doi:10.11959/j.issn.1000-436x.2017219

新的格上基于身份的分级加密方案

叶青，胡明星，汤永利，刘琨，闫玺玺
（河南理工大学计算机科学与技术学院，河南 焦作 454000）

摘 要：针对格上基于身份的分级加密（HIBE, hierarchical identity-based encryption）体制中用户密钥提取算法复杂度过高和陷门尺寸膨胀率大的问题，提出一种新的 HIBE 方案。首先，利用隐式扩展法对 HIBE 方案中的原像采样算法优化，然后，结合 MP12 陷门派生算法提出一种高效的 HIBE 用户密钥提取算法，并基于该算法结合对偶 LWE 算法完成 HIBE 方案构造。对比分析表明，所提方案的效率较同类方案在系统建立和用户密钥提取阶段均有提升，陷门尺寸与系统分级深度仅成线性增长关系，且优化后的原像采样算法一定程度上可解决 MP12 陷门派生算法在陷门派生后高斯参数增长的问题。在标准模型下，方案安全性归约至判定性 LWE 问题的难解性，并包含严格的安全性证明。

关键词：格；基于身份的分级加密；陷门派生；标准模型；容错学习
中图分类号：TP309 **文献标识码**：A

Novel hierarchical identity-based encryption scheme from lattice

YE Qing, HU Ming-xing, TANG Yong-li, LIU Kun, YAN Xi-xi
(College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China)

Abstract: Aiming at the high complexity in user's private key extraction and large expansion ratio of trapdoor size in previous hierarchical identity-based encryption (HIBE) schemes, a new HIBE scheme was proposed. The implicit extension method to improve preimage sampling algorithm was used, and then combined the improved algorithm with MP12 trapdoor delegation algorithm to construct an efficient HIBE user's private key extraction algorithm. Finally, the new extraction algorithm and the Dual-LWE algorithm was integrated to complete the scheme. Compared with the similar schemes, the efficiency of the proposed scheme was improved in system establishment and user's private key extraction stage, the trapdoor size grows only linearly with the system hierarchical depth, and the improved preimage sample algorithm partly solves the Gaussian parameter increasing problem induced by MP12 trapdoor delegation. The security of the proposed scheme strictly reduces to the hardness of decisional learning with errors problem in the standard model.

Key words: lattice, hierarchical identity-based encryption, trapdoor delegation, standard model, learning with error

1 引言

基于身份的分级加密(HIBE, hierarchical identity-based encryption)体制[1,2]是基于身份加密(IBE, identity-based encryption)体制[3~6]的一种推广，在 IBE 密码体制中，单一的 KGC 在大规模网络中无法满足为每个用户独立地产生身份密钥，因此，在大量的用户请求下，为每个用户完成身份信息的有效验证并为

收稿日期：2017-03-20；**修回日期**：2017-06-05
通信作者：汤永利，yltang@hpu.edu.cn
基金项目：“十三五”国家密码发展基金资助项目（No.MMJJ20170122）；国家自然科学基金资助项目（No.61300216）；河南省科技厅基金资助项目（No.142300410147）；河南省教育厅基金资助项目（No.18A413001, No.16A520013）；河南理工大学博士基金资助项目（No.B2014-044, No.B2016-36）
Foundation Items: The “13th Five-Year” National Crypto Development Foundation (No.MMJJ20170122), The National Natural Science Foundation of China (No.61300216), The Project of Science and Technology Department of Henan Province (No.142300410147), The Project of Education Department of Henan Province (No.18A413001, No.16A520013), Doctoral Fund of Henan Polytechnic University (No.B2014-044, No.B2016-36)

之建立安全信道传送私钥是相当占用系统资源的。因此，需要一种分级的身份基加密体制来完成上述问题，在 HIBE 体制中，多个 KGC 实体按照有向树的结构分布。它的特点是体制中每个子 KGC 陷门均由它的父 KGC 指定，该过程称为陷门派生。应当注意的是陷门派生是单向的，这意味着每个子 KGC 均不能利用它的陷门来恢复父 KGC 陷门。

近几年，基于格理论构造的新型密码体制因具有渐进效率较好、运算简单、可并行化、抗量子攻击和存在最坏情况下的随机实例等优点，成为后量子密码时代的研究热点，并取得一系列的研究成果[7~11]。2010 年，Cash 等[12]于 Eurocrypt'10 上提出一种陷门派生算法，并基于该算法构造了格上首个 HIBE 方案，该方案将用户身份看作由一系列比特组成并为每一比特分配一个均匀随机矩阵，这将导致格的维数随系统分级深度的增加而明显增长，且所提出的陷门派生算法的派生陷门尺寸与系统分级的深度呈二次幂增长关系，则在较高分级深度的 HIBE 体制中会出现陷门尺寸过大而导致系统无法正常使用的问题。另外，该方案采用 Gentry 等[13]于 STOC'08 上提出的原像采样算法，这种原像采样算法需要执行高精度实数的正交化迭代运算，导致用户密钥提取的复杂度过高。同年，Agrawal 等[14]于 Eurocrypt'10 上对 Cash 等的方案进行了改进，将按照用户身份向量每一比特分配矩阵的方式改进为按系统分级中每一级分配一个矩阵的方式，从而使格的维度随着系统分级深度的增长而仅呈线性增长。但方案的陷门派生算法与原像采样算法仍没有改变，因此，用户提取密钥的复杂度和陷门尺寸没有得到根本的改进。2012 年，文献[15]（简称 MP12）提出一种新的格上陷门生成算法和与之对应的原像采样算法，相比之前的陷门生成算法[16]，该陷门生成过程简单，复杂度仅相当于 2 个随机矩阵的一次乘运算，且不涉及计算代价高的 HNF（Hermite normal form）和矩阵求逆操作。相比之前的原像采样算法[13,17]，MP12 原像采样算法较简单高效，且算法支持并行运算且输入项为小整数，对离线空间的需求较低。另外，Micciancio 等还提出了新的陷门派生算法，该算法相比文献[12]的算法较为高效，因为该算法不需对高斯抽样值进行线性无关检测，且消除了 ToBasis 和 HNF 操作，更重要的是派生陷门的尺寸与系统分级的深度仅呈线性增长的关系。但同时本文注意到 MP12 的派生算法也存在不足，陷门派生算法的派生陷门与派生前相比陷门的质量即陷门矩阵的最大奇异值会增长，导致陷门质量变差，进而导致高斯参数增长等一系列问题。因此，采用 MP12 原像采样算法和陷门派生算法来构造 HIBE 方案，会有较低的用户密钥提取复杂度和较小的陷门尺寸膨胀率，但同时应注意避免 MP12 派生算法在构造 HIBE 方案时带来的高斯参数增长的问题。采用 Cash 等[12]提出的隐式扩展法对原像采样算法进行优化，一定程度上可以解决这个问题，且能够避免不必要的计算，降低原像采样算法时间复杂度。Gentry 等[13]指出在构造(H)IBE 方案时应采用对偶 LWE 算法来完成方案的加解密阶段，比采用非对偶 LWE 算法更加合理，随后基于对偶 LWE 算法的(H)IBE 方案[18~22]被相继提出。

为使格上 HIBE 方案更具有实际应用可行性，必须解决用户密钥提取算法复杂度过高和陷门尺寸膨胀率大的问题，因此，本文提出一种新的格上 HIBE 方案，主要贡献有以下几点：1) 利用隐式扩展法对 MP12 原像采样算法在 HIBE 方案中的应用进行改进，解决了陷门派生后原像采样算法的高斯参数会增长的问题；2) 将改进后的原像采样算法与 MP12 陷门派生算法相结合，构造出一种 HIBE 用户密钥提取算法，并与对偶 LWE 算法相结合完成 HIBE 方案构造。采用与同类方案相同的安全模型进行严格的安全性证明，证明结果表明，在标准模型下，本文方案的安全性可归约至判定性容错学习(DLWE, decisional learning with errors)问题的难解性。在效率对比分析中，本文分阶段对比来充分展示所提方案的高效性。首先，在不被系统分级影响的情况下，将系统分级深度设为 1 并选择 3 个 IBE 方案（分级深度为 1 时，HIBE 方案可看作 IBE 方案）来对比，从而展示本方案陷门生成算法在系统建立阶段和原像采样算法在密钥提取阶段的高效性，并指出该优势同样体现在 HIBE 方案中；然后，在不对原像采样算法优化的情况下，选择 4 个 HIBE 方案来对比展示本文方案在陷门派生上的陷门尺寸和格的维度与系统分级深度仅呈线性增长的优势，并指出优势背后存在陷门质量变差导致高斯参数增长的不足；最后，针对存在的不足采用隐式扩展的方法对原像采样算法进行优化，并对优化前后的方案进行对比展示优化效果。

2 预备知识

2.1 格的相关定义

定义 1 格。设 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 是 $\mathbb{R}^n$ 上 m 个线性无关向量，格 Λ 定义为所有这些向量的整系数线性组合，即 $\Lambda=\left\{\sum_{i=1}^{m}x_i\boldsymbol{b}_i : x_i\in\mathbb{Z},i=1,\cdots,m\right\}$，其中，向量组 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 称为格的一组基。

定义 2 q 元格。设 $q,n,m\in\mathbb{Z}$，$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，且 $\boldsymbol{u}\in\mathbb{Z}_q^n$，定义

$$\Lambda^{\perp}(\boldsymbol{A})=\left\{\boldsymbol{x}\in\mathbb{Z}^m:\boldsymbol{A}\boldsymbol{x}=\boldsymbol{0}\bmod q\right\}$$
$$\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})=\left\{\boldsymbol{x}\in\mathbb{Z}^m:\boldsymbol{A}\boldsymbol{x}=\boldsymbol{u}\bmod q\right\}$$

