格上可撤销的基于身份的适应性安全的加密方案

张彦华* 胡予濮 江明明 来齐齐
(西安电子科技大学综合业务网理论与关键技术国家重点实验室 西安 710071)

摘 要：用户撤销是基于身份的加密(IBE)方案在实际应用中所必须解决的问题。Chen等人在ACISP 2012上给出了第1个格上可撤销的基于身份的加密(RIBE)方案，但其只能达到选择性安全。利用Agrawal等人在欧密2010上给出的IBE方案，该文构造出一个格上适应性安全的RIBE方案，从而解决了Chen等人提出的公开问题；进一步指出利用Singh等人在SPACE 2012上给出的块方法，可以有效地缩短该方案的公钥尺寸。

关键词：密码学；基于身份加密；用户撤销；格；适应性身份安全
中图分类号： TP309 **文献标识码**： A **文章编号**：1009-5896(2015)02-0423-06
DOI: 10.11999/JEIT140421

A Lattice-based Revocable Adaptive-ID Secure Encryption Scheme

Zhang Yan-hua Hu Yu-pu Jiang Ming-ming Lai Qi-qi
(*State Key Laboratory of Integrated Service Networks*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: User revocation is crucial to the practical application of Identity Based Encryption (IBE). The first Revocable Identity Based Encryption (RIBE) scheme from lattice is given by Chen *et al.* in ACISP 2012, but its security can only be proved in the selective-ID model. Using the IBE scheme suggested by Agrawal *et al.* in EUROCPYPT 2010, this paper constructs a lattice-based adaptive-ID secure RIBE scheme, so as to solve a problem left open by Chen *et al.*. This paper also points out that using the blocking technique given by Singh *et al.* in SPACE 2012, the public key size can be reduced effectively.

Key words: Cryptography; Identity Based Encryption (IBE); User revocation; Lattice; Adaptive-ID secure

1 引言

1984年，Shamir[1]首次提出基于身份的公钥密码(Identity Based Encryption, IBE)体制。在此密码体制中，用户的身份标志符(如姓名、e-mail地址等)可以看作公钥，而相应的私钥由可信中心来产生。IBE消除了对用户证书的需求和依赖，极大地简化了密钥管理。基于双线性Diffie-Hellman假设，Boneh等人[2]于2001年给出了第1个有效的IBE方案。自此以后，IBE引起了众多学者的广泛关注，很多基于身份的加密和签名方案被提出[3–5]。

系统用户的公私钥因各种原因有时需要被撤销并替换为新的密钥，例如：与公钥相对应的私钥被偷了；用户丢失了私钥或者不再是一个合法用户。为解决密钥撤销和更新问题，文献[2]提出消息的发送者在进行加密时可将当前的有效时间添加到身份信息中，并且消息的接收者周期性地获得新密钥。然而，上述方法需要可信中心执行非撤销用户的线性级别的工作量，并且可信中心需要与每一位非撤销用户建立安全信道来发送更新后的密钥。最近，Boldyreva等人[6]给出了一个选择性安全的可撤销的基于身份的加密(Revocable Identity Based Encryption, RIBE)方案，使得可信中心执行非撤销用户的对数级别的工作量，这有效地减轻了可信中心的负担，并且第1次获得非交互的密钥撤销，发送者和接收者的效率也得以有效提高。随后，Libert和Vergnaud[7]采用类似的密钥撤销方法将文献[6]改进为适应性安全。

近年来，基于格构造新型密码系统因具有较高的渐进效率、运算简单、抗量子攻击和存在最坏情况下的随机实例等特点，成为后量子时代密码领域的研究热点，并取得了一系列研究成果[8–11]。Chen等人[12]构造出第1个基于格的RIBE方案，但是他们仅获得选择性安全。该文利用Agrawal等人[13]的IBE方案，构造出一个格上适应性安全的RIBE方案，从而解决了Chen等人提出的如何构造格上适应性安全的RIBE方案的公开问题；进一步指出，利用Singh等人[14]给出的块方法，可以有效地缩短本文方案的公钥尺寸。

2014-03-31收到，2014-06-19改回
国家自然科学基金(61173151, 61173152)资助课题
*通信作者：张彦华 yhzhangxidian@163.com

2 基础知识

2.1 格

定义 1 设 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 是 $\mathbb{R}^n$ 上 m 个线性无关的向量，格 Λ 定义为所有这些向量的整数线性组合构成的集合，即

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

其中向量组 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 构成格 Λ 的一组基 $\boldsymbol{B}$。

定义 2 设 q 是一个素数，$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，且 $\boldsymbol{u}\in\mathbb{Z}_q^n$，定义

$$\left.\begin{aligned}\Lambda_q^{\perp}(\boldsymbol{A})&=\{\boldsymbol{x}\in\mathbb{Z}^m\,|\boldsymbol{A}\boldsymbol{x}=\boldsymbol{0}\bmod q\}\\ \Lambda_q^{\boldsymbol{u}}(\boldsymbol{A})&=\{\boldsymbol{x}\in\mathbb{Z}^m\,|\boldsymbol{A}\boldsymbol{x}=\boldsymbol{u}\bmod q\}\end{aligned}\right\}\tag{1}$$

定义 3 对任意 $s>0$，定义以向量 $\boldsymbol{c}$ 为中心，s 为参数的格 Λ 上的离散高斯分布为

$$D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{s,\boldsymbol{c}}(\Lambda)}=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\sum\limits_{\boldsymbol{x}\in\Lambda}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})},$$

$$\boldsymbol{x}\in\Lambda,\ \rho_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2/s^2)\tag{2}$$

2.2 相关算法和困难问题

引理 1[8] 存在概率多项式时间(Probabilistic Polynomial Time, PPT)算法 SampG，输入格 Λ 的一组基 $\boldsymbol{B}$，参数 $s\geq||\widetilde{\boldsymbol{B}}||\cdot\omega(\sqrt{\log_2 n})$ 以及中心 $\boldsymbol{c}\in\mathbb{R}^n$，输出一个统计接近 $D_{\Lambda,s,\boldsymbol{c}}$ 的格向量。

