一个新的理想格上基于属性的加密方案

王彩芬,邓云霞,牛淑芬
WANG Caifen, DENG Yunxia, Niu Shufen

西北师范大学 计算机科学与工程学院,兰州 730070
College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China

WANG Caifen, DENG Yunxia, Niu Shufen. New attribute-based encryption on ideal lattices. Computer Engineering and Applications, 2016, 52(17):123-127.

Abstract: With the continuous development of cryptological technique, attribute-based encryption has received wide attention in recent years as a new concept of cryptographic algorithm. But now most of attribute-based encryption schemes are based on the traditional public key cryptography of math problems, such as the large integer factorization and discrete logarithm problems, which has the low operation efficiency and can't resist the index attack and the quantum attack, limiting its development in the encryption system. This paper presents a new attribute-based encryption over ideal lattice. Compared with the existing attribute-based encryption schemes, the new scheme uses the special structure of ideal lattice, easy to implement and with a short public key and the ciphertext, its encryption and decryption algorithms are realized through a function, reducing the computational complexity greatly.

Key words: ideal lattice; problem of LWE; attribute-based encryption

摘 要:随着密码学技术不断发展,基于属性的密码学作为密码算法的新概念,近年来受到广泛关注。但是,已提出的基于属性的加密方案大都是基于大整数分解和离散对数问题等传统数学问题之上的公钥密码方案,这些方案存在运算效率较低、不能抵抗亚指数攻击和量子攻击等缺点,这限制了其在密码体制中的发展。提出了一个新的理想格上基于属性的加密方案,与已有的基于属性的加密方案相比,该加密方案利用了理想格上的特殊结构,容易实现,具有较短的公钥和密文;加密、解密都通过格上的函数调用实现,大大减小了运算量。

关键词:理想格;LWE问题;基于属性的加密
文献标志码:A **中图分类号:**TN918.1 doi:10.3778/j.issn.1002-8331.1511-0225

1 引言

基于属性的加密体制拓展了基于身份的加密体制,这种加密体制是将属性和身份相结合的密码学体制,最早于2005年欧洲密码学年会上,由Sahai和Waters等学者[1]提出。Sahai和Waters等学者将生物识别技术采集并处理后的特征值直接作为一种身份信息应用到基于身份的加密方案中,从而构造了一个模糊身份加密方案,提出了基于属性加密的思想,这种思想奠定了属性密码学产生的基础。2006年,Goyal,Sahai和Waters等学者[2]明确提出了属性加密,他们根据密文和密钥表现形式和应用场景不同,阐明了属性加密的概念,并定义了细粒度划分的访问控制结构。2007年,Ostrovsky等学者[3]在CSS会议上提出了非单调存取结构,补充了访问树的"非"操作,使访问控制结构更加完整。之后,基于属性的加密方案引起众多学者的关注,他们纷纷提出了很多基于属性的加密方案。

但是,已提出的基于属性的加密方案大多是基于大整数分解和离散对数问题等传统数学问题上的公钥密码方案,这些方案存在运算效率较低、不能抵抗亚指数攻击和量子攻击等缺点,这极大限制了其在密码体制中

基金项目:国家自然科学基金(No.61262057,No.61163038,No.61562077)。

作者简介:王彩芬(1963—),女,教授,博士研究生导师,研究方向为密码学与信息安全;邓云霞(1990—),女,硕士研究生,研究方向为密码学与信息安全,E-mail:1602614526@qq.com;牛淑芬(1976—),女,副教授,研究生导师,研究方向为云安全与密码技术。

收稿日期:2015-11-18 **修回日期:**2016-02-29 **文章编号:**1002-8331(2016)17-0123-05
CNKI**网络优先出版:**2016-05-10, http://www.cnki.net/kcms/detail/11.2127.TP.20160510.1102.014.html

