计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20170394
54(10):2193-2204,2017

基于 LWE 的高效身份基分级加密方案

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)
(yeqing@hpu.edu.cn)

Efficient Hierarchical Identity-Based Encryption Scheme from Learning with Errors

Ye Qing, Hu Mingxing, Tang Yongli, Liu Kun, and Yan Xixi
(*School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, Henan* 454000)

Abstract Hierarchical identity-based encryption (HIBE) in fixed dimension has drawn wide attention because its lattice dimension keeps unchanged upon delegation, but there is a common defect of high complexity in trapdoor delegation stage of these schemes. Aiming at this problem, we propose two improved HIBE schemes under random oracle model and standard model respectively. We first use the MP12 trapdoor function to construct an optimized $\mathbb{Z}_q$-invertible matrix sample algorithm. Based on this optimized algorithm, combined with trapdoor delegation algorithm in fixed dimension and MP12 trapdoor function, we design system setup and trapdoor delegation stages. And we complete the HIBE scheme under random oracle model in conjunction with Dual-Regev algorithm. And then, we remove the random oracle by employing binary tree encryption system. The security of both proposed schemes strictly reduce to the hardness of learning with errors (LWE) problem, in which the scheme under random oracle model satisfies the adaptive security while the scheme under standard model satisfies selective security. Comparative analysis shows that, under the same security level, the overhead of trapdoor delegation in our scheme under random oracle model is reduced significantly compared with the relevant schemes, while the overhead of our scheme under standard model is reduced nearly 6 times compared with the relevant optimal schemes. Furthermore, the parameters such as lattice dimension, trapdoor size and ciphertext expansion rate etc., all decrease in some degree, and the computational cost is reduced obviously.

Key words lattice; hierarchical identity-based encryption (HIBE); trapdoor delegation; learning with errors (LWE); random oracle model; standard model

摘 要 格上可固定维数陷门派生的身份基分级加密(hierarchical identity-based encryption, HIBE)体制,因其具有在陷门派生前后格的维数保持不变的特性而受到广泛关注,但这种体制普遍存在陷门派生复杂度过高的问题.针对这一问题,分别给出随机预言模型和标准模型下的改进方案.首先利用 MP12

收稿日期:2017-06-05;**修回日期**:2017-07-28
基金项目:国家自然科学基金项目(61300216);河南省科技厅基础与前沿技术研究计划项目(142300410147);河南省教育厅自然科学研究项目(12A520021);河南省教育厅高等学校重点科研项目(16A520013)
This work was supported by the National Natural Science Foundation of China (61300216), the Foundation and Advanced Technology Research Plan of Henan Provincial Department of Science and Technology (142300410147), the Natural Science Research Project of Henan Provincial Department of Education (12A520021), and the Key Research Project of Henan Provincial Department of Education (16A520013).
通信作者:汤永利(yltang@hpu.edu.cn)

陷门函数的特性提出一种优化的$\mathbb{Z}_q$可逆矩阵提取算法,再基于该优化算法结合固定维数的陷门派生算法和MP12陷门函数完成方案的建立和陷门派生阶段,然后与对偶Regev算法相结合完成随机预言模型下HIBE方案的构造.并且利用二进制树加密系统将该方案改进为标准模型下的HIBE方案.两方案安全性均可归约至LWE问题的难解性,其中随机预言模型下的方案满足适应性安全,而标准模型下的方案满足选择性安全,并给出严格的安全性证明.对比分析表明:在相同的安全性下,随机预言模型下的方案较同类方案在陷门派生复杂度方面显著降低,而标准模型下的方案是同类最优方案的1/6,且格的维数、陷门尺寸和密文扩展率等参数均有所降低,计算效率明显优化.

关键词 格;基于身份的分级加密;陷门派生;容错学习;随机预言模型;标准模型

中图法分类号 TP309

基于身份加密(identity-based encryption, IBE)是一种高级的公钥加密体制,该体制可使用用户任意的身份标识符(如邮箱地址、手机号码等)作为公钥,相应的私钥由可信第三方私钥生成中心(key generation center, KGC)利用系统主私钥生成.基于身份加密的思想首先于1984年由Shamir[1]首次提出,但直到2001年,可实际应用的IBE方案才由Boneh等人[2]提出并定义了IBE的安全模型.此后IBE的研究引起密码学者的广泛关注,很多IBE的相关方案被相继提出[3-6].

基于身份的分级加密(hierarchical identity-based encryption, HIBE)体制是IBE体制的一种推广.在HIBE体制中,多个KGC实体按照有向树的结构分布.HIBE可以更好地应用在大规模网络的应用场景中,有效解决IBE体制在大量的用户请求下无法为每一用户完成身份信息的有效验证并为之安全传送私钥的问题.HIBE体制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或同级KGC的陷门.

近几年,基于格理论构造的新型密码体制因具有较好的渐进效率、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].2008年,Gentry等人[12]于STOC'08上利用格的短基作为陷门构造出一种格上原像采样算法,并提出对偶Regev算法;基于这2个算法和Ajtai等人[13]提出的陷门生成算法构造出格上IBE方案,并且指出在构造(H)IBE方案时应采用对偶Regev算法来完成方案的加解密阶段,比采用非对偶Regev算法更加合理,随后基于对偶Regev算法的(H)IBE方案[14-17]被相继提出.但Gentry等人提出的IBE体制的缺陷是所基于的原像采样算法和陷门生成算法太过复杂,算法的运行时间不满足实际应用;2010年,Cash等人[18]基于Gentry等人的原像采样算法构造出一种格上陷门派生算法,并基于此构造出格上首个HIBE方案,但陷门派生算法的派生陷门的维数与系统分级的深度呈2次幂增长关系,这将导致在较高的系统分级中出现格的维数、陷门尺寸等参数过大而导致陷门派生的复杂度过高的问题;2010年,Agrawal等人[19]于EUROCRYPT 2010上对Cash等人的方案进行了改进,将按照用户身份向量每1比特分配矩阵的方式改进为按系统分级中每一级分配1个矩阵的方式,从而使格的维数随着系统分级深度的增长而仅呈线性增长,但维数的增长仍然会导致格的维数、陷门尺寸等参数的膨胀而导致陷门派生复杂度过大;2010年,Agrawal等人[20]于CRYPTO 2010上提出一种固定维数的格上陷门派生技术,即格的维数在陷门派生前后保持不变,并基于此构造出一种高效的HIBE方案.格的维数是格上密码方案的重要参数与密钥长度、密文尺寸和密文膨胀率等参数密切相关,因此格上固定维数的陷门派生技术引起密码学领域的广泛关注.但该方案和陷门派生算法的构造均依赖一种$\mathbb{Z}_q$可逆矩阵的提取算法(SampleR),而该算法效率取决于原像采样算法,但Agrawal等人所采用的原像采样算法由上述的文献[12]中提出,该算法的输入是高精度的实数且是迭代化运算,这将导致SampleR算法的复杂度过高,进而影响陷门派生的效率.

2012年,Micciancio等人[21](Micciancio和Peikert于2012年发表的文章简称MP12)于EUROCRYPT 2012上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,相比文献[17,22]提出的陷门生成算法,该陷门生成过程简单,复杂度仅相当于2个随机矩阵的1次乘运算,且不涉及计算代价高的埃

尔米特正规形式(hermite normal form, HNF)和矩阵求逆操作.相比文献[12]的原像采样算法,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 等人还提出了一种新的陷门派生算法,该算法相比 Cash 等人的算法较高效,因为该算法无须进行线性无关检测,且派生陷门的维数与系统分级的深度仅呈线性增长的关系,但维数增长导致陷门派生低效的问题仍然没有解决.

