基于格的细粒度访问控制内积函数加密方案

侯金秋[1)] 彭长根[1),2)] 谭伟杰[1),2)] 叶延婷[1)]

[1)](贵州大学计算机科学与技术学院公共大数据国家重点实验室 贵阳 550025)

[2)](贵州大学贵州省大数据产业发展应用研究院 贵阳 550025)

摘 要 函数加密作为一种多功能的新型公钥加密原语,因其能实现细粒度的密文计算,在云存储中有着广阔的应用前景,受到研究者们的广泛研究.因此,将数据的访问权限控制有机地融合到加解密算法中,实现"部分加解密可控、按需安全计算"是一个非常有意义的探索方向.但现有函数加密方案无法精细控制发送者权限且使用了较复杂的理论工具(如不可区分性混淆、多线性映射等),难以满足一些特定应用场合需求.面对量子攻击挑战,如何设计抗量子攻击的特殊、高效的函数加密方案成为一个研究热点.内积函数加密是函数加密的特殊形式,不仅能够实现更复杂的访问控制策略和策略隐藏,而且可以有效地控制数据的"部分访问",提供更细粒度的查询,在满足数据机密性的同时提高隐私保护.针对更加灵活可控按需安全计算的难点,该文基于格上 Learning with errors 困难问题提出一种基于身份的细粒度访问控制内积函数加密方案.该方案首先将内积函数与通过原像抽样算法产生的向量相关联,生成函数私钥以此控制接收方的计算能力.其次,引入一个第三方(访问控制中心)充当访问控制功能实施者,通过剩余哈希引理及矩阵的秩检验密文的随机性,完成对密文的重随机化以实现控制发送者权限的目的.最后,接收者将转换后的密文通过内积函数私钥解密,仅计算得到关于原始消息的内积值.理论分析与实验评估表明,所提方案在性能上有明显优势,不仅可以抵御量子攻击,而且能够控制接收者的计算权限与发送者的发送权限,在保护用户数据机密性的同时,有效实现开放环境下数据可用不可见、数据可算不可识的细粒度权限可控密文计算的目标.

关键词 访问控制加密;内积函数加密;容错学习问题;格

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2023.01172

Fine-Grained Access Control Functional Encryption for Inner Product on Lattice

HOU Jin-Qiu[1)] PENG Chang-Gen[1),2)] TAN Wei-Jie[1),2)] YE Yan-Ting[1)]

[1)](*State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang* 550025)

[2)](*Guizhou Big Date Academy, Guizhou University, Guiyang* 550025)

Abstract Functional encryption is a brand-new multi-functional public key encryption primitive that has received a lot of attention from researchers since it can produce fine-grained ciphertext computation and has a wide range of potential applications in cloud storage. For this reason, it is a very meaningful exploration direction to organically integrate the access control of data into the encryption and decryption algorithm to achieve "partial encryption and decryption controllable, on-demand security computing". However, the existing functional encryption schemes have the following problems: on the one hand, the existing functional encryption schemes cannot precisely control the sender's permissions; on the other hand, the current functional encryption schemes usually use more complex theoretical tools (such as indistinguishable confusion, multilinear map,

收稿日期:2022-09-14;在线发布日期:2023-01-17.本课题得到国家自然科学基金项目(62272124)、贵州省科技计划基金项目([2018]3001,[2018]2159,[2020]5017)、贵州省研究生科研基金项目(YJSKYJJ[2021]028)资助.**侯金秋**,博士研究生,中国计算机学会(CCF)会员,主要研究方向为数据安全、函数加密.E-mail:Jinqiu_hou@126.com.**彭长根**(通信作者),博士,教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为密码学与信息安全、大数据隐私保护等.E-mail:peng_stud@163.com.**谭伟杰**,博士,副教授,硕士生导师,中国计算机学会(CCF)会员,主要研究方向为隐私保护、信息安全.**叶延婷**,博士研究生,中国计算机学会(CCF)会员,主要研究方向为信息安全、密码学.

etc.), which is difficult to meet the requirements of some specific access control applications. Facing the challenge of quantum attack, how to design a special and efficient functional encryption scheme against quantum attackhas become one of research highlights in recent years. Besides, inner product functional encryption is the most special form of functional encryption that executes the computation for the inner product of vectors. More importantly, inner product functional encryption can not only realize more complex access control strategies and policy hiding, but also effectively control "partial access" of data, provide finer grained queries, and improve privacy protection while meeting data confidentiality. In light of the challenges posed by more adaptable and programmable on-demand security computing, this paper proposes an identity-based access control inner product functional encryption scheme based on the learning with errors problem on the lattice. First, the designed scheme associates the inner product function with the vector generated by the SamplePre algorithm, and generates the function private key to control the computing capacity of the receiver. Second, a third party (access control center) is introduced to act as the implementer of the access control function. The purpose of controlling the sender's sending authority is achieved through this access control center. What's more, the randomness of the sender's ciphertext is checked by the leftover hash lemma and the rank of the matrix. In addition, the re-randomization of the ciphertext is completed to achieve the purpose of controlling the authority of the sender. Finally, the receiver decrypts the converted ciphertext through their inner product function private key, and only calculates the inner product value of the original message after decryption. Theoretical analysis and experimental evaluation are also given in this paper, and the results show that, the proposed scheme has obvious advantages in terms of functions, which can not only resist quantum attacks, but also control the computing authority of the receiver and the sending authority of the sender. While protecting the confidentiality of user data, it effectively realizes the goal of fine-grained permission controlled ciphertext computing where data can be used and invisible, and data can be calculated and unrecognized in an open environment.

Keywords　access control encryption; inner product functional encryption; learning with errors problem; lattice

1　引　言

传统的公钥加密允许拥有私钥的用户能解密由公钥加密的密文，同时，若无私钥则无法得到关于明文的任何信息. 然而，如何对密文数据进行计算成为当下一个新问题. 特别是，在大数据计算环境下，许多应用场景需要较细粒度的访问控制. 访问控制作为解决授权用户合法访问数据的关键技术，近年来已被引入大数据领域保障数据安全共享[1]. 为适用于复杂开放的云计算环境，诸多学者关注云环境下的访问控制密码技术[2]. 函数加密克服了公钥加密所固有的"全有或全无"的访问，达到了细粒度的权限控制，而内积函数加密作为函数加密最特殊的形式，不仅可以实现更复杂的访问控制策略及策略的隐藏，而且能有效控制数据的"部分访问"，提供较细粒度的查询，在满足数据机密性的同时提高隐私保护能力，十分适用于云计算等领域. 因此，受到学者们的广泛关注，如函数隐藏的内积函数加密[3]、多客户端的内积函数加密[4]、谓词的内积函数加密[5]. 然而，现有的内积加密方案无法控制恶意发送者权限，且大都基于双线性对构造，难以抵抗量子攻击. 面对更加复杂的访问控制场景及量子计算机所带来的安全威胁，如何构造抗量子攻击的细粒度内积函数加密方案成为新挑战.

1.1　相关工作

在函数加密体制中，主密钥用来生成与某些函数(如内积函数)相关联的子密钥，解密时用户只能

得到关于明文的函数值. 函数加密的诞生最早可追溯到身份基加密[6],身份基加密是公钥加密的第一个重要推广. 随后,Sahai 等人[7]结合秘密共享[8]提出具有容错性的模糊身份加密方案,也被视为属性基加密的雏形. 后来,Goyal 等人[9]和 Bethencourt 等人[10]结合秘密共享和树形访问结构分别提出了基于密钥策略的属性密码体制和基于密文策略的属性密码体制. 为适用多用户协同访问需求,Xue 等人[11]提出属性协同访问控制加密方案. 上述方案主要是以门限秘密共享为工具构造访问控制机制,缺乏通用性和灵活性. 在身份加密和属性加密的基础上,Katz 等人[12]通过谓词运算提出了相对灵活可控的谓词加密方案,但不支持部分加解密功能. 对此,文献[13-14]给出了具备部分加解密功能的函数加密形式化定义与安全模型,能够为特定的用户提供密文上的函数计算,通过将私钥与函数相关联,使得私钥持有者解密后只能得到关于明文对应的函数值,这一新型加密体制打破了传统的公钥加密方案的"all or nothing"的局限性,实现了更为细粒度的访问控制. Goldwasser 等人[15]提出了第一个通用函数加密方案. 之后,相关学者相继对函数加密进行了优化和改进.

2015 年,Abdalla 等人[16]给出了对加密数据上的线性函数计算的内积函数加密原语,与内积谓词函数加密[17]不同的是,密文和密钥与向量相关联,解密后得到两个向量的内积,而不再是通过判断两向量的内积是否为零解密得到原始明文. 同年,Bishop 等人[18]为达到适应性安全,基于双线性映射构造了一个函数隐藏的内积加密方案. Agrawal 等人[19]基于 Learning With Errors(LWE)问题设计了一个内积函数加密方案(ALS16 方案),方案中使用了大维数矩阵,导致密钥尺寸过大. Chen 等人[20]给出了属性函数加密的形式化定义,并基于双线性群设计了一个密文策略的属性内积加密方案,然而,他们的方案只是在一个相对较弱的环境下达到了自适应安全性,即不允许敌手查询任何可以解密挑战密文的密钥. Abdalla 等人[21]基于 ALS16 方案[19]构造了支持双系统加密的属性内积函数加密方案. 方案允许敌手拥有不同属性的密钥,且密钥可以解密挑战密文,但敌手的优势随着密钥查询的数量呈线性增长,并且方案只达到了选择性安全. Pal 等人[22]首次采用通用电路作为访问结构,通过编码机制,结合属性加密及内积函数加密构造了基于属性加密的内积函数加密方案. 密文与密钥的大小仅依赖于电路的深度而不是其大小,并且达到了 co-selective 不可区分安全级别,即敌手提前提交一个挑战属性和函数并允许敌手询问挑战密文的私钥. 并将该方案扩展为 coAdp-IND 安全的基于属性的多输入内积函数加密方案. 为提高加解密效率,Mera 等人[23]首次基于格上的 Ring-LWE(RLWE)困难问题构造了一个内积函数加密方案,且方案达到了自适应安全.