的发展。为了克服这些缺点,密码学界开始关注和设计更加高效、安全的以及能够抵抗量子攻击的新型密码体制,就此产生了格构造的新型密码体制。而格构造的新型密码方案具有安全性高、容易实现、运算简单、具有丰富的难题假设、抗量子攻击和存在最坏情况下的强可证明安全特性等优点,那么基于格难题问题设计的密码算法,就为密码体制的发展提供了一种新的设计思路。从Ajtai[4]开始,学者们提出了许多有效的基于格的函数和密码学方案,例如原像采样函数[5]、格基扩展函数[6]、基于随机格和理想格的陷门函数[5]、基于格的签名方案[7]和基于格的全同态加密方案[8]等等。

本文利用Cash和Hofheinz等学者[5]提出的格基扩展函数,结合Agrawal等学者[9]提出的在固定维度下格授权的HIBE方案和徐春根等学者[10]提出的理想格上基于身份的签名方案,利用理想格技术,提出一个新的理想格上基于属性的加密方案。针对已有的基于属性加密的方案,本文的方案试图克服已有方案存在的缺点,诸如大多数已有方案用双线性对来构造,虽然实际应用中效率高,但计算复杂度很高,本文提出的加密方案运算简单、容易实现、具有较短的公钥和密文等优点。

2 预备知识

2.1 CP-ABE方案的系统定义及安全模型

定义1 一个密文策略基于属性的加密方案主要由下面的四个算法描述:

$Setup(1^n)$:系统建立算法,输入安全常数 n,输出系统的主密钥 MK 和公共参数 PP,是一个随机算法。

$KeyGen(PP, MK, L)$:给定系统主密钥 MK 和公共参数 PP,输入一个用户的属性列表 L,该算法生成一个与属性列表 L 相关的用户私钥 sk_L,是一个概率算法。

$Encryption(PP, m, W)$:该算法输入系统公共参数 PP,一个访问结构 W 和一个消息 m,输出一个根据访问结构 W 对消息 m 加密得到的密文 C,是一个概率算法。

$Decryption(PP, C, e_L)$:该算法输入一个用户的私钥 sk_L 和一个根据访问结构 W 对消息 m 加密得到的密文 C,输出消息 m 当且仅当 $L \in M$。

定义2 下面定义的安全模型修改自文献[11]中的安全模型,可以通过下面的选择安全游戏来定义。该游戏表达了一个较强的私有特性,即挑战密文和密文空间中的一个随机密文是不可区分的。

攻击者初始化:敌手 A 声明一个访问结构 W^*,并把它给挑战者,该访问结构作为敌手的攻击对象。

系统初始化:挑战者运行方案中的系统建立算法,把输出的公共参数 PP 发送给敌手。

第一阶段:在该阶段,允许敌手询问一系列的密钥提取询问,限制是敌手询问的属性列表 L 必须满足条件 $L \notin W^*$。挑战者运行算法 $KeyGen(PP, MK, L)$ 来获得一个私钥 sk_L,并把它返回给敌手。

挑战:在该阶段,敌手将提交一个消息位 $b^* \in \{0, 1\}$。挑战者抛一枚公平的硬币 r,并在密文空间中选择一个随机的密文 C。如果 $r=0$,挑战者设置挑战密文为 $C^* = Encryption(PP, W^*, b^*)$,否则(也就是说 $r=1$),挑战者设置 $C^* = C$,最后挑战者把 C^* 发送给敌手。

第二阶段:该阶段与第一阶段一样。

猜测:在该阶段,敌手输出 r' 作为对 r 的猜测。

在上述游戏中,敌手 A 获得胜利的优势定义为 $\left| Pr[r' = r] - \frac{1}{2} \right|$。

定义3 如果对于所有的多项式时间算法,敌手在上述游戏中最多取得胜利的优势可忽略,那么说一个格密文策略基于属性加密方案在上述选择安全模型下是安全的。

2.2 格

定义4 设 $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_m$ 是 R^m 上的 m 个线性无关向量,由 $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_m$ 生成的格 L 是指向量 $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_m$ 的线性组合构成的向量集合,即

$$\Lambda = L(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_m) = \left\{ \sum_{i=1}^{m} x_i \boldsymbol{b}_i \middle| x_i \in Z \right\}$$

其中,向量 $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_m$ 成为格 L 的一组基。此外,如果定义一个 $m \times m$ 的矩阵 $\boldsymbol{B}$,设置 $\boldsymbol{B}$ 的列向量依次为 $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_m$,那么等价的有以下定义:

$$\Lambda = L(\boldsymbol{B}) = L(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_m) = \left\{ \boldsymbol{B}x \middle| x \in Z^m \right\}$$