即所有与矩阵 $\boldsymbol{A}$ 行向量模 q 内积为 0 的 m 维列向量构成格 $\Lambda^{\perp}(\boldsymbol{A})$；格 $\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})$ 是格 $\Lambda^{\perp}(\boldsymbol{A})$ 的陪集，满足 $\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})=\Lambda^{\perp}(\boldsymbol{A})+\boldsymbol{t}$，其中，$\boldsymbol{t}\in\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})$。

定义 3 离散高斯分布。对任意 $\sigma>0$，定义以向量 $\boldsymbol{c}$ 为中心，σ 为参数的格 Λ 上的离散高斯分布为 $D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{y})=\dfrac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{y})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}=\dfrac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{y})}{\sum_{\boldsymbol{y}\in\Lambda}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{y})}$，其中，$\boldsymbol{y}\in\Lambda$，$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{y})=\exp\left(\dfrac{-\pi\|\boldsymbol{y}-\boldsymbol{c}\|^2}{\sigma^2}\right)$。

2.2 相关算法和困难问题

本文方案所基于的陷门生成算法和与之对应的原像采样算法分别由引理 1 和引理 3 给出；陷门派生算法由引理 2 给出；隐式扩展法具体请参阅文献[12]；对偶 LWE 算法的具体描述请参考文献[13]；方案的正确性证明基于引理 3、引理 6 和引理 7；方案的安全性证明基于引理 1、引理 3 和定义 4。

引理 1[15] 设整数 $n\geqslant 1$，$q\geqslant 2$ 和充分大的 $m=O(n\mathrm{lb}q)$，$\bar{m}=m-nk$，$w=nk$，$k=\lceil\mathrm{lb}q\rceil$，可逆矩阵 $\boldsymbol{H}\in\mathbb{Z}_q^{n\times n}$，构造公开的矩阵 $\boldsymbol{G}\in\mathbb{Z}_q^{n\times w}$。选取一个均匀随机矩阵 $\bar{\boldsymbol{A}}\in\mathbb{Z}_q^{n\times\bar{m}}$，存在概率多项式时间 (PPT, probabilistic polynomial time) 算法 TrapGen$(1^n,q)$，输出矩阵 $\boldsymbol{A}_0=[\bar{\boldsymbol{A}}\|\boldsymbol{H}\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R}_0]\in\mathbb{Z}_q^{n\times m}$ 和陷门矩阵 $\boldsymbol{R}_0\in\mathbb{Z}_q^{\bar{m}\times w}$，陷门尺寸 $s_1(\boldsymbol{R}_0)\leqslant\sqrt{m}\cdot\omega(\sqrt{\mathrm{lb}n})$，其中，$\boldsymbol{A}_0$ 在 $\mathbb{Z}_q^{n\times m}$ 上是统计均匀的，$\boldsymbol{R}_0$ 是矩阵 $\boldsymbol{A}_0$ 的陷门。

引理 2[15] 与引理 1 参数相同，存在概率多项式时间算法 DelTrap，输入矩阵 $\boldsymbol{A}'=[\boldsymbol{A}_0\|\boldsymbol{A}_1]\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^{n\times w}$ 和可逆矩阵 $\boldsymbol{H}'\in\mathbb{Z}_q^{n\times n}$，高斯参数 $\sigma'\geqslant\eta_{\epsilon}(\Lambda^{\perp}(\boldsymbol{A}_0))$，其中，$\epsilon\leqslant\dfrac{1}{2}$，输出陷门矩阵 $\boldsymbol{R}'\in\mathbb{Z}_q^{m\times w}$ 和可逆矩阵 $\boldsymbol{H}\in\mathbb{Z}_q^{n\times n}$，满足 $\boldsymbol{A}_0\boldsymbol{R}'=\boldsymbol{H}'\boldsymbol{G}-\boldsymbol{A}_1$。

引理 3[15] 与引理 1 参数相同，设 d 是系统分级最大深度，$1\leqslant\ell\leqslant d$，$\sigma_{\ell}=s_1(\boldsymbol{R}_{\ell})\omega(\sqrt{\mathrm{lb}n})$ 是充分大的高斯参数，存在概率多项式时间算法 SampleL$(\boldsymbol{A}_{\boldsymbol{id}_{\ell}},\boldsymbol{M},\boldsymbol{R}_{\ell},\boldsymbol{0},\sigma_{\ell})$，其中，$\boldsymbol{M}\in\mathbb{Z}_q^{n\times w}$，$\boldsymbol{A}_{\boldsymbol{id}_{\ell}}=\left[\boldsymbol{A}_0\|\boldsymbol{A}_1+\boldsymbol{H}_{\boldsymbol{id}_1}\boldsymbol{G}\|\boldsymbol{A}_2+\boldsymbol{H}_{\boldsymbol{id}_2}\boldsymbol{G}\|\cdots\|\boldsymbol{A}_{\ell}+\boldsymbol{H}_{\boldsymbol{id}_{\ell}}\boldsymbol{G}\right]\in\mathbb{Z}_q^{n\times(m+\ell w)}$，输出向量 $\boldsymbol{e}\in\mathbb{Z}^{m+\ell w}$，且 $\boldsymbol{e}$ 的分布与 $\mathcal{D}_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}_{\boldsymbol{id}_{\ell}}),\sigma_{\ell}\cdot\omega(\sqrt{\mathrm{lb}n})}$ 统计不可区分，$\Pr[\boldsymbol{e}\leftarrow\mathcal{D}_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}_{\boldsymbol{id}_{\ell}}),\sigma_{\ell}\omega(\sqrt{\mathrm{lb}n})}:\|\boldsymbol{e}\|>\sigma_{\ell}\sqrt{\ell m}]\leqslant negl(n)$，其中，$negl(n)$ 为可忽略函数。

引理 4[14] 与引理 1 参数相同，设 d 是系统分级最大深度，$1\leqslant\ell\leqslant d$，$\sigma_{\ell}=s_1(\boldsymbol{R}_{\ell})\|\bar{\boldsymbol{R}}_{\ell}\|\omega(\sqrt{\mathrm{lb}n})$ 是充分大的高斯参数，选取 ℓ 个均匀随机矩阵 $\bar{\boldsymbol{R}}_{\ell}=\left[\boldsymbol{R}_1^*\|\cdots\|\boldsymbol{R}_{\ell}^*\right]\in\mathbb{Z}_q^{m\times\ell w}$，则存在 PPT 算法 SampleR$\left(\boldsymbol{A}_0,\boldsymbol{G}_{\boldsymbol{id}},\bar{\boldsymbol{R}}_{\ell},\boldsymbol{R}_{\boldsymbol{G}},\boldsymbol{0},\sigma_{\ell}\right)$，其中，$\boldsymbol{G}_{\boldsymbol{id}}=[[\boldsymbol{H}_{\boldsymbol{id}_1}-\boldsymbol{H}_{\boldsymbol{id}_1^*}]\boldsymbol{G}\|\cdots\|[\boldsymbol{H}_{\boldsymbol{id}_{\ell}}-\boldsymbol{H}_{\boldsymbol{id}_{\ell}^*}]\boldsymbol{G}]\in\mathbb{Z}_q^{n\times\ell w}$，输出向量 $\boldsymbol{e}\in\mathbb{Z}^{m+\ell w}$，且 $\boldsymbol{e}$ 的分布与 $\mathcal{D}_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}_{\boldsymbol{id}}),\sigma_{\ell}\omega(\sqrt{\mathrm{lb}\ell n})}$ 统计不可区分。

引理 5[14] 与引理 1 参数相同，设 $m>(n+1)\mathrm{lb}q+\omega(\mathrm{lb}n)$，选取均匀随机矩阵 $\boldsymbol{R}^*\leftarrow\{-1,1\}^{m\times kw}$，$k=k(n)$，则分布 $(\boldsymbol{A}_0,\boldsymbol{A}_0\boldsymbol{R}^*,\boldsymbol{z})$ 与 $(\boldsymbol{A}_0,\boldsymbol{A}_1',\boldsymbol{z})$ 是统计不可区分的，其中，$\boldsymbol{A}_1'$ 在 $\mathbb{Z}_q^{n\times kw}$ 上是统计均匀的，$\boldsymbol{z}=\boldsymbol{R}^{*\mathrm{T}}\boldsymbol{y}\in\mathbb{Z}_q^{kw}$，$\boldsymbol{y}\xleftarrow{\Psi_{\alpha}^m}\mathbb{Z}_q^m$。

引理 6[14] 与引理 1 参数相同，设 $\boldsymbol{e}$ 为 $\mathbb{Z}^{\ell w}$ 中某向量，整数 $w=n\lceil\mathrm{lb}q\rceil$，$1\leqslant\ell\leqslant d$，选取均匀随机矩阵 $\bar{\boldsymbol{R}}\leftarrow\{-1,1\}^{m\times\ell w}$，$C$ 为常数，有 $\Pr[\|\bar{\boldsymbol{R}}\|>C\sqrt{\ell w+m}]<\boldsymbol{e}^{-(\ell w+m)}$。

引理 7[13] 与引理 1 参数相同，设 $\boldsymbol{e}$ 为 $\mathbb{Z}^m$ 中某向量，向量 $\boldsymbol{y}\xleftarrow{\bar{\Psi}_{\alpha}^m}\mathbb{Z}_q^m$，则 $|\boldsymbol{e}^{\mathrm{T}}\boldsymbol{y}|$ 可看作 $[0,q-1]$ 中的整数，满足 $|\boldsymbol{e}^{\mathrm{T}}\boldsymbol{y}|\leqslant\|\boldsymbol{e}\|q\alpha\omega\left(\sqrt{\mathrm{lb}m}\right)+\dfrac{\|\boldsymbol{e}\|\sqrt{m}}{2}$。