引理 2[8] 设 n 是正整数，素数 $q\geq 2$，$m\geq 2n\log_2 q$，对于除了至多 $2q^{-n}$ 的部分之外所有的 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 以及任意 $s\geq\omega(\sqrt{\log_2 n})$，向量 $\boldsymbol{u}=\boldsymbol{A}\boldsymbol{e}\bmod q$ 的分布统计接近 $\mathbb{Z}_q^n$ 上的均匀分布，其中 $\boldsymbol{e}\in D_{\mathbb{Z}^m,s}$。

引理 3[9] 设 n 是正整数，素数 $q\geq 2$，$m>5n\log_2 q$，存在 PPT 算法 TrapG(q,n)，输出矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}_q^{m\times m}$，其中 $\boldsymbol{A}$ 在 $\mathbb{Z}_q^{n\times m}$ 上是统计均匀的，$\boldsymbol{T}_{\boldsymbol{A}}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基，且满足 $\|\widetilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\leq O(\sqrt{n\log_2 q})$。

引理 4[9] 设 n 是正整数，素数 $q\geq 2$，$m>(n+1)\log_2 q+\omega(\log_2 n)$，则分布 $(\boldsymbol{A},\boldsymbol{A}\boldsymbol{R},\boldsymbol{R}^{\mathrm{T}}\boldsymbol{w})$ 和 $(\boldsymbol{A},\boldsymbol{B},\boldsymbol{R}^{\mathrm{T}}\boldsymbol{w})$ 是统计不可区分的。其中 $\boldsymbol{A}$，$\boldsymbol{B}$ 是 $\mathbb{Z}_q^{n\times m}$ 上的均匀随机矩阵，$\boldsymbol{R}\in\{1,-1\}^{m\times m}$，$\boldsymbol{w}\in\mathbb{Z}_q^n$。

引理 5[13] 设 n 是正整数，素数 $q>2$，$m\geq 2n\log_2 q$，存在 PPT 算法 SampL$(\boldsymbol{A},\boldsymbol{M},\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{u},s)$，输出向量 $\boldsymbol{e}\in\mathbb{Z}^{m+m_1}$，且 $\boldsymbol{e}$ 的分布与 $D_{\Lambda_q^{\boldsymbol{u}}(\boldsymbol{F}_1),s}$ 统计不可区分。其中矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m},\boldsymbol{M}\in\mathbb{Z}_q^{n\times m_1}$，$\boldsymbol{T}_{\boldsymbol{A}}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基，向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$，高斯参数 $s>||\widetilde{\boldsymbol{T}}_{\boldsymbol{A}}||\cdot\omega(\sqrt{\log_2(m+m_1)})$，矩阵 $\boldsymbol{F}_1=(\boldsymbol{A}|\boldsymbol{M})$。特别的，$\boldsymbol{e}\in\Lambda_q^{\boldsymbol{u}}(\boldsymbol{F}_1)$。

引理 6[13] 设 n 是正整数，素数 $q>2$，$m>n$，存在 PPT 算法 SampR$(\boldsymbol{A},\boldsymbol{B},\boldsymbol{R},\boldsymbol{T}_{\boldsymbol{B}},\boldsymbol{u},s)$，输出向量 $\boldsymbol{e}\in\mathbb{Z}^{2m}$，且 $\boldsymbol{e}$ 的分布与 $D_{\Lambda_q^{\boldsymbol{u}}(\boldsymbol{F}_2),s}$ 统计不可区分。其中矩阵 $\boldsymbol{A}$，$\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$，$\boldsymbol{R}\in\{1,-1\}^{m\times m}$，$\boldsymbol{T}_{\boldsymbol{B}}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的陷门基，向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$，高斯参数 $s>||\widetilde{\boldsymbol{T}}_{\boldsymbol{B}}||\cdot\sqrt{m}\cdot\omega(\log_2 m)$，矩阵 $\boldsymbol{F}_2=(\boldsymbol{A}|\boldsymbol{A}\boldsymbol{R}+\boldsymbol{B})$。特别地，$\boldsymbol{e}\in\Lambda_q^{\boldsymbol{u}}(\boldsymbol{F}_2)$。

定义 4[15] 判定性差错学习问题(Decisional Learning With Errors, DLWE) 设 n 是正整数，q 为素数，对任意 $\alpha>0$，定义 Ψ_α 为中心为 $\boldsymbol{0}$，方差为 $\alpha/\sqrt{2\pi}$ 的 $[0,1)$ 上的正态分布，对应的 $\mathbb{Z}_q$ 上的离散分布为 $\overline{\Psi}_\alpha$。设 χ 为 $\mathbb{Z}_q$ 上的差错分布，定义 $A_{\boldsymbol{s},X}$ 为 $(\boldsymbol{u}_i,v_i)=(\boldsymbol{u}_i,\boldsymbol{u}_i^{\mathrm{T}}\boldsymbol{s}+x_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的分布，其中 $\boldsymbol{u}_i\in\mathbb{Z}_q^n$ 是随机选取的向量，$x_i\in\mathbb{Z}_q$ 依分布 X 独立随机选取。$(\mathbb{Z}_q,n,X)$-DLWE 是指区分伪随机分布 $A_{\boldsymbol{s},X}$ 和 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的真随机分布。

2.3 撤销二叉树结构

BT 表示二叉树，Root 表示根节点，若 v 是叶子节点，则 Path(v) 表示 v 到 Root 的路径上所有节点的集合(包含 v 和 Root)。若 θ 非叶子节点，则 θ_l 和 θ_r 分别表示它的左右子节点，每个用户对应一个叶子节点。算法 KUNo 用来计算密钥更新时二叉树 BT 所需要更新的节点的最小集合。算法 KUNo(BT, RL,t): $X,Y\leftarrow\varnothing$(空集合)；$\forall(v_i,t_i)\in$ RL，若 $t_i\leq t$，添加 $\theta\in$ Path(v_i) 到集合 X；$\forall\theta\in X$，若 $\theta_l\notin X$，添加 θ_l 到集合 Y；若 $\theta_r\notin X$，添加 θ_r 到集合 Y；若 $Y=0$，添加 Root 到集合 Y；返回 Y。