为使基于固定维数派生技术的 HIBE 方案更具有实际应用可行性,必须解决其陷门派生复杂度过高的问题.因此,本文提出一种高效的格上 HIBE 方案.主要贡献有:1)利用 MP12 陷门函数[21]的特性构造出一种优化的 SampleR 算法;2)基于优化的 SampleR 算法结合固定维数的陷门派生算法和高效 MP12 陷门生成算法完成 HIBE 方案的陷门生成和陷门派生阶段,然后与对偶 Regev 算法有机结合完成随机预言模型下的方案构造;3)利用 Cash 等人提出的二进制树加密系统消除随机预言机假设,从而改进为标准模型下的 HIBE 方案.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:本文 2 个方案的安全性均可归约至容错学习(learning with errors, LWE)问题的难解性,其中随机预言下的 HIBE 方案满足 IND-aID-CPA 安全性,标准模型下的 HIBE 方案满足 IND-sID-CPA 安全性.在效率对比分析中,为更好地体现对比结果,我们将 HIBE 陷门派生前的参数和计算效率与派生后的分开进行对比.对比结果表明:与相同安全性的方案相比,本文随机预言模型下的方案在陷门派生复杂度方面显著降低,而标准模型下的方案是同类最优方案的 1/6,且格的维数、陷门尺寸和密文扩展率等参数均有所降低,计算效率明显优化.

1　预备知识

1.1　格的相关定义

定义 1. 格的定义.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:

$$\Lambda=\left\{\sum_{i=1}^{m}x_i\boldsymbol{b}_i:x_i\in\mathbb{Z},i=1,2,\cdots,m\right\},$$

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:

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

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

即所有与矩阵 $\boldsymbol{A}$ 行向量模 q 内积为 $\boldsymbol{0}$ 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

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

其中,$\boldsymbol{y}\in\Lambda,\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{y})=\exp(-\pi\|\boldsymbol{y}-\boldsymbol{c}\|/\sigma^2)$.

1.2　相关算法和困难问题

本文方案构造所基于的 MP12 陷门生成算法和与之对应的 MP12 原像采样算法分别由引理 1 和引理 2 给出;SampleR 算法由引理 3 给出;固定维数的陷门派生算法由引理 6 给出;引理 4 是引理 6 的基本算法;对偶 Regev 算法的具体描述请参阅文献[12];随机预言模型下方案的安全性证明基于引理 7、引理 8 和定义 4;标准模型下方案的安全性证明基于引理 8 和定义 4;方案的正确性证明基于引理 2 和引理 9.

定义 4[7]. 容错学习(learning with errors, LWE)问题.设 n 为正整数,q 为素数,对任意 $0<\alpha\leqslant 1/\omega(\sqrt{\lg n})$,定义 Ψ_α 为中心是 0、标准差是 $\alpha/\sqrt{2\pi}$ 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 $\mathbb{Z}_q$ 上的容错分布,$(\mathbb{Z}_q,n,\chi)$-LWE 问题实例由未指明的挑战预言机 $\mathcal{O}$ 构成:预言机 $\mathcal{O}$ 是带噪音的伪随机预言机 $\mathcal{O}_s$ 或者是真随机的预言机 $\mathcal{O}_\$$,2 种预言机的输出分别如下:

$\mathcal{O}_s$:输出的采样值形式为 $(\boldsymbol{u}_i,v_i)=(\boldsymbol{u}_i,\boldsymbol{u}_i^{\mathrm{T}}\boldsymbol{s}+x_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$,其中 $\boldsymbol{s}\in\mathbb{Z}_q^n$ 是随机均匀且不变的秘密向量;

$\mathcal{O}_\$$:输出 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的真随机且均匀的采样值.

$(\mathbb{Z}_q,n,\chi)$-LWE 问题允许对挑战预言机 $\mathcal{O}$ 重复查询.我们称一个攻击算法 $\mathcal{A}$ 可以解决 $(\mathbb{Z}_q,n,\chi)$-LWE 问题如果

$$\text{LWE-adv}[\mathcal{A}]=|Pr[\mathcal{A}^{\mathcal{O}_s}=1]-Pr[\mathcal{A}^{\mathcal{O}_\$}=1]|$$

是不可忽略的,其中 LWE-adv$[\mathcal{A}]$表示 $\mathcal{A}$ 解决 $(\mathbb{Z}_q,n,\chi)$-*LWE* 问题的优势.

引理 1[18]. Randbasis 算法.设整数 $n\geqslant 1,q\geqslant 2$ 和充分大的 $m=O(n\lg q)$,$\overline{m}=m-nk$,$w=nk$,$k=\lceil\lg q\rceil$.利用类似引理 7 的陷门生成算法输出一个均匀随机的矩阵 $\boldsymbol{A}$ 和格 $\Lambda^{\perp}(\boldsymbol{A})$ 的基 $\boldsymbol{T}_{\boldsymbol{A}}$,输入相关高斯参数 σ,输出一个新的格 $\Lambda^{\perp}(\boldsymbol{A})$ 的基 $\boldsymbol{T}'_{\boldsymbol{A}}$,满足

$Pr[\|\widetilde{\boldsymbol{T}}'_{\boldsymbol{A}}\|>\sigma\sqrt{m}]\leqslant negl(n)$，且 Randbasis($\boldsymbol{T}_{\boldsymbol{A}}$, σ) 的输出与输入为格 $\Lambda^{\perp}(\boldsymbol{A})$ 的任意基 $\boldsymbol{T}$ 的 Randbasis($\boldsymbol{T}$, σ) 输出是统计不可区分的，其中 $\|\widetilde{\boldsymbol{T}}\|\leqslant\sigma/\omega(\sqrt{\mathrm{lb}\,n})$.

引理 2[20]. 陷门派生算法 TrapDel. 与引理 1 参数相同，利用 SampleR 算法(见引理 6)抽取一个可逆矩阵 $\boldsymbol{R}$，令 $\boldsymbol{B}=\boldsymbol{A}_0\boldsymbol{R}^{-1}$，计算 $\boldsymbol{T}'_{\boldsymbol{B}}=\{\boldsymbol{Ra}_1,\boldsymbol{Ra}_2,\cdots,\boldsymbol{Ra}_m\}\subseteq\mathbb{Z}^m$，利用 ToBasis 算法(见引理 9)的算法将 $\boldsymbol{T}'_{\boldsymbol{B}}$ 转换为矩阵 $\boldsymbol{B}$ 的陷门矩阵 $\boldsymbol{T}''_{\boldsymbol{B}}$，运行引理 1 中的 Randbasis($\boldsymbol{T}''_{\boldsymbol{B}}$, σ)算法并输出矩阵 $\boldsymbol{B}$ 的陷门矩阵 $\boldsymbol{T}_{\boldsymbol{B}}$.