定义 4[7] 容错学习问题（LWE, learning with

error）和判定性容错学习问题（DLWE, decisional learning with error）设 n 为正整数，q 为素数，对 $0<\alpha\leqslant\dfrac{1}{\omega\left(\sqrt{\mathrm{lb}n}\right)}$，定义 Ψ_α 为中心是 0，标准差是 $\dfrac{\alpha}{\sqrt{2\pi}}$ 的 $[0,1)$ 上的正态分布，对应的 $\mathbb{Z}_q$ 上的离散分布为 $\bar{\Psi}_\alpha$。设 χ 为 $\mathbb{Z}_q$ 上的错误分布，定义 $A_{\boldsymbol{s},\chi}$ 为 $(\boldsymbol{u}_i,v_i)=\left(\boldsymbol{u}_i,\boldsymbol{u}_i^{\mathrm{T}}\boldsymbol{s}+x_i\right)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的分布，其中，$\boldsymbol{u}_i\in\mathbb{Z}_q^n$ 是随机选取向量，$x_i\in\mathbb{Z}_q$ 依分布 χ 随机独立选取。$\left(\mathbb{Z}_q,n,\chi\right)$-LWE 定义为给出 m 个 $A_{\boldsymbol{s},\chi}$ 上相互独立的变量，求其对应的向量 $\boldsymbol{s}$。$\left(\mathbb{Z}_q,n,\chi\right)$-DLWE 定义为要求以不可忽略的概率区分 $A_{\boldsymbol{s},\chi}$ 伪随机分布和 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的真随机分布，对 $\left(\mathbb{Z}_q,n,\chi\right)$-LWE 问题的求解可在概率多项式时间内归约到 $\left(\mathbb{Z}_q,n,\chi\right)$-DLWE 的求解。

3　算法设计及方案构造

3.1　符号说明

为表述方便，对本文的符号进行说明，如表 1 所示。

表 1　　符号说明

符号	说明
$\boldsymbol{A}^{m\times n}$	m 行 n 列矩阵
$\boldsymbol{A}_i$	矩阵 $\boldsymbol{A}$ 的第 i 行
$\boldsymbol{u}$	向量，默认为列向量形式
$\boldsymbol{u}^{\mathrm{T}}$	向量 $\boldsymbol{u}$ 的转置
$\|S\|$	向量集合 S 的长度，等于其中所有向量欧几里得范数的最大值
$\|\tilde{S}\|$	向量集合 S 的 Gram-Schmidt 范数的最大值
$s_1(\boldsymbol{R})$	矩阵 $\boldsymbol{R}$ 的最大奇异值
$\|\|$	矩阵或向量的拼接
$\lfloor\cdot\rfloor$	向下取整
$negl(n)$	n 的可忽略函数：$f(n)<(n^{-\mathrm{c}})$，c 为常数
$poly(n)$	n 的多项式函数：$f(n)=O(n^{\mathrm{c}})$，c 为常数

3.2　优化的 HIBE 原像采样算法

本文首先利用隐式扩展的方法对引理 3 的原像采样算法在 HIBE 中的应用进行优化，然后与引理 2 的陷门派生算法相结合构造出一种高效的 HIBE 用户密钥提取算法。

结论 1　针对引理 2 所述的陷门派生算法在陷门派生过程中存在高斯参数增长的问题，在原像采样过程中采用隐式扩展的方法可对高斯参数 σ' 优化，同时，可避免对派生矩阵 $\boldsymbol{R}'$ 的计算和存储。

证明　已知MP12输出的派生陷门 $\boldsymbol{R}'\in\mathbb{Z}_q^{m\times w}$ 是非满秩矩阵，相比派生前陷门矩阵 $\boldsymbol{R}\in\mathbb{Z}_q^{\bar{m}\times w}$ 扩张 $m-\bar{m}$ 维，且陷门质量即陷门矩阵的最大奇异值 $s_1(\boldsymbol{R}')>s_1(\boldsymbol{R})$，高斯参数与陷门质量关系为 $s_1(\boldsymbol{R})\omega\left(\sqrt{\mathrm{lb}n}\right)$，则 $\sigma'>\sigma$，因此，原像采样算法 $\boldsymbol{v}\leftarrow SampleL\left(\boldsymbol{R}',\boldsymbol{u}',\sigma'\right)$ 的时间复杂度会因派生陷门维数的扩张而明显提升，且高斯参数 σ' 的增长使算法的输出向量的范数变大。采用隐式扩展的方法可有效解决以上问题，具体算法如下。

设引理 1 中的 TrapGen 算法输出的矩阵和陷门矩阵分别是 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{R}\in\mathbb{Z}_q^{\bar{m}\times w}$，矩阵 $\boldsymbol{A}$ 的扩展矩阵 $\boldsymbol{A}'=\left[\boldsymbol{A}\|\bar{\boldsymbol{A}}\right]\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^{n\times w}$，其中，$\bar{\boldsymbol{A}}\in\mathbb{Z}_q^{n\times w}$ 是均匀随机矩阵。$\boldsymbol{R}'\in\mathbb{Z}_q^{m\times w}$ 是由引理 2 中 DelTrap 算法输出的矩阵 $\boldsymbol{A}'$ 的陷门矩阵。令 $\boldsymbol{a}$ 为 w 维向量，$\mathcal{O}(\boldsymbol{a},\sigma')$ 为用来生成随机均匀且与 $D_{\mathbb{Z}^w,\sigma'}$ 分布统计不可区分向量的算法。

1) 生成 $\bar{\boldsymbol{v}}\leftarrow\mathcal{O}(\boldsymbol{a},\sigma')$，判断 $\bar{\boldsymbol{v}}$ 与 $D_{\mathbb{Z}^w,\sigma'}$ 是否统计接近，如不是，则再次生成。

2) 计算 $\bar{\boldsymbol{u}}=f_{\bar{A}}(\bar{\boldsymbol{v}})=\bar{\boldsymbol{A}}\bar{\boldsymbol{v}}\in\mathbb{Z}_q^n$。

3) 执行算法 $\boldsymbol{v}\leftarrow SampleL(\boldsymbol{R},\boldsymbol{u}'-\bar{\boldsymbol{u}},\sigma)$，输出 $\boldsymbol{v}'=\boldsymbol{v}\|\bar{\boldsymbol{v}}$。

因为 $\mathcal{O}(\boldsymbol{a},\sigma)$ 的输出是随机均匀的，由非齐次小整数解问题（ISIS, inhomogeneous small integer solution problem）可知 $\bar{\boldsymbol{u}}$ 是统计均匀的，再由引理 3 可知原像采样算法的输出向量 $\boldsymbol{v}$ 是统计均匀的，因此，$\boldsymbol{v}'$ 也是统计均匀的。

相比传统的原像采样算法 $\boldsymbol{v}'\leftarrow SampleL(\boldsymbol{R}',\boldsymbol{u}',\sigma')$：步骤 1)所采用的 $\mathcal{O}(\boldsymbol{a},\sigma)$ 算法仅负责生成最终输出向量 $\boldsymbol{v}'$ 的部分，相比调用原像采样算法的递归操作进行完整输出具有明显的计算代价节省；步骤 2)中的 $\bar{\boldsymbol{u}}$ 采用高效正向计算的方式输出，复杂度等同于执行一次散列算法；基于步骤 1)，步骤 3)所执行的原像采样算法仅采用派生前的陷门矩阵和高斯参数即可完成，避免了对派生陷门 $\boldsymbol{R}'$ 矩阵的求解和存储，且一定程度上解决了 MP12 陷门派生算法在陷门派生过程中高斯参数增长的问题。

从以上算法的 3 个步骤可以看出，本文算法优

化了原像采样算法的参数，且节省了原像采样过程中不必要的求解和存储，因此，优化后的算法具有更低的时间复杂度和较高的输出质量。

3.3 高效的 HIBE 用户密钥提取算法

本节利用 MP12 陷门派生算法与 3.2 节所述的优化原像采样算法进行结合，构造出一种高效的 HIBE 用户密钥提取算法。该算法主要完成方案中 HIBE 用户密钥提取操作，如算法 1 所示。

算法 1 HIBE 用户密钥提取算法 HIBE-ExtractSK($MPK, \boldsymbol{A}_{\boldsymbol{id}_{\ell-1}}, \boldsymbol{R}_{\ell-1}, (\boldsymbol{id}_1 \| \cdots \| \boldsymbol{id}_{\ell-1}) \| \boldsymbol{id}_\ell$)

输入 主公钥 MPK，矩阵 $\boldsymbol{A}_{\boldsymbol{id}_{\ell-1}} \in \mathbb{Z}_q^{n\times[m+(\ell-1)w]}$，陷门矩阵 $\boldsymbol{R}_{\ell-1} \in \mathbb{Z}^{\bar{m}(\ell-1)\times w}$ 和用户身份 $(\boldsymbol{id}_1 \| \cdots \| \boldsymbol{id}_{\ell-1}) \| \boldsymbol{id}_\ell \in \mathbb{Z}_q^{\ell n}$。

输出 用户密钥 $\boldsymbol{e}_{\boldsymbol{id}_\ell}$。

1)利用 FRD(full-rank differences)函数[14]将用户身份 $\boldsymbol{id}_\ell$ 映射成矩阵 $\boldsymbol{H}_{id_\ell}$，令 $\boldsymbol{A}_{\boldsymbol{id}_\ell} = \left[\boldsymbol{A}_{\boldsymbol{id}_{\ell-1}} \| \boldsymbol{A}_\ell + \boldsymbol{H}_{\boldsymbol{id}_\ell}\boldsymbol{G}\right]$，其中，$\boldsymbol{A}_\ell$ 是均匀随机矩阵。