3 格上适应性安全的 RIBE 方案

3.1 方案构造

系统建立：输入安全参数 1^n 和最大用户数 N；运行算法 TrapG(q,n) 生成随机矩阵 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$ 和格 $\Lambda_q^{\perp}(\boldsymbol{A}_0)$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{A}_0}$，且 $||\widetilde{\boldsymbol{T}}_{\boldsymbol{A}_0}||\leq O(\sqrt{n\log_2 q})$；选取 $l+1$ 个均匀随机矩阵 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_l$ 及 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$，选取 n 维均匀随机向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$，输出公开参数 PP $=(\boldsymbol{A}_0,\boldsymbol{A}_1,\cdots,\boldsymbol{A}_l,\boldsymbol{B},\boldsymbol{u})$ 和主私钥 MK $=\boldsymbol{T}_{\boldsymbol{A}_0}$。

用户密钥生成：输入公开参数 PP，主私钥 MK，用户身份 id $=(b_1,b_2,\cdots,b_l)\in\{1,-1\}^l$，撤销列表 RL 和状态 ST；从 BT 上选取一个空的叶子节点 v，将用户 id 存储在该节点，令 $\boldsymbol{A}_{\mathrm{id}}=\boldsymbol{B}+\sum_{i=1}^{l}b_i\boldsymbol{A}_i$，$\forall\theta\in$ Path(v)，若 $\boldsymbol{u}_{\theta,1}$，$\boldsymbol{u}_{\theta,2}$ 为空，随机选取 $\boldsymbol{u}_{\theta,1}\in\mathbb{Z}_q^n$，$\boldsymbol{u}_{\theta,2}=\boldsymbol{u}-\boldsymbol{u}_{\theta,2}$，并存储在节点 θ；运行算法

$\mathrm{SampL}(\boldsymbol{A}_0,\ \boldsymbol{A}_{\mathrm{id}},\boldsymbol{T}_{\boldsymbol{A}_0},\boldsymbol{u}_{\theta,1},s)$ 得向量 $\boldsymbol{e}_{\theta,1}\in\mathbb{Z}_q^{2m}$，输出 $\mathrm{SK}_{\mathrm{id}}=\{(\theta,\boldsymbol{e}_{\theta,1})\}_{\theta\in\mathrm{Path}(v)}$ 和 ST。

密钥更新：输入公开参数 PP，主私钥 MK，密钥更新时间 $t=(t_1,t_2,\cdots,t_l)\in\{1,-1\}^l$，撤销列表 RL 和状态 ST；令 $\boldsymbol{A}_t=\boldsymbol{B}+\sum_{i=1}^{l}t_i\boldsymbol{A}_i\in\mathbb{Z}_q^{n\times m}$，$\forall\theta\in\mathrm{KUNo(BT,RL,}t)$，若 $\boldsymbol{u}_{\theta,1},\boldsymbol{u}_{\theta,2}$ 为空，随机选取 $\boldsymbol{u}_{\theta,1}\in\mathbb{Z}_q^n$, $\boldsymbol{u}_{\theta,2}=\boldsymbol{u}-\boldsymbol{u}_{\theta,2}$, 并存储在节点 θ；运行算法 $\mathrm{SampL}(\boldsymbol{A}_0,\boldsymbol{A}_t,\boldsymbol{T}_{\boldsymbol{A}_0},\boldsymbol{u}_{\theta,2},s)$ 得向量 $\boldsymbol{e}_{\theta,2}\in\mathbb{Z}_q^{2m}$，输出 $\mathrm{KU}_t=\{(\theta,\boldsymbol{e}_{\theta,2})\}_{\theta\in\mathrm{KUNo(BT,RL,}t)}$。

解密密钥生成：输入私钥 $\mathrm{SK}_{\mathrm{id}}=\{(i,\boldsymbol{e}_{i,1})\}_{i\in I}$ 和更新密钥 $\mathrm{KU}_t=\{(j,\boldsymbol{e}_{j,2})\}_{j\in J}$，其中 I 和 J 是节点集；若存在 (i,j) 使得 $i=j$，则输出 $\mathrm{DK}_{\mathrm{id},t}=(\boldsymbol{e}_{i,1},\boldsymbol{e}_{j,2})$；否则，$\mathrm{DK}_{\mathrm{id},t}\leftarrow\perp$。由于 $i=j$，简记 $\mathrm{DK}_{\mathrm{id},t}=(\boldsymbol{e}_1,\boldsymbol{e}_2)$。

加密：输入公开参数 PP，用户身份 id，密钥更新时间 t 和消息 $m\in\{0,1\}$；选取 n 维均匀随机向量 $\boldsymbol{s}\in\mathbb{Z}_q^n$ 和 l 个均匀随机矩阵 $\boldsymbol{R}_i\in\{1,-1\}^{m\times m}$，$i=1,2,\cdots,l$；令 $\boldsymbol{F}_{\mathrm{id},t}=\left(\boldsymbol{A}_0\left|\boldsymbol{B}+\sum_{i=1}^{l}b_i\boldsymbol{A}_i\right|\boldsymbol{B}+\sum_{i=1}^{l}t_i\boldsymbol{A}_i\right)\in\mathbb{Z}_q^{3m}$, $\boldsymbol{R}_{\mathrm{id}}=\sum_{i=1}^{l}b_i\boldsymbol{R}_i$, $\boldsymbol{R}_t=\sum_{i=1}^{l}t_i\boldsymbol{R}_i$，选取差错量 $x\xleftarrow{\bar{\Psi}_\alpha}\mathbb{Z}_q$ 和差错向量 $\boldsymbol{y}\xleftarrow{\bar{\Psi}_\alpha^m}\mathbb{Z}_q^m$；令 $\boldsymbol{z}_1=\boldsymbol{R}_{\mathrm{id}}^{\mathrm{T}}\boldsymbol{y}\in\mathbb{Z}_q^m$, $\boldsymbol{z}_2=\boldsymbol{R}_t^{\mathrm{T}}\boldsymbol{y}\in\mathbb{Z}_q^m$，$c_0=\boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}+x+m\left\lfloor\frac{q}{2}\right\rfloor$, $\boldsymbol{c}_1=\boldsymbol{F}_{\mathrm{id},t}^{\mathrm{T}}\boldsymbol{s}+\begin{bmatrix}\boldsymbol{y}\\\boldsymbol{z}_1\\\boldsymbol{z}_2\end{bmatrix}$，输出密文 $\mathrm{CT}_{\mathrm{id},t,m}=(c_0,\boldsymbol{c}_1)\in\mathbb{Z}_q\times\mathbb{Z}_q^{3m}$。

