdots,s_{\max}\}}$在$\mathbb{Z}_q^n$上是均匀独立分布的，矩阵$\{\boldsymbol{B}_j\}_{j\in\{2,3,\cdots,s_{\max}\}}$在$\mathbb{Z}_q^{m\times n}$上是均匀独立分布的，因此$\{\hat{\boldsymbol{v}}_j\boldsymbol{B}_j\}_{j\in\{2,3,\cdots,s_{\max}\}}$在$\mathbb{Z}_q^m$也是均匀独立分布的，进而得出对于任意的敌手$\mathcal{A}$，有$p_{\mathcal{A},0}(\lambda)=p_{\mathcal{A},1}(\lambda)$。

同理分析可知，在Hyb_1与Hyb_2中，$p_{\mathcal{A},1}(\lambda)=p_{\mathcal{A},2}(\lambda)$。

由于$\mathrm{EnLT}=(\mathrm{EnTrapGen},\mathrm{EnSamplePre})$满足剩余哈希定理，因此在$\mathrm{Hyb}_3$到$\mathrm{Hyb}_{10}$中，对于任意敌手$\mathcal{A}$，存在一个可忽略函数$\mathrm{negl}_i(\cdot)$，使得对于所有的$\lambda\in\mathbb{N}$，有：$\left|p_{\mathcal{A},i-1}(\lambda)-p_{\mathcal{A},i}(\lambda)\right|\leqslant\mathrm{negl}_i(\cdot)$。

又由于LWE困难问题假设成立，因此对于任意PPT敌手$\mathcal{A}$，存在一个可忽略函数$\mathrm{negl}_{11}(\cdot)$，使得对于所有的$\lambda\in\mathbb{N}$，满足：$\left|p_{\mathcal{A},10}(\lambda)-p_{\mathcal{A},11}(\lambda)\right|\leqslant\mathrm{negl}_{11}(\cdot)$。

由此可知，敌手$\mathcal{A}$在混合博弈游戏中的优势为0。证毕。

4.3 链上安全性分析

本节将介绍常见的区块链攻击模型及本文方案如何抵抗这些典型攻击。

合谋攻击：在分布式体系中，攻击者通过多个秘密集合反向计算出授权方的主密钥或其他用户的用户属性私钥。在本文方案中，每个用户属性私钥在生成时会生成一个均匀独立分布的随机向量$\hat{t}\leftarrow\mathcal{X}_1$，任意的用户属性私钥的随机向量均不同，因此该用户属性私钥对于任何人都是信息论隐藏的，无法实现合谋攻击。

中间人攻击：中间人攻击是指攻击者在通信方两端分别建立独立联系，交换其所收到的数据，监听或篡改信息。在本文方案中，各节点间所有的通信均以交易的方式进行，交易由发起方利用其区块链私钥进行签名，返回的秘密数据通过对方公钥进行加密，中间人无法通过篡改地址或伪造签名来通过验证。因此，本文方案可以很好地防止中间人攻击。

链接攻击：链接攻击是指攻击者通过链接同一地址的多条交易查找用户的隐私数据。在本文方案中，用户属性相关授权过程可由用户自己决定，用户可以选择公开其身份属性，也可以隐藏身份信息以保护隐私。此外，相关数据在链上均为密文，安全性通过算法安全性得到保证，攻击者无法获取用户相关信息，做到抗链接攻击。

4.4 性能对比分析

通过对比本文方案与文献[5]方案的功能特性，分析本文方案在数据共享上的优缺点，如表1所示。

表1 不同方案的性能对比分析

Table 1 Performance comparison and analysis of different schemes

特征	文献[5]方案	本文方案
抗量子攻击	×	√
可证明安全	非绝对安全	绝对安全
安全类型	平均困难	最高困难
困难问题	q-PBDHE	Lattice
计算复杂性	模指运算、双线性映射等	加法运算