当 $\Lambda \subseteq Z^m$ 时,成为整数格。

定义5 设 q 为素数,$\boldsymbol{A} \in Z_q^{n \times m}$ 和 $u \in Z_q^n$,定义:

$$\Lambda_q(\boldsymbol{A}) = \{e \in Z^m \text{ s.t. } \exists s \in Z_q^n \text{ where } \boldsymbol{A}^{\mathrm{T}} s = e (\mathrm{mod}\, q)\}$$

$$\Lambda_q^{\perp}(\boldsymbol{A}) = \{e \in Z^m \text{ s.t. } \boldsymbol{A}e = 0 (\mathrm{mod}\, q)\}$$

$$\Lambda_q(\boldsymbol{A}) = \{e \in Z^m \text{ s.t. } \boldsymbol{A}e = u (\mathrm{mod}\, q)\}$$

由定义可知,若 $t \in \Lambda_q^u(\boldsymbol{A})$,则 $\Lambda_q^u(\boldsymbol{A}) = \Lambda_q^{\perp} + t$。

因此 $\Lambda_q^u(\boldsymbol{A})$ 是 $\Lambda_q^{\perp}(\boldsymbol{A})$ 经过平移得到。

定理1 设 $q \geqslant 3$ 是奇数并且 $m = \lceil 6n \operatorname{lb} q \rceil$,存在一个概率多项式时间算法 $TrapGen(q, n)$,它能输出 $(\boldsymbol{A} \in Z_q^{n \times m}, \boldsymbol{S} \in Z^{m \times m})$,其中 $\boldsymbol{A}$ 是一个与 $Z_q^{n \times m}$ 上的均匀分布统计上接近的分布中的矩阵,$\boldsymbol{S}$ 是 $\Lambda_q^{\perp}(A)$ 的一个基,且除了 n 的可忽略的概率外,满足:

$$\|\tilde{S}\| \leqslant O(\sqrt{n \operatorname{lb} q}) \quad 和 \quad \|S\| \leqslant O(n \operatorname{lb} q)$$

2.3 离散高斯分布

定义6 设 L 是 Z^m 的一个子集,对任意的向量 $\boldsymbol{c} \in R^m$,任意正整数 $s \in R$,m 维高斯函数定义为:$\rho_{s,c}(x) = \exp(-\pi(\|x - \boldsymbol{c}\|/s)^2)$。另外,$\rho_{s,c}(L) = \sum \rho_{s,c}(x)$ 表示 L 上所有 $\rho_{s,c}(x)$ 的和。

定义7 设 L 是 Z^m 的一个子集,对任意的向量 $\boldsymbol{c} \in R^m$,任意正整数 $s \in R$,则 L 上的高斯分布为:

$D_{L,s,c}(y)=\frac{\rho_{s,c}(y)}{\rho_{s,c}(L)}, \forall y\in L$。

2.4 LWE问题

所设计的方案的安全性规约到LWE问题，它是Regev在文献[12]中从机器学习领域引入进来的，把 $T=R/Z$ 记作实数[0，1)上的群，该群上的二元运算为模1加法。在这里采用如下的描述。

定义8 设一个素数 q，一个正整数 n，和一个 Z_q 上的分布 $\aleph$ 都是公共的。一个 $(Z_q, n, \aleph)$ -LWE问题实例由一个未确定的挑战预言机 O 组成，它要么是一个有噪声的伪随机取样器 O_s，含有某个常量随机密钥 $s\in Z_q^n$，要么是一个完全随机取样器 O_s。O 的行为如下：

O_s：输出形式为 $(u_i, v_i)=(u_i, u_i^{\mathrm{T}}s+x_i)\in Z_q^n\times Z_q$ 的取样，其中 $s\in Z_q^n$ 是一个均匀分布的常数值，在多次调用中保持不变；$x_i\in Z_q^n$ 是来自于 $\aleph$ 的新鲜取样，u_i 来自于 Z_q^n 的均匀取样。