解密：输入公开参数 PP，解密密钥 $\mathrm{DK}_{\mathrm{id},t}=(\boldsymbol{e}_1,\boldsymbol{e}_2)$ 和密文 $\mathrm{CT}_{\mathrm{id},t,m}=(c_0,\boldsymbol{c}_1)$；令 $\boldsymbol{c}_1=\begin{bmatrix}\boldsymbol{c}_{1,0}\\\boldsymbol{c}_{1,1}\\\boldsymbol{c}_{1,2}\end{bmatrix}$，其中 $\boldsymbol{c}_{1,i}\in\mathbb{Z}_q^m$，计算 $w=c_0-\boldsymbol{e}_1^{\mathrm{T}}\begin{bmatrix}\boldsymbol{c}_{1,0}\\\boldsymbol{c}_{1,1}\end{bmatrix}-\boldsymbol{e}_2^{\mathrm{T}}\begin{bmatrix}\boldsymbol{c}_{1,0}\\\boldsymbol{c}_{1,2}\end{bmatrix}=m\left\lfloor\frac{q}{2}\right\rfloor+x-\boldsymbol{e}_1^{\mathrm{T}}\begin{bmatrix}\boldsymbol{y}\\\boldsymbol{z}_1\end{bmatrix}-\boldsymbol{e}_2^{\mathrm{T}}\begin{bmatrix}\boldsymbol{y}\\\boldsymbol{z}_2\end{bmatrix}\in\mathbb{Z}_q$，若 $\left|w-\left\lfloor\frac{q}{2}\right\rfloor\right|<\left\lfloor\frac{q}{4}\right\rfloor$，输出 1；否则，输出 0。

用户撤销：输入用户身份 id，密钥更新时间 t，撤销列表 RL 和状态 ST，添加 id 对应节点 v 与时间 t 到撤销列表 RL，并输出新的撤销列表 RL。

3.2 参数设置

与文献[13]一样，噪声上界为 $q\sigma lm\alpha\cdot\omega(\sqrt{\log_2 m})+O(\sigma m^{3/2})$，为保证噪声小于 $q/5$ 和系统的有效运行，设置参数如下：$m=6n^{1+\delta}$，$q=\max(2Q,m^2\sqrt{n}\cdot\omega(\sqrt{\log_2 n}))$，$s=ml\cdot\omega(\sqrt{\log_2 n})$，$\alpha=[l^2m^2\cdot\omega(\sqrt{\log_2 n})]^{-1}$, $n^\delta>\lceil\log_2 q\rceil=O(\log_2 n)$，其中 Q 是敌手进行用户密钥询问的次数。

3.3 安全性证明

解密的正确性显然成立。利用类似文献[13]的 Abort-Resistant 哈希函数：设 q 为素数，令 $(\mathbb{Z}_q^l)^*=\mathbb{Z}_q^l\setminus\{0^l\}$，定义 $\mathrm{H}=\{H_h:(\mathbb{Z}_q^l)^*\to\mathbb{Z}_q\}:\mathrm{H}_h(\mathrm{id})=\left(1+\sum_{i=1}^{l}h_ib_i\right)$，$\mathrm{H}_h(t)=\left(1+\sum_{i=1}^{l}h_it_i\right)$，其中 $h_i\in\mathbb{Z}_q$。

定理　若 $(\mathbb{Z}_q,n,\overline{\Psi}_\alpha)$-DLWE 假设成立，则本文的 RIBE 方案是适应性身份选择明文攻击安全的。

证明　将敌手分为两类：第 1 类，敌手询问过挑战身份 id^*，但是要求在时间 t^* 该用户已被撤销；第 2 类，敌手从未询问过挑战身份 id^*。本文用随机比特 $k\in\{0,1\}$ 作为对敌手类型的一个猜测，W_i 表示敌手在 Game i 中正确猜测出挑战比特这一事件，即在 Game i 结束时，$r'=r$。

Game 0　Game 0 是一个攻击本文方案的攻击者与挑战者进行的适应性身份选择明文攻击的游戏。

Game 1　改变矩阵 $\boldsymbol{A}_i,i=1,2,\cdots,l$ 的生成方式，挑战者在系统建立阶段选取 l 个矩阵 $\boldsymbol{R}_i^*\in\{1,-1\}^{m\times m}$ 和 l 个量 $h_i\in\mathbb{Z}_q,i=1,2,\cdots,l$，构造矩阵 $\boldsymbol{A}_i=\boldsymbol{A}_0\cdot\boldsymbol{R}_i^*+h_i\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$，其中 $i=1,2,\cdots,l$。矩阵 $\boldsymbol{R}_i^*$ 仅用来构造矩阵 $\boldsymbol{A}_i$ 和挑战密文。令 $\boldsymbol{R}^*=(\boldsymbol{R}_1^*|\boldsymbol{R}_2^*|\cdots|\boldsymbol{R}_l^*)$，由引理 4 可知，$(\boldsymbol{A}_0,\boldsymbol{A}_0\cdot\boldsymbol{R}^*,(\boldsymbol{R}^*)^{\mathrm{T}}y)$ 和 $(\boldsymbol{A}_0,(\boldsymbol{A}_1'|\boldsymbol{A}_2'|\cdots|\boldsymbol{A}_l'),(\boldsymbol{R}^*)^{\mathrm{T}}y)$ 统计不可区分，其中 $\boldsymbol{A}_i'\in\mathbb{Z}_q^{n\times m}$ 是均匀独立矩阵。由 $\boldsymbol{z}_1=\boldsymbol{R}_{\mathrm{id}}^{\mathrm{T}}\boldsymbol{y}$，$\boldsymbol{z}_2=\boldsymbol{R}_t^{\mathrm{T}}\boldsymbol{y}$ 可得 $(\boldsymbol{A}_0,\boldsymbol{A}_0\boldsymbol{R}_1^*,\cdots,\boldsymbol{A}_0\boldsymbol{R}_l^*,\boldsymbol{z}_i)$ 和 $(\boldsymbol{A}_0,\boldsymbol{A}_1',\cdots,\boldsymbol{A}_l',\boldsymbol{z}_i)$ 统计不可区分，其中 $i=1,2$。矩阵 $\boldsymbol{A}_0\boldsymbol{R}_i^*$ 是统计均匀的且和 $\boldsymbol{z}_1,\boldsymbol{z}_2$ 相对独立，因此上述构造的 $\boldsymbol{A}_i$ 是统计均匀的。在敌手看来，它们与在 Game 0 中一样，都是独立随机矩阵，从而