然而,以上密码方案仅考虑数据接收者的访问权限,如何在访问控制机制中限制恶意发送者权限是一个新的挑战问题.

针对上述问题,Damgård 等人[24]首次提出面向信息流的访问控制加密体制,利用谓词密码严格控制发送者的发送权限和接收者的接收权限[25],提供了一种更加细粒度的分级访问控制. 同时,文章提出两个公开问题:(1)如何基于标准假设构建抗量子攻击的访问控制加密方案;(2)如何在给定有限谓词的条件下构建更有效的访问控制加密方案. Tan 等人[26]基于格上 Decision-LWE(DLWE)困难假设设计了一个支持同态运算的访问控制加密方案,解决了 Damgård 等人[24]所提的其中一个公开问题. Fuchsbauer 等人[27]基于标准配对假设构造了渐近效率的访问控制加密方案,但只支持受限谓词策略. 随后,有学者研究如何构造高效且具备任意策略的访问控制加密方案[28-30]. 此外,有学者研究访问控制加密的功能扩展,相继提出可验证访问控制加密[31]、跨域访问控制加密[32]、群组访问控制加密[33]、无可信中心访问控制加密[34].

但这些访问控制加密方案仅针对数据,尚未考虑对函数计算进行加解密控制,因此,如何基于格上标准困难假设构造更加细粒度的访问控制函数加密方案是一个非常具有挑战的问题.

1.2 本文贡献

(1)本文提出了访问控制内积函数加密(Access Control Inner Product Functional Encryption, ACIPFE),不仅可以控制发送方与接收方的通信权限,而且允许接收方能够进行内积运算.

(2)本文设计了一个格上基于身份的 ACIPFE 方案,将用户身份映射为一个向量,通过矩阵的秩检测密文的随机性,完成对发送者密文的检测,控制恶意发送方的发送权限.

(3)本文在 LWE 困难假设下,基于标准模型严格证明了 ACIPFE 方案的安全性,并通过理论和实验分析了 ACIPFE 的效率.

2 基础知识

表 1 给出了相关符号的说明，并参照文献[35-38]，介绍本文所用到的格理论知识及相关算法.

表 1　符号说明表

符号	符号说明
$\mathbb{Z}$	整数环
$\mathbb{R}$	实数域
$\boldsymbol{A}\in\mathbb{Z}^{m\times n}$	一个整数环上 $m\times n$ 的矩阵
$\boldsymbol{a}\in\mathbb{Z}^m$	一个整数环上长度为 m 的向量
$\boldsymbol{e}\leftarrow\Psi^m$	从噪声分布 Ψ^m 中随机抽样一个长度为 m 的向量
$\mathbb{Z}_p$	模 p 的剩余类环
$\|\cdot\|$	欧几里得范数

定义 1.　格. 给定 n 维空间中一组无关向量，其整系数组合构成的集合称为格，即：

$$L(\boldsymbol{B})=L(\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n)=\left\{\sum a_i\boldsymbol{b}_i\,|\,a_i\in\mathbb{Z}\right\},$$

其中，矩阵 $\boldsymbol{B}=(\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n)\in\mathbb{Z}^{m\times n}$ 称为格 $L(\boldsymbol{B})$ 一个基，n 称为格的秩，m 称为格的维数. 当 $m=n$ 时，称 $L(\boldsymbol{B})$ 为 m 维满秩格.

定义 2.　q 模格. 给定正整数 $q,m,n\in\mathbb{Z}$，q 是素数，矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{m\times n}$，可定义如下两个 n 维的 q 模格：

$$L_q(\boldsymbol{A})=\{\boldsymbol{x}\in\mathbb{Z}^n\,|\,\exists\boldsymbol{y}\in\mathbb{Z}^m,\boldsymbol{A}^{\mathrm{T}}\boldsymbol{y}=\boldsymbol{x}\bmod q\},$$

$$L_q^{\perp}(\boldsymbol{A})=\{\boldsymbol{x}\in\mathbb{Z}^n\,|\,\boldsymbol{A}\boldsymbol{x}=0\bmod q\}.$$

给定向量 $\boldsymbol{u}$，定义 m 维向量空间

$$L_q^{\boldsymbol{u}}(\boldsymbol{A})=\{\boldsymbol{x}\in\mathbb{Z}^n\,|\,\boldsymbol{A}\boldsymbol{x}=\boldsymbol{u}\bmod q\},$$

若 $z\in L_q^{\boldsymbol{u}}(\boldsymbol{A})$，则有 $L_q^{\boldsymbol{u}}(\boldsymbol{A})=L_q^{\perp}(\boldsymbol{A})+z$，可知，$L_q^{\boldsymbol{u}}(\boldsymbol{A})$ 由 $L_q^{\perp}(\boldsymbol{A})$ 平移得到.

定义 3.　格上离散高斯分布. 令 $\sigma>0$，对于向量 $\boldsymbol{c}\in\mathbb{R}^m$ 和格 L，定义

$$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(-\pi\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{\sigma^2}\right),$$

$$\rho_{\sigma,\boldsymbol{c}}(L)=\sum_{\boldsymbol{x}\in L}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x}).$$

则格 L 上，以 $\boldsymbol{c}$ 为中心的离散高斯分布为

$$D_{L,\sigma,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(L)}.$$

定理 1.　TrapGen算法. 输入 $q\geq2,m\geq5n\log q$，存在一个概率多项式时间算法 TrapGen，使其输出一个矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和格 $L_q^{\perp}(\boldsymbol{A})$ 上的一个短基 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}_q^{m\times m}$，且 $\|\boldsymbol{T}_{\boldsymbol{A}}\|\geq O(\sqrt{n\log q})$.

定理 2.　SamplePre 算法. 给定模数 q，高斯参数 σ 和一个向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$，输入一个矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 及其陷门 $\boldsymbol{T}_{\boldsymbol{A}}$，该算法输出一个向量 $\boldsymbol{s}\leftarrow\mathrm{SamplePre}(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\sigma,\boldsymbol{u},q)$ 且满足 $\boldsymbol{A}\boldsymbol{s}=\boldsymbol{u}(\bmod q)$，抽样的原像 $\boldsymbol{s}$ 与格上高斯分布 $D_{\mathbb{Z}^m,\sigma}$ 不可区分.

引理 1.　给定正整数 n 和 q，其中 q 是素数，令 $m\geq2n\log_2 q$，对于一个矩阵 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$，$\sigma\geq\omega(\sqrt{\log_2 m})$，$\boldsymbol{s}\leftarrow D_{\mathbb{Z}^m,\sigma}$，则 $\boldsymbol{u}=\boldsymbol{A}\boldsymbol{s}$ 的分布统计接近于 $\mathbb{Z}_q^n$ 上的均匀分布.

引理 2.　给定格 $L,\sigma\in\mathbb{R},\boldsymbol{v}_i\in\mathbb{Z}^n,i=1,2,\cdots,k$. 从高斯分布 $D_{L+\boldsymbol{v}_i,\sigma}$ 中抽取两两线性无关的随机变量 X_i. 对于向量 $\boldsymbol{c}=(c_1,c_2,\cdots,c_k)\in\mathbb{Z}^k$，定义 $g:=\gcd(c_1,c_2,\cdots,c_k)$，$v:=\sum_{i=1}^{k}c_i\boldsymbol{v}_i$. 对于一个可忽略的 ε，$\sigma>\|\boldsymbol{c}\|\cdot\eta_\varepsilon(L)$，有 $Z=\sum_{i=1}^{k}c_iX_i$ 的分布统计上接近于高斯分布 $D_{gL+v,\|\boldsymbol{c}\|\sigma}$.

引理 3.　Leftover hash lemma. 给定一个素数 $q>2,m>(n+1)\log q+\omega(\log n)$，令矩阵 $\boldsymbol{S}\leftarrow\{-1,0,1\}^{m\times k}$，随机选择两个矩阵 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{B}\leftarrow\mathbb{Z}_q^{n\times k}$. 则对于向量 $\boldsymbol{e}\in\mathbb{Z}_q^m$，$(\boldsymbol{A},\boldsymbol{A}\boldsymbol{S},\boldsymbol{S}^{\mathrm{T}}\boldsymbol{e})$ 的分布与 $(\boldsymbol{A},\boldsymbol{B},\boldsymbol{S}^{\mathrm{T}}\boldsymbol{e})$ 的分布统计上不可区分.

定义 4.　LWE. 输入整数 n,m，素数 q 和一个噪声分布 $\boldsymbol{e}\leftarrow\Psi^m$，LWE 问题即给定矩阵 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$，$\boldsymbol{s}\leftarrow\mathbb{Z}_q^n,\boldsymbol{u}\leftarrow\mathbb{Z}_q^m$，区分两个分布 $(\boldsymbol{A},\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e})$ 与 $(\boldsymbol{A},\boldsymbol{u})$ 是不可区分的. 搜索型 LWE 问题：寻找一个向量 $\boldsymbol{s}$，使其满足 $\boldsymbol{u}=\boldsymbol{A}\boldsymbol{s}+\boldsymbol{e}\bmod q$；判定型 LWE 问题：给定 $(\boldsymbol{A},\boldsymbol{u})$，判定 $\boldsymbol{u}$ 是从 $\mathbb{Z}_q^n$ 上随机均匀选取的，还是由 $\boldsymbol{u}=\boldsymbol{A}\boldsymbol{s}+\boldsymbol{e}\bmod q$ 计算得到的.