$O_{\$}$：输出来自于 $Z_q^n\times Z_q$ 的完全均匀的随机取样。

$(Z_q, n, \aleph)$ -LWE问题允许挑战预言机 O 重复询问。一个算法 A 判定 $(Z_q, n, \aleph)$ -LWE问题的优势定义为 $\left|Pr[A^{O_s}=1]-Pr[A^{O_{\$}}=1]\right|$。

下面给出具体的定义：整数 $q=q(n)$，Z_q 上的分布 $\aleph$，(平均情况)错误学习问题 $(Z_q, n, \aleph)$ -LWE问题的目标是以不可忽略的概率区分下面两个分布：一是 $A_{s,\aleph}$（$s\leftarrow Z_q^n$ 是均匀的），二是 $Z_q^n\times Z_q$ 上的均匀分布。换句话说，如果LWE是困难的，那么分布 $A_{s,\aleph}$ 的集合是伪随机的。

Regev指出，对特定的模 q 和高斯分布 $\aleph$；$(Z_q, n, \aleph)$ -LWE和使用量子算法解决标准最坏情况格问题一样困难。

定理2[13] 已知整数 $\alpha=\alpha(n)\in(0, 1)$，素数 $q=q(n)$ 满足 $\alpha q>2\sqrt{n}$，使用 Ψ_α 表示 Z_q 上的正态分布，且它以0为中心，它的标准偏移量为 $\alpha q/\sqrt{2\pi}$（即得到特定的值后，取整到与其最近的整数并模 q 的结果），如果存在一个预言机能够解决 $(Z_q, n, \aleph)$ -LWE问题，则存在一个多项式级的量子算法能够解决近似最短向量问题和最短线性无关向量问题。

定义9 设一个实数 $\alpha=\alpha(n)\in(0, 1)$，一个素数 q。$T=R/Z$ 指示加法模为1的实数 [0, 1) 的群。Ψ_α 指示模为1的随机变量在 T 上的一个均值为0，方差为 $\alpha/\sqrt{2\pi}$ 的正态分布。$[x]=\left\lfloor x+\frac{1}{2}\right\rfloor$ 指示与 $x\in R$ 最近的整数。$\bar{\Psi}_\alpha$ 指示随机变量为 $(qX)\bmod q$ 在 Z_q 上的离散分布，其中随机变量 $X\in T$ 具有分布 Ψ_α。

3 理想格上CP-ABE的方案设计

本章所设计的方案主要基于以下算法和定义，其中算法 $ExtBasis(T_B, B, \bar{B})$ 修改自文献[5]，算法 $SampleR(1^m)$ 和 $SamplePre(B, T_B, u, \sigma)$ 修改自文献[11]。算法的具体构造如下：

设 $D_{m\times m}$ 指示 $Z^{m\times m}$ 上矩阵的一个分布，该分布定义为 $(D_{Z^m,\sigma})^m$，且依次分布取样的矩阵可以满足是 Z_q-可逆的。$D_{Z^m,\sigma}$ 是 Z^m 上参数为 $\sigma=\sqrt{n\,\mathrm{lb}\,q}.w(\sqrt{\mathrm{lb}\,m})$ 的离散高斯分布。

$SampleR(1^m)$：

该算法返回一个可逆矩阵 $\boldsymbol{R}\in Z^{m\times m}$，它取样于 $D_{m\times m}$。

$ExtBasis(T_B, B, \bar{B})$：

输入 矩阵 $\boldsymbol{B}\in Z_q^{n\times m}$，格 $\Lambda^{\perp}(\boldsymbol{A})$ 的基 $T_B\in Z^{m\times m}$，矩阵 $\bar{\boldsymbol{B}}\in Z_q^{n\times\bar{m}}$

输出 格 $\Lambda^{\perp}(\boldsymbol{B}'=\boldsymbol{B}\|\bar{\boldsymbol{B}})$ 的基 $T_B'\in Z^{(m+m')\times(m+m')}$

