可撤销属性的格基属性加密方案

张欣威， 张串绒， 尚福特
(空军工程大学信息与导航学院,西安,710077)

摘要 针对量子环境下属性加密体制中属性撤销的问题,结合Zhang等提出的格上基于密文的属性加密方案,在格上构建了一个可撤销属性的格基属性加密方案。通过属性撤销列表,在二叉树结构下将未被撤销属性对应的密钥进行更新,从而达到撤销属性的目的。利用Shamir门限秘密共享的思想,实现了门限访问控制策略。该方案在随机预言机模型下是选择性安全的,安全性规约到错误学习问题。分析表明该方案在量子攻击下是安全的,并且支持灵活的门限访问控制策略。

关键词 属性加密;属性撤销;格理论;二叉树结构;门限访问控制;错误学习问题
DOI 10.3969/j.issn.1009-3516.2015.03.018
中图分类号 TN918.1 **文献标志码** A **文章编号** 1009-3516(2015)03-0087-05

Revocable Attribute-based Encryption from Lattice

ZHANG Xinwei ,ZHANG Chuanrong ,SHANG Fute
(Information and Navigation College, Air Force Engineering University, Xi′an 710077, China)

Abstract: To resolve the problems of revocation under the quantum computing, combined with Zhang′s scheme, the paper constructs an attributed-based encryption which is revocable from lattice. This scheme updates the key which is associated with un-revocable attributes under the binary tree structure. By using the idea of Shamir′s threshold secret sharing scheme, a threshold access policy is realized in this paper. The scheme is selectively secure where the security is reduced to the hardness of learning with error problems in the random oracle model. The analysis shows that the scheme is secure under the quantum attack and supports the flexible threshold access policy.

Key words: attribute-based encryption; attribute revocation; lattice; binary tree structure; threshold access policy; learning with error (LWE)

属性加密是公钥加密和身份加密的一种扩展,与传统的密码学相比,属性加密在很多方面表现出了优良的特性,如:加解密的高效性、用户的动态性、访问控制策略的灵活性以及用户身份的隐私性等等[1]。在一个属性加密方案中,由于用户权限的更新以及密钥泄露等问题的存在,必须考虑属性撤销的问题。然而,在属性加密算法中,一个属性涉及到多个用户的密钥或者访问控制策略,也就是说一个属性的撤销会影响到多个用户的密钥撤销或者访问控制结构的更改。整个系统的开销会随之增大,造

收稿日期:2015-01-27
基金项目:国家自然科学基金资助项目(61272486,61103231)
作者简介:张欣威(1992—),男,湖北襄阳人,硕士生,主要从事密码学与网络安全研究.E-mail:wallace-gen@163.com

引用格式:*张欣威,张串绒,尚福特. 可撤销属性的格基属性加密方案[J]. 空军工程大学学报:自然科学版,2015,16(3):87-91. ZHANG Xinwei ,ZHANG Chuanrong ,SHANG Fute.Revocable Attribute-based Encryption from Lattice[J]. Journal of Air Force Engineering University: Natural Science Edition,2015,16(3):87-91.*

成系统巨大的负担。Goyal 等人[2]通过给每个用户添加一个时间属性,来达到属性撤销的目的。但是,密钥分发中心需要定期向未撤销权限用户分发密钥,其工作量和用户数呈线性关系。Sahai 等人[3]利用二叉树结构,将每个用户设置为与二叉树的叶节点相关,使得密钥更新数量与用户数量呈对数关系,并结合"密文代理"(ciphertext delegation)的性质,提出了一个高效的可撤销属性的加密方案。Chen 的方案[4]采用了子集差分算法无状态组密钥分发机制来更新密钥,有效降低了传输的开销。

在以往的属性加密方案中,其安全性基于经典的数学问题,如双线性对问题等。但是,随着量子计算机的不断发展,基于双线性对问题的属性加密算法将不能保证数据的安全性。而格上困难问题在量子算法的攻击下仍然保持着良好的特性,成为量子时代保障密码算法安全性的基石。同时,由于格具有运算量小,计算简单等特性,格上的属性加密成为近年来研究的热点问题。Agrawal 等人[5]利用门限方案构造了一个基于错误学习问题(LWE)问题的属性加密方案。之后,Zhang 等人[6]将一般的属性加密方案推广到密文策略的属性加密。Gorbunov 等人[7]在一般电路函数模型上实现了访问控制策略,扩展了电路的深度。Wang[8]构造了一个支持与门策略的基于密文的多值属性加密方案。

在格基属性加密方案中,属性撤销的问题同样存在。Chen 等人[9]构建了第一个格基身份加密的撤销方案,但是没有考虑格上的属性撤销方案。格理论和双线性对问题的不同特性导致构造属性撤销不同与以往方案。针对上述问题,本文构建了一个支持属性撤销的基于密文策略的属性加密方案。本方案以 Zhang 等人[6]提出的格上基于密文的属性加密方案为基础,利用二叉树结构来更新密钥,实现对用户属性的撤销。分析表明,该方案的安全性规约到 LWE 问题,在标准模型下是选择性安全的。