引理 3[20]. 与引理 1 参数相同，设可逆矩阵 $\boldsymbol{R}$ 是由 SampleR 算法(见引理 6)抽取且高斯参数 σ 满足 $\sigma>\|\widetilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\times\sigma_{\boldsymbol{R}}\sqrt{m}\omega(\mathrm{lb}^{3/2}m)$，令 $\boldsymbol{T}_{\boldsymbol{B}}$ 为调用引理 2 中陷门派生算法 TrapDel 输出的矩阵 $\boldsymbol{AR}^{-1}$ 的陷门矩阵，则 $\boldsymbol{T}_{\boldsymbol{B}}$ 的分布与引理 1 中的 Randbasis($\boldsymbol{T}$, σ) 的输出是统计不区分的，其中 $\boldsymbol{T}$ 是矩阵 $\boldsymbol{AR}^{-1}$ 的任意陷门矩阵，$\|\widetilde{\boldsymbol{T}}\|\leqslant\sigma/\omega(\sqrt{\mathrm{lb}\,n})$. 若 $\boldsymbol{R}$ 是由 ℓ 个利用 SampleR 算法抽取矩阵的积，则高斯参数 σ 的界降至 $\sigma>\|\widetilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\times(\sigma_{\boldsymbol{R}}\sqrt{m}\omega(\mathrm{lb}^{1/2}m))^{\ell}\omega(\mathrm{lb}\,m)$.

引理 4[20]. SampleRwithTrap 算法. 与引理 1 参数相同. 设除了至多 q^{-n} 部分之外所有的 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$，算法 SampleRwithTrap 输出一个 $\mathbb{Z}^{m\times m}$ 矩阵 $\boldsymbol{R}$，具体是从与 $\mathcal{D}_{m\times m}$ 统计接近的分布上随机选取矩阵 $\boldsymbol{R}$ 的列向量. 且算法 SampleRwithTrap 输出的 $\boldsymbol{A}_0\boldsymbol{R}^{-1}$ 的陷门矩阵 $\boldsymbol{T}_{\boldsymbol{B}}$ 满足：

$$Pr[\|\widetilde{\boldsymbol{T}}_{\boldsymbol{B}}\|>\sigma_{\boldsymbol{R}}/\omega(\sqrt{\mathrm{lb}\,m})]\leqslant negl(n).$$

引理 5[20]. 与引理 1 参数相同，设 $\boldsymbol{e}$ 为 $\mathbb{Z}^m$ 中某向量，向量 $\boldsymbol{y}\xleftarrow{\Psi_{\alpha}^{m}}\mathbb{Z}_q^m$，则 $|\boldsymbol{e}^{\mathrm{T}}\boldsymbol{y}|$ 可看作 $[0,q-1]$ 中的整数，满足 $|\boldsymbol{e}^{\mathrm{T}}\boldsymbol{y}|\leqslant\|\boldsymbol{e}\|q\alpha\omega(\sqrt{\mathrm{lb}\,m})+\|\boldsymbol{e}\|\sqrt{m}/2$.

引理 6[20]. SampleR 算法. 与引理 1 参数相同，设 $\boldsymbol{T}$ 是格 $\mathbb{Z}^m$ 的格基，利用与引理 8 类似的原像采样算法随机抽取 m 个向量 $\boldsymbol{r}_i\leftarrow\mathrm{Sample}(\mathbb{Z}^m,\boldsymbol{T},\sigma_{\boldsymbol{R}},\boldsymbol{0})$，其中 $i=1,2,\cdots,m$，将 $\boldsymbol{r}_i$ 作为矩阵 $\boldsymbol{R}$ 的列向量. 如果矩阵 $\boldsymbol{R}$ 是 $\mathbb{Z}_q$ 可逆(矩阵 $\boldsymbol{R}$ 是 $\mathbb{Z}_q$ 可逆指矩阵 $\boldsymbol{R}$ mod q 仍是 $\mathbb{Z}^{m\times m}$ 上的可逆矩阵)的，则输出 $\boldsymbol{R}$，否则重新抽取 $\boldsymbol{r}_i$.

引理 7[21]. MP12 陷门生成算法. 与引理 1 参数相同，令 $\boldsymbol{H}\in\mathbb{Z}_q^{n\times n}$ 为可逆矩阵，$\boldsymbol{G}\in\mathbb{Z}_q^{n\times w}$ 是构造公开的矩阵. 选取一个均匀随机矩阵 $\bar{\boldsymbol{A}}\in\mathbb{Z}_q^{n\times m}$，存在概率多项式时间(probabilistic polynomial time, PPT)算法 TrapGen($\bar{\boldsymbol{A}}$, $\boldsymbol{H}$)，输出矩阵 $\boldsymbol{A}_0=[\bar{\boldsymbol{A}}\|\boldsymbol{HG}-\bar{\boldsymbol{A}}\boldsymbol{T}_{\boldsymbol{A}_0}]\in\mathbb{Z}_q^{n\times m}$ 和陷门矩阵 $\boldsymbol{T}_{\boldsymbol{A}_0}=[\boldsymbol{a}_1\|\boldsymbol{a}_2\|\cdots\|\boldsymbol{a}_w]\in\mathbb{Z}^{\bar{m}\times w}$，陷门尺寸 $s_1(\boldsymbol{T}_{\boldsymbol{A}_0})\leqslant\sqrt{m}\times\omega(\sqrt{\mathrm{lb}\,n})$，其中 $\boldsymbol{A}_0$ 在 $\mathbb{Z}_q^{n\times m}$ 上是统计均匀的，$\boldsymbol{T}_{\boldsymbol{A}_0}$ 是矩阵 $\boldsymbol{A}_0$ 的陷门.

引理 8[21]. MP12 原像采样算法. 与引理 1 参数相同，设 $\boldsymbol{u}\in\mathbb{Z}_q^n$ 为均匀随机向量，充分大的高斯参数 $\sigma=O(\sqrt{n\,\mathrm{lb}\,q})$，$\omega(\sqrt{\mathrm{lb}\,n})$ 表示渐进性高于 $\sqrt{\mathrm{lb}\,n}$，则存在概率多项式时间算法 MP12Sample($\boldsymbol{A}_0$, $\boldsymbol{M}$, $\boldsymbol{T}_{\boldsymbol{A}_0}$, $\boldsymbol{u}$, σ)，其中，$\boldsymbol{M}\in\mathbb{Z}_q^{n\times w}$，输出向量 $\boldsymbol{e}\in\mathbb{Z}^{\bar{m}+w}$，且 $\boldsymbol{e}$ 的分布与 $D_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{F}_1),\sigma\omega(\sqrt{\mathrm{lb}\,n})}$ 统计不可区分，$Pr[\boldsymbol{e}\leftarrow D_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{F}_1),\sigma\omega(\sqrt{\mathrm{lb}\,n})}:\|\boldsymbol{e}\|>\sigma\sqrt{m}]\leqslant negl(n)$，其中，$\boldsymbol{F}_1=(\bar{\boldsymbol{A}}|\boldsymbol{M})$.

引理 9[23]. ToBasis 算法. 与引理 1 参数相同，设 Λ 是一个 m 维格，存在一个确定性多项式算法：输入格 Λ 的任意一组基和格 Λ 中的一个满秩集合 $\boldsymbol{S}=\{\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots,\boldsymbol{s}_m\}$，输出格 Λ 的一组基 $\boldsymbol{T}$，满足 $\|\widetilde{\boldsymbol{T}}\|\leqslant\|\tilde{\boldsymbol{S}}\|$，且 $\|\boldsymbol{T}\|\leqslant\|\boldsymbol{S}\|\sqrt{m}/2$.