2) 执行陷门派生算法 $\boldsymbol{R}_\ell \leftarrow DelTrap^{\mathcal{O}}(\boldsymbol{A}' = [\boldsymbol{A}_{\boldsymbol{id}_{\ell-1}} \| \boldsymbol{A}_\ell + \boldsymbol{H}_{\boldsymbol{id}_\ell}\boldsymbol{G}], \boldsymbol{H}_\ell, \sigma_\ell)$，该算法的具体细节是使用预言机 $\mathcal{O}$ 在格 $\Lambda^\perp(\boldsymbol{A})$ 的合适陪集且高斯参数是 σ_ℓ 的离散高斯分布上进行独立采样，采样的结果作为陷门矩阵 $\boldsymbol{R}_\ell$ 的列向量，最终满足 $\boldsymbol{A}_{\boldsymbol{id}}\boldsymbol{R}_\ell = \boldsymbol{H}_\ell\boldsymbol{G} - (\boldsymbol{A}_\ell + \boldsymbol{H}_{\boldsymbol{id}_\ell}\boldsymbol{G})$。

3)执行优化后的即 3.2 节中的原像采样算法 $\boldsymbol{e}_{id_\ell} \leftarrow SampleL(\boldsymbol{R}_\ell, \boldsymbol{u}_\ell, \sigma_\ell)$，其中，$\sigma_\ell = s_1(\boldsymbol{R}) \cdot \omega(\sqrt{\mathrm{lb}\,\ell n})$，满足 $\boldsymbol{A}_{\boldsymbol{id}_\ell} \cdot \boldsymbol{e}_{\boldsymbol{id}_\ell} = \boldsymbol{u}_\ell$ 且 $\left\|\boldsymbol{e}_{\boldsymbol{id}_\ell}\right\| \leqslant \sigma_\ell\sqrt{m+\ell w}$，输出 $\boldsymbol{e}_{\boldsymbol{id}_\ell}$。

由引理 1 和 *FRD* 函数定义[14]可知 HIBE 用户密钥提取算法第 1)步的矩阵 $\left[\boldsymbol{A}_\ell + \boldsymbol{H}_{\boldsymbol{id}_\ell}\boldsymbol{G}\right]$ 是均匀随机的，由引理 2 可知算法第 2)步的陷门矩阵 $\boldsymbol{R}_\ell$ 的派生过程满足单向性，由引理 3 可知第 3)步原像采样算法的输出与格 $\Lambda_{\boldsymbol{u}}^\perp(\boldsymbol{A}')$ 上的离散高斯分布是统计不可区分的。

随着 HIBE 方案分级深度的增长，MP12 陷门派生算法输出的陷门尺寸与格 $\Lambda^\perp(\boldsymbol{A}')$ 的维度仅呈线性增长关系，而不是二次幂增长关系，并且不需检测所派生陷门的线性无关性，也无需运行计算代价高的 ToBasis 和 HNF 操作。综上，结合 3.2 节，算法 1 的用户密钥提取算法构造安全可行，且具有更低的时间复杂度和陷门尺寸膨胀率。

3.4 方案构造

为解决 HIBE 方案中用户密钥提取算法复杂度过高和陷门尺寸膨胀率大的问题，应从方案的系统建立和用户密钥提取阶段入手。前者的复杂度主要取决于陷门生成算法，后者的复杂度主要取决于陷门派生和原像采样算法。与已有的格上 HIBE 方案相比[12,14,19,22]，本文方案的特点在于首次采用文献[15]提出的陷门生成、原像采样和陷门派生算法来构造方案，提升了系统建立和用户密钥提取阶段的性能和效率；并首次利用隐式扩展的方法对 MP12 原像采样算法进行优化。至于本文方案的加密解密阶段，与其他格上 HIBE 方案[12,14,19,22]类似仍采用对偶 LWE 算法。

方案具体构造如下，其基本参数包括均匀随机矩阵 $\boldsymbol{A}_0 \in \mathbb{Z}_q^{n\times m}$ 和其陷门 $\boldsymbol{R}_0 \in \mathbb{Z}^{\bar{m}\times w}$，其中，$n$ 是安全参数，d 是系统支持的最大分级深度，用户身份 $\boldsymbol{id} = (\boldsymbol{id}_1 \| \cdots \| \boldsymbol{id}_\ell)$，$1 \leqslant \ell \leqslant d$，其中，$\boldsymbol{id}_i \in \mathbb{Z}_q^n \setminus \{0\}$，$i \in [1, \ell]$；一个构造公开的矩阵 $\boldsymbol{G} = \boldsymbol{I}_n \otimes \boldsymbol{g}^{\mathrm{T}} \in \mathbb{Z}_q^{n\times nk}$，其中，$\boldsymbol{I}_n$ 是 $n\times n$ 单位矩阵，$\boldsymbol{g}^{\mathrm{T}} = [1, 2, 2^2, \cdots, 2^{k-1}] \in \mathbb{Z}_q^k$；FRD 函数[14] $H: \mathbb{Z}_q^n \to \mathbb{Z}_q^{n\times n}$。

HIBE-Setup($1^n, d$)：输入安全参数 1^n 和系统最大分级深度 d，运行算法 TrapGen($1^n, q$)，输出均匀随机矩阵 $\boldsymbol{A}_0 \in \mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{A}_0$ 的陷门矩阵 $\boldsymbol{R}_0 \in \mathbb{Z}_q^{\bar{m}\times w}$，且 $s_1(\boldsymbol{R}_0) \leqslant O(\sqrt{n\mathrm{lb}q})\omega(\sqrt{\mathrm{lb}n})$，选取 d 个均匀随机矩阵 $\boldsymbol{A}_1, \cdots, \boldsymbol{A}_d \in \mathbb{Z}_q^{n\times w}$，选取 n 维均匀随机向量 $\boldsymbol{u} \in \mathbb{Z}_q^n$，输出主公钥 $MPK = (\boldsymbol{A}_0, \boldsymbol{A}_1, \cdots, \boldsymbol{A}_d, \boldsymbol{G}, \boldsymbol{u})$ 和主私钥 $MSK = \boldsymbol{R}_0 \in \mathbb{Z}_q^{\bar{m}\times w}$。

HIBE-Extract($MPK, \boldsymbol{R}_{\ell-1}, (\boldsymbol{id}_1 \| \cdots \| \boldsymbol{id}_{\ell-1}) \| \boldsymbol{id}_\ell$)：输入主公钥 MPK，用户身份 $\boldsymbol{id}_\ell \in \mathbb{Z}_q^n$，$\boldsymbol{R}_{\ell-1}$ 表示系统分级深度为 $\ell-1$ 时用户公钥矩阵 $\boldsymbol{A}_{\boldsymbol{id}_{\ell-1}}$ 所对应的陷门，其中，$\boldsymbol{A}_{\boldsymbol{id}_{\ell-1}} = [\boldsymbol{A}_0 \| \boldsymbol{A}_1 + \boldsymbol{H}_{\boldsymbol{id}_1}\boldsymbol{G} \| \boldsymbol{A}_2 + \boldsymbol{H}_{\boldsymbol{id}_2}\boldsymbol{G} \| \cdots \| \boldsymbol{A}_{\ell-1} + \boldsymbol{H}_{\boldsymbol{id}_{\ell-1}}\boldsymbol{G}] \in \mathbb{Z}_q^{n\times[m+(\ell-1)w]}$，调用 3.3 节的用户密钥提取算法 HIBE-ExtractSK($MPK, \boldsymbol{A}_{\boldsymbol{id}_{\ell-1}}, \boldsymbol{R}_{\ell-1}, (\boldsymbol{id}_1 \| \cdots \| \boldsymbol{id}_{\ell-1}) \| \boldsymbol{id}_\ell$)，输出用户密钥 $\boldsymbol{e}_{\boldsymbol{id}_\ell}$。

HIBE-Encrypt$(MPK, \boldsymbol{id}, b)$：输入主公钥 MPK，分级深度为 ℓ 的用户身份 $\boldsymbol{id} = (\boldsymbol{id}_1 \| \cdots \| \boldsymbol{id}_\ell)$ 和待加密消息 $b \in \{0,1\}$。构造矩阵 $\boldsymbol{A}_{\boldsymbol{id}_\ell} = [\boldsymbol{A}_0 \| \boldsymbol{A}_1 + \boldsymbol{H}_{\boldsymbol{id}_1}\boldsymbol{G} \| \boldsymbol{A}_2 + \boldsymbol{H}_{\boldsymbol{id}_2}\boldsymbol{G} \| \cdots \| \boldsymbol{A}_\ell + \boldsymbol{H}_{\boldsymbol{id}_\ell}\boldsymbol{G}] \in \mathbb{Z}_q^{n\times(m+\ell w)}$，其中，$\boldsymbol{H}_{\boldsymbol{id}_i} \leftarrow H(\boldsymbol{id}_i)$，$i \in [1, \ell]$，选取一个均匀随机