3 访问控制内积函数加密

3.1 系统模型

为了能够控制恶意发送方权限且在保护隐私的同时允许对数据执行简单统计计算，本文构建了一种新型访问控制内积函数加密模型，如图 1 所示. 该模型主要有四个实体：密钥管理中心、发送者、访问控制中心以及接收者. 其中，访问控制中心的作用是按照访问控制策略对发送者的密文进行过滤. 该访问控制策略将一个系统中的用户划分为多个级别，从低到高依次为“普通”、“机密”和“绝密”，规定高级别用户不能向低级别用户发送消息，且低权限用户不能读取高权限用户的信息. 过滤是指访问控制中心通过 Acc 算法阻止低权限用户或恶意发送者向不满足访问控制策略的非法用户发送消息，且在过滤过程中仅仅知晓收到的密文长度，而对其他信息一无所知. 具体过程如下：首先，密钥管理中心执行 $\mathrm{Setup}(1^\lambda,P,\mathcal{X},\mathcal{Y})$ 算法，生成公共参数和主私钥，然

后执行 KeyGen($pp,msk,id,\boldsymbol{y}$)算法产生公私钥对发送给用户(发送者/接收者);其次,发送者利用公钥将消息加密后发送给访问控制中心,访问控制中心收到该密文后执行 Acc($\boldsymbol{c}$)算法将密文过滤并广播,以实现授权用户只能解密对应的密文;最后,满足访问控制策略的接收者拿到转换后的密文,使用自己的函数私钥进行解密,得到关于明文的内积值$\langle \boldsymbol{x},\boldsymbol{y}\rangle$.

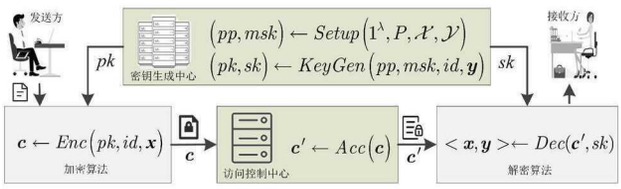

图 1 访问控制内积函数加密模型

3.2 访问控制内积函数加密定义

一个访问控制内积函数加密方案 ACIPFE=(Setup,KeyGen,Enc,Acc,Dec)由以下 5 个概率多项式时间(Probabilistic Polynomial Time,PPT)算法构成. 其中,安全参数为 λ,消息空间为$\mathcal{X}:=\{0,1,\cdots,M(\lambda)-1\}^l$,谓词空间为$\mathcal{Y}:=\{0,1,\cdots,V(\lambda)-1\}^l$. 在 ACIPFE 方案中,密文 $\boldsymbol{c}$ 与一个消息向量$\boldsymbol{x}\in\mathcal{X}$及一个身份 id 相关联,私钥 sk 与一个谓词向量$\boldsymbol{y}\in\mathcal{Y}$及身份 id 相关联,当身份匹配时,接收者使用私钥解密后得到内积值$\langle \boldsymbol{x},\boldsymbol{y}\rangle$,$K=lMV$.

(1) Setup($1^{\lambda},P,\mathcal{X},\mathcal{Y}$). 输入安全参数 1^{λ},访问控制策略 $P:\{0,1\}^l\times\{0,1\}^l\rightarrow\{0,1\}$,消息空间$\mathcal{X}$及谓词空间$\mathcal{Y}$. 算法返回公共参数 pp 及主私钥 msk.

(2) KeyGen($pp,msk,id,\boldsymbol{y}$). 输入公共参数 pp,主私钥 msk,发送者的身份 id_i、接收者的身份 id_j,以及向量 $\boldsymbol{y}\in\mathcal{Y}$,输出公钥 pk,私钥 sk.

(3) Enc($pk,id,\boldsymbol{x}$). 输入公钥 pk 及消息向量$\boldsymbol{x}\in\mathcal{X}$,输出原始密文 $\boldsymbol{c}$.

(4) Acc($\boldsymbol{c}$). 输入原始密文 $\boldsymbol{c}$,输出重随机化后的密文 $\boldsymbol{c}'$.

(5) Dec($\boldsymbol{c}',sk$). 输入重随机化密文 $\boldsymbol{c}'$及接收者的私钥 sk,输出内积值$\langle \boldsymbol{x},\boldsymbol{y}\rangle$.

注:(1) 对于$(i,j)\in[l]\times[l]$,如果 $P(i,j)=1$,那么发送者 id_i可以向接收者 id_j写入(发送),否则无法向用户 id_j写入;

(2) 如果 $i=0$ or $j=0$,表示非法用户,0 代表发送者或接收者没有权限,即 $P(0,j)=0=P(i,0)$,$i,j\in[l]$,则从密文空间中随机选择一个密文;

(3) $i=l+1$ 代表策略控制中心,不能接收任意用户 $\forall i\in[l]$的消息但允许发送,即 $P(l+1,j)=1$且 $P(i,l+1)=0$.

正确性. 对于所有的 $\boldsymbol{x}\in\mathcal{X},\boldsymbol{y}\in\mathcal{Y},(i,j)\in[l]\times[l]$,使得 $P(i,j)=1$,若满足以下条件,则证明该访问控制内积函数加密方案是正确的,即:

$\Pr[\mathrm{Dec}(\mathrm{Acc}(\mathrm{Enc}(pk,id,\boldsymbol{x})),sk)\neq\langle \boldsymbol{x},\boldsymbol{y}\rangle]\leq negl(\lambda)$.

3.3 访问控制内积函数加密安全模型

针对访问控制内积函数方案 ACIPFE 的安全模型,假设敌手具有概率多项式时间的计算能力,我们主要考虑两个方面:(1) 如果接收者是敌手,则需满足 IND-sID-CPA 安全,保证只有满足访问控制策略的接收者才能正确解密;(2) 如果发送者是敌手,则需满足 Sanitizability 安全,使得非法用户不能伪造密文进行发送. 因此,基于上述分析,根据敌手的攻击能力,给出 ACIPFE 的形式化安全定义.

定义 5. IND-sID-CPA. 该安全模型通过挑战者$\mathcal{C}$与敌手$\mathcal{A}$之间的游戏展示密文间的不可区分性,主要包括以下 6 个阶段.

初始化:敌手向挑战者宣布一个要挑战的身份 id^* 和两个挑战消息向量 $\boldsymbol{x}_0^*,\boldsymbol{x}_1^*,\boldsymbol{x}_0^*\neq\boldsymbol{x}_1^*$.

系统设置:挑战者生成并发布公钥.

阶段 1:敌手向挑战者发起私钥询问,但不允许对同一个身份 id 进行重复询问,确保一个身份 id 与一个消息向量相关联;若 $id=id^*$,则应满足$\langle \boldsymbol{x}_0^*-\boldsymbol{x}_1^*,\boldsymbol{y}\rangle=0$.

阶段 2:与阶段 1 相同.

挑战:挑战者选择 $\beta\in\{0,1\}$,生成挑战密文并发送给敌手.

猜测:敌手输出对 β 的猜测 β'. 若$\langle \boldsymbol{x}_\beta^*,\boldsymbol{y}\rangle=\langle \boldsymbol{x}_0^*,\boldsymbol{y}\rangle$,敌手输出 0,否则,输出 1.

定义敌手$\mathcal{A}$赢得该 IND-sID-CPA 游戏的优势为

$$Adv_{\text{IND-sID-CPA}}=|\Pr[\beta'-\beta]-1/2|\leq negl(\lambda).$$

对于所有的概率多项式时间敌手$\mathcal{A}$赢得该游戏的优势是可忽略的,则 ACIPFE 方案是 IND-sID-CPA 安全的.

定义 6. Sanitizability 安全. 针对恶意的发送者,访问控制中心必须对发送者的密文进行过滤(重随机化),即发送方只能按照访问控制策略所允许通信的接收方发送密文. 该性质要求给定两个密文,一个为敌手选择的,另一个为密文空间随机挑选的,通过 Acc 算法过滤后的密文与诚实地执行加密算法 Enc($pk,id,\boldsymbol{x}$)所都得到的密文在计算上保持不可区分,即只要敌手没有私钥,则无法区分两个密文. Q_S表示对$\mathcal{O}_S(j,id)$的所有询问 q,$q=(j,id_j)$构成

的集合；I_S表示对Q_S询问中发送者构成的集合，即$(i,id_i)\in Q_S, i\in[l]$；Q表示对$\mathcal{O}_S(j,id)$和$\mathcal{O}_R(j,id)$的所有密钥询问构成的集合；J表示对Q询问中接收者构成的集合，即$(j,id_j)\in Q, j\in[l]$.

挑战者$\mathcal{C}$与敌手$\mathcal{A}$之间的游戏如下：

系统设置：挑战者$\mathcal{C}$生成并发布公钥.

询问：敌手$\mathcal{A}$向挑战者$\mathcal{C}$发起私钥询问，但不允许对同一个身份id进行重复询问，确保一个身份id与一个消息向量相关联；若$id=id^*$，则应满足$\langle \boldsymbol{x}_0^*-\boldsymbol{x}_1^*,\boldsymbol{y}\rangle=0$.

挑战：敌手$\mathcal{A}$向挑战者$\mathcal{C}$宣布其攻击目标(c,i')，如果满足以下条件，那么敌手$\mathcal{A}$赢得 Sanitizability 游戏，即：

(1) $(l+1,id_{i\to j})\notin Q$；

(2) $i'\in I_S\cup\{0\}, i'\in\{1,0\}$；

(3) $\forall i\in I_S\cup\{0\}, j\in J, P(i,j)=0$.