1 理论基础

本文中,$\mathbb{R}$ 表示实数,$\mathbb{Z}$ 表示整数,q 为 1 个素数。对于正整数 n,$[n]$ 表示 $(1,\cdots,n)$,安全参数设置为 n。1 个矩阵的长度为其最长向量范数的长度:$\|\mathrm{X}\|=\max_i\|\mathrm{x}_i\|$。$\mathrm{negl}(n)$ 是一个可忽略的函数,即 $\lim\limits_{n\to\infty}\dfrac{\mathrm{negl}(n)}{n^c}=0, c>0$。我们称一个事件是不可忽略地则其概率为 $1-\mathrm{negl}(n)$。

1.1 格

定义 1 设 $\boldsymbol{B}=(b_1,\cdots,b_n)\in\mathbb{R}^n$,其中 $b_1,\cdots,b_n$ 是 n 个线性独立的向量,由 $\boldsymbol{B}$ 生成的 n 维格定义如下:

$$\Lambda=L(\boldsymbol{B})=\{\boldsymbol{B}c=\sum_{i=1}^{n}c_ib_i\mid\boldsymbol{c}\in\mathbb{Z}\}$$

我们称 $\boldsymbol{B}$ 是格的一组基向量。

定义 2 设 q 是一个素数,$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,$\boldsymbol{e}\in\mathbb{Z}^m$ 我们定义 2 个格如下:

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

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

定理 1 [10]:设 Λ 为一个 m 维格。存在一个确定的多项式时间算法使得,输入格 Λ 的任意一个基向量和格中的满秩集合 $S=(s_1,\cdots,s_m)$,输出 Λ 的一个基向量,满足 $\|\tilde{\boldsymbol{T}}\|\leqslant\|\tilde{\boldsymbol{S}}\|$ 和 $\|\boldsymbol{T}\|\leqslant\|\boldsymbol{S}\|\sqrt{m}/2$。

1.2 二叉树结构

BT 表示一个二叉树,其根节点表示为 root。v 是一个叶子节点,代表用户的属性,路径 Path(v) 表示从叶节点 v 到根节点 root 的集合。如果 θ 是一个中间节点,则 θ_l,θ_r 表示节点 θ 的左右子节点。

每一个用户属性和一个叶子节点绑定,定义 t 为撤销属性的时间,X 为在时间 t 之后被撤销的属性所在路径 Path(v) 中所有节点的集合,Y 为在时间 t 之后未撤销的属性集合,实现属性撤销的算法 KUNodes 如下:

对于任意叶节点 $(v_i,t_i)\in RL$,如果则添加 Path(v_i) 到集合 X。对所有的节点 $\theta\in X$,如果 $\theta_l\notin X$,则添加 θ_l 到集合 Y;如果 $\theta_r\notin X$,则添加 θ_r 到集合 Y。如果集合 Y 为空集则添加根节点 root 到集合 Y。

通过运行属性撤销算法 KUNodes,被撤销节点的所有父节点均被撤销。算法输出被撤销节点的所有未被撤销的子节点,表示系统在时刻 t 未被撤销的属性。

图 1 表示属性 1 被撤销。图中标记为 X 的表示被撤销的节点,标记为 Y 的表示被撤销节点的未被撤销的子节点。

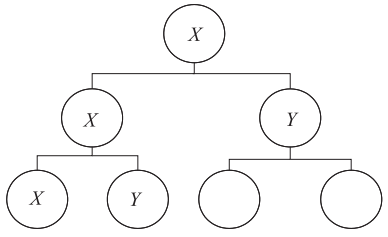

图 1 属性 1 被撤销的二叉树结构

Fig.1 Affribute was revocated in the binary tree

1.3 重要算法

算法 1[11]:TrapGen(q,n)

令 q 为大于 3 的奇数,$m=\lceil 6n\log_2^q\rceil$,存在一个多项式时间算法,输出矩阵 $\boldsymbol{A}$ 为 $\mathbb{Z}_q^{n\times m}$ 上的随机矩阵,$\boldsymbol{S}$ 为 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的基,并且满足 $\|\tilde{\boldsymbol{S}}\|\leqslant$

$O(\sqrt{n\log q})$，并 $\|S\| \leqslant O(n\log q)$。

算法 2[12]：SampleLeft($\boldsymbol{A}, \boldsymbol{M}_1, \boldsymbol{T}_A, s, \boldsymbol{u}$)

输入：矩阵 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$，$\boldsymbol{M}_1 \in \mathbb{Z}_q^{n\times m_1}$，格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的基 $\boldsymbol{T}_A \in \mathbb{Z}_q^{m\times m}$，一个向量 $\boldsymbol{u} \in \mathbb{Z}_q^n$，高斯参数 $s > \|\tilde{\boldsymbol{T}}_A\| \cdot \omega(\sqrt{\log(m+m_1)})$。