向量 $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$，均匀随机矩阵 $\overline{\boldsymbol{R}} \leftarrow \{-1,1\}^{m\times \ell w}$，计算 $c_0 = \boldsymbol{u}^{\mathrm{T}}\boldsymbol{s} + x + b\left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q$，$\boldsymbol{c}_1 = \boldsymbol{A}_{\boldsymbol{id}_\ell}^{\mathrm{T}}\boldsymbol{s} + \begin{bmatrix} \boldsymbol{y} \\ \boldsymbol{z} \end{bmatrix} \in \mathbb{Z}_q^{m+\ell w}$，其中，容错量 $x \xleftarrow{\overline{\Psi}_\alpha} \mathbb{Z}_q$，容错向量 $\boldsymbol{y} \xleftarrow{\overline{\Psi}_\alpha^m} \mathbb{Z}_q^m$，$\boldsymbol{z} = \overline{\boldsymbol{R}}^T\boldsymbol{y} \in \mathbb{Z}_q^{\ell w}$，输出密文 $\boldsymbol{CT} = (c_0, \boldsymbol{c}_1) \in \mathbb{Z}_q \times \mathbb{Z}_q^{m+\ell w}$。

HIBE-Decrypt(MPK, $\boldsymbol{e}_{\boldsymbol{id}_\ell}$, $\boldsymbol{CT}$)：输入主公钥 MPK，密文 $\boldsymbol{CT} = (c_0, \boldsymbol{c}_1)$ 和用户密钥 $\boldsymbol{e}_{\boldsymbol{id}_\ell}$，计算 $b' = c_0 - \boldsymbol{e}_{\boldsymbol{id}_\ell}^{\mathrm{T}}\boldsymbol{c}_1 \in \mathbb{Z}_q$，将 b' 与 $\left\lfloor \frac{q}{2} \right\rfloor$ 视为 $\mathbb{Z}$ 中的整数并比较，如果 $\left| b' - \left\lfloor \frac{q}{2} \right\rfloor \right| < \left\lfloor \frac{q}{4} \right\rfloor$，输出 1，否则输出 0。

4　安全性证明

本文方案采用文献[14]在 Eurocrypt'10 上提出的标准模型下格上 HIBE 方案的 INDr-sID-CPA 安全模型进行安全性证明，基于该安全模型进行安全证明的还有文献[19]和文献[22]提出的 HIBE 方案。

正确性。与文献[14]HIBE 方案的噪声上界相同，上界为 $q\ell^2\sigma_\ell m\alpha_\ell \cdot \omega\left(\sqrt{\mathrm{lb}m}\right) + O\left(\ell^2\sigma_\ell m^{\frac{3}{2}}\right)$，为保证系统有效运行且在 $1 \leqslant \ell \leqslant d$ 中满足噪声小于 $\frac{q}{5}$，设置参数如表 2 所示。在表 2 参数的设置下，本文方案的正确性是显然成立的。

表 2　　**参数设定**

参数	值
m	$2n\mathrm{lb}q$
σ_ℓ	$w\omega\left(\sqrt{\mathrm{lb}n}\right)$
α_ℓ	$\left[wm\omega\left(\sqrt{\mathrm{lb}n}\right)\right]^{-1}$
q	$w\sqrt{m^3}\omega\left(\sqrt{\mathrm{lb}n}\right)$

在表 2 中，本文对参数 m 和 q 采取向上取整的方式取值。

安全性证明。本文方案的安全性由定理 2 刻画。

定理 2　若 $(\mathbb{Z}_q, n, \overline{\Psi}_\alpha)$-DLWE 难解性成立，则本文的 HIBE 方案是 INDr-sID-CPA 安全的。

证明　定理证明采用基于游戏序列的证明方法，用 W_i 来定义攻击者在 Game i 中正确猜测出挑战比特的事件，即在 Game i 结束时，$r' = r$，其中，$r \in \{0,1\}$ 是挑战者为决定挑战密文类型时所使用的随机比特，$r' \in \{0,1\}$ 是在游戏结束时的猜测阶段，攻击者所输出的对挑战比特 r 的猜解，证明对任意 PPT 敌手对挑战比特的猜解优势为 0，攻击者无法以不可忽略的优势在 INDr-sID-CPA 的 Game 中获胜。DLWE 问题用于证明 Game2 和 Game3 是不可区分的。

Game 0　Game 0 是一个攻击本文方案的攻击者与挑战者之间进行的 INDr-sID-CPA 游戏。

Game 1　设 $\boldsymbol{id}^* = \left(\boldsymbol{id}_1^* \| \cdots \| \boldsymbol{id}_k^*\right)$ 为攻击者待攻击的目标，如果 $k < d$，则在空余部分补充 $d-k$ 个零向量。改变 $\boldsymbol{A}_1, \cdots, \boldsymbol{A}_d$ 的生成方式，选取 d 个随机矩阵 $\boldsymbol{R}_1^*, \cdots, \boldsymbol{R}_d^* \leftarrow \{-1,1\}^{m\times w}$，构造矩阵 $\boldsymbol{A}_i = \left[-\boldsymbol{H}_{\boldsymbol{id}_i^*} \cdot \boldsymbol{G} - \boldsymbol{A}_0\boldsymbol{R}_i^*\right]$，$i = 1, \cdots, d$。设 $\overline{\boldsymbol{R}}_k^* = (\boldsymbol{R}_1^* \| \cdots \| \boldsymbol{R}_k^*) \in \{-1,1\}^{m\times kw}$，在挑战阶段使用 $\overline{\boldsymbol{R}}_k^*$ 来生成挑战密文。由引理 5 可知分布 $\left(\boldsymbol{A}_0, \boldsymbol{A}_0\boldsymbol{R}^*, \boldsymbol{z}\right)$ 与分布 $\left(\boldsymbol{A}_0, \boldsymbol{A}_1', \boldsymbol{z}\right)$ 是统计不可区分的，其中，$\boldsymbol{A}_1'$ 是 $n \times dw$ 均匀矩阵，随机矩阵 $\boldsymbol{R}^* \in [-1,1]^{m\times kw}$，$\boldsymbol{z} \leftarrow \left(\overline{\boldsymbol{R}}_k^*\right)^{\mathrm{T}}\boldsymbol{y}$。因此，矩阵 $\boldsymbol{A}_i$ 在 Game1 与 Game0 中是统计不可区分的，在攻击者看来 $\boldsymbol{A}_1, \cdots, \boldsymbol{A}_d$ 在 Game0 和 Game1 中是一样的。从而

$$\Pr[W_0] = \Pr[W_1] \tag{1}$$

Game 2　Game2 与 Game1 的区别在于 Game2 中使用 TrapGen 算法来生成 $\boldsymbol{G} \in \mathbb{Z}_q^{n\times w}$ 和矩阵 $\boldsymbol{G}$ 的陷门矩阵 $\boldsymbol{R}_{\boldsymbol{G}}$，$\boldsymbol{A}_i$ 仍保留为 Game 1 中的形式，$\boldsymbol{A}_i = \left[-\boldsymbol{H}_{id_i^*} \cdot \boldsymbol{G} - \boldsymbol{A}_0\boldsymbol{R}_i^*\right]$。为回应攻击者的用户密钥查询，设查询身份为 $\boldsymbol{id} = \left(\boldsymbol{id}_1 \| \cdots \| \boldsymbol{id}_\ell\right)$，攻击者需输出矩阵 $\boldsymbol{A}_{\boldsymbol{id}}$ 的陷门矩阵，其中，$\boldsymbol{A}_{\boldsymbol{id}} = \left[\boldsymbol{A}_1 \| \cdots \| \boldsymbol{A}_\ell \| \boldsymbol{A}_{\ell+1}\right] + [\boldsymbol{0} \| \boldsymbol{H}_{\boldsymbol{id}_1} \cdot \boldsymbol{G} \| \cdots \| \boldsymbol{0} \| \boldsymbol{H}_{\boldsymbol{id}_\ell} \cdot \boldsymbol{G} \| \boldsymbol{0}] = \left[\boldsymbol{G}_{id} - \boldsymbol{A}_0\overline{\boldsymbol{R}}_\ell\right]$，$\overline{\boldsymbol{R}}_\ell = \left[\boldsymbol{R}_1^* \| \cdots \| \boldsymbol{R}_\ell^*\right] \in \mathbb{Z}_q^{m\times \ell w}$，$\boldsymbol{G}_{id} = \left[\left(\boldsymbol{H}_{\boldsymbol{id}_1} - \boldsymbol{H}_{\boldsymbol{id}_1^*}\right)\boldsymbol{G} \| \cdots \| \left(\boldsymbol{H}_{\boldsymbol{id}_\ell} - \boldsymbol{H}_{\boldsymbol{id}_\ell^*}\right)\boldsymbol{G}\right] \in \mathbb{Z}_q^{n\times \ell w}$，由 FRD 编码函数的定义[14]可知，$\left[\boldsymbol{H}_{\boldsymbol{id}_i} - \boldsymbol{H}_{\boldsymbol{id}_i^*}\right]$ 为可逆矩阵，则挑战者可使用陷门矩阵 $\boldsymbol{R}_{\boldsymbol{G}}$ 进行原像采样来回应攻击者的私钥查询，由安全模型的定义知攻击者的查询 $\boldsymbol{id}$ 不是目标身份 $\boldsymbol{id}^*$ 的前缀，且 $\boldsymbol{id}_i \in \mathbb{Z}_q^n \setminus \{0\}$，$i = 1, \cdots, \ell$，因此，挑战者可使用陷门矩阵 $\boldsymbol{R}_{\boldsymbol{G}}$ 进行原像采样来回应攻击者的用户密钥