文献[5]由于采用q-PBDHE困难问题假设，即无法在多项式时间内破解私钥和对单向函数求逆，以可以忽略的概率被破解，但随着量子计算的不断发展，这些困难问题假设将会面临被破解的风险，因此基于此类困难问题所构造的密码学方案是非绝对安全的，但本文所构造的LWE-CPABE方案可以得到绝对的安全性证明。此外，本文的LWE-CPABE方案是基于最高困难的安全类型，其他代数结构中均为平均困难的安全类型。在该安全类型中，若破解密码算法，则需要解决最高情况的困难问题。最后，文献[5]所构造的CPABE方案在计算上需要乘法运算、模指数运算和双线性映射等开销较大的运算，而本文方案则只需进行开销较小的加法运算，极大地提高了运算效率。

另外，通过对比本文方案和文献[26]方案的功能特性，分析本文方案在数据共享上的优缺点，结果如表2所示。

表2 不同方案的功能对比分析

Table 2 Functional comparison and analysis of different schemes

特征	文献[26]方案	本文方案
策略更新	无策略更新	数据拥有者更新访问控制矩阵
适用于区块链	否	是
公共数据验证	无	交易验证合约
密钥溯源	无	支持永久溯源

在文献[26]方案中，若数据使用者群体发生改变，则需要数据使用者重新生成访问控制矩阵并对明文数据进行重新加密。而在本文方案中，增加了策略撤销与更新算法，当数据使用者集合发生改变时，数据拥有者仅需生成新的访问控制矩阵即可实现对密文访问控制策略的变更。同时，通过策略撤销交易即可实现原有访问策略的撤销，有效地减少了计算代价和存储代价。另外，本文方案支持公共数据（如密文、公钥等）的共识验证，可有效保证公共数据的安全性、完整性与来源真实性。在基于密码学的数据共享方案中，其安全性依赖于密钥的安全性，而密钥盗版及滥用问题一直是属性基加密中难以解决的问题。因此，在本文方案中，利用格式化的交易结构、改进的密钥生成算法、严格的密钥申请交易和密钥传递交易，可实现密钥流转的全过程行为记录，实现快速、准确的密钥相关行为追溯。因此，对比文献[26]方案，本文方案更适用于区块链数据共享。

4.5 实验仿真分析

本节主要针对方案的实现性能进行分析。实验采用一台主机（Intel Core i7-8750H CPU @2.20 GHz,8.0 GB RAM,Win10操作系统），并利用PBC密码库、PALISADE密码库和编程语言C++来构建实验框架。在对性能指标进行选择时，本文方案并未对区块链网络的交易流程进行改动，只是将网络中上链的数据采用LWE-CPABE进行加密，不会影响到区块链网络的运行效率。因此，本文首先对LWE-CPABE方案的性能指标进行评估。

在实验中，明文数据设置为308 Byte。因为本文方案无需进行模指数、双线性映射等复杂运算，仅需要进行加法运算，所以在各阶段的时间代价均明显优于文献[5]方案。

如图3所示，系统初始化时间与系统属性数量呈线性增长关系。该阶段文献[5]方案时间代价增长率明显大于本文方案，即随着属性数量的增加，本文方案在分布式数据共享和访问控制方面更具优势。

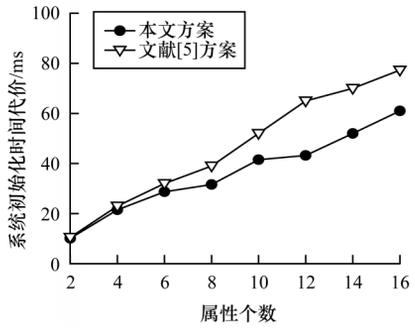

图3　不同方案的系统初始化时间

Fig.3　System initialization time of different schemes

如图4所示，随着系统中属性的不断增加，本文方案中数据拥有者在链下加密所花费的时间明显少于文献[5]的方案，其原因是在以文献[5]方案为代表的传统属性基加密方案中需要复杂的双线性配对运算和指数运算，而本文方案仅需加法运算，因此，将本文LWE-CPABE方案应用于区块链数据共享，将对系统的整体效率有极大的提升。