$$\Pr[W_0]=\Pr[W_1]\tag{3}$$

Game 2　在 Game 2 中，添加一个在敌手看来独立的终止事件，其他与在 Game 1 中一样。对用户身份集 $I=(\mathrm{id}^*,\mathrm{id}^1,\cdots,\mathrm{id}^Q)$ 和密钥更新时间集 $J=(t^*,t^1,\cdots,t^Q)$，Game 2 中的挑战者进行如下操作：

(1)系统建立阶段，挑战者随机选择一个哈希函数 $h\in H$ 并秘密保留，其他与在 Game 1 中一样。

(2)挑战者对敌手的用户身份，密钥更新询问的应答和挑战密文的生成与在 Game 1 中一样。

(3)猜测阶段，终止检查：检查是否 $H_h(\mathrm{id}^*)=0$,

$H_h(\mathrm{id}^i)\neq 0, H_h(t^*)=0, H_h(t^i)\neq 0$，若不满足，挑战者返回随机比特 $r'\in\{0,1\}$，然后终止游戏。人为终止：引入该操作是为了使得游戏终止概率增大，若存在人为终止，挑战者选择随机比特 $r'\in\{0,1\}$，然后终止游戏。令 $\varepsilon(\cdot)$ 表示没有发生游戏终止的概率，$\varepsilon(\cdot)\in[\varepsilon_{\min},\varepsilon_{\max}]$。

引理 7[13] 假设 W_i 表示敌手在 Game i 中正确猜测出挑战比特这一事件，即在 Game i 结束时，$r=r'$，则 $|\Pr[W_2]-1/2|\geq\varepsilon_{\min}|\Pr[W_1]-1/2|-1/2(\varepsilon_{\max}-\varepsilon_{\min})$，若存在人为终止，$(\varepsilon_{\max}-\varepsilon_{\min})\leq\alpha_{\min}|\Pr[W_1]-1/2|$，因此

$$\begin{aligned}\left|\Pr[W_2]-1/2\right|&\geq 1/2\cdot\alpha_{\min}\left|\Pr[W_1]-1/2\right|\\&\geq 1/4q\cdot\left|\Pr[W_1]-1/2\right|\end{aligned}\tag{4}$$

Game 3 改变每个节点的 $\boldsymbol{u}_{\theta,1},\boldsymbol{u}_{\theta,2}$ 的生成方式，对用户身份 id 满足 $H_h(\mathrm{id})=0$ 和密钥更新时间 t 满足 $H_h(t)=0$ 的询问，挑战者作如下返回：若 $k=0$，模拟与第 1 类敌手的游戏：若 $\theta\in\mathrm{Path}(v)$，运行算法 $\mathrm{SampG}(\boldsymbol{B}_{\mathbb{Z}},s,\boldsymbol{0})$ 得 $\boldsymbol{e}_{\theta,1}$，$\boldsymbol{F}_{\mathrm{id}}=\left(\boldsymbol{A}_0\middle|\boldsymbol{B}+\sum_{i=1}^{l}b_i\boldsymbol{A}_i\right)=(\boldsymbol{A}_0\,|\boldsymbol{A}_0\boldsymbol{R}_{\mathrm{id}})$，令 $\boldsymbol{u}_{\theta,1}=\boldsymbol{F}_{\mathrm{id}}\cdot\boldsymbol{e}_{\theta,1},\boldsymbol{u}_{\theta,2}=\boldsymbol{u}-\boldsymbol{u}_{\theta,1},\boldsymbol{u}_{\theta,2}=\boldsymbol{u}-\boldsymbol{u}_{\theta,1}$，并存储在节点 θ；若 $\theta\notin\mathrm{Path}(v)$，运行算法 $\mathrm{SampG}(\boldsymbol{B}_{\mathbb{Z}},s,\boldsymbol{0})$ 得 $\boldsymbol{e}_{\theta,2}$，$\boldsymbol{F}_t=\left(\boldsymbol{A}_0\middle|\boldsymbol{B}+\sum_{i=1}^{l}t_i\boldsymbol{A}_i\right)=(\boldsymbol{A}_0\,|\boldsymbol{A}_0\boldsymbol{R}_t)$，令 $\boldsymbol{u}_{\theta,2}=\boldsymbol{F}_t\cdot\boldsymbol{e}_{\theta,2},\boldsymbol{u}_{\theta,1}=\boldsymbol{u}-\boldsymbol{u}_{\theta,2}$，并存储在节点 θ。在密钥更新时间 t^*，用户 id^* 已被撤销，因此 $\mathrm{KUNo}(\mathrm{BT},\mathrm{RL},t^*)\cap\mathrm{Path}(v^*)=\varnothing$，挑战者用 $\{(\theta,\boldsymbol{e}_{\theta,1})\}_{\theta\in\mathrm{Path}(v)}$ 和 $\{(\theta,\boldsymbol{e}_{\theta,2})\}_{\theta\in\mathrm{KUNo}(\mathrm{BT},\mathrm{RL},t)}$ 作为对用户身份 id 和密钥更新时间 t 询问的应答。若 $k=1$，模拟与第 2 类敌手的游戏：运行算法 $\mathrm{SampG}(\boldsymbol{B}_{\mathbb{Z}},s,\boldsymbol{0})$ 得 $\boldsymbol{e}_{\theta,2}$，令 $\boldsymbol{u}_{\theta,2}=\boldsymbol{F}_t\cdot\boldsymbol{e}_{\theta,2},\boldsymbol{u}_{\theta,1}=\boldsymbol{u}-\boldsymbol{u}_{\theta,2}$，并存储在节点 θ。由于用户 id^* 从未被询问过，因此挑战者用 $\{(\theta,\boldsymbol{e}_{\theta,2})\}_{\theta\in\mathrm{KUNo}(\mathrm{BT},\mathrm{RL},t)}$ 作为对密钥更新时间 t 询问的返回。