查询。若 $\boldsymbol{id} \neq \boldsymbol{id}^*$，调用算法 $\boldsymbol{e}_{id_\ell} \leftarrow \text{SampleR}(\boldsymbol{A}_0, \bar{\boldsymbol{R}}_\ell, \boldsymbol{G}_{id}, \boldsymbol{R}_G, \sigma_\ell)$，输出 $sk_{id} = \boldsymbol{e}_{id_\ell}$ 并发送给攻击者；若 $\boldsymbol{id} = \boldsymbol{id}^*$，则 $\left[\boldsymbol{H}_{id_i} - \boldsymbol{H}_{id_i^*}\right]$ 为零矩阵不可逆，游戏终止并返回一个随机比特 $r' \in \{0,1\}$。由引理 4 可知，当 $\sigma_\ell > s_1(\boldsymbol{R}_\ell)\left\|\bar{\boldsymbol{R}}_\ell\right\|\omega\left(\sqrt{\text{lb}n}\right)$ 时，$\boldsymbol{e}_{id}$ 的分布与 Game1 中的分布 $\mathcal{D}_{\Lambda_u^\perp(\boldsymbol{A}_{id}),\sigma_\ell}$ 是统计不可区分的。因此 Game2 中的私钥查询回应方法和矩阵 $\boldsymbol{G}$ 与 Game1 是统计不可区分的，故攻击者在 Game2 与 Game1 中的优势是相同的，即

$$\Pr[W_2] = \Pr[W_1] \tag{2}$$

Game 3 Game3 与 Game2 的区别在于挑战密文 $\left(c_0^*, \boldsymbol{c}_1^*\right)$ 不再由加密算法生成，而是从密文空间 $\mathbb{Z}_q \times \mathbb{Z}_q^{\ell w+m}$ 中独立随机选取。因为挑战密文是随机选取，所以攻击者的优势可忽略不计。

接下来，利用 DLWE 问题的难解性，证明对于 PPT 敌手来说，Game3 与 Game2 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 Game2 与 Game3，本文利用敌手 $\mathcal{A}$ 来构造求解 DLWE 问题的算法。模拟者 $\mathcal{B}$ 有一系列样本 $\left(\boldsymbol{u}_i, v_i\right) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$，$i = 0,1,\cdots,\bar{m}$。敌手 $\mathcal{A}$ 向模拟者 $\mathcal{B}$ 宣布自己的攻击身份 id^*。

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 $\boldsymbol{A}$ 的第 i 列是向量 $\boldsymbol{u}_i$，$i = 0,1,\cdots,m$，将样本向量 $\boldsymbol{u}_0$ 作为公共随机向量 $\boldsymbol{u} \in \mathbb{Z}_q^n$，其余参数与 Game2 中生成方式相同。

询问阶段。与 Game2 类同，模拟者 $\mathcal{B}$ 对敌手 $\mathcal{A}$ 多项式次密钥生成。

挑战阶段。敌手 $\mathcal{A}$ 提交信息 $b^* \in \{0,1\}$，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 $c_0^* = v_0 + b^*\left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q$，令 $\boldsymbol{c}_1^* = \begin{bmatrix} \boldsymbol{v}^* \\ \left(-\bar{\boldsymbol{R}}_k^*\right)^{\text{T}} \boldsymbol{v}^* \end{bmatrix} \in \mathbb{Z}_q^{m+kw}$，其中，$\bar{\boldsymbol{R}}_k^* = \left[\boldsymbol{R}_1^* \| \cdots \| \boldsymbol{R}_k^*\right]$；选取随机比特 $r \in \{0,1\}$，若 $r = 0$，将 $\left(c_0^*, \boldsymbol{c}_1^*\right)$ 发送给敌手，若 $r = 1$，随机选择 $\left(c_0, \boldsymbol{c}_1\right) \in \mathbb{Z}_q \times \mathbb{Z}_q^{m+kw}$，并发送给敌手。

若 DLWE 问题中的分布是伪随机的，则 $\boldsymbol{c}^*$ 的分布与 Game2 相同。此时 $\boldsymbol{A}_{id^*} = \left[\boldsymbol{A}_0 \| -\boldsymbol{A}_0\bar{\boldsymbol{R}}_k^*\right]$，由样本定义可知 $\boldsymbol{v}^* = \boldsymbol{A}_0^{\text{T}}\boldsymbol{s} + \boldsymbol{y}$，其中，$\boldsymbol{y} \xleftarrow{\bar{\varphi}_\alpha^m} \mathbb{Z}_q^m$。因此，上述定义的 $\boldsymbol{c}_1^*$ 满足

$$\boldsymbol{c}_1^* = \begin{bmatrix} \boldsymbol{A}_0^{\text{T}}\boldsymbol{s} + \boldsymbol{y} \\ -\bar{\boldsymbol{R}}_k^{*\text{T}}\boldsymbol{A}_0^{\text{T}}\boldsymbol{s} - \bar{\boldsymbol{R}}_k^{*\text{T}}\boldsymbol{y} \end{bmatrix} = \begin{bmatrix} \boldsymbol{A}_0^{\text{T}}\boldsymbol{s} + \boldsymbol{y} \\ \left(-\boldsymbol{A}_0^{\text{T}}\bar{\boldsymbol{R}}_k^*\right)^{\text{T}}\boldsymbol{s} - \bar{\boldsymbol{R}}_k^{*\text{T}}\boldsymbol{y} \end{bmatrix}$$

$$= \left(\boldsymbol{A}_{id^*}\right)^{\text{T}}\boldsymbol{s} + \begin{bmatrix} \boldsymbol{y} \\ -\bar{\boldsymbol{R}}_k^{*\text{T}}\boldsymbol{y} \end{bmatrix} \tag{3}$$

式(3)的右端是 Game2 中的挑战密文的 $\boldsymbol{c}_1$。又由 $v_0 = \boldsymbol{u}_0^{\text{T}}\boldsymbol{s} + x$，其中，$x \xleftarrow{\bar{\varphi}_\alpha} \mathbb{Z}_q$，上述定义的 c_0^* 满足 $c_0^* = \boldsymbol{u}_0^{\text{T}}\boldsymbol{s} + x + b^*\left\lfloor \frac{q}{2} \right\rfloor$，是 Game2 中的挑战密文的 c_0。若 DLWE 问题中的分布是真随机的，则 v_0 在 $\mathbb{Z}_q$ 上是均匀的，$\boldsymbol{v}^*$ 在 $\mathbb{Z}_q^m$ 上是均匀的。由标准的左引散列引理[23]可知上述定义的 $\boldsymbol{c}_1^*$ 是 $\mathbb{Z}_q^m$ 上独立均匀的。因此，挑战密文的分布与在 Game3 中同样是 $\mathbb{Z}_q \times \mathbb{Z}_q^{m+kw}$ 上均匀的。

猜测阶段。多项式次选择性询问结束后，敌手 $\mathcal{A}$ 猜测与之交互的是 Game2 还是 Game3。模拟者 $\mathcal{B}$ 输出 $\mathcal{A}$ 的猜测结果作为对 DLWE 问题的求解。

因此，$\mathcal{B}$ 求解 DLWE 问题的优势与 $\mathcal{A}$ 区分 Game2 和 Game3 的优势相同。因为 $\Pr[W_3] = \frac{1}{2}$。所以

$$\left|\Pr[W_2] - \frac{1}{2}\right| = \left|\Pr[W_2] - \Pr[W_3]\right| \leqslant \text{DLWE-Adv}_{\mathcal{B}} \tag{4}$$

由式(1)、式(2)和式(4)可得

$$\left|\Pr[W_0] - \frac{1}{2}\right| \leqslant \text{DLWE-Adv}_{\mathcal{B}} \tag{5}$$

由于不存在 PPT 算法有效求解 DLWE 问题，因此本文方案是 INDr-sID-CPA 安全的。

5 效率分析

当系统分级深度 $d = 1$ 时，HIBE 方案可以看作是 IBE 方案，因此，本节首先令 HIBE 方案中参数 $d = 1$，然后对此 IBE 方案进行效率对比分析，在此基础上，对 3.4 节所提 HIBE 方案进行效率对比分析。

5.1 IBE 方案效率分析

IBE 方案的高效性主要体现在方案的建立阶段和用户密钥提取阶段。方案建立阶段高效与否主要取决于陷门生成算法的复杂度，而用户密钥提取阶段高

表 3　　IBE 方案效率分析对比

方案	格的维数	陷门尺寸/MB	陷门生成复杂度（$\mathbb{Z}_q$ 乘加次数）	原像采样复杂度（$\mathbb{Z}_q$ 乘加次数）	用户公钥尺寸/MB	用户私钥尺寸/KB
文献[5]方案	13 632	22.15	乘 $\approx 64.65\times10^{10}$ 加 $\approx 64.64\times10^{10}$	乘 $\approx 55.75\times10^{7}$ 加 $\approx 74.33\times10^{7}$	22.15	79.92
文献[6]方案	40 896	199.38	乘 $\approx 15.31\times10^{12}$ 加 $\approx 15.30\times10^{12}$	乘 $\approx 50.17\times10^{8}$ 加 $\approx 66.90\times10^{8}$	66.72	239.52
本文方案	13 632	5.54	乘 $\approx 13.74\times10^{9}$ 加 $\approx 13.73\times10^{9}$	乘 $\approx 96.87\times10^{6}$ 加 $\approx 96.87\times10^{6}$	11.08	39.84

效与否取决于原像采样算法的复杂度。在方案建立阶段中，本文采用 Micciancio 等[15]于 Eurocrypt'12 提出的陷门生成算法（MP12 陷门生成算法），相比以往的陷门生成算法[16]，该算法的执行过程简单且输出矩阵的维数较低。另外，MP12 中还提出了与陷门生成算法相对应的原像采样算法，该算法可将原像采样过程中对 $f_{\boldsymbol{A}}^{-1}$ 的求解高效归约至 $f_{\boldsymbol{G}}^{-1}$，相比之前的原像采样算法[13,17]效率明显提升。