2 算法设计及方案构造

2.1 符号说明

为表述方便，对文中符号进行说明，如表 1 所示：

Table 1 Notations Description

表 1 符号说明

Symbol	Description
$\boldsymbol{A}^{m\times n}$	A matrix with m rows and n columns.
$\boldsymbol{u}$	Vectors, assumed to be in column form.
$\boldsymbol{u}^{\mathrm{T}}$	Row vectors, a transpose vector of $\boldsymbol{u}$.
$\|\boldsymbol{R}\|$	The length of matrix $\boldsymbol{R}$ is the norm of its longest column.
$\widetilde{\boldsymbol{R}}$	The Gram-Schmidt orthogonalization of matrix $\boldsymbol{R}$.
$s_1(\boldsymbol{R})$	The maximal singular value of matrix $\boldsymbol{R}$.
$\|$	The (ordered) concatenation of vectors or marices.
$\lfloor x\rfloor$	The largest integer is not greater than x.
$negl(n)$	A negeligible function is an $f(n)$ such that $f(n)<(n^{-c})$ for every fixed constant c.
$poly(n)$	An unspecified function $f(n)=O(n^c)$ for some constant c.

2.2 优化的 SampleR 算法

本节给出一种优化的 SampleR 算法，算法输出是 $\mathbb{Z}_q$ 可逆矩阵 $\boldsymbol{R}\in\mathbb{Z}^{m\times m}$. SampleR 算法是基于固定维数陷门派生技术的 HIBE 方案的重要组成部分. 其重要性主要体现在：SampleR 算法的时间复杂度不仅支配着陷门派生算法的效率，而且支配着在标准模型下的 HIBE 方案构造中系统建立阶段

(Setup)和陷门派生阶段(Derive)的性能. 此外,SampleR 算法还是我们 2 个方案安全性证明中 SampleRwithTrap 算法(见引理 4)的基本算法.

本节构造的优化 SampleR 算法的功能与 Agrawal 等人提出的陷门派生算法中的(见引理 6)相同. 由于 SampleR 算法输出的 $\boldsymbol{R}$ 矩阵是公开的,且算法的时间复杂度主要来自于算法中循环调用的原像采样算法. 所以我们考虑采用较高效的 MP12 原像采样算法 MP12Sample(见引理 8). 具体方法是利用 MP12 陷门函数中构造公开的特殊矩阵 $\boldsymbol{G}$ 和其公开陷门矩阵 $\boldsymbol{T}_G$ 来进行 SampleR 算法中的原像采样操作. 具体优化算法如下:

算法 1. SampleR$^{\mathcal{O}_G}(1^m)$.

输入:整数 $m=O(n\lg q)$、用来在陪集 $\Lambda^{\perp}(\boldsymbol{G})$ 高斯采样的预言机 $\mathcal{O}_G$、其高斯参数为 σ_G;

输出:$\mathbb{Z}_q$ 可逆矩阵 $\boldsymbol{R}\in\mathbb{Z}^{m\times m}$.

1) 与引理 1 的参数相同:$\bar{\boldsymbol{A}}$ 是随机均匀选取的 $n\times\bar{m}$ 矩阵,$\boldsymbol{G}$ 为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,$\boldsymbol{g}^{\mathrm{T}}=(1,2,2^2,\cdots,2^{k-1})\in\mathbb{Z}_q^k$,$k=\lceil\lg q\rceil$,$\boldsymbol{T}_G$ 是矩阵 $\boldsymbol{G}$ 的公开陷门;

2) For $i=1,2,\cdots,m$ do:

① 调用预言机 $\mathcal{O}_G:\bar{\boldsymbol{r}}_i\leftarrow D_{\Lambda^{\perp}(\boldsymbol{G}),\sigma_G}$,$\bar{\boldsymbol{r}}_i\in\mathbb{Z}^w$,判断 $\bar{\boldsymbol{r}}_i$ 与 $D_{\mathbb{Z}^w,\sigma_G}$ 是否统计接近,如不是,则再次生成;

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

③ 计算 $\hat{\boldsymbol{r}}_i\leftarrow$MP12Sample$(\boldsymbol{G},\boldsymbol{T}_G,\sigma_G,\boldsymbol{u})$,$\hat{\boldsymbol{r}}_i\in\mathbb{Z}^{\bar{m}}$;

④ 令 $\boldsymbol{r}_i=(\bar{\boldsymbol{r}}_i\parallel\hat{\boldsymbol{r}}_i)$并输出 $\boldsymbol{r}_i\in\mathbb{Z}^m$;

3) 将 $\boldsymbol{r}_i$ 作为矩阵 $\boldsymbol{R}$ 的列向量,检测 $\boldsymbol{R}$ 是否是 $\mathbb{Z}_q$ 可逆,是则输出 $\boldsymbol{R}$,否则重新进行步骤 2.

分析:因为 $\mathcal{O}_G$ 的输出是随机均匀的,由非齐次小整数解问题(inhomogeneous small integer solution problem, ISIS)可知 $\boldsymbol{u}$ 是统计均匀的,再由引理 8 可知原像采样算法 MP12Sample 的输出向量 $\hat{\boldsymbol{r}}_i$ 是统计均匀的,因此由 $\bar{\boldsymbol{r}}_i$ 和 $\hat{\boldsymbol{r}}_i$ 的拼接向量 $\boldsymbol{r}_i$ 也是统计均匀的.

相比 Agrawal 等人[20]提出的 SampleR 算法:首先,在效率上,MP12Sample 算法的输入项是小整数可支持并行化运算而不是输入项是高精度实数的正交化迭代运算,且原像采样过程中利用 $\boldsymbol{G}$ 矩阵和 $\boldsymbol{G}$ 矩阵陷门的特殊构造,时间复杂度相比通常的原像采样算法的 $\Omega(n^2\lg^2 n)$ 可降至 $O(n\lg^c n)$,其中 c 是常数. 因此,相比 Agrawal 等人提出复杂度是 $\Omega(n^3\lg^3 nn)$的SampleR 算法,我们的算法复杂度是 $O(n^2\lg^c n)$. 其次,在输出质量(原像采样算法的输出质量为所采样向量的范数)上,质量好坏与原像采样大小限制参数 β 负相关. Agrawal 等人的 HIBE 方案采用的是文献[21]的陷门生成算法和文献[12]的原像采样算法,则 $\beta_{\text{Agrawal}}>45n\lg q$,而本文 $\beta_{\text{our}}\approx 2.3n\lg q$,相比之下本文有近 19 倍的提升.

我们的优化算法存在的不足是相比 Agrawal 等人的 SampleR 算法多了第 2 步中的②操作,该操作采用高效正向计算的方式输出,复杂度仅等同于执行 1 次 Hash 算法.

2.3　随机预言模型下的 HIBE 方案

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 $\boldsymbol{id}=(\boldsymbol{id}_1\parallel\boldsymbol{id}_2\parallel\cdots\parallel\boldsymbol{id}_\ell)\in(\{0,1\}^*)^\ell$,其中 $\ell\in[d]$,$i\in[1,\ell]$. 令 $\boldsymbol{id}_{|\bar{k}}=(\boldsymbol{id}_1,\boldsymbol{id}_2,\cdots,\boldsymbol{id}_{\bar{k}})$,其中 $1\leqslant\bar{k}\leqslant\ell$. 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,$\boldsymbol{g}^{\mathrm{T}}=(1,2,2^2,\cdots,2^{k-1})\in\mathbb{Z}_q^k$;随机预言机 $H:(\{0,1\}^*)^{\leqslant d}\rightarrow\mathbb{Z}_q^{m\times m}:\boldsymbol{id}\mapsto H(\boldsymbol{id})\sim\mathcal{D}_{m\times m}$.