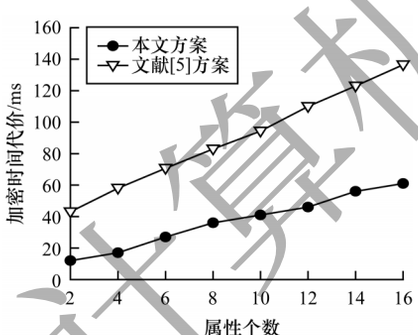

图4　不同方案的加密时间

Fig.4　Encrypt time of different schemes

如图5所示，在密钥生成阶段，随着属性的不断增加，本文方案明显优于文献[5]的方案，在进行多用户、多属性集合的密钥生成时，本文方案具有更强的实用性。

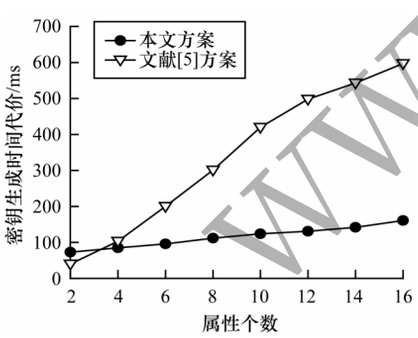

图5　不同方案的密钥生成时间

Fig.5　Key generation time of different schemes

如图6所示，在解密阶段，本文方案在0~2 ms左右远低于文献[5]方案，对于分布式系统的整体效率有非常大的提升，因此更适合区块链数据共享。为完整模拟整个策略更新过程，本文实验利用1台主机4个节点并采用C++编写的PBFT共识算法对数据流转操作进行模拟。访问控制策略更新过程可分解为策略生成、策略更新和策略上链3个步骤。通过模拟本文算法步骤得到各部分时间代价如图7所示，当更新算法的属性个数依次为2、4、6、8、12、14和16时，策略生成、更新和上链时间代价总和维持在1 500 ms以内。

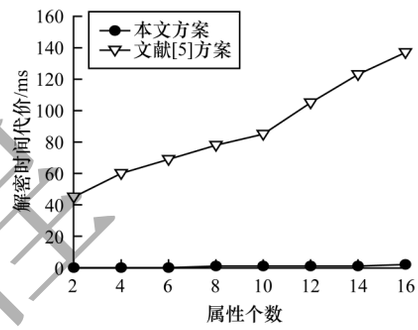

图6　不同方案的解密时间

Fig.6　Decrypt time of different schemes

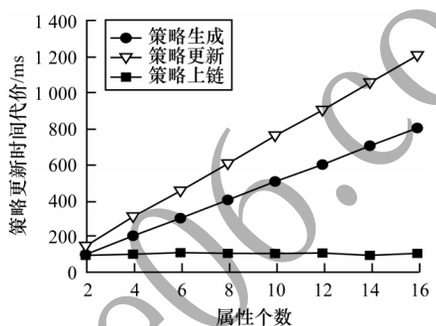

图7　策略更新时间

Fig.7　Policy update time

如图8所示，在模拟交易数量与交易响应时间及TPS的关系时，测试对象为从区块链网络中随机挑选的一个节点，测试内容为调用CITA SDK生成交易与交易信息查询，并发数条件分别为200~800。在性能测试时，单节点保持较高的响应速度和TPS。在400~700并发数下，交易生成和验证时间保持在14 s内，TPS为每秒80条以上。因此，本文方案可以实现区块链上数据访问控制策略的快速更新，且拥有较快的交易生成及验证速度，可以提供高性能的服务。