该算法实现了低维格到高维格的转化。

$SamplePre(B, T_B, u, \sigma)$：

输入 矩阵 $\boldsymbol{B}\in Z_q^{n\times m}$，格 $\Lambda^{\perp}(\boldsymbol{B})$ 的基 $T_B\in Z^{m\times m}$，向量 $\boldsymbol{u}\in Z_q^n$ 和一个高斯参数 $\sigma>\left\|\tilde{T}_A\right\|\cdot\omega(\sqrt{\mathrm{lb}\,m})$

输出 一个向量 $\boldsymbol{x}\in\Lambda_q^{\perp}(\boldsymbol{B})$，它取样于一个与分布 $D_{\Lambda_q^u(\boldsymbol{B}),\sigma}$ 统计上接近的一个分布，其中分布 $D_{\Lambda_q^u(\boldsymbol{B}),\sigma}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 上参数为 σ 的一个离散高斯分布

定义10(FRD函数)[9] 设 n 是一个正整数，q 是一个素数，一个FRD函数 $H: Z_q^n\to Z_q^{n\times n}$ 满足下面的条件：

(1)对于所有不同的 $u, v\in Z_q^n$，矩阵 $\boldsymbol{H}(u)-\boldsymbol{H}(v)\in Z_q^{n\times m}$ 是满秩的。

(2) H 是多项式时间可计算的。

本方案中：对于 $i\in[M]$，$j\in[M_i]$ 的一个属性值 $v_{i,j}$，将选择一个均匀随机的向量 $\boldsymbol{u}_{i,j}\in Z_q^n$ 与之对应。然后，通过FRD函数 H 来映射 $u_{i,j}$ 到一个矩阵 $\boldsymbol{H}(u_{i,j})\in Z_q^{n\times n}$。根据 H 构建的方法，使得对于每个属性列表 L，可以计算 $\sum_{v_{i,j}\in L}H(u_{i,j})$，这一点很重要，是本方案的基础。

3.1 方案描述

设方案中的安全参数 n 是2的幂次方，定义环 $R_q=Z[X]/(\Phi_{2n}(X), q)$，这里 $\Phi_{2n}(x)=X^n+1$ 是分圆多项式。设方案中的属性列表为 $L=(L_1, L_2, \cdots, L_M)$，假定 δ 满足 $n^{\delta}>\lceil\mathrm{lb}\,q\rceil=O(\mathrm{lb}\,n)$，$w$ 是一个函数，其他参数设置如下：$m=6n^{1+\delta}, \sigma=m\cdot w(\mathrm{lb}\,n), \alpha=[l=m^2w(\mathrm{lb}\,n)]^{-1}, q=m^2\sqrt{n}\,w(\mathrm{lb}\,n)$。根据以上参数构造本文的加密方案如下：

$Setup(1^n)$：输入一个安全参数 n，中心调用算法 $TrapGen(q, n)$（见定理1）来生成一个均匀随机的矩阵 $\boldsymbol{B}\in Z_q^{n\times m}$ 和格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的一个短基 $T_B\in Z_q^{n\times m}$，对于 $i\in[M]$，$j\in[M_i]$ 的每一个属性值，调用算法 $SampleR(1^m)$，根据分

布 $D_{m\times m}$ 选择矩阵 $\boldsymbol{R}_{i,j}\in Z_q^{m\times m}$，选择一个均匀随机的矩阵 $\boldsymbol{u}\in Z_q^n$。最后，公共参数 PP 和系统主密钥 MK 的设置如下：

$PP=(\boldsymbol{B},\{\boldsymbol{R}_{i,j}\}_{i\in M,j\in M_{[i]}},u),MK=(T_B)$

$KeyGen(PP,MK,L)$：输入公共参数 PP 和系统主密钥 MK 和一个属性列表 $L=(L_1,L_2,\cdots,L_M)$，其中 $L_i=V_{i,j}$ 是位置为 $i\in[M]$ 和 $j\in[M_i]$ 的属性取值。

(1)中心首先设置 $F_L=B\|\prod_{V_{i,j}\in L}R_{i,j}$。

(2)调用算法 $ExtBasis(B,\prod_{V_{i,j}\in L}R_{i,j},T_B)$ 来生成 $\Lambda_q^{\perp}(F_L)$ 的一个基 T_L。