在表 3 中，将本文 HIBE 方案在系统分级深度 $d=1$ 的情况下与采用以往陷门生成算法和原像采样算法的 IBE 方案进行对比，对比方案分别是文献[5]方案和文献[6]方案。设安全参数 n =284，$q=2^{24}$。

由表 3 可以看出，本文陷门生成的复杂度约是效率较高的文献[5]方案的 2%，其原因在于 MP12 陷门生成算法在陷门生成过程中不存在计算代价高的 HNF 和矩阵求逆操作，陷门生成的复杂度仅相当于 2 个随机矩阵的一次乘运算，且陷门的生成质量较好即陷门的最大奇异值较低，且输出的矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 的维数仅为 $2n\mathrm{lb}q$ 时，矩阵 $\boldsymbol{A}$ 的分布与均匀分布的统计距离即可满足为安全参数 n 的可忽略函数。另外，陷门生成算法所输出陷门不再是格 $\Lambda^{\perp}(\boldsymbol{A})$ 的格基，而是从特定概率分布随机抽取的短向量组成的陷门矩阵，因此，陷门矩阵的尺寸相比表 3 中其他方案较小。此外，低维数和小的陷门尺寸也是用户公钥和私钥尺寸较短的主要原因。在原像采样复杂度方面，采用与 MP12 陷门生成算法相对应的原像采样算法，本文方案的计算复杂度是文献[5]方案的 17%，原因在于原像采样算法使用小整数作为输入项，不再使用输入项是高精度实数的正交化迭代运算，支持并行化运算，算法的复杂度相比所对比方案的 $O(n^4)$，本算法复杂度为 $O(n^3)$。

另外，表 3 中本文方案用户公钥较短的另一个原因是方案主公钥参数 $\boldsymbol{A}_0$ 的构成仅包含一个与 $\boldsymbol{G}$ 矩阵相同维度 ($\approx n\mathrm{lb}q$) 的非满秩陷门矩阵，相比通常方案采用 2 个满秩陷门矩阵（每个矩阵维度 $\approx 2n\mathrm{lb}q$），明显节省存储开销。该优点与上述分析中的陷门生成算法和原像采样算法的高效优点同样体现在更高的系统分级深度 ($d\geqslant 1$) 的 HIBE 方案中。

5.2　HIBE 方案效率分析

在通常的格上 HIBE 方案中，方案的建立算法的高效与否仍然与陷门生成算法直接相关，但用户密钥提取算法的高效性不仅与原像采样算法的复杂度相关，还与陷门派生算法相关。为突出本文所采用 MP12 陷门派生算法的高效性，本文在不采用 3.2 节优化的原像采样算法的情况下与其他 HIBE 方案作比较。本文方案采用 MP12 陷门派生算法与其他 HIBE 方案相比具有一定的效率提升，且派生的陷门矩阵无须进行线性无关检测和 ToBasis 操作。

本文选择 4 个方案作为参考对比对象。文献[12]方案（CHKP 方案）；文献[14]的 HIBE 方案（ABB 方案）；文献[19]的 HIBE 方案（YZWLY 方案）和 HIBE 方案（WWL 方案）。

为更好体现本文 HIBE 方案的优越性，将 HIBE 陷门派生前的参数与派生后的参数分开对比，派生前的参数如表 4 所示，派生后的参数如表 5 所示。

由表 4 和表 5 对比可以看出，在方案陷门派生后：陷门的维数膨胀率一致，但陷门尺寸上 CHKP、ABB 和 YZWLY 方案均膨胀约 4 倍，而本文方案仅膨胀约 2 倍，原因在于本文方案的陷门矩阵是非满秩矩阵而不是满秩格基，所派生陷门矩阵 $\boldsymbol{R}'\in\mathbb{Z}_q^{m\times w}$，比派生前陷门 $\boldsymbol{R}\in\mathbb{Z}_q^{\bar{m}\times w}$ 仅增加 $w\times w$ 存储，而 CHKP、ABB 和 YZWLY 方案的陷门派生算法输出的陷门矩阵为 $\boldsymbol{R}'=\begin{bmatrix}\boldsymbol{R} & \boldsymbol{W}\\ \boldsymbol{0} & \boldsymbol{I}\end{bmatrix}\in\mathbb{Z}_q^{2m\times 2m}$。因此，

表 4 **HIBE 方案派生前效率分析对比**

方案	陷门维数	用户公钥维数	陷门尺寸/MB	陷门质量	用户公钥尺寸/MB	用户私钥尺寸/KB	明文—密文扩展率	计算效率（$\mathbb{Z}_q$ 乘加次数）		
								陷门生成	原像采样	加密&解密
CHKP 方案	40 896	81 792	199.38	$O\left(\sqrt{n\text{lb}q}\right)$	66.48	9.98	1 963 032	乘≈15.31×10^{12} 加≈15.30×10^{12}	乘≈50.17×10^{8} 加≈66.90×10^{8}	乘≈65.97×10^{8} 加≈65.74×10^{8}
ABB 方案	34 080	68 160	138.46	$O\left(\sqrt{n\text{lb}q}\right)$	55.44	8.32	1 635 864	乘≈12.75×10^{12} 加≈12.74×10^{12}	乘≈34.84×10^{8} 加≈46.46×10^{8}	乘≈54.98×10^{8} 加≈54.78×10^{8}
YZWLY 方案	13 632	27 264	22.15	$O\left(\sqrt{n\ln q}\right)$	22.08	3.33	654 360	乘≈64.65×10^{10} 加≈64.64×10^{10}	乘≈55.75×10^{7} 加≈74.33×10^{7}	乘≈21.99×10^{8} 加≈21.91×10^{8}
WWL 方案	40 896	40 896	199.38	$O\left(n^2\text{lb}^2n\cdot\text{lb}^2q\right)$	33.23	4.99	981 528	乘≈15.31×10^{12} 加≈15.30×10^{12}	乘≈50.17×10^{8} 加≈66.90×10^{8}	乘≈32.99×10^{8} 加≈32.87×10^{8}
本文方案	6 816	13 632	5.54	$O\left(\sqrt{m}+\sqrt{w}\right)$	11.08	1.66	327 192	乘≈13.74×10^{9} 加≈13.73×10^{9}	乘≈96.87×10^{6} 加≈96.87×10^{6}	乘≈11.00×10^{8} 加≈10.96×10^{8}

表 5 **HIBE 方案派生后效率分析对比**

方案	陷门维数	用户公钥维数	陷门尺寸/MB	陷门质量	用户公钥尺寸/MB	用户私钥尺寸/kB	明文—密文扩展率	计算效率（$\mathbb{Z}_q$ 乘加次数）		
								陷门派生	原像采样	加密&解密
CHKP 方案	81 792	122 688	797.50	$O\left(\sqrt{n\text{lb}q}\right)$	99.69	14.98	2 944 536	乘≈16.42×10^{14} 加≈21.89×10^{14}	乘≈20.07×10^{9} 加≈26.76×10^{9}	乘≈98.96×10^{8} 加≈98.61×10^{8}
ABB 方案	68 160	102 240	553.82	$O\left(\sqrt{n\text{lb}q}\right)$	83.04	12.48	2 453 784	乘≈95.00×10^{13} 加≈12.67×10^{14}	乘≈13.94×10^{9} 加≈18.58×10^{9}	乘≈82.46×10^{8} 加≈82.17×10^{8}
YZWLY 方案	27 264	40 896	88.61	$O\left(\sqrt{n\log q}\right)$	33.12	4.99	98 1528	乘≈60.80×10^{12} 加≈81.06×10^{12}	乘≈22.30×10^{8} 加≈29.73×10^{8}	乘≈32.99×10^{8} 加≈32.87×10^{8}
WWL 方案	40 896	40 896	199.38	$O\left(n^3\text{lb}^3n\cdot\text{lb}^3q\right)$	33.23	4.99	981 528	乘≈27.36×10^{13} 加≈34.20×10^{13}	乘≈50.17×10^{8} 加≈66.90×10^{8}	乘≈68.40×10^{12} 加≈68.40×10^{12}
本文方案	13 632	20 448	11.08	$O\left(\sqrt{m}+\sqrt{w}\right)$	16.61	2.50	490 776	乘≈19.80×10^{11} 加≈19.80×10^{11}	乘≈14.53×10^{7} 加≈14.53×10^{7}	乘≈16.49×10^{8} 加≈16.43×10^{8}

随着系统分级深度的增长，本文方案的陷门尺寸呈线性增长，而 CHKP、ABB 和 YZWLY 方案的陷门尺寸呈二次幂增长，这也是本文方案用户的公钥维数和用户的公私钥尺寸相比其他方案增长缓慢的一个原因。同时，用户公私钥尺寸又与明文密文扩展率和计算效率中的加密解密复杂度直接相关。另外，计算效率中陷门生成和原像采样的计算方式与 5.1 节的 IBE 相同，其中，陷门派生的复杂度主要取决于派生过程中的 RandBasis 操作，该操作至少需要调用与派生后陷门维数（设为 m'）相同次数（至多 $O(m'^2)$ 次，具体次数取决于线性无关检测算法的通过率）的原像采样操作，最后还需调用 ToBasis 算法来输出派生陷门。此外，CHKP、ABB 和 YZWLY 的陷门派生操作均需计算一个矩阵 $\boldsymbol{W}$，满足 $\boldsymbol{AW}=-\overline{\boldsymbol{A}}$（$\boldsymbol{A}$ 和 $\overline{\boldsymbol{A}}$ 具体设置参考 3.2 节）。