由引理 1 可知，$\boldsymbol{e}_{\theta,1}$ 和 $\boldsymbol{e}_{\theta,2}$ 的分布统计接近 $D_{\mathbb{Z}^m,s}$。$\boldsymbol{F}_{\mathrm{id}}$ 和 $\boldsymbol{F}_t$ 可以看作 $\mathbb{Z}_q^{n\times 2m}$ 上的随机矩阵，由引理 2 可知，$\boldsymbol{u}_{\theta,1}$ 和 $\boldsymbol{u}_{\theta,2}$ 是 $\mathbb{Z}_q^n$ 上统计均匀的。敌手无法区分挑战者的模拟类型，挑战者有 1/2 的概率正确模拟，因此，若游戏被正确模拟，Game 2 和 Game 3 是不可区分的。

Game 4 改变 $\boldsymbol{A}_0$ 和 $\boldsymbol{B}$ 的生成方式，选取随机矩阵 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$，运行算法 TrapG 生成矩阵 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$ 和格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{B}}$。$\boldsymbol{A}_i,i=1,2,\cdots,l$ 的构造与在 Game 3 中一样，即 $\boldsymbol{A}_i=\boldsymbol{A}_0\cdot\boldsymbol{R}_i^*+h_i\boldsymbol{B}$。

$$\boldsymbol{F}_{\mathrm{id}}=\left(\boldsymbol{A}_0\middle|\boldsymbol{B}+\sum_{i=1}^{l}b_i\boldsymbol{A}_i\right)=(\boldsymbol{A}_0\,|\boldsymbol{A}_0\boldsymbol{R}_{\mathrm{id}}+h_{\mathrm{id}}\boldsymbol{B})$$

其中 $\boldsymbol{R}_{\mathrm{id}}=\sum_{i=1}^{l}b_i\boldsymbol{R}_i^*\in\mathbb{Z}_q^{m\times m}$，$h_{\mathrm{id}}=1+\sum_{i=1}^{l}b_ih_i\in\mathbb{Z}_q$。

$$\boldsymbol{F}_t=\left(\boldsymbol{A}_0\middle|\boldsymbol{B}+\sum_{i=1}^{l}t_i\boldsymbol{A}_i\right)=(\boldsymbol{A}_0\,|\boldsymbol{A}_0\boldsymbol{R}_t+h_t\boldsymbol{B})$$

其中 $\boldsymbol{R}_t=\sum_{i=1}^{l}t_i\boldsymbol{R}_i^*\in\mathbb{Z}_q^{m\times m}$，$h_t=1+\sum_{i=1}^{l}t_ih_i\in\mathbb{Z}_q$

挑战者用陷门基 $\boldsymbol{T}_{\boldsymbol{B}}$ 对用户身份 id 的密钥询问和更新密钥时间 t 的更新密钥询问进行应答：若 $H(\mathrm{id})\neq 0$，运行算法 $\mathrm{SampR}(\boldsymbol{A}_0,h_{\mathrm{id}}\boldsymbol{B},\boldsymbol{R}_{\mathrm{id}},\boldsymbol{T}_{\boldsymbol{B}},\boldsymbol{u}_{\theta,1},s)$ 得 $\boldsymbol{e}_{\theta,1}$；若 $H(t)\neq 0$，运行算法 $\mathrm{SampR}(\boldsymbol{A}_0,h_t\boldsymbol{B},\boldsymbol{T}_{\boldsymbol{B}},\boldsymbol{u}_{\theta,2},s)$ 得 $\boldsymbol{e}_{\theta,2}$；若 $H(\mathrm{id})=0$ 或者 $H(t)=0$，与在 Game 3 中一样生成 $\boldsymbol{e}_{\theta,1}$ 或者 $\boldsymbol{e}_{\theta,2}$，并发送给敌手。挑战阶段，挑战者检查挑战身份 $\mathrm{id}^*=(b_1^*,\cdots,b_l^*)$ 和密钥更新时间 $t^*=(t_1^*,\cdots,t_l^*)$ 是否满足 $H(\mathrm{id}^*)=0$，$H(t^*)=0$。若不满足，挑战者与在 Game 3 中一样，终止游戏，并返回一个随机比特 $r'\in\{0,1\}$。猜测阶段，挑战者与在 Game 3 中一样，执行人为终止。在敌手看来，Game 3 和 Game 4 统计不可区分，因此，敌手的优势是相同的，即

$$\Pr[W_3]=\Pr[W_4]\tag{5}$$

Game 5 在 Game 5 中，挑战密文 $(c_0^*,\boldsymbol{c}_1^*)$ 是从 $\mathbb{Z}_q\times\mathbb{Z}_q^{3m}$ 上独立随机选取的，其他与 Game 4 一样。由于挑战密文是随机的，因此敌手的优势为 0。

接下来利用 DLWE 问题的困难性证明对于 PPT 敌手来说，Game 4 和 Game 5 是统计不可区分的。

假设存在一个 PPT 敌手 $\mathcal{A}$ 能以不可忽略的优势区分 Game 4 和 Game 5，本文利用敌手 $\mathcal{A}$ 来构造求解 DLWE 问题的算法 $\mathcal{B}$。模拟者 $\mathcal{B}$ 得到一系列样本 $(\boldsymbol{u}_i,v_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$，其中 $i=0,1,\cdots,m$。