(3)如下取样 e_L 作为属性列表 L 的私钥。

$e_L\leftarrow SamplePre(F_L,T_L,u,\sigma)$

此外，参数有正确的形式，即满足 $e_L\cdot F_L=u$。

$Encryption(PP,m,W)$：输入公共参数 PP，一个消息为 $m\in\{0,1\}$ 和一个访问结构 $W=(W_1,W_2,\cdots,W_M)$，如下加密消息位：

(1)中心首先设置 $F_W=B\|\prod_{V_{i,j}\in W}R_{i,j}$。

(2)均匀随机选择一个 $s\in Z_q^n$。

(3)根据分布 $\bar{\Psi}_\alpha$，选择 $x\in Z_q$，$y\in Z_q^m$。

(4)设置 $c_1\leftarrow u^{\mathrm{T}}s+x+m\left\lfloor\frac{q}{2}\right\rfloor$，$c_2\leftarrow F_W^{\mathrm{T}}s+y\in Z_q^m$，最后设置 $C=(W,c_1,c_2)$。

$Decryption(PP,C,e_L)$：设 C 是根据访问结构 W 加密得到的密文。如果 $L\in W$，如下解密：

(1)计算 $W=c_0-e_L^{\mathrm{T}}c_1\in Z_q$。

(2)如果 $|w-\left\lfloor\frac{q}{2}\right\rfloor|<\left\lfloor\frac{q}{4}\right\rfloor$，并输入 Z，输出1；否则，输出0。

3.2 安全性证明和分析

当 $L\in W$ 时，有下述关系：

$$W=c_0-e_L^{\mathrm{T}}c_1=m\left\lfloor\frac{q}{2}\right\rfloor+x-e_L^{\mathrm{T}}y$$

式子 $x-e_L^{\mathrm{T}}y$ 叫做错误项，关于错误项的详细讨论以及方案安全参数的具体设置可以参考文献[11]。具体的安全性证明如下：

定理3 假定 $(Z_q,n,\aleph)$-LWE问题难解，上述方案在选择安全模型下是安全的。

证明 假设存在一个概率多项式时间的敌手 A 攻击上述的方案的优势为 ε，也就是说，存在一个模拟器 β，它判定 $(Z_q,n,\aleph)$-LWE问题的优势为 ε。即模拟器 β 利用敌手 A 可以以优势 ε 区分LWE预言机 O，并收到如下的值 $(u_k,v_k)\in Z_q^n\times Z_q$，其中 $k=0,1,2,\cdots,m$，然后，模拟器 β 如下进行处理：

初始化：A 声明访问结构 $W^*=(W_1^*,W_2^*,\cdots,W_M^*)$ 作为敌手 A 的攻击对象，并把它发送给模拟器 β。β 如下准备公共参数：

(1)设置 u 为 u_0 并如下构造一个矩阵 $\boldsymbol{B}_0$，对于 $k=0,1,2,\cdots,m$，设置 $\boldsymbol{B}_0$ 的第 k 列为 u_k。

(2)设 $i\in[M]$，$j\in[M_i]$，对于每一个 $v_{i,j}=W_i^*$（用 v_{i,j^*} 指示这样的 $v_{i,j}$），调用算法 $TrapGen(q,n)$ 生成一个均匀随机的矩阵 $\boldsymbol{B}$ 和一个 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的基 $T_B\in Z_q^{m\times m}$，并保存 T_B。

(3)对于 $i=1,2,\cdots,m$，设置 $F_i=\boldsymbol{B}\|B_{1,j_1^*},\cdots,B_{i-1,j_{i-1}^*}$，对于每一个 F_i，模拟器 β 调用算法 $ExtBasis(\boldsymbol{B},B_{1,j_1^*},\cdots,B_{i-1,j_{i-1}^*},T_B)$ 共 M_{i-1} 次得到 $\Lambda_q^{\perp}(F_i)$ 的基 $T_{i,j}$，其中 $j\in[M_i],j\neq j_i^*$。

(4)最后模拟器 β 发送公共参数 $(\boldsymbol{B},\{R_{i,j}\}_{i\in M,j\in M_{[i]}},u)$ 给敌手 A。保存 $\Lambda_q^{\perp}(F_i)$ 的基 $T_{i,j}$，其中 $i\in[M]$，$j\in[M_i],j\neq j_i^*$。同时注意到公共参数具有正确的分布。