输出：一个向量 $\boldsymbol{e} \in \Lambda_q^u(A|M_1)$，即 $(A|M_1)e = u$。

算法 3 [12]：SampleRight($\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{R}, \boldsymbol{T}_B, \boldsymbol{u}, s$)

输入：矩阵 $\boldsymbol{A}, \boldsymbol{B} \in \mathbb{Z}_q^{n\times m}$，一个均匀随机矩阵 $\boldsymbol{R} \in \{1,-1\}^{m\times m}$，格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的基 $\boldsymbol{T}_B \in \mathbb{Z}_q^{m\times m}$，一个向量 $\boldsymbol{u} \in \mathbb{Z}_q^n$，高斯参数 $s > \|\tilde{\boldsymbol{T}}_B\| \cdot \sqrt{m} \cdot \omega(\log m)$。

输出：向量 $\boldsymbol{e} \in \Lambda_q^u(\boldsymbol{A}|\boldsymbol{AR}+\boldsymbol{B})$，即 $(\boldsymbol{A}|\boldsymbol{AR}+\boldsymbol{B})\boldsymbol{e} = \boldsymbol{u}$。

2　具体方案

设系统中有个 l 个属性，即 $R = \{1, \cdots, l\}$。每一个密文 C 和访问控制策略 (W, k) 相关联，其中 $W \in R$ 为属性集合，k 为一个门限值，访问控制策略 (W, k) 表示用户拥有的属性和 W 的交集超过 k 个即可正确解密密文。

2.1　初始化 Setup(n, m, q, d, R)

n 为安全参数，n, m, q, d 均为正整数，其中 d 为默认的属性个数。首先选择一个默认的属性集合 $D = \{l+1, \cdots, l+d\}$，令 $R' = R \cup D$。利用 TrapGen(q, n) 生成一个均匀随机矩阵 $\boldsymbol{A}_0 \in \mathbb{Z}_q^{n\times m}$ 和格 $\Lambda_q^{\perp}(\boldsymbol{A}_0)$ 的满秩基向量 $\boldsymbol{T}_{A_0} \in \mathbb{Z}_q^{m\times m}$。随机选取 $\boldsymbol{B}_1, \boldsymbol{B}_2 \in \mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{u} = (u_1, \cdots, u_n)^{\mathrm{T}} \in \mathbb{Z}_q^n$。对每一个 $i \in R'$，随机选择 $\boldsymbol{A}_i \in \mathbb{Z}_q^{n\times m}$。输出公钥 PK $= (\boldsymbol{A}_0, \boldsymbol{B}_1, \boldsymbol{B}_2, \{\boldsymbol{A}_i\}_{i\in R'}, u)$，主私钥 MSK $= \boldsymbol{T}_{A_0}$。

2.2　生成属性节点私钥 AttNodeKey(PK, MSK, S)

向密钥授权中心提交公钥 PK，主私钥 MSK，用户的属性 $S \subseteq R$，令 $S' = S \cup D$。对 $j = 1, 2, \cdots, n$，随机选择次数为 d 的多项式 $p_j(x) \in \mathbb{Z}_q[x]$，使得 $p_j(0) = u_j$。对每一个属性 $i \in S'$，我们令 $\hat{\boldsymbol{u}}_i = (p_1(i), \cdots, p_n(i))^T$。对二叉树上的所有节点从根节点依次进行编号，节点 θ 的编号为 θ。对 Path(i) 中的任意节点 θ，随机选取 $\boldsymbol{u}_{i,\theta,1} \in \mathbb{Z}_q^n$，令 $\boldsymbol{u}_{i,\theta,2} = \hat{\boldsymbol{u}}_i - \boldsymbol{u}_{i,\theta,1}$，并将其存储在节点 θ 中。计算 SampleLeft($\boldsymbol{A}_0, \boldsymbol{A}_i + \boldsymbol{B}_1, \boldsymbol{T}_{A_0}, s, \hat{\boldsymbol{u}}_{i,\theta,1}$) $\rightarrow \boldsymbol{e}_{i,\theta,1}$。输出属性节点私钥 $\mathrm{SK}_S = (\boldsymbol{\theta}, \boldsymbol{e}_{i,\theta,1})_{\theta\in \mathrm{Path}(i)}$。

2.3　密钥更新 KeyUpdate(MSK, t, RL)