系统建立：模拟者 $\mathcal{B}$ 利用样本生成随机矩阵 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$，矩阵 $\boldsymbol{A}_0$ 的第 i 列是向量 $\boldsymbol{u}_i,i=1,2,\cdots,m$，将样本向量 $\boldsymbol{u}_0$ 作为公共随机矩阵 $\boldsymbol{u}\in\mathbb{Z}_q^n$；与 Game 4 一样生成矩阵 $\boldsymbol{B}$ 和利用随机选择的 h_i 和 $\boldsymbol{R}_i^*$ 构造公共矩阵 $\boldsymbol{A}_i,i=1,2,\cdots,l$；将公开参数 $\mathrm{PP}=(\boldsymbol{A}_0,\boldsymbol{A}_1,\cdots,\boldsymbol{A}_l,\boldsymbol{B},\boldsymbol{u})$ 发送给敌手 $\mathcal{A}$。

询问阶段：模拟者 $\mathcal{B}$ 对敌手 $\mathcal{A}$ 多项式次用户密钥生成，密钥更新和密钥撤销询问的应答与 Game 4 一样。

挑战阶段：敌手 $\mathcal{A}$ 提交挑战身份 id^*，密钥更新

时间 t^* 和信息 $m^* \in \{0,1\}$，模拟者 $\mathcal{B}$ 操作如下：$v_0, v_1, \cdots, v_m$ 表示DLWE问题中的 $m+1$ 个样本分量，令 $\boldsymbol{v}^* = \begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix} \in \mathbb{Z}_q^m$，盲化消息比特得 $c_0^* = v_0 + m^* \lfloor q/2 \rfloor \in \mathbb{Z}_q$，令 $\boldsymbol{R}_{\mathrm{id}^*}^* = \sum_{i=1}^{l} b_i^* \boldsymbol{R}_i^*$，$\boldsymbol{R}_{t^*}^* = \sum_{i=1}^{l} t_i^* \boldsymbol{R}_i^*$，$\boldsymbol{c}_1^* = \begin{bmatrix} \boldsymbol{v}^* \\ (\boldsymbol{R}_{\mathrm{id}^*}^*)^{\mathrm{T}} \boldsymbol{v}^* \\ (\boldsymbol{R}_{t^*}^*)^{\mathrm{T}} \boldsymbol{v}^* \end{bmatrix} \in \mathbb{Z}_q^{3m}$；选取随机比特 $r \in \{0,1\}$，若 $r=0$，将 $c^* = (c_0^*, \boldsymbol{c}_1^*)$ 发送给敌手，反之，随机选择 $(c_0, \boldsymbol{c}_1) \in \mathbb{Z}_q \times \mathbb{Z}_q^{3m}$，并发送给敌手。

若DLWE问题中的分布是伪随机的，那么 c^* 的分布与在Game 4 中一样。此时，$\boldsymbol{F}_{\mathrm{id}^*} = (\boldsymbol{A}_0 \,|\, \boldsymbol{A}_0 \boldsymbol{R}_{\mathrm{id}^*}^*)$，$\boldsymbol{F}_{t^*} = (\boldsymbol{A}_0 \,|\, \boldsymbol{A}_0 \boldsymbol{R}_{t^*}^*)$，由样本定义知道 $\boldsymbol{v}^* = \boldsymbol{A}_0^{\mathrm{T}} \boldsymbol{s} + \boldsymbol{y}$，其中 $\boldsymbol{y} \in \mathbb{Z}_q^m$ 的分布为 $\overline{\Psi}_\alpha^m$。因此，上述定义的 $\boldsymbol{c}_1^*$ 满足

$$\begin{aligned} \boldsymbol{c}_1^* &= \begin{bmatrix} \boldsymbol{A}_0^{\mathrm{T}} \boldsymbol{s} + \boldsymbol{y} \\ (\boldsymbol{R}_{\mathrm{id}^*}^*)^{\mathrm{T}} \boldsymbol{A}_0^{\mathrm{T}} \boldsymbol{s} + (\boldsymbol{R}_{\mathrm{id}^*}^*)^{\mathrm{T}} \boldsymbol{y} \\ (\boldsymbol{R}_{t^*}^*)^{\mathrm{T}} \boldsymbol{A}_0^{\mathrm{T}} \boldsymbol{s} + (\boldsymbol{R}_{t^*}^*)^{\mathrm{T}} \boldsymbol{y} \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{A}_0^{\mathrm{T}} \boldsymbol{s} + \boldsymbol{y} \\ (\boldsymbol{A}_0 \boldsymbol{R}_{\mathrm{id}^*}^*)^{\mathrm{T}} \boldsymbol{s} + (\boldsymbol{R}_{\mathrm{id}^*}^*)^{\mathrm{T}} \boldsymbol{y} \\ (\boldsymbol{A}_0 \boldsymbol{R}_{t^*}^*)^{\mathrm{T}} \boldsymbol{s} + (\boldsymbol{R}_{t^*}^*)^{\mathrm{T}} \boldsymbol{y} \end{bmatrix} \\ &= (\boldsymbol{F}_{\mathrm{id}^*, t^*})^{\mathrm{T}} \boldsymbol{s} + \begin{bmatrix} \boldsymbol{y} \\ (\boldsymbol{R}_{\mathrm{id}^*}^*)^{\mathrm{T}} \boldsymbol{y} \\ (\boldsymbol{R}_{t^*}^*)^{\mathrm{T}} \boldsymbol{y} \end{bmatrix} \in \mathbb{Z}_q^{3m} \end{aligned}$$

上式右端是 Game 4 中挑战密文的 $\boldsymbol{c}_1$；又由 $v_0 = \boldsymbol{u}_0^{\mathrm{T}} \boldsymbol{s} + x$，其中 x 的分布为 $\overline{\Psi}_\alpha$，上述定义中的 c_0^* 满足 $c_0^* = \boldsymbol{u}_0^{\mathrm{T}} \boldsymbol{s} + x + m^* \lfloor q/2 \rfloor$，是 Game 4 中挑战密文的 c_0。

若 DLWE 问题中的分布是真随机的，则 v_0 是 $\mathbb{Z}_q$ 上均匀的，$\boldsymbol{v}^*$ 是 $\mathbb{Z}_q^m$ 上均匀的。由 Left over hash 引理可知上述定义的 $\boldsymbol{c}_1^*$ 是 $\mathbb{Z}_q^{3m}$ 上独立均匀的。因此，挑战密文的分布与在 Game 5 中一样是 $\mathbb{Z}_q \times \mathbb{Z}_q^{3m}$ 上均匀的。