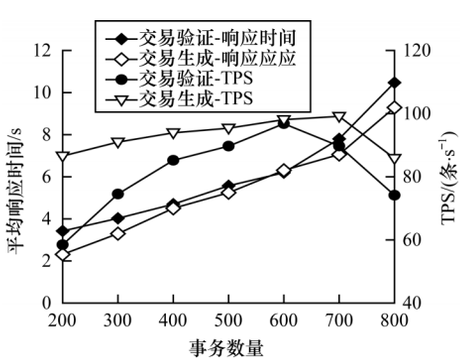

图8　交易平均响应时间与TPS

Fig.8　Average transaction response time and TPS

5 结束语

区块链上的隐私保护技术是数据安全共享的重要因素，随着量子计算的快速发展，传统的以数论为基础的公钥密码体系无法抵抗量子攻击。因此，本文将区块链技术与格属性基加密算法有效融合，提出一种基于LWE-CPABE的区块链数据共享方案。通过对CPABE方案进行改进，给出可更新策略的抗量子攻击属性基加密算法，以实现数据的动态保护。在此基础上，设计区块链格式化交易结构实现基于格的CPABE细粒度访问控制，在保证算法抗量子攻击特性的同时，确保过程的可追溯性。实验结果表明，与传统CPABE算法相比，基于格的算法可以明显提升计算速度。下一步将研究区块链上基于LWE-CPABE的分布式密钥生成方案及策略隐藏，以实现更加安全高效的基于属性基加密的分布式数据共享。

参考文献

[1] 黄穗，陈丽炜，范冰冰. 基于CP-ABE和区块链的数据安全共享方法[J]. 计算机系统应用，2019，28(11)：79-86.
HUANG S，CHEN L W，FAN B B. Data security sharing method based on CP-ABE and blockchain[J]. Computer Systems & Applications，2019，28(11)：79-86. (in Chinese)

[2] 王秀利，江晓舟，李洋. 应用区块链的数据访问控制与共享模型[J]. 软件学报，2019，30(6)：1661-1669.
WANG X L，JIANG X Z，LI Y. Model for data access control and sharing based on blockchain[J]. Journal of Software，2019，30(6)：1661-1669. (in Chinese).

[3] 杨亚涛，蔡居良，张筱薇，等. 基于SM9算法可证明安全的区块链隐私保护方案[J]. 软件学报，2019，30(6)：1692-1704.
YANG Y T，CAI J L，ZHANG X W，et al. Privacy preserving scheme in block chain with provably secure based on SM9 algorithm[J]. Journal of Software，2019，30(6)：1692-1704. (in Chinese)

[4] 田有亮，杨科迪，王缵，等. 基于属性基加密的区块链数据溯源算法[J]. 通信学报，2019，40(11)：101-111.
TIAN Y L，YANG K D，WANG Z，et al. Algorithm of blockchain data provenance based on ABE[J]. Journal on Communications，2019，40(11)：101-111. (in Chinese)

[5] FAN Y K，LIN X D，LIANG W，et al. TraceChain：a blockchain-based scheme to protect data confidentiality and traceability[J]. Software：Practice and Experience，2022，52(1)：115-129.

[6] WANG H，SONG Y J. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain[J]. Journal of Medical Systems，2018，42(8)：152.

[7] ZHANG Y R，HE D B，CHOO K K R. BaDS：blockchain-based architecture for data sharing with ABS and CP-ABE in IoT[J]. Wireless Communications and Mobile Computing，2018，18：1-9.

[8] SAHAI A，WATERS B. Fuzzy identity-based encryption[C]// Proceedings of Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin，Germany：Springer，2005：457-473.

[9] GOYAL V，PANDEY O，SAHAI A，et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. New York，USA：ACM Press，2006：89-98.

[10] WATERS B. Ciphertext-policy attribute-based encryption：an expressive，efficient and provable secure realization[C]// Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Washington D. C.，USA：IEEE Press，2011：53-70.