向密钥授权中心提交公钥 PK，私钥 MSK，时间 t 和属性撤销列表 RL。对于任意的节点 $\theta \in$ KUNodes(BT, RL, t)，如果 $\boldsymbol{u}_{i,\theta,1}, \boldsymbol{u}_{i,\theta,2}$ 没有定义，根据 AttNodeKey(MSK, S, ST) 算法生成 $\boldsymbol{u}_{i,\theta,1}, \boldsymbol{u}_{i,\theta,2}$。计算 SampleLeft($\boldsymbol{A}_0, H(t_i) + \boldsymbol{B}_2, \boldsymbol{T}_{A_0}, s, \hat{\boldsymbol{u}}_{i,\theta,2}$) $\rightarrow \boldsymbol{e}_{i,\theta,2}$，其中 H 为一个函数将时间 t 映射为一个 $n \times m$ 的矩阵。输出更新后的密钥为：

$$\mathrm{KU}_t = (\theta, e_{i,\theta,2})_{\theta\in \mathrm{KUNodes(BT,RL},t)}$$

2.4　生成用户解密密钥 DecKeyGen(SK$_S$, KU$_t$)

接收方接收 2 个集合 $\mathrm{SK}_S = (x, e_{i,x,1})_{x\in X}$ $\mathrm{KU}_t = (y, e_{i,y,2})_{y\in Y}$，其中 X 表示路径 Path(i) 包含的节点，Y 表示撤销节点的未被撤销的子节点。如果存在 (x, y) 使得 $x = y$，那么令 $\mathrm{DK}_{S,t} = (e_{i,x,1}, e_{i,y,2})$，由于 $x = y$，故省略 x, y，$\mathrm{DK}_{S,t} = (e_{i,1}, e_{i,2})$；若 SK$_S$ 和 KU$_t$ 没有任何相同的节点，则令 $\mathrm{DK}_{S,t} = \perp$。

2.5　加密 Enc(MPK, W, M)

输入公钥 PK $= (\boldsymbol{A}_0, \boldsymbol{B}_1, \boldsymbol{B}_2, \{\boldsymbol{A}_i\}_{i\in R'}, \boldsymbol{u})$，属性集合 W，门限值 k 满足 $1 \leqslant k \leqslant \min(|W|, d)$，令 $W' = W \cup \{l+1, \cdots, l+d+1-k\}$。构造 $\boldsymbol{F}_i = (\boldsymbol{A}_0 | \boldsymbol{A}_i + \boldsymbol{B}_1 | H(t_i) + \boldsymbol{B}_2)$，随机均匀地选择 $s \in \mathbb{Z}_q^n$。选取噪声 $x \leftarrow \mathbb{Z}_q$，$\boldsymbol{y} \leftarrow \mathbb{Z}_q^m$，对每一个 $i \in W'$，随机选取 2 个矩阵 $\boldsymbol{R}_{i,1}, \boldsymbol{R}_{i,2} \in \{-1,1\}^{m\times m}$，计算 $\boldsymbol{z}_{i,1} \leftarrow \boldsymbol{R}_{i,1}^{\mathrm{T}} \boldsymbol{y} \in \mathbb{Z}_q^m$，$\boldsymbol{z}_{i,2} \leftarrow \boldsymbol{R}_{i,2}^{\mathrm{T}} \boldsymbol{y} \in \mathbb{Z}_q^m$。待加密的消息 $M \in \{0,1\}$。

输出密文 $C = (c_0, c_1)$，其中：

$$c_0 \leftarrow \boldsymbol{u}^{\mathrm{T}} \boldsymbol{s} + x + M \left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q$$

$$c_i \leftarrow \boldsymbol{F}_i^{\mathrm{T}} \boldsymbol{s} + [\boldsymbol{y} \quad \boldsymbol{z}_{i,1} \quad \boldsymbol{z}_{i,2}]^{\mathrm{T}} \in \mathbb{Z}_q^{3m}$$

2.6　解密 Dec(MPK, DK$_{S,t}$, C)

输入密文 C，用户属性集合 S，访问控制策略 (W, k)。如果 $|S \cap W| < k$ 则返回 $\perp$。反之，令 $S' = S \cup D$，$W' = W \cup \{l+1, \cdots, l+d+1-k\}$，因为 $|S \cap W| \geqslant k$，则有 $|S' \cap W'| \geqslant d+1$。选择 $|S' \cap W'|$ 的一个子集 J，使得 $|J| = d+1$。

将 c_i 重新表示为：

$$\begin{bmatrix} c_{i,0} \\ c_{i,1} \\ c_{i,2} \end{bmatrix} = \begin{bmatrix} \boldsymbol{A}_0^{\mathrm{T}} \boldsymbol{s} \\ (\boldsymbol{A}_i + \boldsymbol{B}_1)^{\mathrm{T}} \boldsymbol{s} \\ (\boldsymbol{H}(t_i) + \boldsymbol{B}_2)^{\mathrm{T}} \boldsymbol{s} \end{bmatrix} + \begin{bmatrix} \boldsymbol{y} \\ \boldsymbol{z}_{i,1} \\ \boldsymbol{z}_{i,2} \end{bmatrix}$$