注：上述条件表明对于某一用户$i'\in I_S\cup\{0\}$，没有权限向接收者$j\in J$发送消息. 对于所有的概率多项式时间敌手$\mathcal{A}$赢得该 Sanitizability 安全游戏的优势为

$$Adv_{\text{San}}=\left|\Pr[\mathcal{A}wins\ Exp_{\text{ACIPFE}}^{\text{Acc}}(\lambda)]-\frac{1}{2}\right|.$$

若敌手$\mathcal{A}$的优势是可忽略的，则称该 ACIPFE 加密方案满足 Sanitizability 安全性.

4　方案构造

本方案，安全参数为λ，消息空间为$\mathcal{X}_\lambda=\{0,1,\cdots,M(\lambda)-1\}^l$，谓词空间为$\mathcal{Y}_\lambda=\{0,1,\cdots,V(\lambda)-1\}^l$，假设对于任意的向量$\boldsymbol{y}\in\mathcal{Y}_\lambda, \boldsymbol{x}\in\mathcal{X}_\lambda$，有$|\langle\boldsymbol{x},\boldsymbol{y}\rangle|<K, K=lMV$. 为控制发送方的通讯权限，访问控制中心采用 Acc($\boldsymbol{c}$)算法将原始密文$\boldsymbol{c}$重随机，如果发送方被禁止向接收者发送消息，Acc($\boldsymbol{c}$)算法将对密文$\boldsymbol{c}$产生主导影响，而接收者只能获得一个随机的明文；如果允许发送方与接收方通信，那么 Acc($\boldsymbol{c}$)算法对密文$\boldsymbol{c}$没有影响，接收方可以解密对应的密文并获得关于原始明文的内积值$\langle\boldsymbol{x},\boldsymbol{y}\rangle$. 方案的过滤依赖于加密 0 作为随机化器，当随机化器形成张成随机化空间的基时，可以通过添加随机化器的随机子集和来重新随机化密文. 由于方案中访问控制中心是半可信的，为防止其不完全随机化密文，方案引入矩阵的秩来检测该行为. 由于随机性向量需要线性独立以张成整个随机性空间，Acc($\boldsymbol{c}$)算法可利用该性质重随机化密文. 为了过滤无法张成整个空间的随机性，引入剩余哈希引理，通过公钥和随机性之间的乘法形成密文分量，判断密文组件中矩阵乘法的秩的关系过滤非线性，张成整个随机性空间，完成密文的重随机化.

(1) Setup($1^\lambda,P,\mathcal{X}_\lambda,\mathcal{Y}_\lambda$)：令$n=O(\lambda), q=\tilde{O}(n)>16m(m+1), m=2n\log q$. 输入安全参数$\lambda$，访问控制策略$P:\{0,1\}^l\times\{0,1\}^l\to\{0,1\}$，消息空间$\mathcal{X}_\lambda$及谓词空间$\mathcal{Y}_\lambda$. 随机选取矩阵$\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$，采用陷门抽样算法 TrapGen 抽取$\boldsymbol{A}$的陷门基$\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}_q^{m\times m}$；构造函数$f_{\boldsymbol{A}}(\boldsymbol{s})=\boldsymbol{A}\boldsymbol{s}\bmod q(f_{\boldsymbol{A}}:\mathbb{Z}^n\to\mathbb{Z}_q^n)$；随机选择$l+1$个线性无关的向量$\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l\in\mathbb{Z}_q^n$，计算矩阵$\boldsymbol{A}$的秩$r_{\boldsymbol{A}}=Rank(\boldsymbol{A})$；主私钥为$msk=\boldsymbol{T}_{\boldsymbol{A}}$. 输出公共参数$pp=(q,n,m,\boldsymbol{A},\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l,r_{\boldsymbol{A}})$.

(2) KeyGen($pp,msk,id,\boldsymbol{y}$)：输入公共参数pp，主私钥msk，向量$\boldsymbol{y}\in\mathbb{Z}_q^l$，用户的身份$id_i\in\mathbb{Z}_q$，将用户身份$id_i=(b_1,b_2,\cdots,b_l)\in\{0,1\}^l$编码为：$\boldsymbol{u}=\boldsymbol{u}_0+\sum_{i=1}^{l}b_i\boldsymbol{u}_i$；给定高斯参数$\sigma\left(\left(1+\sum_{i=1}^{l}b_i\right)/(l+1)\right)$，采用原像抽样算法 SamplePre($\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{u},\sigma$)抽取向量$\boldsymbol{s}\in\mathbb{Z}_q^m$，$\|\boldsymbol{s}\|\le\sigma\left(\left(1+\sum_{i=1}^{l}b_i\right)/(l+1)\right)\sqrt{m}$，使其满足$\boldsymbol{A}\cdot\boldsymbol{s}=\boldsymbol{u}$. 输出公私钥对$(pk,sk)=(\boldsymbol{u},\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}})$.

(3) Enc($pk,id,\boldsymbol{x}$)：输入发送者身份id_i和一个消息向量$\boldsymbol{x}\in\mathbb{Z}_q^l$. 随机选取一个均匀矩阵$\boldsymbol{R}_x\leftarrow\{0,1\}^{n\times n}$和一个线性无关的矩阵$\boldsymbol{R}_r\leftarrow\{0,1\}^{n\times n}$，噪声向量$\boldsymbol{e}_1\leftarrow\Psi^n, \boldsymbol{e}_2\leftarrow\Psi^n$，计算：

$$\boldsymbol{u}=\boldsymbol{u}_0+\sum_{i=1}^{l}b_i\boldsymbol{u}_i,$$

$$\begin{aligned}\boldsymbol{c}_{\boldsymbol{x}}&=(\boldsymbol{c}_{\boldsymbol{x},0},\boldsymbol{c}_{\boldsymbol{x},1})\\&=(\boldsymbol{R}_{\boldsymbol{x}}\boldsymbol{A},\boldsymbol{R}_{\boldsymbol{x}}\boldsymbol{u}+\boldsymbol{e}_1+\lfloor q/K\rfloor\boldsymbol{x})\in\mathbb{Z}_q^{n\times(m+1)},\end{aligned}$$

$$\boldsymbol{c}_r=(\boldsymbol{c}_{r,0},\boldsymbol{c}_{r,1})=(\boldsymbol{R}_r\boldsymbol{A},\boldsymbol{R}_r\boldsymbol{u}+\boldsymbol{e}_2)\in\mathbb{Z}_q^{n\times(m+1)},$$

输出原始密文$\boldsymbol{c}=(\boldsymbol{c}_{\boldsymbol{x}},\boldsymbol{c}_r)$.

(4) Acc($\boldsymbol{c}$)：输入发送者id_i的密文$\boldsymbol{c}=(\boldsymbol{c}_{\boldsymbol{x}},\boldsymbol{c}_r)$，判断$Rank(\boldsymbol{c}_{r,0})\stackrel{?}{=}r_{\boldsymbol{A}}$，若$Rank(\boldsymbol{c}_{r,0})\neq r_{\boldsymbol{A}}$，输出$\perp$，否则，随机抽样一个矩阵$\boldsymbol{R}_s\leftarrow\{0,1,-1\}^{n\times n}$，计算：

$$\boldsymbol{c}'=(\boldsymbol{c}_{\boldsymbol{x},0}+\boldsymbol{R}_s\boldsymbol{c}_{r,0},\boldsymbol{c}_{\boldsymbol{x},1}+\boldsymbol{R}_s\boldsymbol{c}_{r,1})\in\mathbb{Z}_q^{n\times(m+1)},$$

输出转换后的密文$\boldsymbol{c}'$.

(5) Dec($\boldsymbol{c}',sk$)：输入密文$\boldsymbol{c}'$，用户id_j的私钥sk，计算$\xi=\boldsymbol{c}_1\boldsymbol{y}^{\mathrm{T}}-\boldsymbol{c}_0\cdot sk$，输出$\xi'=\underset{\xi'\in\{0,\cdots,K+1\}}{\arg\min}\left|\lfloor q/K\rfloor\cdot\xi-\xi'\right|$.

5　方案分析

5.1　正确性

接收者收到转换后的密文$\boldsymbol{c}'=(\boldsymbol{c}_{\boldsymbol{x},0}+\boldsymbol{R}_s\boldsymbol{c}_{r,0},$

$\boldsymbol{c}_{x,1}+\boldsymbol{R}_s\boldsymbol{c}_{r,1}$)后,使用私钥 sk 解密,其中 $\boldsymbol{c}_0=\boldsymbol{c}_{x,0}+\boldsymbol{R}_s\boldsymbol{c}_{r,0}$,$\boldsymbol{c}_1=\boldsymbol{c}_{x,1}+\boldsymbol{R}_s\boldsymbol{c}_{r,1}$,具体解密过程如下:

$$\begin{aligned}\xi&=\boldsymbol{c}_1\boldsymbol{y}^{\mathrm{T}}-\boldsymbol{c}_0\cdot sk\\&=(\boldsymbol{c}_{x,1}+\boldsymbol{R}_s\boldsymbol{c}_{r,1})\boldsymbol{y}^{\mathrm{T}}-(\boldsymbol{c}_{x,0}+\boldsymbol{R}_s\boldsymbol{c}_{r,0})s\boldsymbol{y}^{\mathrm{T}}\\&=(\boldsymbol{R}_x\boldsymbol{u}+\boldsymbol{e}_1+\lfloor q/K\rfloor\boldsymbol{x}+(\boldsymbol{R}_r\boldsymbol{u}+\boldsymbol{e}_2))\boldsymbol{y}^{\mathrm{T}}-\\&\quad(\boldsymbol{R}_x\boldsymbol{A}+\boldsymbol{R}_s\boldsymbol{R}_r\boldsymbol{A})s\boldsymbol{y}^{\mathrm{T}}\\&=(\boldsymbol{R}_x+\boldsymbol{R}_s\boldsymbol{R}_r)(\boldsymbol{u}-\boldsymbol{A}\boldsymbol{s})\boldsymbol{y}^{\mathrm{T}}+\boldsymbol{e}_1\boldsymbol{y}^{\mathrm{T}}+\\&\quad\boldsymbol{R}_s\boldsymbol{e}_2\boldsymbol{y}^{\mathrm{T}}+\lfloor q/K\rfloor\langle\boldsymbol{x},\boldsymbol{y}\rangle\\&=\lfloor q/K\rfloor\langle\boldsymbol{x},\boldsymbol{y}\rangle+\underbrace{\boldsymbol{e}_1\boldsymbol{y}^{\mathrm{T}}+\boldsymbol{R}_s\boldsymbol{e}_2\boldsymbol{y}^{\mathrm{T}}}_{error\ terms}.\end{aligned}$$