第一阶段：在该阶段，模拟器 β 可以通过上一阶段保存的 $T_{i,j}$ 来返回敌手的密钥询问。假如 A 询问属性列表 L 的私钥，其中 $L\notin W^*$。根据设置肯定存在某个（或某些）i 满足 $v_{i,j}\in L$ 和 $v_{i,j}\notin W^*$，这意味着 $j\neq j_i^*$。设 t 表示最小的这样 i，那么有下述推导：

$$F_L=B\|\prod_{V_{i,j}\in L}R_{i,j}=B\|B_{1,j_1^*},\cdots,B_{t-1,j_{t-1}^*}\|\prod_{V_{i,j}\in L,i\geqslant t}R_{i,j}=F_t\|\prod_{V_{i,j}\in L,i\geqslant t}R_{i,j}$$

根据上述构建过程，模拟器 β 知道 $\Lambda_q^{\perp}(F_t)$ 的基为 $T_{t,j}$，其中 $j\in[M_t],j\neq j_t^*$。模拟器 β 调用格基扩展算法 $ExtBasis(F_t,\prod_{V_{i,j}\in t,i\geqslant t}R_{i,j},T_{t,j})$ 来生成格 $\Lambda_q^{\perp}(F_L)$ 的基 T_L。最后模拟器 β 如下取样 e_L 作为私钥并返回给敌手 A：

$e_L\leftarrow SamplePre(F_L,T_L,u,\sigma)$

挑战阶段：敌手 A 发送一个消息位 $m^*\in\{0,1\}$ 给模拟器 β，并根据访问结构 W^* 生成挑战密文。

(1)设置 $\boldsymbol{V}^*=[v_1,v_2,\cdots,v_m]^{\mathrm{T}}\in Z_q^m$，$C_1^*=v_0+m^*\left\lfloor\frac{q}{2}\right\rfloor$ 和 $c_2^*=v^*$，其中对于 $k=1,2,\cdots,m$，v_k 来自于LWE问题。

(2)模拟器 β 选择一个人随机为 $r\in\{0,1\}$。如果 $r=0$，模拟器返回 $C^*=(W^*,C_1^*,C_2^*)$ 给敌手 A 作为挑战密文。如果 $r=1$，随机选择 $C_1\in Z_q$ 和 $C_2\in Z_q^m$ 并返回 (W^*,C_1,C_2) 给敌手 A 作为挑战密文。

经过简单的分析，可知上述挑战密文具有正确的分布。当 $O=O_S$，由于公共参数的设置有 $F_W=B$ 和 $v^*=A^{\mathrm{T}}s+y$，其中 $y\in Z_q^m$ 来自于分布 $\bar{\Psi}_\alpha$，因此 C_1^* 和 C_2^* 具有正确的形式，当 $O=O_{\$}$，挑战密文是在 $Z_q\times Z_q^{2m}$ 中，

并是均匀随机的。

第二阶段：模拟器 β 的行为同第一阶段。

猜想：模拟器 β 从敌手 A 收到 r' 作为 r 的猜想，并输出 r' 作为对LWE问题的回答。

通过分析可知，模拟器 β 可以以优势 ε 解决 $(Z_q, n, \aleph)$ -LWE问题。

3.3 效率分析

随着密码学研究的不断深入，效率是考虑各种密码体制的一个重要问题。然而一个密码方案的效率性与构造它时所用的数学结构有着密切的关系，一个好的密码方案有一个好的数学结构。现有的基于属性的加密方案[13-15]大多数都是基于双线性群构造的，运算效率较低。而本文的方案是基于理想格构造的，由于理想格特殊的代数结构，其上的运算都为线性运算，执行效率高；加密、解密都是通过格上的函数调用实现的，大大地减小了运算量。另外，本文的方案使用的是整数格，因此本文方案中涉及到的主要运算要么是整数向量的变换，要么是矩阵的加法和乘法运算，计算高效。根据方案中安全参数的具体设置，公钥长度约为 $O(d^2n^2)$，密文和密钥的长度都为 $O(nd^2)$，与其他的基于格的密码方案[16-21]相比，Boneh方案的公钥长度为 $O(d^3n^2)$，密文长度为 $O(d^3n^2)$，密钥长度为 $O(d^3n^3)$（其中 n 表示公共参数，d 表示格的最大维度），因此，本文的方案密钥和密文都较短。