计算：

$$\boldsymbol{E}_{i,1} = \boldsymbol{e}_{i,1}^{\mathrm{T}} \begin{bmatrix} c_{i,0} \\ c_{i,1} \end{bmatrix} = \hat{\boldsymbol{u}}_{i,\theta,1}^{\mathrm{T}} \boldsymbol{s} + \boldsymbol{e}_{i,1}^{\mathrm{T}} \begin{bmatrix} \boldsymbol{y} \\ \boldsymbol{z}_{i,1} \end{bmatrix}$$

$$\boldsymbol{E}_{i,2} = \boldsymbol{e}_{i,2}^{\mathrm{T}} \begin{bmatrix} c_{i,0} \\ c_{i,1} \end{bmatrix} = \hat{\boldsymbol{u}}_{i,\theta,2}^{\mathrm{T}} \boldsymbol{s} + \boldsymbol{e}_{i,2}^{\mathrm{T}} \begin{bmatrix} y \\ \boldsymbol{z}_{i,2} \end{bmatrix}$$

$$\boldsymbol{E}_i = \boldsymbol{E}_{i,1} + \boldsymbol{E}_{i,2} = (\hat{\boldsymbol{u}}_{i,\theta,1}^{\mathrm{T}} + \hat{\boldsymbol{u}}_{i,\theta,2}^{\mathrm{T}}) \boldsymbol{s} + \boldsymbol{e}_{i,1}^{\mathrm{T}} \begin{bmatrix} \boldsymbol{y} \\ \boldsymbol{z}_{i,1} \end{bmatrix} + \boldsymbol{e}_{i,2}^{\mathrm{T}} \begin{bmatrix} \boldsymbol{y} \\ \boldsymbol{z}_{i,2} \end{bmatrix} = \hat{\boldsymbol{u}}_i^{\mathrm{T}} s + \mathrm{error}$$

选取特定的参数，错误项 error 可忽略。

根据 Shamir 秘密共享方案中的[13]拉格朗日差值公式 $\boldsymbol{u} = \sum_{j\in J} L_j \hat{u}_j$ 恢复出 $c' = \boldsymbol{u}^{\mathrm{T}} s + \mathrm{error}'$，其

中,拉格朗日系数为 $L_j=\frac{\prod_{i\in J,i\neq j}-i}{\prod_{i\in J,i\neq j}(j-i)}$。

最后计算 $c_0-c'=M\lfloor\frac{q}{2}\rfloor+\text{error}''$,若 $\left|c_0-c'-\lfloor\frac{q}{2}\rfloor\right|\leqslant\lfloor\frac{q}{4}\rfloor$,返回 $M=1$,反之,返回 0。

3 性能分析

3.1 正确性

当用户的属性满足访问控制策略的门限值时,即 $|S\cap W|\geqslant k$,我们有 $|S'\cap W'|\geqslant d+1$。选取一个属性集合,里面包含 $d+1$ 个合法属性。由上一节可知:

$$E_i=E_{i,1}+E_{i,2}=\boldsymbol{e}_{i,1}^{\mathrm{T}}\begin{bmatrix}c_{i,0}\\c_{i,1}\end{bmatrix}+\boldsymbol{e}_{i,2}^{\mathrm{T}}\begin{bmatrix}c_{i,0}\\c_{i,1}\end{bmatrix}=$$

$$\boldsymbol{e}_{i,1}^{\mathrm{T}}\left[\frac{\boldsymbol{A}_0^{\mathrm{T}}\boldsymbol{s}}{(\boldsymbol{A}_i+\boldsymbol{B}_1)^{\mathrm{T}}\boldsymbol{s}}\right]+\boldsymbol{e}_{i,1}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{y}\\z_{i,1}\end{bmatrix}+$$

$$\boldsymbol{e}_{i,2}^{\mathrm{T}}\left[\frac{\boldsymbol{A}_0^{\mathrm{T}}\boldsymbol{s}}{(H(t_i)+\boldsymbol{B}_2)^{\mathrm{T}}\boldsymbol{s}}\right]+\boldsymbol{e}_{i,2}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{y}\\z_{i,2}\end{bmatrix}=$$

$$([\boldsymbol{A}_0|(\boldsymbol{A}_i+\boldsymbol{B}_1)]\boldsymbol{e}_{i,1})^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e}_{i,1}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{y}\\\boldsymbol{z}_{i,1}\end{bmatrix}+$$

$$([\boldsymbol{A}_0|(H(t_i)+\boldsymbol{B}_2)]\boldsymbol{e}_{i,2})^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e}_{i,2}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{y}\\\boldsymbol{z}_{i,2}\end{bmatrix}=$$

$$(\hat{\boldsymbol{u}}_{i,\theta,1}^{\mathrm{T}}+\hat{\boldsymbol{u}}_{i,\theta,2}^{\mathrm{T}})\boldsymbol{s}+\boldsymbol{e}_{i,1}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{y}\\\boldsymbol{z}_{i,1}\end{bmatrix}+\boldsymbol{e}_{i,2}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{y}\\\boldsymbol{z}_{i,2}\end{bmatrix}=\hat{\boldsymbol{u}}_i^{\mathrm{T}}\boldsymbol{s}+\text{error}$$