HIBE-Setup$(1^n,1^d)$:输入安全参数 n 和系统最大分级深度 d,运行引理 7 的算法 TrapGen$(\bar{\boldsymbol{A}},\boldsymbol{H})$,输出均匀随机矩阵 $\boldsymbol{A}_0=[\bar{\boldsymbol{A}}\parallel\boldsymbol{HG}-\bar{\boldsymbol{A}}\boldsymbol{T}_{\boldsymbol{A}_0}]\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{A}_0$ 的陷门矩阵 $\boldsymbol{T}_{\boldsymbol{A}_0}=[\boldsymbol{a}_1\parallel\boldsymbol{a}_2\parallel\cdots\parallel\boldsymbol{a}_w]\in\mathbb{Z}^{\bar{m}\times w}$,选取 n 维均匀随机向量 $\boldsymbol{u}\in\mathbb{R}_q^n$,输出主公钥 $MPK=(\boldsymbol{A}_0,\boldsymbol{u}_0)$ 和主私钥 $MSK=(\boldsymbol{T}_{\boldsymbol{A}_0})$.

HIBE-Derive(MPK, $SK_{\boldsymbol{id}_{|\ell}}$, $\boldsymbol{id}$):输入主公钥 MPK;输入 $SK_{\boldsymbol{id}_{|\ell}}$ 表示系统分级深度为 ℓ 时用户公钥矩阵 $\boldsymbol{A}_{\boldsymbol{id}_{|\ell}}$ 所对应的陷门矩阵,其中 $\boldsymbol{A}_{\boldsymbol{id}_\ell}=\boldsymbol{A}_0\boldsymbol{R}_{\boldsymbol{id}_{|\ell}}^{-1}\in\mathbb{Z}_q^{n\times m}$,父用户身份 $\boldsymbol{id}_{|\ell}=(\boldsymbol{id}_1\parallel\boldsymbol{id}_2\parallel\cdots\parallel\boldsymbol{id}_\ell)$,可逆矩阵 $\boldsymbol{R}_{\boldsymbol{id}_{|\ell}}=H(\boldsymbol{id}_{|1})H(\boldsymbol{id}_{|2})\cdots H(\boldsymbol{id}_{|\ell})\in\mathbb{Z}^{m\times m}$;输入子用户身份 $\boldsymbol{id}=(\boldsymbol{id}_1\parallel\boldsymbol{id}_2\parallel\cdots\parallel\boldsymbol{id}_\ell\parallel\boldsymbol{id}_{\ell+1}\parallel\cdots,\parallel\boldsymbol{id}_k)$,其中 $\bar{k}\leqslant d$. 计算 $\boldsymbol{R}=H(\boldsymbol{id}_{|\ell+1})H(\boldsymbol{id}_{|\ell+2})\cdots H(\boldsymbol{id}_{|k})\in\mathbb{Z}^{m\times m}$ 并令 $\boldsymbol{A}_{\boldsymbol{id}}=\boldsymbol{A}_{\boldsymbol{id}_\ell}\boldsymbol{R}^{-1}$. 调用引理 2 的陷门派生算法 TrapDel$(\boldsymbol{A}_{\boldsymbol{id}_{|\ell}},\boldsymbol{R},SK_{\boldsymbol{id}_{|\ell}},\sigma_k)$,输出陷门矩阵 $SK_{\boldsymbol{id}}=\boldsymbol{S}'$. 另外,将参数 $\boldsymbol{A}_{\boldsymbol{id}_0}$ 设为 $\boldsymbol{A}_0$,$SK_{\boldsymbol{id}_{|0}}$ 设为 $\boldsymbol{T}_{\boldsymbol{A}_0}$,HIBE-Derive 算法相当于 IBE 方案中的用户密钥提取算法 IBE-Extract.

HIBE-Encrypt(MPK, $\boldsymbol{id}$, b):输入主公钥 MPK、分级深度为 $\bar{k}$ 的接收方用户身份 $\boldsymbol{id}$ 和待加密消息 $b\in\{0,1\}$. 计算可逆矩阵 $\boldsymbol{R}_{\boldsymbol{id}}=H(\boldsymbol{id}_{|1})H(\boldsymbol{id}_{|2})\cdots H(\boldsymbol{id}_{|\bar{k}})\in\mathbb{Z}^{m\times m}$. 计算用户公钥矩阵$\boldsymbol{A}_{\boldsymbol{id}}\leftarrow\boldsymbol{A}_0\boldsymbol{R}_{\boldsymbol{id}}^{-1}\in\mathbb{Z}_q^{n\times m}$. 利用对偶 Regev 算法来加密消息 b:首先选取均匀随机向量 $\boldsymbol{s}\leftarrow\mathbb{R}_q^n$;然后选取容错值 $x\xleftarrow{\Psi_{\alpha_1}}\mathbb{Z}_q$ 和容错向量 $\boldsymbol{y}\xleftarrow{\Psi_{\alpha_1}^m}\mathbb{Z}_q^m$;计算并输出密文 $CT=(c_0=\boldsymbol{u}_0^{\mathrm{T}}\boldsymbol{s}+x+b\lfloor q/2\rfloor,\boldsymbol{c}_1=\boldsymbol{A}_{\boldsymbol{id}}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{y})\in\mathbb{Z}_q\times\mathbb{Z}_q^m$.

HIBE-Decrypt(MPK, SK_{id}, CT):输入主公钥 MPK;输入陷门矩阵 SK_{id},其中用户身份 $\boldsymbol{id}$ 的分级深度为 $|\boldsymbol{id}|=\bar{k}$;输入密文 CT. 令高斯参数 $\tau_k=\sigma_k\sqrt{m}\times\omega(\sqrt{\text{lb}\,m})$,计算如 HIBE-Encrypt 中的矩阵 $\boldsymbol{A}_{id}\in\mathbb{Z}_q^{n\times m}$,运行引理 8 中的原像采样算法 $\boldsymbol{e}_{id}\leftarrow$ MP12Sample($\boldsymbol{A}_{id}$, SK_{id}, $\boldsymbol{u}_0$, τ_k),满足 $\boldsymbol{A}_{id}\boldsymbol{e}_{id}=\boldsymbol{u}_0$. 计算 $b'=c_0-\boldsymbol{e}_{id}^{\mathrm{T}}\boldsymbol{c}_1\in\mathbb{Z}_q$,将 b' 与 $\lfloor q/2\rfloor$ 视为 $\mathbb{Z}$ 中的整数并比较,如果 $\left|b'-\lfloor q/2\rfloor\right|<\lfloor q/4\rfloor$,输出 1,否则输出 0.

2.4 标准模型下的 HIBE 方案

与 2.3 节随机预言模型下的 HIBE 方案不同的是,在标准模型下我们采用 Cash 等人[18]提出的二进制树加密(binary tree encryption, BTE)系统来构造方案. 具体是将系统分级中每一级的用户身份看作长度是 $\bar{k}$ 的二进制向量. 因加解密算法与随机预言模型下的 HIBE 加解密算法相同,因此本节只给出系统建立算法和陷门派生算法的构造.