4 结束语

本文利用理想格构造了一个密文策略的基于属性的加密方案，实现的访问结构为一个特殊的多值属性与门访问结构，并且给出了方案的安全性证明。与已有的基于属性的加密方案相比，本文提出的基于属性的加密方案利用理想格的特殊结构，减小了运算的复杂度，使其具有较高的运算效率。总之，格的密码方案优点很多，考虑利用格来构建基于属性的加密在密码学中有广阔的发展前景。

参考文献：

[1] Sahai A，Waters B.Fuzzy identity based encryption[C]//Advances in Cryptology Lecture Notes in Computer Science，Berlin，2005，3494：457-473.

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

[3] Ostrovsky R，Sahai A，Waters B.Attribute based encryption with non monotonic access structures[C]//Proceedings of the 14th ACM Conference on Computer and Communications Security，Virginia，USA，2007：195-203.

[4] Ajtai M.Generating hard instances of lattice problems[M].New York：[s.n.]，1996：99-108.

[5] 韩敬利，杨明，王兆丽.基于格的密码函数构造方法及其应用[J].军事通信技术，2014，35(1)：75-80.

[6] Cash D，Hofheinz D，Kiltz E，et al.Bonsai trees，or how to delegate a lattice basis[J].Journal of Cryptology，2012，25(4)：601-639.

[7] El Bansarkhani R，Buchmann B.Improvement and efficient implementation of a lattice-based signature scheme[C]//Advances in Cryptology.Berlin/Heidelberg：Springer-Verlag，2014：48-67.

[8] 韩敬利，杨明，王兆丽.基于格的全同态加密实现方案与相关技术[J].军事通信技术，2014，35(2)：423-428.

[9] Agrawal S，Boneh D，Boyen X.Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE[C]//Advances in Cryptology Lecture Notes in Computer Science，2010，6223：98-115.

[10] 杨丹婷，许春根，徐磊，等.理想格上基于身份的签名方案[J].密码学报，2015，2(4)：306-316.

[11] Agrawal S，Boneh D，Boyen X.Efficient lattice (H)IBE in the standard model[C]//Advances in Cryptology Lecture Notes in Computer Science，2010，6110：553-579.

[12] Regev O.New lattice-based cryptographic constructions[J].J ACM，2004，51(6)：899-942.

[13] Regev O.On lattices，learning with errors，random linear codes，and cryptography[C]//Proceedings of the 37th Annual ACM Symposium on Theory of Computing，2005：84-93.

[14] 王云涛.基于属性密码体制的相关研究[D].上海：上海交通大学，2011.

[15] Lewko A，Okamoto T，Sahai A，et al.Fully secure functional encryption：attribute-based encryption and (hierarchical) inner product encryption[C]//Advances in Cryptology EUROCRYPT 2010.Berlin/Heidelberg：Springer，2010：62-91.

[16] Okamoto T，Takashima K.Fully secure functional encryption with general relations from the decisional linear assumption[C]//Advances in Cryptology-CRYPTO 2010.Berlin/Heidelberg：Springer-Verlag，2010：191-208.

[17] 张应辉，郑东，李进，等.密文长度恒定且属性直接可撤销的基于属性的加密[J].密码学报，2014，1(5)：465-480.

[18] Rückert M.Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles[C]//Post-Quantum Cryptography.Berlin/Heidelberg：Springer，2010：182-200.

[19] 王小云，刘明洁.格密码学研究[J].密码学报，2014，1(1)：13-27.

[20] Boneh D，Boyen X.Secure identity based encryption without random oracles[C]//Proceedings of Advances in Cryptology，2004：443-459.

[21] Boneh D，Sahai A，Waters B.Fully collusion resistant traitor tracing with short ciphertexts and private keys[C]//Lecture Notes in Computer Science，2006：573-592.