为使方案能够正确解密,参数应满足如下条件:

(1)为满足陷门生成算法 TrapGen,设置 $m\geq 6n\log q$,$q=ploy(n)$,$\sigma\geq\|\widetilde{\boldsymbol{T}_A}\|\cdot\omega(\sqrt{\log_2 n})$;

(2)为获得一个短的陷门基,要求 $\rho>n\cdot\omega\sqrt{n}$;

(3)为满足 LWE 困难问题,设置 $\alpha q>2\sqrt{n}$;

(4)为保证噪音 $\boldsymbol{E}=\boldsymbol{e}_1\boldsymbol{y}^{\mathrm{T}}+\boldsymbol{R}_s\boldsymbol{e}_2\boldsymbol{y}^{\mathrm{T}}$ 在合理范围内,由于 $\|\boldsymbol{y}\|\leq\sqrt{l}V$,$\|\boldsymbol{R}_s\|\leq C\sqrt{2l}$,$C\approx 1/\sqrt{2\pi}$,$\|\boldsymbol{e}_1\|\leq\sigma\sqrt{l}$,$\|\boldsymbol{e}_2\|\leq\sigma\sqrt{l}$,故 $\|\boldsymbol{e}_1\boldsymbol{y}^{\mathrm{T}}\|\leq\sigma lV$,$\|\boldsymbol{R}_s\boldsymbol{e}_2\boldsymbol{y}^{\mathrm{T}}\|\leq C'\sigma lV\sqrt{1l}$,噪音上界为 $\sigma lV+C'\sigma lV\sqrt{1l}$.

综上,参数设置为 $m=6n\log q$,$q=m\sqrt{n}\omega(\sqrt{\log n})$,$\sigma=m\omega(\log n)$,$\alpha=1/(l+1)\sigma m\omega(\log m)$.

5.2 安全性

定理 3. IND-sID-CPA 安全. 假设方案参数按照 5.1 节设置,且 LWE 是困难的,则该 ACIPFE 方案在标准模型下是 IND-sID-CPA 安全的.

证明. 通过游戏的方式证明任意一个多项式时间敌手 $\mathcal{A}$ 攻击该 ACIPFE 方案的优势是可忽略的.

Game0. 该游戏是原始的 IND-sID-CPA 游戏.

Game1. 该游戏改变了矩阵 $\boldsymbol{A}$ 与向量 $\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l$ 的生成方式,其他参数设置不变. 敌手 $\mathcal{A}$ 与挑战者 $\mathcal{C}$ 之间的交互如下:

初始化:敌手选择一个挑战身份 id^* 和两个挑战向量 $\boldsymbol{x}_0^*=(\boldsymbol{x}_{0,1}^*,\boldsymbol{x}_{0,2}^*,\cdots,\boldsymbol{x}_{0,l}^*)$,$\boldsymbol{x}_1^*=(\boldsymbol{x}_{1,1}^*,\boldsymbol{x}_{1,2}^*,\cdots,\boldsymbol{x}_{1,l}^*)$,$\boldsymbol{x}_0^*\neq\boldsymbol{x}_1^*$.

系统设置:(1)挑战者随机选择一个矩阵 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$,而不再是通过陷门抽样算法产生矩阵($\boldsymbol{A}$,$\boldsymbol{T}_A$)$\leftarrow$TrapGen($1^\lambda$);(2)随机选择($\boldsymbol{s}_0,\boldsymbol{s}_1,\cdots,\boldsymbol{s}_l$)$\leftarrow D_{L,s,c}$;(3)计算 $\boldsymbol{A}\boldsymbol{s}_i=\boldsymbol{u}_i(\mathrm{mod}q)$,$i=0,1,\cdots,l$;(4)检查 $\boldsymbol{u}_i$ 是否线性无关,若不是,则重复(2). 最后,挑战者 $\mathcal{C}$ 将公共参数 $pp=(q,n,m,\boldsymbol{A},\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l,r_A)$ 发送给敌手 $\mathcal{A}$.

阶段 1:敌手 $\mathcal{A}$ 可进行私钥提取询问. 敌手发送用户身份 $id_i\in\mathbb{Z}_q$,挑战者将用户身份编码 $id_i=(b_1,b_2,\cdots,b_l)\in\{0,1\}^l$,计算 $\boldsymbol{s}=\boldsymbol{s}_0+\sum_{i=1}^{l}b_i\boldsymbol{s}_i$. $\boldsymbol{s}_i\leftarrow D_{\sigma/l+1,0}$,$i=0,1,\cdots,l$. 根据引理 2 可知,$\boldsymbol{s}\leftarrow D_{\sigma\cdot\sum_{i=1}^{l}b_i/l+1,0}$,因为 $\boldsymbol{A}\boldsymbol{s}_i=\boldsymbol{u}_i(\mathrm{mod}q)$,故 $\boldsymbol{A}\boldsymbol{s}=\boldsymbol{u}_0+\sum_{i=1}^{l}b_i\boldsymbol{u}_i$,挑战者将私钥 $s\boldsymbol{y}^{\mathrm{T}}=\left(\boldsymbol{s}_0+\sum_{i=1}^{l}b_i\boldsymbol{s}_i\right)\boldsymbol{y}^{\mathrm{T}}$ 发送给敌手 $\mathcal{A}$.

阶段 2:与阶段 1 相同.

挑战:$\mathcal{A}$ 将 $(id^*,\boldsymbol{x}_0^*,\boldsymbol{x}_1^*)$ 发送给 $\mathcal{C}$,$\mathcal{C}$ 随机选择一个消息向量 $\boldsymbol{x}_\beta^*$,$\beta\in\{0,1\}$,计算:

$$\begin{aligned}\boldsymbol{c}_{\boldsymbol{x}_\beta^*}&=(\boldsymbol{c}_{\boldsymbol{x}_\beta^*,0},\boldsymbol{c}_{\boldsymbol{x}_\beta^*,1})\\&=(\boldsymbol{R}_x\boldsymbol{A},\boldsymbol{R}_x\boldsymbol{u}_{id^*}+\boldsymbol{e}_1+\lfloor q/K\rfloor\boldsymbol{x}_\beta^*)\in\mathbb{Z}_q^{l\times(m+1)},\\\boldsymbol{c}_r&=(\boldsymbol{c}_{r,0},\boldsymbol{c}_{r,1})=(\boldsymbol{R}_r\boldsymbol{A},\boldsymbol{R}_r\boldsymbol{u}_{id^*}+\boldsymbol{e}_2)\in\mathbb{Z}_q^{l\times(m+1)}.\end{aligned}$$

将挑战密文 $\boldsymbol{c}^*=(\boldsymbol{c}_{\boldsymbol{x}_\beta^*},\boldsymbol{c}_r)$ 发送给敌手.

猜测:敌手给出猜测,若 $\beta'=\beta$,则挑战者输出 1,否则,输出 0.

Game2. 该游戏与 Game1 的不同之处在于挑战密文的生成方式,不再通过加密算法产生挑战密文,而是从 $\mathbb{Z}_q^{l\times(m+1)}\times\mathbb{Z}_q^{l\times(m+1)}$ 中随机挑选.

下面通过两个引理说明 Game0 与 Game1 不可区分,Game2 与 Game1 不可区分.

引理 4. Game1 与 Game0 是不可区分的,且挑战者对于敌手的私钥询问的回答与真实的访问控制内积函数加密方案是不可区分的.

证明. (1)在 Game0 中,由于矩阵 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$ 是利用陷门生成算法 TrapGen(1^λ)产生的,根据定理 1 可知,矩阵 $\boldsymbol{A}$ 与 $\mathbb{Z}_q^{n\times m}$ 上的均匀分布是不可区分的. 而在 Game1 中,矩阵 $\boldsymbol{A}$ 是从 $\mathbb{Z}_q^{n\times m}$ 中随机选择的. 因此,在敌手看来,公共参数 $\boldsymbol{A}$ 是不可区分的.

(2)在 Game0 中,向量 $\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l$ 是随机选择的,而在 Game1 中,是通过算法 $\boldsymbol{A}\boldsymbol{s}_i=\boldsymbol{u}_i(\mathrm{mod}q)$,$i=0,1,\cdots,l$ 计算产生的,根据引理 1 可知,$\boldsymbol{u}_i$ 的分布统计接近于 $\mathbb{Z}_q^n$ 上的均匀分布. 因此,在敌手看来,公共参数 $\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l$ 是不可区分的.