HIBE-Setup(1^n, 1^d):输入安全参数 n 和 BTE 可支持的最大分级深度 d,运行引理 7 的算法 TrapGen($\bar{\boldsymbol{A}}$, $\boldsymbol{H}$),输出均匀随机矩阵 $\boldsymbol{A}_0=[\bar{\boldsymbol{A}}\,\|\,\boldsymbol{HG}-\bar{\boldsymbol{A}}\boldsymbol{T}_{\boldsymbol{A}_0}]\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{A}_0$ 的陷门矩阵 $\boldsymbol{T}_{\boldsymbol{A}_0}=[\boldsymbol{a}_1\,\|\,\boldsymbol{a}_2\,\|\,\cdots\,\|\,\boldsymbol{a}_w]\in\mathbb{Z}^{\bar{m}\times w}$,选取 n 维均匀随机向量 $\boldsymbol{u}\in\mathbb{R}_q^n$. 运行 2.2 节优化的 SampleR($1^m$)算法,输出 $2d$ 个矩阵 $\boldsymbol{R}_{1,0}$, $\boldsymbol{R}_{1,1}$, $\boldsymbol{R}_{2,0}$, $\boldsymbol{R}_{2,1}$, $\cdots$, $\boldsymbol{R}_{d,0}$, $\boldsymbol{R}_{d,1}\in\mathbb{Z}^{m\times m}$. 输出主公钥 $MPK=(\boldsymbol{A}_0,\boldsymbol{u},\boldsymbol{R}_{1,0},\boldsymbol{R}_{1,1},\boldsymbol{R}_{2,0},\boldsymbol{R}_{2,1},\cdots,\boldsymbol{R}_{d,0},\boldsymbol{R}_{d,1})$和主私钥 $MSK=(\boldsymbol{T}_{\boldsymbol{A}_0})$.

HIBE-Derive(MPK, $SK_{id_{|\ell}}$, $\boldsymbol{id}$):输入主公钥 MPK;输入 $SK_{id_{|\ell}}$ 表示系统分级深度为 ℓ 时用户公钥矩阵 $\boldsymbol{A}_{id_{|\ell}}$ 所对应的陷门矩阵,其中 $\boldsymbol{A}_{id_\ell}=\boldsymbol{A}_0(\boldsymbol{R}_{1,id_1})^{-1}(\boldsymbol{R}_{2,id_2})^{-1}\cdots(\boldsymbol{R}_{\ell,id_\ell})^{-1}\in\mathbb{Z}_q^{n\times m}$,父用户身份 $\boldsymbol{id}_{|\ell}=\{0,1\}^{\ell\leqslant d}$;输入子用户身份 $\boldsymbol{id}=(\boldsymbol{id}_1\,\|\,\boldsymbol{id}_2\,\|\,\cdots\,\|\,\boldsymbol{id}_\ell\,\|\,\boldsymbol{id}_{\ell+1}\,\|\,\cdots,\|\,\boldsymbol{id}_k)$,其中 $\bar{k}\leqslant d$. 令 $\boldsymbol{R}=(\boldsymbol{R}_{\ell+1,id_{\ell+1}})^{-1}(\boldsymbol{R}_{\ell+2,id_{\ell+2}})^{-1}\cdots(\boldsymbol{R}_{\bar{k},id_{\bar{k}}})^{-1}\in\mathbb{Z}^{m\times m}$, $\boldsymbol{A}_{id}=\boldsymbol{A}_{id_\ell}\boldsymbol{R}\in\mathbb{Z}_q^{n\times m}$. 调用 2.3 节的陷门派生算法 HIBE-TrapDel($\boldsymbol{A}_{id_{|\ell}}$, $\boldsymbol{R}$, $SK_{id_{|\ell}}$, σ_k),输出陷门矩阵 $SK_{id}=\boldsymbol{S}'$.

3 安全性证明

通常,一个 HIBE 方案的安全性需满足选择身份攻击和选择明文攻击下的密文不可区分性(IND-ID-CPA),根据安全强度不同,分为适应性选择身份选择明文攻击(IND-aID-CPA)和选择性选择身份选择明文攻击(IND-sID-CPA). 本文方案在随机预言模型下满足 IND-aID-CPA 安全,在标准模型下满足 IND-sID-CPA 安全.

本方案采用 Agrawal 等人[19]在 EEUROCRYPT 2010 上提出的格上 HIBE 方案的 INDr-s/aID-CPA 安全模型进行安全性证明,该安全模型不仅可证明 IND-s/aID-CPA 安全,还可以保护接收方的匿名性,且主公钥的私密性可被其创建的密文保护. 基于该安全模型进行安全证明的还有 2010 年 Agrawal 等人[20]于 CRYPTO 2010 和 2016 年 Wang 等人[24]于 FITEE 提出的 HIBE 方案.

正确性. 本文 HIBE 方案的解密正确性由定理 1 刻画.

定理 1. 本文 HIBE 方案的解密是正确的,对任意的 $\boldsymbol{id}_\ell\in ID$, $(MPK, MSK)\leftarrow$ HIBE-Setup(1^n, d), $\boldsymbol{sk}_{id}\leftarrow$HIBE-Extract($MPK$, $\boldsymbol{R}_{\ell-1}$, $(\boldsymbol{id}_1\,\|\,\boldsymbol{id}_2\,\|\,\cdots\,\|\,\boldsymbol{id}_{\ell-1})\,\|\,\boldsymbol{id}_\ell$)和消息 $b\in\{0,1\}$,其中 ID 为身份空间,有

$Pr[\text{Decrypt}(MPK, \boldsymbol{sk}_{id}, \text{Encrypt}(MPK, \boldsymbol{id}, b))=b]=1-negl(n)$成立.

证明. HIBE 方案解密算法的输出为

$b'=c_0-\boldsymbol{e}_{id_\ell}^{\mathrm{T}}\boldsymbol{c}_1=\boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}+x+b\times\lfloor q/2\rfloor-\boldsymbol{e}_{id}^{\mathrm{T}}[\boldsymbol{A}_{id}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{y}]=b\lfloor q/2\rfloor+\underbrace{x-\boldsymbol{e}_{id}^{\mathrm{T}}\boldsymbol{y}}_{error\text{-}term}$,由引理 8 可知,$\|\boldsymbol{e}_{id}\|\leqslant\tau_\ell\sqrt{m+w}=\sigma_\ell m\omega(\sqrt{\text{lb}\,m})$,再由引理 5 可知,$error\text{-}term$ 被约束为 $|x-\boldsymbol{e}_{id}^{\mathrm{T}}\boldsymbol{y}|\leqslant q\sigma_\ell m\alpha_\ell\omega(\text{lb}\,m)+\sigma_\ell m^{3/2}\omega(\sqrt{\text{lb}\,m})$. 为保证解密的正确性,我们需要确保在 $1\leqslant\ell\leqslant d$ 中 $error\text{-}term$ 小于 $q/5$,则 $\alpha_\ell<[\sigma_\ell m\omega(\text{lb}\,m)]^{-1}$, $q=\sigma_\ell m^{3/2}\omega(\sqrt{\text{lb}\,m})$,且 $q>2\sqrt{n}/\alpha_\ell$,引理 7 中 TrapGen 算法要求 $m\geqslant 2n\,\text{lb}\,q$,引理 2 中 TrapDel 算法要求高斯参数 $\sigma_\ell>\sigma_{\ell-1}m^{3/2}\omega(\text{lb}^2 m)$. 方案的参数(随机预言模型)设定如表 2 所示:

Table 2 Parameters Setting of HIBE Scheme Under Random Oracle Model

表 2 随机预言模型下 HIBE 方案的参数设置

Parameters	Value
m	$2n\,\text{lb}\,q$
σ_ℓ	$m^{\frac{3}{2}\ell+\frac{1}{2}}\omega(\text{lb}^{2\ell}n)$
α_ℓ	$[m^{\frac{3}{2}(\ell+1)}\omega(\text{lb}^{2\ell+1}n)]^{-1}$
q	$m^{\frac{3}{2}d+2}\omega(\text{lb}^{2d+1}n)$

标准模型下方案的参数计算方式与随机预言模型下的相同,不同在于标准模型下的系统分级中的身份向量为二进制形式. 设每级用户身份的二进制

向量长度为 $\hat{k}$. 方案的参数(标准模型)设定如表 3 所示:

Table 3　Parameters Setting of HIBE Scheme Under Standard Model

表 3　标准模型下 HIBE 方案的参数设置

Parameter	Value
m	$2n\,\mathrm{lb}\,q$
σ_ℓ	$(km)^{\frac{3}{2}\hat{k\ell}+\frac{1}{2}}\omega(\mathrm{lb}^{\frac{\hat{k\ell}}{2}}n)$
α_ℓ	$[(km)^{\frac{3}{2}(\hat{k\ell}+1)}\omega(\mathrm{lb}^{\frac{1}{2}(\hat{k\ell}+1)}n)]^{-1}$
q	$(\hat{km})^{\frac{3}{2}d+2}\omega(\mathrm{lb}^{2d\hat{k}+1}n)$

表 2 和表 3 所示的参数设定下,本文 2.3 节和 2.4 节的 HIBE 方案中的 *error-term* 均小于 $q/5$,则方案正确性得以保证.　　证毕.

安全性. 本文随机预言模型下的 HIBE 方案的安全性由定理 2 刻画.

定理 2. 设 $\mathcal{A}$ 为攻击 2.3 节随机预言模型下 HIBE 方案的 PPT 攻击者,H 为随机预言机 $H:(\{0,1\}^*)^{\leqslant d}\rightarrow\mathbb{Z}_q^{m\times m}$. 令 Q_H 为敌手 $\mathcal{A}$ 对可对 H 询问的最大次数,d 为系统可支持的最大分级深度,则存在一个 PPT 算法 $\mathcal{B}$ 满足:如果 $\mathcal{A}$ 是一个具有优势 ε 的适应性攻击者(INDr-aID-CPA),那么 $\varepsilon\leqslant$ LWE-adv$[\mathcal{B}]\times(dQ_H^d)+negl(n)$.

证明. 已知 LWE 问题是区分定义 4 中预言机 $\mathcal{O}$ 的输出是来自伪随机预言机 $\mathcal{O}_s$ 还是真随机预言机 $\mathcal{O}_\$$. 基于 $\mathcal{A}$ 的能力,构造一个优势是 ε/dQ_H^d 的 DLWE 算法 $\mathcal{B}$.

$\mathcal{B}$ 对预言机 $\mathcal{O}$ 进行询问并获取一组实例$(\boldsymbol{u}_i,v_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$,其中 $i=1,2,\cdots,m$,要求 $\mathcal{B}$ 通过模拟游戏并基于 $\mathcal{A}$ 的能力区分出实例来自预言机 $\mathcal{O}_s$ 或 $\mathcal{O}_\$$. 模拟过程如下:

系统建立. $\mathcal{B}$ 选取 d 个均匀随机整数 $Q_1^*,Q_2^*,\cdots,Q_d^*\in[Q_H]$;运行 2.3 节的 $\boldsymbol{R}_i^*\leftarrow\mathrm{SampleR}(1^m)$ 算法来抽取 d 个随机矩阵 $\boldsymbol{R}_1^*,\boldsymbol{R}_2^*,\cdots,\boldsymbol{R}_d^*\sim\mathcal{D}_{m\times m}$,其中 $i=1,2,\cdots,d$;$\mathcal{B}$ 利用实例$(\boldsymbol{u}_i,v_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$ 生成随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,矩阵 $\boldsymbol{A}$ 的第 i 列是向量 $\boldsymbol{u}_i$,$i=1,2,\cdots,m$,将向量 $\boldsymbol{u}_0$ 作为公共随机向量 $\boldsymbol{u}_0\in\mathbb{Z}_q^n$;选取一个随机整数 $\varphi\in[d]$ 并令 $\boldsymbol{A}_0\leftarrow\boldsymbol{A}\boldsymbol{R}_1^*\cdot\boldsymbol{R}_2^*\cdots\boldsymbol{R}_\varphi^*$. 因 $\mathcal{A}$ 在$\mathbb{Z}_q^{n\times m}$上是均匀的,且 $\boldsymbol{R}_i^*$ 是模 q 可逆的,则 $\boldsymbol{A}_0$ 在$\mathbb{Z}_q^{n\times m}$上是均匀的. 输出主公钥 $MPK=(\boldsymbol{A}_0,\boldsymbol{u}_0)$.

模拟随机预言机. 对于适应性的攻击者 $\mathcal{A}$,$\mathcal{A}$ 能够在任意时间适应性地选择任意用户身份 $\boldsymbol{id}=\boldsymbol{id}_1,\boldsymbol{id}_2,\cdots,\boldsymbol{id}_i$ 提交给随机预言机 H 进行询问. 假设 A 的询问是唯一的,否则 $\mathcal{B}$ 对相同的输入返回相同的内容且不增加询问计数器 Q 的值. 令 $i=|\boldsymbol{id}|$ 为用户身份的深度,对于 $\mathcal{A}$ 的询问 $\mathcal{B}$ 的回应分 2 种情况:

如果 $Q=Q_i^*$,定义 $H(\boldsymbol{id})\leftarrow\boldsymbol{R}_i^*$ 并返回 $H(\boldsymbol{id})$;

如果 $Q\neq Q_i^*$,计算 $\boldsymbol{A}_i=\boldsymbol{A}_0\cdot(\boldsymbol{R}_1^*\boldsymbol{R}_2^*\cdots\boldsymbol{R}_{i-1}^*)^{-1}\in\mathbb{Z}_q^{n\times m}$,运行引理 4 中的 SampleRwithTrap$(\boldsymbol{A}_i)$算法输出一个随机矩阵 $\boldsymbol{R}\sim\mathcal{D}_{m\times m}$ 和矩阵 $\boldsymbol{B}=\boldsymbol{A}_i\boldsymbol{R}^{-1}\bmod q$ 的一个陷门 $\boldsymbol{T}_{\boldsymbol{B}}$. 保存五元组$(i,\boldsymbol{id},\boldsymbol{R},\boldsymbol{B},\boldsymbol{T}_{\boldsymbol{B}})$并返回 $H(\boldsymbol{id})\leftarrow\boldsymbol{R}$.

模拟私钥派生. 对于适应性的攻击者 $\mathcal{A}$,$\mathcal{A}$ 能够在任意时间适应性地选择任意用户身份进行私钥询问. $\mathcal{B}$ 对某用户身份 $\boldsymbol{id}=(\boldsymbol{id}_1,\boldsymbol{id}_2,\cdots,\boldsymbol{id}_k)$ 询问的回应如下:

1) 令 $j\in[\bar{k}]$作为 $H(\boldsymbol{id}_{|j})\neq\boldsymbol{R}_j^*$ 的最低系统分级深度. 对于不可能事件 $H(\boldsymbol{id}_{|j})=\boldsymbol{R}_j^*$,$j=1,2,\cdots,\bar{k}$,$\mathcal{B}$ 将终止模拟.