根据拉格朗日差值公式 $u=\sum_{j\in J}L_j\hat{u}_j$ 恢复出 $c'=\boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}+\text{error}'$。

为保证算法的正确性我们需要:①确保 LWE 的困难性,即 $\alpha q>2\sqrt{n}$。②TrapGen(q,n)能够运行$(m>6n\log q)$。③确保 SampleLeft 能够正确运行,$s>\|\tilde{T}_{A_0}\|\cdot\omega(\sqrt{\log 2m})$。④保证 SampleLeft 和 SampleRight 输出结果不可区分,$s_i>\|\tilde{T}_{B_i}\|\cdot\sqrt{m}\cdot\omega(\log m)$,$i\in\{1,2\}$。⑤保证误差项可忽略,$\text{error}''<q/5$。

3.2 安全性

定理 2 如果解决 LWE 问题是困难的,则本方案在选择明文攻击下是选择性安全的。

证明:假设攻击者拥有一个概率多项式时间算法∂,能够对方案进行选择性攻击。假设攻击者以 Adv(∂)的优势攻破上述方案,那么我们构建一个以优势 $\mathrm{Adv}_{q,\chi}^{lwe}(\Im)$解决 LWE 问题的算法 $\Im$。攻击者∂—挑战者 $\Im$ 游戏模型构造如下:

3.2.1 初始化

1)挑战者 $\Im$ 拥有一个随机预言机,试图判断随机预言机的输出分布是属于 $A_{s,\chi}$ 分布,还是属于均匀分布。令属性集合 $R=\{1,\cdots,l\}$,默认属性集合 $D=\{l+1,\cdots,l+d\}$,并且 $R'=R\cup D$。

2)攻击者∂提交一个访问控制策略(W^*,k^*)给挑战者 $\Im$,其中 $1\leqslant k^*\leqslant\min(|W^*|,d)$。令 $W'=W^*\cup\{l+1,\cdots,l+d+1-k^*\}$。

3) 挑战者 $\Im$ 接收到(W^*,k^*)之后,$\Im$ 从随机预言机中获取$(\boldsymbol{u},\boldsymbol{v}_u)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$,$(\boldsymbol{A}_0,\boldsymbol{v}_0)\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^m$。利用 TrapGen$(q,n)$分别生成$(\boldsymbol{B}_1,\boldsymbol{T}_{B_1})$,$(B_2,T_{B_2})$。对于 $i\in W'$,$\Im$ 随机选择$\boldsymbol{R}_{i,1}^*,\boldsymbol{R}_{i,2}^*\in\{-1,1\}^{m\times m}$,计算$\boldsymbol{A}_i=\boldsymbol{A}_0\boldsymbol{R}_{i,1}^*-\boldsymbol{B}_1$,$H(t_i^*)=\boldsymbol{A}_0\boldsymbol{R}_{i,2}^*-\boldsymbol{B}_2$。对于 $i\in R'/W'$,$\Im$ 随机选择$\boldsymbol{R}_{i,1}^*,\boldsymbol{R}_{i,2}^*\in\{-1,1\}^{m\times m}$,计算$\boldsymbol{A}_i=\boldsymbol{A}_0\boldsymbol{R}_{i,1}^*$,$H(t_i^*)=\boldsymbol{A}_0\boldsymbol{R}_{i,2}^*$。

4)挑战者设置公钥为$(\boldsymbol{A}_0,\boldsymbol{B}_1,\boldsymbol{B}_2,\{\boldsymbol{A}_i\}_{i\in R'},\boldsymbol{u})$,私钥为$(\boldsymbol{T}_{\boldsymbol{B}_1},\boldsymbol{T}_{\boldsymbol{B}_2},\{R_{i,1}^*,R_{i,2}^*\}_{i\in R'},v_u,v_0)$。

3.2.2 问询阶段

攻击者∂可以问询挑战者,挑战者返回问询属性对应的私钥:

1)当攻击者问询的属性 $S\in R$ 满足访问控制策略(W^*,k^*)时,挑战者返回$\perp$。

2) 当攻击者问询的属性 $S\in R$ 不满足访问控制策略(W^*,k^*),即 $|S\cap W^*|\leqslant t^*-1$,令 $S'=S\cup\{l+1,\cdots,l+d\}$,$|S'\cap W'|\leqslant d$。选择一个子集 $\hat{S}$,满足 $S'\cap W'\subseteq\hat{S}\subset S'$,$|\hat{S}|=d$。