(3)在 Game0 中,向量 $\boldsymbol{s}\in\mathbb{Z}_q^m$ 是通过原像抽样算法 SamplePre($\boldsymbol{A}$,$\boldsymbol{T}_A$,$\boldsymbol{u}$,σ)产生的,而在 Game1 中,向量 $\boldsymbol{s}_i$,$i=0,1,\cdots,l$. 是从高斯分布 $D_{\sigma/l+1,0}$ 中随机抽取的,满足 $\|\boldsymbol{s}\|\leq\sigma\left(\left(1+\sum_{i=1}^{l}b_i\right)/(l+1)\right)\sqrt{m}$,且对于向量 $\boldsymbol{u}_i$,$i=0,1,\cdots,l$,满足 $\boldsymbol{A}\boldsymbol{s}_i=\boldsymbol{u}_i(\mathrm{mod}q)$. 因此,挑战者对于敌手关于私钥询问的回答是与 Game0 不可区分的.

综上,对于敌手而言,Game0 与 Game1 是不可区分的. 证毕.

引理 5. Game2 与 Game1 是不可区分的.

证明. 假设敌手以不可忽略的优势 ε 区分 Game2 与 Game1，则可构造一个算法 $\mathcal{B}$ 解决判定性 LWE 问题.

将 $2l$ 个随机实例 $(\boldsymbol{R}_x, \boldsymbol{c}_{x,1}=\boldsymbol{R}_x\boldsymbol{u}+\boldsymbol{e}_1)$ 和 $(\boldsymbol{R}_r, \boldsymbol{c}_{r,1}=\boldsymbol{R}_r\boldsymbol{u}+\boldsymbol{e}_2)$ 发送给 $\mathcal{B}$，令

$$\boldsymbol{c}_{x,0}=\boldsymbol{R}_x\boldsymbol{A},$$

$$\boldsymbol{c}^*_{x,1}=\boldsymbol{c}_{x,1}+\lfloor q/K\rfloor \boldsymbol{x}^*_\beta;$$

计算：

$$\boldsymbol{c}^*_x=(\boldsymbol{c}_{x,0}, \boldsymbol{c}^*_{x,1}+\lfloor q/K\rfloor \boldsymbol{x}^*_\beta)\in\mathbb{Z}_q^{l\times(m+1)};$$

令 $\boldsymbol{c}^*_r=(\boldsymbol{R}_r\boldsymbol{A}, \boldsymbol{c}_{r,1})\in\mathbb{Z}_q^{l\times(m+1)}$，$\boldsymbol{c}^*=(\boldsymbol{c}^*_x, \boldsymbol{c}^*_r)$，并将挑战密文 $\boldsymbol{c}^*$ 发送给敌手，若敌手 $\mathcal{A}$ 猜对了 β，则输出 1，否则输出 0.

由于 $\boldsymbol{R}_x\boldsymbol{A}$ 与 $\boldsymbol{R}_r\boldsymbol{A}$ 是 $\boldsymbol{A}$ 的随机子集和，由引理 3 可知，其分布统计上与一个均匀分布不可区分. 如果随机实例 $(\boldsymbol{R}_x, \boldsymbol{c}_{x,1}=\boldsymbol{R}_x\boldsymbol{u}+\boldsymbol{e}_1)$ 和 $(\boldsymbol{R}_r, \boldsymbol{c}_{r,1}=\boldsymbol{R}_r\boldsymbol{u}+\boldsymbol{e}_2)$ 是均匀随机产生的，则挑战密文 $\boldsymbol{c}^*$ 也是均匀随机的，则算法 $\mathcal{B}$ 输出 1 的概率至多为 1/2；如果随机实例 $(\boldsymbol{R}_x, \boldsymbol{c}_{x,1}=\boldsymbol{R}_x\boldsymbol{u}+\boldsymbol{e}_1)$ 和 $(\boldsymbol{R}_r, \boldsymbol{c}_{r,1}=\boldsymbol{R}_r\boldsymbol{u}+\boldsymbol{e}_2)$ 是 LWE 实例，则挑战密文 $\boldsymbol{c}^*$ 也是均匀随机的，该情况与采用加密算法得到的密文分布相同，则算法 $\mathcal{B}$ 输出 1 的概率为 $(1+\varepsilon)/2$，ε 为不可忽略的值. 敌手 $\mathcal{A}$ 赢得该游戏的优势为

$$Adv_{\text{IND-sID-CPA}}=(1+\varepsilon)/2-1/2=\varepsilon/2.$$

因此，$\mathcal{B}$ 至少以 $\varepsilon/2$ 的概率求解 DLWE 问题，这与已知的 DLWE 问题是困难的相悖，故 Game2 与 Game1 是不可区分的.

综上，该 ACIPFE 方案在标准模型下是 IND-sID-CPA 安全的. 证毕.

定理 4. Sanitizability 安全. 如果函数 f_A 是抗碰撞的，那么本文基于格所构造的 ACIPFE 方案是 Sanitizability 安全.

证明. 假设敌手能够以不可忽略的优势赢得该游戏，那么能够以不可忽略的概率找到该陷门抗碰撞哈希函数的一个碰撞. 敌手与挑战者之间的交互游戏如下：

系统设置：该阶段与 IND-sID-CPA 中 Game1 的系统设置一样.

询问：敌手 $\mathcal{A}$ 可向挑战者 $\mathcal{C}$ 发起多项次的私钥询问. 敌手发送用户身份 $id_i\in\mathbb{Z}_q$，挑战者将用户身份编码 $id_i=(b_1, b_2, \cdots, b_l)\in\{0,1\}^l$，计算 $\boldsymbol{s}=\boldsymbol{s}_0+\sum_{i=1}^{l} b_i\boldsymbol{s}_i$. $\boldsymbol{s}_i\leftarrow D_{\sigma/l+1,0}$，$i=0,1,\cdots,l$. 根据引理 2 可知，$\boldsymbol{s}\leftarrow D_{\sigma\cdot\sum_{i=1}^{l} b_i/l+1,0}$，因为 $\boldsymbol{A}\boldsymbol{s}_i=\boldsymbol{u}_i(\text{mod}q)$，故 $\boldsymbol{A}\boldsymbol{s}=\boldsymbol{u}_0+\sum_{i=1}^{l} b_i\boldsymbol{u}_i$，挑战者将私钥 $\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}=\left(\boldsymbol{s}_0+\sum_{i=1}^{l} b_i\boldsymbol{s}_i\right)\boldsymbol{y}^{\mathrm{T}}$ 发送给敌手 $\mathcal{A}$.

挑战：I_S 为对发送者密钥生成预言机 Q_S 询问中发送者构成的集合，故 $I_S=\{1\}\cup\{\varnothing\}$，即要么查询发送者的私钥，要么不询问. 设敌手的攻击目标为 $(\boldsymbol{c}, i')$.

(1) $I_S=\{1\}$，有 $j=0$，敌手不能查询解密预言机，无论攻击目标密文 $c\in(\boldsymbol{c}, i')$ 是从密文空间 $\mathbb{Z}_q^{n\times(m+1)}\times\mathbb{Z}_q^{n\times(m+1)}$ 中随机选取的还是通过加密算法生成的，挑战密文为

$$\boldsymbol{c}'=(\boldsymbol{c}_{x,0}+\boldsymbol{R}_s\boldsymbol{c}_{r,0}, \boldsymbol{c}_{x,1}+\boldsymbol{R}_s\boldsymbol{c}_{r,1})\in\mathbb{Z}_q^{n\times(m+1)},$$

敌手无解密密钥，因此，无论 $\beta=0$ 还是 $\beta=1$，挑战密文 $\boldsymbol{c}'$ 与 $\mathbb{Z}_q^{n\times(m+1)}$ 上均匀分布不可区分，敌手的优势为 $Adv\leq negl(\lambda)$.

(2) $I_S=\{\varnothing\}$，有 $i'=\{0\}$，$j\in\{0,1\}$. 当 $j=0$ 时，与上述(1)情况类似；当 $j=1$ 时，敌手生成攻击目标 $(\boldsymbol{c}, i')$ 时，可以获得私钥 sk 和公钥 pk. 现分析即使敌手拥有 sk 也无法区分挑战密文 $\boldsymbol{c}'$，即访问控制中心输入的密文与输出的密文是独立的.

访问控制中心的输入密文为 $\boldsymbol{c}=(\boldsymbol{c}_x, \boldsymbol{c}_r)$，其中，$\boldsymbol{c}_x=(\boldsymbol{c}_{x,0}, \boldsymbol{c}_{x,1})=(\boldsymbol{R}_x\boldsymbol{A}, \boldsymbol{R}_x\boldsymbol{u}+\boldsymbol{e}_1+\lfloor q/K\rfloor \boldsymbol{x})\in\mathbb{Z}_q^{n\times(m+1)}$；$\boldsymbol{c}_r=(\boldsymbol{c}_{r,0}, \boldsymbol{c}_{r,1})=(\boldsymbol{R}_r\boldsymbol{A}, \boldsymbol{R}_r\boldsymbol{u}+\boldsymbol{e}_2)\in\mathbb{Z}_q^{n\times(m+1)}$；

访问控制中心输出的密文为 $\boldsymbol{c}'=(\boldsymbol{c}_{x,0}+\boldsymbol{R}_s\boldsymbol{c}_{r,0}, \boldsymbol{c}_{x,1}+\boldsymbol{R}_s\boldsymbol{c}_{r,1})\in\mathbb{Z}_q^{n\times(m+1)}$.

利用以下引理，通过线性代数中矩阵乘法的秩来检测输出密文的随机性.

引理 6. 给定一个 n 维方阵 $\boldsymbol{R}$ 和一个矩阵 $\boldsymbol{A}\rightarrow\mathbb{Z}_q^{n\times m}$，若 $\boldsymbol{R}$ 是满秩的，则 $Rank(\boldsymbol{R}\boldsymbol{A})=Rank(\boldsymbol{A})$.