[11] 王悦，樊凯. 隐藏访问策略的高效CP-ABE方案[J]. 计算机研究与发展，2019，56(10)：2151-2159.
WANG Y，FAN K. Effective CP-ABE with hidden access policy[J]. Journal of Computer Research and Development，2019，56(10)：2151-2159. (in Chinese)

[12] ZHOU Z，HUANG D，WANG Z. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption[J]. IEEE Transactions on Computers，2015，64(1)：126-138.

[13] YANGLI C，LINGLING S，GNEG Y. Attribute-based access control for multi-authority systems with constant size ciphertext in clouds[J]. China Communications，2016，13(2)：146-162.

[14] PHUONG T V X，YANG G M，SUSILO W. Hidden ciphertext policy attribute-based encryption under standard assumptions[J]. IEEE Transactions on Information Forensics and Security，2016，11(1)：35-45.

[15] RUJ S，STOJMENOVIC M，NAYAK A. Decentralized access control with anonymous authentication of data stored in clouds[J]. IEEE Transactions on Parallel and Distributed Systems，2014，25(2)：384-394.

[16] BETHENCOURT J，SAHAI A，WATERS B. Ciphertext-policy attribute-based encryption[C]//Proceedings of 2007 IEEE Symposium on Security and Privacy. Washington D. C.，USA：IEEE Press，2007：321-334.

[17] OKAMOTO T，TAKASHIMA K. Fully secure unbounded inner-product and attribute-based encryption[C]//Proceedings of Advances in Cryptology-ASIACRYPT'12. Washington D. C.，USA：IEEE Press，2012：349-366.

[18] GORBUNOV S，VAIKUNTANATHAN V，WEE H. Attribute-based encryption for circuits[C]//Proceedings of the 45th Annual ACM Symposium on Theory of Computing. New York，USA：ACM Press，2013：545-554.

[19] HOHENBERGER S，WATERS B. Online/offline attribute-based encryption[C]//Proceedings of International Conference on Theory and Application of Cryptology. New York，USA：ACM Press，2014：293-310.

[20] ROUSELAKIS Y，WATERS B. Practical constructions and new proof methods for large universe attribute-based encryption[C]// Proceedings of 2013 ACM SIGSAC Conference on Computer & Communications Security. New York，USA：ACM Press，2013：463-474.

[21] AJTAI M. Generating hard instances of lattice problems[C]// Proceedings of STOC'96. Washington D. C.，USA：IEEE Press，1996：99-108.

[22] REGEV O. On lattices，learning with errors，random linear-codes，and cryptography[J]. Journal of the ACM，2009，48(5)：1-40.

[23] 钱心缘，吴文渊. 基于R-SIS和R-LWE构建的IBE加密方案[J]. 计算机科学，2021，48(6)：315-323.
QIAN X Y，WU W Y. Identity-based encryption scheme based on R-SIS/R-LWE[J]. Computer Science，2021，48(6)：315-323. (in Chinese)

（下转第175页）

（上接第168页）

[24] 周艺华，董松寿，杨宇光. 标准模型下基于格的身份代理部分盲签名方案[J]. 信息网络安全，2021，21(3)：37-43.
ZHOU Y H，DONG S S，YANG Y G. A lattice-based identity-based proxy partially blind signature scheme in the standard model[J]. Netinfo Security，2021，21(3)：37-43.（in Chinese）

[25] 张彦华，胡予濮，刘西蒙，等. 格上本地验证者撤销属性基群签名的零知识证明[J]. 电子与信息学报，2020，42(2)：315-321.
ZHANG Y H，HU Y P，LIU X M，et al. Zero-knowledge proofs for attribute-based group signatures with verifier-local revocation over lattices[J]. Journal of Electronics & Information Technology，2020，42(2)：315-321.（in Chinese）.

[26] DATTA P，KOMARGODSKI I，WATERS B. Decentralized multi-authority abe for DNFs from LWE[C]//Proceedings of Advances in Cryptology-EUROCRYPT'21. Washington D. C.，USA：IEEE Press，2021：145-158.

编辑　索书志