应该注意的是，WWL 方案具有陷门维数在派生前后保持不变的优点，因此，用户公钥维数和尺寸、陷门尺寸、明文—密文扩展率和原像采样复杂度保持不变。但是，在每次陷门派生过程中 WWL 方案除了需要执行上述的 RandBasis 操作外还需计算 m 个 $m\times m$ 随机可逆矩阵与 m 维随机向量的乘积，因此，陷门派生复杂度明显过高。同时，这也是 WWL 方案的陷门质量的值在派生后会增长导致陷门质量变差的原因。此外，由表 5 可知，已知表 5 的分级深度仅为 2，而 WWL 方案的加解密复杂度已明显高于其他方案，原因在于，假设为分级深度为 ℓ 的用户发送消息，加密者需要计算 ℓ 个 $m\times m$ 矩阵的乘积。因此，WWL 方案难以应用在较高分级深度需求的应用中。

本文方案的陷门派生复杂度仅相当于执行 m'

表 6　　HIBE 方案原像采样算法优化前后效率分析对比

原像采样算法	陷门维数	陷门尺寸/MB	原像采样复杂度（$\mathbb{Z}_q$ 乘加次数）	高斯参数
优化前算法	13 632	11.08	乘 $\approx 14.53\times10^7$ 加 $\approx 14.53\times10^7$	$s_1(\boldsymbol{R}')\omega\left(\sqrt{\mathrm{lb}n}\right)$
优化后算法	6 816	5.54	乘 $\approx 96.87\times10^6$ 加 $\approx 96.87\times10^6$	$s_1(\boldsymbol{R})\omega\left(\sqrt{\mathrm{lb}n}\right)$

次 MP12 原像采样算法，不需额外计算代价过高的 RandBasis 和 ToBasis 操作。但是，由表 4 和表 5 可以看出，除 WWL 方案外所对比方案仍具有本文方案所不具有的优点，陷门矩阵的质量在陷门派生前后保持不变，即 $\left\|\tilde{\boldsymbol{R}}'\right\|=\left\|\tilde{\boldsymbol{R}}\right\|$。本文方案的陷门质量（陷门矩阵的最大奇异值）会在陷门派生后随陷门矩阵维数的增加而增长，造成 $s_1(\boldsymbol{R}')>s_1(\boldsymbol{R})$，则高斯参数 $\sigma'=s_1(\boldsymbol{R}')\omega\left(\sqrt{\mathrm{lb}n}\right)>\sigma=s_1(\boldsymbol{R})\omega\left(\sqrt{\mathrm{lb}n}\right)$，从而使原像长度限制参数 $\beta=\sigma\sqrt{m}$ 增高而影响原像采样算法的输出质量，进一步造成本文方案的陷门函数单向性所依赖的 ISIS 问题所对应的 SIVP(shortest independent vector problem)近似因子 $\beta\tilde{O}(\sqrt{n})$ 增长，从而导致方案所基于难题的难解性有所降低。

以上问题可采用 3.2 节的优化算法来解决，并且可以减少不必要的计算存储以及降低原像采样算法的复杂度，表 6 将展示本文方案采用该算法优化前和优化后的效率对比。

由表 6 可以看出，采用 3.2 节的优化后的原像采样算法可以仅采用派生前的高斯参数完成原像采样过程，解决了上述不足。由表 6 对比表 4 可看出，算法的输入陷门矩阵的维数和尺寸均与派生前相等，因此算法复杂度明显降低。另外，在采用优化算法之后可看出完成派生后的原像采样算法的过程不需派生的陷门矩阵 $\boldsymbol{R}'$ 的参与即可完成，从而节省了对陷门矩阵 $\boldsymbol{R}'$ 的计算和存储消耗。

综上所述，本文方案的陷门派生算法和优化后的原像采样算法所构成的用户密钥提取算法复杂度和陷门尺寸膨胀率低并节省了不必要的存储和计算，且建立阶段的密钥生成算法复杂度较低。因此本文方案总体上是较高效的。

6　结束语

本文提出了一种新的格上基于身份的分级加密方案，新方案利用了隐式扩展的方法对 MP12 原像采样算法在 HIBE 中的应用进行了改进，一定程度上解决了与 MP12 陷门派生算法结合时高斯参数在陷门派生后会增长的问题，并节省了不必要的计算和存储。然后结合 MP12 陷门派生算法构造出一种高效的 HIBE 用户密钥提取算法，最后，结合对偶 LWE 算法完成 HIBE 方案构造。在标准模型下，方案的安全性可归约至判定性容错学习问题(DLWE)的难解性，并给出了严格的安全性证明。对比分析表明，本文方案在系统建立阶段和用户密钥提取阶段效率较同类方案均有提升。

本文方案的不足之出在于陷门派生算法的派生陷门矩阵不支持任意维数的扩展，在某些应用场景中会有使用限制，如何构造支持任意维数扩展的陷门派生算法且用户密钥提取复杂度和陷门尺寸膨胀率低的 HIBE 方案将是值得进一步研究的问题。

参考文献：

[1] GENTRY C,SILVERBERG A. Hierarchical id-based cryptography, advances in cryptology[C]//ASIACRYPT 2002. 2002: 548-566.

[2] HORWITZ J,LYNN B. Toward hierarchical identity-based encryption[C]//EUROCRYPT. 2002: 466-481.

[3] BONEH D, FRANKLIN M. Identity-based encryption from theweil pairing[C]//Advances in Cryptology CRYPTO 2001. 2001: 213-229.

[4] LAI J, DENG R H, LIU S, et al. Identity-based encryption secure against selective opening chosen-ciphertextattack[C]//Advances in Cryptology EUROCRYPT 2012. 2012: 77-92.

[5] YAMADA S. Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters[C]//Advances in Cryptology EUROCRYPT2016. 2016: 32-62.

[6] WANG F H, LIU Z H, WANG C X. Full secure identity-based encryption scheme with short public key size over lattices in the standard model[J]. The International Journal of Computer Mathematics, 2016, 93(6): 854-863.

[7] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. The Annual ACM Symposium on Theory of Computing, 2009, 56(6): 84-93.

[8] NGUYEN P, ZHANG J, ZHANG Z F. Simpler efficient group signatures from lattices[C]//Public-Key Cryptography. 2015: 401-426.

[9] BRAKERSKI Z, PERLMAN R. Lattice-based fully dynamic multi-key FHE with short ciphertexts[C]//CRYPTO2016. 2016: 190-213.

[10] LIBERT B, LING S, NGUYEN K, et al. Zero-knowledge arguments for lattice-based accumulators, logarithmic-size ring signatures and group signatures without trapdoors[C]//Advances in Cryptology EU-

ROCRYPT 2016. 2016: 1-31.

[11] 段然, 顾纯祥, 祝跃飞, 等. NTRU 格上高效的基于身份的全同态加密体制[J]. 通信学报, 2017, 38(1): 66-75.
DUAN R, GU C X, ZHU Y F, et al. Efficient identity-based fully homomorphic encryption over NTRU[J]. Journal on Communications, 2017, 38 (1): 66-75.

[12] CASH D, HOFHEINZ D, KILTZ E, et al. Bonsai trees, or how to delegate lattice basis[C]//Advances in Cryptology EUROCRYPT 2010. 2010, 25(4): 523-552.

[13] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]//The 40th ACM Symposium on Theory of Computing. 2008:197-206.

[14] AGRAWAL S,BONEH D,BOYEN X. Efficient lattice (H)IBE in the standard model[C]//Advances in Cryptology EUROCRYPT2010, 2010: 553-572.

[15] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: simpler, tighter, faster, smaller[C]//Advances in Cryptology EUROCRYPT2012. 2012: 700-718.

[16] ALWEN J, PEIKERT C. Generating shorter bases for hard random lattices [C]//The 26th International Symposium on Theoretical Aspects of Computer Science. 2009: 535-553.

[17] PEIKERT C. An efficient and parallel Gaussian sampler for lattices[C]//Advances in Cryptology CRYPTO 2010. 2010: 80-97.

[18] AGRAWAL S, BOYEN X, VAIKUNTANATHAN V, et al. Functional encryption for threshold functions(or fuzzy IBE) from lattices[C]//15th International Conference on Practice and Theory in Public Key Cryptography. 2012: 280-297.

[19] YANG C, ZHENG S, WANG L, et al. Hierarchical identity-based broadcast encryption scheme from LWE[J]. Journal of Communications & Networks, 2014, 16(3): 258-263.

[20] KATSUMATA S, YAMADA S. Partitioning via non-linear polynomial functions: more compact IBEs from ideal lattices and bilinear maps[C]//Advances in Cryptology ASIACRYPT 2016. 2016: 682-712.

[21] ZHANG J, CHEN Y, ZHANG Z. Programmable hash functions from lattices: short signatures and IBEs with small key sizes[C]//Advances in Cryptology CRYPTO 2016. 2016: 302-332.

[22] WANG F H, WANG C X, LIU Z H. Efficient hierarchical identity based encryption scheme in the standard model over lattices[J]. Frontiers of Information Technology & Electronic Engineering, 2016, 17(8): 781-791.

[23] DODIS Y, OSTROVSKY R, REYZIN L, et al. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data[J]. The Society for Industrial and Applied Mathematics (SIAM), 2008, 38(1): 97-139.

作者简介：

叶青（1981-），女，辽宁营口人，博士，河南理工大学讲师、硕士生导师，主要研究方向为密码学。

胡明星（1994-），男，河南鹿邑人，河南理工大学硕士生，主要研究方向为密码学。

汤永利（1972-），男，河南孟州人，博士后，河南理工大学教授、硕士生导师，主要研究方向为信息安全、密码学。

刘琨（1978-），女，河南焦作人，河南理工大学副教授、硕士生导师，主要研究方向为信息安全、密码学。

闫玺玺（1985-），女，河南灵宝人，博士，河南理工大学讲师、硕士生导师，主要研究方向为密码学。