由于密文 $\boldsymbol{c}_{r,0}=\boldsymbol{R}_r\boldsymbol{A}$，如果 $Rank(\boldsymbol{c}_{r,0})=Rank(\boldsymbol{A})$，则表示 $\boldsymbol{R}_r$ 是满秩的(线性无关)，那么访问控制中心的操作可将随机性用于张成整个随机性空间. 由于随机空间的变化(从二进制到整数)，则经过访问控制中心重随机化的密文与重随机化密文空间中的随机元素不可区分. 因此，输出密文 $\boldsymbol{c}'$ 与 $\mathbb{Z}_q^{n\times(m+1)}$ 上均匀分布不可区分，即与输入密文 $\boldsymbol{c}=(\boldsymbol{c}_x, \boldsymbol{c}_r)$ 独立，即访问控制中心的输出是任意消息向量 $\boldsymbol{x}$ 的任意密文.

该阶段假设敌手可以按照如下方式伪造一个合法的密钥. 挑战者随机选择一个向量 $\boldsymbol{s}'\leftarrow D_{\mathbb{Z}^m,\sigma}$，计算 $f_A(\boldsymbol{s}')$，由引理 1 可知，$f_A(\boldsymbol{s}')$ 的分布统计接近于真实方案中 $\boldsymbol{u}\leftarrow\mathbb{Z}_q^n$ 的分布. 现固定 $\boldsymbol{u}$，挑战者计算 $\boldsymbol{u}=\boldsymbol{A}\boldsymbol{s}'$，将 $\boldsymbol{s}'\leftarrow D_{\mathbb{Z}^m,\sigma}$ 发送给敌手，这与真实方案中采用原像抽样算法 $\text{SamplePre}(\boldsymbol{A}, \boldsymbol{T}_A, \boldsymbol{u}, \sigma)$ 抽取的向量 $\boldsymbol{s}\in\mathbb{Z}_q^m$ 具有相同分布. 假设敌手能够伪造一个合

法的密钥 s^*，则有 $f_A(s^*)=f_A(s')$，$\Pr[s^*=s']\leq 1/2^{\omega(\log n)}$，也就是说，$s^*$ 和 s' 是函数 f_A 的一个碰撞，这与已知的陷门抗碰撞哈希函数的性质相悖.

综上，该 ACIPFE 方案满足 Sanitizability 安全.

证毕.

5.3 性能分析

本节首先从理论上将 ACIPFE 方案与相关方案进行了比较；其次，通过仿真实验评估了 ACIPFE 方案的实际性能.

5.3.1 理论分析

本方案与相关访问控制加密方案在困难性假设、抗量子性、是否支持内积运算、密文复杂度及访问控制复杂度做了比较，结果如表 2 所示. 从表 2 中可以看出，现有的访问控制加密方案大都依赖于较为复杂的数学理论构造(文献[25,27,30,32])，而本方案基于格上 LWE 问题构建的，算法简单且能够抵抗量子攻击；与已有的基于 LWE 问题构建的访问控制加密方案(文献[26,33,34])相比，TZM17[26] 方案密文复杂度较高，且需要依赖于第三方密钥(Acc's Key)实现细粒度的访问控制功能；虽然本方案的密文复杂度高于 WXL21[34] 方案，但不需要 Acc's Key，并且支持内积运算，更加适用于复杂的云计算环境，且通过运行多次该 ACIPFE 方案，可实现多个用户之间的通信，具有较强的可用性.

表 2 相关方案性能对比

方案	困难性问题	抗量子	内积	密文	访问控制
DHO16[25]	DDH/IO	×	×	$O(2^n)$	$O(2^n)$
TZM17[26]	LWE	√	×	$O(2^n)$	$O(2^n)$
FGK17[27]	SXDH	×	×	$poly(n)$	$O(1)$
KW17[30]	DDH/RAS	×	×	$poly(n)$	$O(1)$
WC21[32]	DDH	×	×	$O(1)$	—
WWC21[33]	LWE	√	×	$O(n^2)$	$O(n^2)$
WXL21[34]	LWE	√	×	$O(n)$	—
本方案	LWE	√	√	$O(n^2)$	$O(n^2)$

表 3 为方案 WXL21[34] 中各算法的时间开销与本方案的对比表，其中，T_{TG}，T_{SP}，T_{MV} 分别为陷门生成算法 TrapGen，原像抽样算法 SamplePre 以及矩阵向量间运算的平均时间消耗. 通过表 3 可以看出，在 Setup 阶段，本方案与 WXL21[34] 方案生成系统主私钥都需要运行 1 次 TrapGen 算法，但是，在 KeyGen 阶段中，本方案只需运行 1 次 SamplePre 算法，而方案 WXL21[34] 需要运行 2 次 SamplePre 算法产生密钥. 在 Enc 阶段和 Dec 阶段，本方案与 WXL21[34] 都需要进行矩阵向量间的运算，差别不大. 由于方案 WXL21[34] 无第三方访问控制中心，因此不需要 Acc 算法.

表 3 时间开销对比

方案	Setup	KeyGen	Enc	Acc	Dec
WXL21[34]	T_{TG}	$2T_{SP}+T_{MV}$	T_{MV}	—	T_{MV}
本方案	T_{TG}	$T_{SP}+T_{MV}$	T_{MV}	T_{MV}	T_{MV}

表 4 为方案 WXL21[34] 与本方案的存储空间比较结果. 从表 4 可以看出，本方案的主私钥与公钥尺寸明显小于方案 WXL21[34]，虽然私钥尺寸与密文尺寸相对较大，但本方案的目的是在实现发送者权限控制的同时，接收者能对密文实施内积计算，因此，功能更健全，具有较强可用性.

表 4 存储开销对比

方案	主私钥尺寸	公钥尺寸	私钥尺寸	密文尺寸
WXL21[34]	$O((m^2+n)\log_2 q)$	$O((n+m)\log_2 q)$	$O(m\log_2 q)$	$O(m\log_2 q)$
本方案	$O(m^2\log_2 q)$	$O(n\log_2 q)$	$O(ml\log_2 q)$	$O(n(m+1)\log_2 q)$

5.3.2 实验评估

实验的硬件环境为 MacOS 操作系统、2 GHz 四核 Intel Core i5 处理器，编译环境为 C++14、Microsoft Visual Studio Code1.71.0，基于 NTL 库，设置 $q=17$，$n=5$，$m=37$，长度参数 $l=1,3,5,7,9,11$，测试在 $\lambda=10$ 的安全等级下，运行 ACIPFE 方案所花费的时间成本. 其中，实验中得到的时间结果为运行 ACIPFE 方案 10 次后的平均值. 表 5 和图 2 为参数 l 对 ACIPFE 方案中的每个算法(Setup、KeyGen、Enc、Acc、Dec)运行时间影响结果.

表 5 ACIPFE 方案中各算法时间开销

l	Setup/ms	KeyGen/s	Enc/ms	Acc/ms	Dec/ms
1	38.9761	15.1688	9.4223	10.3212	8.3256
3	38.8313	15.2792	17.4471	10.6903	11.3219
5	38.9177	15.9724	28.2976	10.4397	15.9562
7	38.9501	16.1606	36.3063	10.6558	19.1197
9	38.8964	16.4499	44.4465	10.5021	23.7703
11	38.9942	16.5470	50.9788	10.6166	28.0715

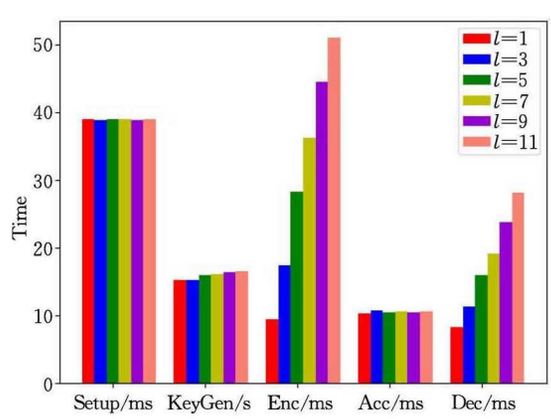

图 2 各算法运行时间消耗

从图 2 可以看出，运行本访问控制内积函数加密 ACIPFE 方案的 Setup 算法和 Acc 算法的时间成本不受参数 l 的影响；运行 KeyGen 算法时所消耗的时间主要是在生成私钥时，参数 l 影响了两向量间的加法与乘法操作，该操作所花费的时间较少，因此，方案中的 KeyGen 算法几乎不受参数 l 的影响；运行 Enc 算法和 Dec 算法则随着参数 l 线性增加.

6 结　语

本文基于格上 LWE 困难问题构造了一个细粒度的访问控制内积函数加密方案，为 Damgård 等人在最初的访问控制加密方案中遗留的其中一个公开问题提供了一个解决方案. 不再使用复杂的不可区分性混淆或全同态技术实现重随机化，而是通过引入一个第三方(访问控制中心)，利用线性代数中矩阵的秩完成对原始密文的重随机性检测，使得低级别用户不能读取高级别用户消息，高级别用户不能向低级别用户发送消息；同时，方案突破函数加密与访问控制加密有机融合的瓶颈，使得接收方解密转换后的密文后只能得到关于消息的内积值. 方案在标准模型下达到了选择性 IND-CPA 安全，并通过理论和实验对其性能进行了分析，功能上不仅能抵抗量子攻击，实现了更加细粒度的访问控制功能，而且能够进行密文上的内积运算，保证了数据机密性. 效率上具有更快的加解密速度，具有明显优势.

在下一步的研究工作中，拟基于格上 RLWE 困难问题构造更加高效、灵活、安全的访问控制内积函数加密方案.