3)对于 $i\in\hat{S}$,定义$\boldsymbol{E}_{i,1}=(\boldsymbol{A}_0|\boldsymbol{A}_i+\boldsymbol{B}_1)$,$\boldsymbol{E}_{i,2}=(\boldsymbol{A}_0|H(t_i)+\boldsymbol{B}_2)$。选择$\boldsymbol{e}_{i,1},\boldsymbol{e}_{i,2}\leftarrow D_{\mathbb{Z}^{2m},s}$,计算$\hat{\boldsymbol{u}}_{i,1}=\boldsymbol{E}_{i,1}\boldsymbol{e}_{i,1}$,$\hat{\boldsymbol{u}}_{i,2}=\boldsymbol{E}_{i,2}\boldsymbol{e}_{i,2}$。$\hat{\boldsymbol{u}}_i=\hat{\boldsymbol{u}}_{i,1}+\hat{\boldsymbol{u}}_{i,2}$。

4)选取 n 个次数为 d 的多项式 $p_1(x),\cdots,p_n(x)\in\mathbb{Z}_q[x]$,使得 $u=(p_1(0),\cdots,p_n(0))^{\mathrm{T}}$。对于每一个 $i\in\hat{S}$,$\hat{\boldsymbol{u}}_i=(p_1(i),\cdots,p_n(i))^{\mathrm{T}}$,通过拉格朗日插值公式我们可以恢复多项式 $p_1(x),\cdots,p_n(x)\in\mathbb{Z}_q[x]$。

5)如果 $i\in S'/\hat{S}$,即 $i\notin W'$时

$\boldsymbol{E}_{i,1}=(\boldsymbol{A}_0|\boldsymbol{A}_i+\boldsymbol{B}_1)=(\boldsymbol{A}_0|\boldsymbol{A}_0\boldsymbol{R}_{i,1}^*+\boldsymbol{B}_1)$

$\boldsymbol{E}_{i,2}=(\boldsymbol{A}_0|H(t_i)+\boldsymbol{B}_2)=(\boldsymbol{A}_0|\boldsymbol{A}_0\boldsymbol{R}_{i,2}^*+\boldsymbol{B}_2)$。

使用基向量$\boldsymbol{T}_{B_1}$,$\boldsymbol{T}_{B_2}$,运行 SampleRight 算法:

$\boldsymbol{e}_{i,1}\leftarrow\text{SampleRight}(\boldsymbol{A}_0,\boldsymbol{B}_1,\boldsymbol{R}_{i,1}^*,\boldsymbol{T}_{B,1},\hat{\boldsymbol{u}}_{i,1},s_1)$

$\boldsymbol{e}_{i,2}\leftarrow\text{SampleRight}(\boldsymbol{A}_0,\boldsymbol{B}_2,\boldsymbol{R}_{i,2}^*,\boldsymbol{T}_{B,2},\hat{\boldsymbol{u}}_{i,2},s_2)$

返回密钥为$(\boldsymbol{e}_{i,1},\boldsymbol{e}_{i,2})$。

3.2.3 挑战阶段

攻击者提交 2 个消息比特 $M_0,M_1\in\{0,1\}$发送给挑战者,挑战者随机选取 $b\in\{0,1\}$,计算 $c_0=v_u+M_b\lfloor\frac{q}{2}\rfloor$,$c'=v_0$。对 $i\in W'$,计算$c_{i,1}=(\boldsymbol{R}_{i,1}^*)^{\mathrm{T}}\boldsymbol{v}_0$ $c_{i,2}=(\boldsymbol{R}_{i,2}^*)^{\mathrm{T}}\boldsymbol{v}_0$。返回挑战密文 $C^*=(c_0,c',\{c_{i,1}\}_{i\in W'},\{c_{i,2}\}_{i\in W'})$。

攻击者仍可以问询密钥,但其问询的属性不能

满足访问控制策略。最后，攻击者判断 b 为 0 或者为 1。游戏结束。

上述游戏使用算法 SampleRight，由文献[6]可知，选取合适参数，由 SampleRight 和 SampleLeft 产生的 e 在概率上是不可区分的。如果随机预言机是关于 s 的，则对于每一个 $i\in W'$，我们有：

$$c_{i,1}=(\boldsymbol{R}_{i,1}^{*})^{\mathrm{T}}(\boldsymbol{A}_0^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{y})=(\boldsymbol{A}_0\boldsymbol{R}_{i,1}^{*})^{\mathrm{T}}\boldsymbol{s}+(\boldsymbol{R}_{i,1}^{*})^{\mathrm{T}}\boldsymbol{y}=(\boldsymbol{A}_i+\boldsymbol{B}_1)^{\mathrm{T}}\boldsymbol{s}+(\boldsymbol{R}_{i,1}^{*})^{\mathrm{T}}\boldsymbol{y}$$

$$c_{i,2}=(\boldsymbol{R}_{i,2}^{*})^{\mathrm{T}}(\boldsymbol{A}_0^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{y})=(\boldsymbol{A}_0\boldsymbol{R}_{i,2}^{*})^{\mathrm{T}}\boldsymbol{s}+(\boldsymbol{R}_{i,2}^{*})^{\mathrm{T}}\boldsymbol{y}=(\boldsymbol{A}_i+\boldsymbol{B}_2)^{\mathrm{T}}\boldsymbol{s}+(\boldsymbol{R}_{i,2}^{*})^{\mathrm{T}}\boldsymbol{y}$$