猜测阶段：多项式次适应性询问结束之后，敌手 $\mathcal{A}$ 猜测与之交互的是 Game 4 还是 Game 5。模拟者 $\mathcal{B}$ 输出 $\mathcal{A}$ 的猜测作为对 DLWE 问题的求解。

因此，$\mathcal{B}$ 求解 DLWE 问题的优势与 $\mathcal{A}$ 区分 Game 4 和 Game 5 的优势相同。由于 $\Pr[W_5] = 1/2$，可得

$$\left|\Pr[W_4] - 1/2\right| = \left|\Pr[W_4] - \Pr[W_5]\right| \le \text{DLWE-Adv}_{\mathcal{B}} \quad (6)$$

由式(3)，式(4)，式(5)和式(6)可得

$$\left|\Pr[W_0] - 1/2\right| \le 4q \cdot \text{DLWE-Adv}_{\mathcal{B}} \quad (7)$$

由于不存在 PPT 算法有效求解 DLWE 问题，因此本文的方案是适应性身份选择明文攻击安全的。

Singh 等人在文献[14]中利用块方法将 Agrawal 等人的 IBE 方案的公钥尺寸有效缩短。利用类似的块方法，可以进一步改善本文的方案，缩短公钥尺寸，构造方法为：

用户身份 $\mathrm{id} = (b_1, b_2, \cdots, b_{l'}) \in \{1,-1\}^l$，密钥更新时间 $t = (t_1, t_2, \cdots, t_{l'}) \in \{1,-1\}^l$，其中 b_i 和 t_i 都是 $l/l' = \beta$ 长的串。公开参数 $\mathrm{PP} = (\boldsymbol{A}_0, \boldsymbol{A}_1, \cdots, \boldsymbol{A}_{l'}, \boldsymbol{B}, \boldsymbol{u})$ 和主私钥 $\mathrm{MK} = \boldsymbol{T}_{\boldsymbol{A}_0}$，其他与上述方案类似。

4　结束语

本文利用 Agrawal 等人的 IBE 方案和撤销二叉树结构，构造出一个格上适应性安全的 RIBE 方案。在标准模型下证明了方案的安全性是基于格上 DLWE 问题，从而解决了 Chen 等人提出的公开问题；又利用 Singh 等人的块技术，可以将本文的 RIBE 方案的公钥尺寸进一步缩短，从而提高效率。

参 考 文 献

[1] Shamir A. Identity-based crypto systems and signature schemes[C]. Crypto 1984, Lecture Notes in Computer Science, Santa Barbara, USA, 1985, 196: 47–53.

[2] Boneh D and Franklin M. Identity-based encryption from the weil pairing[C]. Crypto 2001, Lecture Notes in Computer Science, California, USA, 2001, 2139: 213–229.

[3] Paterson K G and Schuldt J C N. Efficient identity based signatures secure in the standard model[C]. Proceedings of the 11th Australasian Conference on Information Security and Privacy, Lecture Notes in Computer Science, Melbourne, Australia, 2006, 4058: 207–222.

[4] Boneh D, Raghunathan A, and Segev G. Function-private identity-based encryption: hiding the function in functional encryption[C]. Crypto 2013, Lecture Notes in Computer Science, Santa Barbara, USA, 2013, 8043: 461–478.

[5] Tessaro S and Wilson D A. Bounded-Collusion identity-based encryption from semantically-secure public-key encryption: generic constructions with short ciphertexts[C]. Proceedings of the 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, 2014, 8383: 257–274.

[6] Boldyreva A, Goyal V, and Kumar V. Identity-based

encryption with efficient revocation[C]. Proceedings of the 15th ACM Conference on Computer and Communications Security, Alexandria, USA, 2008: 417–426.

[7] Libert B and Vergnaud D. Adaptive-ID secure revocable identity-based encryption[C]. Proceedings of the Cryptographers' Track at the RSA Conference, Lecture Notes in Computer Science, San Francisco, USA, 2009, 5473: 1–15.

[8] Gentry C, Peikert C, and Vaikuntanathan V. Trapdoors for hard lattice and new cryptographic constructions[C]. Proceedings of the Symposium on Theory of Computing, Victoria, Canada, 2008: 197–206.

[9] Alwen J and Peikert C. Generating shorter bases for hard random lattices[C]. Proceedings of the 26th International Symposium on Theoretical Aspects of Computer Science, Freiburg, Germany, 2009: 535–553.

[10] Micciancio D and Peikert C. Trapdoors for lattices: simpler, tighter, faster, smaller[C]. Eurocrypt 2012, Lecture Notes in Computer Science, Cambridge, UK, 2012, 7237: 700–718.

[11] Boyen X. Attribute-based functional encryption on lattices [C]. Proceedings of the 10th Theory of Cryptography Conference, Lecture Notes in Computer Science, Tokyo, Japan, 2013, 7785: 122–142.

[12] Chen J, Lim H W, Ling S, *et al*.. Revocable identity-based encryption from lattices[C]. Proceedings of the 17th Australasian Conference on Information Security and Privacy, Lecture Notes in Computer Science, Wollongong, Australia, 2012, 7372: 390–403.

[13] Agrawal S, Boneh D, and Boyen X. Efficient lattice (H)IBE in the standard model[C]. Eurocrypt 2010, Lecture Notes in Computer Science, Riviera, France, 2010, 6110: 553–572.

[14] Singh K, Pandurangan C, and Banerjee A K. Adaptively secure efficient lattice (H)IBE in standard model with short public parameters[C]. Proceedings of the Second International Conference on Security, Privacy and Applied Cryptography Engineering, Chennai, India, 2012: 153–172.

[15] Regev O. On lattices, learning with errors, random linear codes, and cryptography[C]. Proceedings of the Symposium on Theory of Computing, Baltimore, USA, 2005: 84–93.

张彦华： 男，1989 年生，硕博连读生，研究方向为格公钥密码的设计与分析.

胡予濮： 男，1955 年生， 博士生导师，教授，研究方向为信息安全、网络安全.

江明明： 男，1984 年生， 博士，研究方向为格公钥密码、数字签名.