致　谢　诚挚地感谢编辑老师和匿名审稿专家对该稿件提出的中肯意见！

参　考　文　献

[1] Qian Wen-Jun, Shen Qing-Ni, Wu Peng-Fei, et al. Research progress on privacy-preserving techniques in big data computing environment. Chinese Journal of Computers, 2022, 45(4): 669-701(in Chinese)
(钱文君，沈晴霓，吴鹏飞等. 大数据计算环境下的隐私保护技术研究进展. 计算机学报，2022，45(4)：669-701)

[2] Zhang Ming-Wu, Yang Bo, Wang Chun-Zhi, Takagi Tsuyoshi. Privacy-preserving and adaptively-secure encryptions with deterministic finite automata policy and their applications. Chinese Journal of Computers, 2015, 38(4): 897-908 (in Chinese)
(张明武，杨波，王春枝，Takagi Tsuyoshi. 隐私保护的推理机策略加密及应用. 计算机学报，2015，38(4)：897-908)

[3] Kim S, Lewi K, Mandal A, et al. Function-hiding inner product encryption is practical//Proceedings of the 11th International Conference on Security and Cryptography for Networks. Amalfi, Italy, 2018: 544-562

[4] Chotard J, Dufour Sans E, Gay R, et al. Decentralized multi-client functional encryption for inner product//Proceedings of the 24th International Conference on the Theory and Application of Cryptology and Information Security. Brisbane, Australia, 2018: 703-732

[5] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption//Proceedings of the 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques. French Riviera, France, 2010: 62-91

[6] Shamir A. Identity-based cryptosystems and signature schemes //Proceedings of the 4th Advances in Cryptology. Santa Barbara, USA, 1984: 47-53

[7] Sahai A, Waters B. Fuzzy identity-based encryption//Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Aarhus, Denmark, 2005: 457-473

[8] Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11): 612-613

[9] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data// Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, USA, 2006: 89-98

[10] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption//Proceedings of the 28th IEEE Symposium on Security and Privacy. California, USA, 2007: 321-334

[11] Xue Y J, Xue K P, Gai N, et al. An attribute-based controlled collaborative access control scheme for public cloud storage. IEEE Transactions on Information Forensics and Security, 2019, 14(11): 2927-2942

[12] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products// Proceedings of the 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Istanbul, Turkey, 2008: 146-162

[13] Dan B, Amit S, Brent W. Functional encryption: Definitions and challenges//Proceedings of the 8th Theory of Cryptography. Providence, USA, 2011: 253-273

[14] O'Neill A. Definitional issues in functional encryption. Cryptology ePrint Archive, 2010. https://eprint.iacr.org/2010/556

[15] Goldwasser S, Kalai Y, Popa R A, et al. Reusable garbled circuits and succinct functional encryption//Proceedings of the 45th Symposium on Theory of Computing. California, USA, 2013: 555-564

[16] Abdalla M, Bourse F, Caro A D, et al. Simple functional encryption schemes for inner products//Proceedings of the 18th IACR International Workshop on Public Key Cryptography. Gaithersburg, USA, 2015: 733-751

[17] Agrawal S, Freeman D M, Vaikuntanathan V. Functional encryption for inner product predicates from learning with errors//Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security. Seoul, South Korea, 2011: 21-40

[18] Bishop A, Jain A, Kowalczyk L. Function-hiding inner product encryption//Proceedings of the 21st International Conference on the Theory and Application of Cryptology and Information Security. Auckland, New Zealand, 2015: 470-491

[19] Agrawal S, Libert B, Stehlé D. Fully secure functional encryption for inner products, from standard assumptions// Proceedings of the 36th Annual International Cryptology Conference. California, USA, 2016: 333-362

[20] Chen Y, Zhang L, Yiu S M. Practical attribute based inner product functional encryption from simple assumptions. Cryptology ePrint Archive, 2019. https://eprint.iacr.org/2019/846

[21] Abdalla M, Catalano D, Gay R, et al. Inner-product functional encryption with fine-grained access control//Proceedings of the 26th International Conference on the Theory and Application of Cryptology and Information Security. Daejeon, South Korea, 2020: 467-497

[22] Pal T, Dutta R. Attribute-based access control for inner product functional encryption from LWE//Proceedings of the 7th International Conference on Cryptology and Information Security in Latin America. Bogotá, Colombia, 2021: 127-148

[23] Mera J M B, Karmakar A, Marc T, et al. Efficient lattice-based inner-product functional encryption//Proceedings of the 25th IACR International Conference on Public-Key Cryptography. Virtual Event, 2022: 163-193

[24] Damgård I, Haagh H, Orlandi C. Access control encryption: Enforcing information flow with cryptography//Proceedings of the 14th Theory of Cryptography Conference. Beijing, China, 2016: 547-576

[25] Badertscher C, Matt C, Maurer U. Strengthening access control encryption//Proceedings of the 23rd International Conference on the Theory and Application of Cryptology and Information Security. Hong Kong, China, 2017: 502-532

[26] Tan G, Zhang R, Ma H, et al. Access control encryption based on LWE//Proceedings of the 4th ACM International Workshop on ASIA Public-Key Cryptography. New York, USA, 2017: 43-50

[27] Fuchsbauer G, Gay R, Kowalczyk L, et al. Access control encryption for equality, comparison, and more//Proceedings of the 20th IACR International Workshop on Public Key Cryptography. Amsterdam, Netherlands, 2017: 88-118

[28] Han J, Chen L, Susilo W, et al. Fine-grained information flow control using attributes. Information Sciences, 2019, 484: 167-182

[29] Yao Z, Mu Y. ACE with compact ciphertext size and decentralized sanitizers. International Journal of Foundations of Computer Science, 2019, 30(4): 531-549

[30] Kim S, Wu D J. Access control encryption for general policies from standard assumptions//Proceedings of the 23rd International Conference on the Theory and Application of Cryptology and Information Security. Hong Kong, China, 2017: 471-501

[31] Wang H, Chen K, Liu J K, et al. Access control encryption with efficient verifiable sanitized decryption. Information Sciences, 2018, 465: 72-85

[32] Wang X, Chow S S M. Cross-domain access control encryption: Arbitrary-policy, constant-size, efficient//Proceedings of the IEEE Symposium on Security and Privacy (S&P). California, USA, 2021: 388-401

[33] Wang X, Wong H W H, Chow S S M. Access control encryption from group encryption//Proceedings of the 19th International Conference on Applied Cryptography and Network Security. Kamakura, Japan, 2021: 417-441

[34] Wang P, Xiang T, Li X, et al. Access control encryption without sanitizers for Internet of energy. Information Sciences, 2021, 546: 924-942

[35] Cai J Y, Cusick T W. A lattice-based public-key cryptosystem //Proceedings of the 5th International Workshop on Selected Areas in Cryptography. Kingston, Canada, 1998: 219-233

[36] Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. SIAM Journal on Computing, 2007, 37(1): 267-302

[37] Agrawal S, Boneh D, Boyen X. Efficient lattice (H) IBE in the standard model//Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. French Riviera, France, 2010: 553-572

[38] Alwen J, Peikert C. Generating shorter bases for hard random lattices. Theory of Computing Systems, 2011, 48(3): 535-553

HOU Jin-Qiu, Ph. D. candidate. Her research interests include date security, functional encryption.

PENG Chang-Gen, Ph. D. , professor, Ph. D. supervisor. His research interests include cryptography, information security and privacy protection in big data, etc.

TAN Wei-Jie, Ph. D. , associate professor, M. S. supervisor. His research interests include privacy protection and information security.

YE Yan-Ting, Ph. D. candidate. Her research interests include information security and cryptography.

Background

Functional encryption (FE) is a multifunctional encryption primitive that provides a reference framework for fine-grained function computation. FE associates the function with the private key. The user with the function private key can only get the function value about the message after decryption, which can realize the access control of data and the selection and calculation of ciphertext. Therefore, it is a very meaningful exploration direction to organically integrate the access permission level of data into the encryption and decryption algorithm to achieve "partial encryption and decryption controllable and on-demand security computing". What's more, inner product functional encryption (IPFE) is the most special form of FE that executes the computation for the inner product of vectors. IPFE can not only realize more complex access control strategies and policy hiding, but also effectively control "partial access" of data, provide finer grained queries, and improve privacy protection while meeting data confidentiality. Therefore, it is very suitable for cloud computing and other fields. However, existing functional encryption schemes can not finely control the sender's authority and uses more complex theoretical tools, which is difficult to be practical. Access control encryption (ACE) is a useful cryptographic primitive first proposed by Damgård et al. By adding a "sanitizer" between the traditional encrypting party and the decrypting party, the encrypted text of the sender is processed according to the access policy, so that the receiver and the sender can only communicate according to the access policy, which not only realizes the encryption protection of the sent message, but also controls the message sending authority of the sender. However, most of the existing ACE schemes only introduced the requirement for heavy-tools, such as indistinguishable obfuscation and multilinear maps. In addition, these works are only for data, and do not consider encryption and decryption control for function calculation. Therefore, the practicality of these works remains uncertain. Facing the challenge of quantum attack, how to design a special and efficient functional encryption scheme against quantum attack has become one of research highlights. The access control inner product functional encryption (ACIPFE) scheme proposed in this paper based on the LWE problem on the lattice can not only resist quantum attacks, but also effectively control the permissions of the sender and the receiver. It can effectively achieve the goals of flexible, controllable and manageable "invisible data availability" and fine-grained permission controllable secret computing in the zero-trust open environment.

This work is supported in part by the National Natural Science Foundation of China (No. 62272124), the Science and Technology Program of Guizhou Province (No. [2018]3001, No. [2018]2159, No. [2020]5017), and the Guizhou Province Graduate Research Foundation (YJSKYJJ[2021]028).