因为攻击者无法从公钥中获取 $\{\boldsymbol{R}_{i,1}^{*},\boldsymbol{R}_{i,2}^{*}\}_{i\in R'}$ 相关信息，所以攻击者无法区分实际密文分布来自预言机 O_s 还是 $O_{\$}$。如果攻击者能以不可忽略的概率猜出 b 值，那么就存在算法解出 LWE 问题。

3.3　灵活性

本方案引入了默认属性概念，实现了灵活的门限访问控制策略。假设所有的用户均包含一些默认的属性，系统中有 l 个属性，其门限值为 $d(d\leqslant l)$，我们添加 d 个默认属性到系统中。这样一个用户至少拥有 $d+1$ 个属性。利用 Shamir 门限秘密共享方案来恢复密钥，选择一个次数为 d 的随机多项式，并将每一个属性和秘密份额联系在一起。如果加密方希望将门限策略设置为 t/k，即用户拥有在集合 k 中的属性超过 $t\leqslant\min(d,k)$ 个才可以解开密文，其首先选择 $d-t+1$ 个默认属性，使用 $k+(d-t+1)$ 个属性加密消息。因为所有的用户均拥有 $d-t+1$ 个默认的属性，故门限策略更改为 $d+1/k+d-t+1$。实现了灵活的门限策略。

4　结语

属性撤销是属性密码体制中的热点也是难点问题。本文从量子环境下密码的安全性考虑，构建了一个格上属性可撤销的属性加密方案。本方案利用二叉树的结构，通过属性撤销列表完成了对合法用户密钥的更新，实现了格基属性加密算法中的属性撤销。但是本文设计的基于密文策略的属性加密算法，虽然实现了灵活的门限访问控制策略，但是如何在格上构造更加复杂的访问结构（如访问树结构、电路结构等）并且实现属性撤销等问题是下一步将要开展的工作。另外，如何设计出抵抗适应性攻击的算法也是我们下一步将要开展的工作。

参考文献(References)：

[1] 冯登国，陈成.属性密码学研究[J].密码学报，2014，1(1)：1-12.
FENG Dengguo，CHEN Cheng. Research on Attribute-based Cryptography[J]. Journal of Cryptologic Research 2014，1(1)：1-12.(in Chinese)

[2] 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. ACM，2006：89-98.

[3] Sahai A，Seyalioglu H，Waters B. Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption[J]. Advances in Cryptology-CRYPTO 2012，2012：199-217.

[4] 陈燕俐，宋玲玲，杨庚. 基于 CP-ABE 和 SD 的高效云计算访问控制方案[J]. 计算机科学，2014，41(9)：152-157，168.
CHEN Yanli，SONG Lingling，YANG Geng. Efficient Access Control Scheme Combining CP-ABE and SD in Cloud Computing[J]. Computer Science，2014，41(9) 152-157，168.(in Chinese)

[5] Agrawal S，Boyen X，Vaikuntanathan V，et al. Functional Encryption for Threshold Functions (Or Fuzzy Ibe) from Lattices[M]//[s.n.]. Public Key Cryptography-PKC 2012. Berlin Heidelberg：Springer，2012：280-297.

[6] Zhang J，Zhang Z，Ge A. CiphertextPolicy Attribute-Based Encryption from Lattices[C]//Proceedings of the 7th ACM Symposium on Information，Computer and Communications Security. ACM，2012：16-17.

[7] Gorbunov S，Vaikuntanathan V，Wee H. Attribute-Based Encryption for Circuits[C]//Proceedings of the 45th Annual ACM Symposium on Symposium on Theory of Computing. ACM，2013：545-554.

[8] Wang Y. Lattice Ciphertext Policy Attribute-based Encryption in the Standard Model[J]. IJ Network Security，2014，16(4)：358-365.

[9] Chen J，Lim H W，Ling S，et al. RevocableIdentity-Based Encryption from Lattices[C]//Information Security and Privacy. Springer Berlin Heidelberg，2012：390-403.

[10] Micciancio D，Regev O. Worst-case toAverage-Case Reductions Based on Gaussian Measures[J]. SIAM Journal on Computing，2007，37(1)：267-302.

[11] Gentry C，Peikert C，Vaikuntanathan V. Trapdoors forHard Lattices and New Cryptographic Constructions[C]// Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing. ACM，2008：197-206.

[12] Agrawal S，Boneh D，Boyen X. Efficient Iattice (H) IBE in the Standard Model[C]//Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag，2010：553-572.

[13] Shamir A. How to Share A Secret[J]. Communications of the ACM，1979，22(11)：612-613.

（编辑：姚树峰）