2) 查询本地存储的五元组$(i,\boldsymbol{id}_{|j},\boldsymbol{R},\boldsymbol{B},\boldsymbol{T}_{\boldsymbol{B}})$,该五元组在模拟者 $\mathcal{B}$ 回应攻击者 $\mathcal{A}$ 的询问 $H(\boldsymbol{id}_{|j})$时创建. 不失一般性地认为当某用户身份 $\boldsymbol{id}$ 被询问时,此 $\boldsymbol{id}$ 的所有前缀已被询问. 构造矩阵 $\boldsymbol{B}=\boldsymbol{A}_0\cdot(\boldsymbol{R}_1^*)^{-1}\cdot(\boldsymbol{R}_2^*)^{-1}\cdots(\boldsymbol{R}_{j-1}^*)^{-1}\cdot H(\boldsymbol{id}_{|j})^{-1}\bmod q$,且 $\boldsymbol{T}_{\boldsymbol{B}}$ 是矩阵 $\boldsymbol{B}$ 的陷门矩阵. 不难看出,矩阵 $\boldsymbol{B}$ 与 2.3 节随机预言模型下 HIBE 方案加密算法中父身份 $\boldsymbol{id}_{|j}=(\boldsymbol{id}_1,\boldsymbol{id}_2,\cdots,\boldsymbol{id}_j)$的用户公钥矩阵 $\boldsymbol{A}_{\boldsymbol{id}_{|j}}$ 相同,则 $\boldsymbol{T}_{\boldsymbol{B}}$ 是 $\boldsymbol{A}_{\boldsymbol{id}_{|j}}$的陷门矩阵.

3) 运行 2.3 节 HIBE 方案中的 Derive$(MPK,\boldsymbol{T}_{\boldsymbol{B}},\boldsymbol{id})$算法,利用父身份 $\boldsymbol{id}_{|j}$的陷门矩阵 $\boldsymbol{T}_{\boldsymbol{B}}$ 派生出子身份 $\boldsymbol{id}$ 的陷门矩阵. 如果 $j=k$,直接运行引理 5 中的 RandBasis$(\boldsymbol{T}_{\boldsymbol{B}},\sigma_k)$算法. 输出并发送 $\boldsymbol{id}$ 的陷门矩阵至攻击者 $\mathcal{A}$.

挑战阶段. 攻击者 $\mathcal{A}$ 向模拟者 $\mathcal{B}$ 宣布待攻击的用户身份 $\boldsymbol{id}^*$ 并输出一个消息比特 $b^*\in\{0,1\}$. 要求 $\boldsymbol{id}^*$ 不能是攻击者 $\mathcal{A}$ 已经询问或即将询问的用户身份的父身份. 令 $\ell=|\boldsymbol{id}^*|$,如果存在 $i\in[\ell]$满足 $H(\boldsymbol{id}_{|i}^*)\neq\boldsymbol{R}_i^*$,模拟终止. 已知 $\boldsymbol{A}_0=\boldsymbol{A}\boldsymbol{R}_1^*\cdot\boldsymbol{R}_2^*\cdots\boldsymbol{R}_\varphi^*$,如果 $\varphi\neq\ell$,模拟终止.

假设 $\varphi=\ell$ 且对任意的 $i\in[\ell]$有 $H(\boldsymbol{id}_{|i}^*)=\boldsymbol{R}_i^*$,定义 $\boldsymbol{A}_{\boldsymbol{id}^*}=\boldsymbol{A}_0\cdot(\boldsymbol{R}_1^*)^{-1}(\boldsymbol{R}_2^*)^{-1}\cdots(\boldsymbol{R}_\ell^*)^{-1}=\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$. $\mathcal{B}$ 将从预言机 $\mathcal{O}$ 获取到的一组实例中的 $v_1,v_2,\cdots,v_m\in\mathbb{Z}_q$设为 $\boldsymbol{v}^*=\begin{pmatrix}v_1\\v_2\\\vdots\\v_m\end{pmatrix}$,并令 $\boldsymbol{c}_1^*=\boldsymbol{v}^*\in\mathbb{Z}_q^m$;

利用 v_0 盲化消息位得 $c_0^*=v_0+b^*\lfloor q/2\rfloor\in\mathbb{Z}_q$;发送挑战密文 $CT^*=(c_0^*,\boldsymbol{c}_1^*)$ 至攻击者 $\mathcal{A}$. 若 $\mathcal{O}$ 是伪随机 LWE 预言机,则 $c_0=\boldsymbol{u}_0^{\mathrm{T}}\boldsymbol{s}+x+b^*\lfloor q/2\rfloor$,$\boldsymbol{c}_1=\boldsymbol{A}_{\boldsymbol{id}^*}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{y}$,其中 $\boldsymbol{s}\leftarrow\mathbb{R}_q^n$ 为均匀随机选取的向量,$x\xleftarrow{\bar{\Psi}_{\alpha_1}}\mathbb{Z}_q$ 和 $\boldsymbol{y}\xleftarrow{\bar{\Psi}_{\alpha_2}^m}\mathbb{Z}_q^m$ 分别为噪音值和噪音向量,则 CT^* 是利用挑战身份 $\boldsymbol{id}^*$ 对消息位 b^* 的有效加密密文;若 $\mathcal{O}$ 是真随机预言机,则 $(v_0,\boldsymbol{v}^*)$ 在 $\mathbb{Z}_q\times\mathbb{Z}_q^m$ 上是均匀的,那么挑战密文 $CT^*=(c_0^*,\boldsymbol{c}_1^*)$ 在 $\mathbb{Z}_q\times\mathbb{Z}_q^m$ 上也是均匀的.

模拟私钥派生. 该阶段与挑战前阶段的前的模拟私钥派生阶段相同,攻击者 $\mathcal{A}$ 可以继续选择用户身份进行私钥询问,模拟者 $\mathcal{B}$ 以同样的方式进行回应. 最后,攻击者 $\mathcal{A}$ 猜测挑战密文 CT^* 是否是利用挑战身份 $\boldsymbol{id}^*$ 对消息位 b^* 的有效加密密文,模拟者 $\mathcal{B}$ 输出 $\mathcal{A}$ 的猜测并结束模拟.

由以上可知,主公钥中参数的分布与实际系统中陷门派生算法所需的参数的分布是相同的. 且由引理 3 可知,对随机预言机 H 询问的回应与实际系统是相同的. 如果模拟者 $\mathcal{B}$ 不终止模拟,则挑战密文 CT^* 的分布在 $(\mathbb{Z}_q\times\mathbb{Z}_q^m)$ 上是独立随机的或与实际系统相同. 因此,如果模拟者 $\mathcal{B}$ 不终止模拟,则 $\mathcal{B}$ 在区分 DLWE 问题上的优势与攻击者 $\mathcal{A}$ 成功攻击方案的优势相同. 对于 PPT 攻击者 $\mathcal{A}$ 来说,$\mathcal{A}$ 在随机预言机上发现碰撞的概率是可忽略的,则模拟者 $\mathcal{B}$ 可进行而不终止的概率是 $Pr[\neg\,\mathrm{abort}]\geqslant Q_H^{-\ell}/d-negl(n)\geqslant Q_H^{-d}/d-negl(n)$. 因此,如果攻击者 $\mathcal{A}$ 的优势是 ε,则模拟者 $\mathcal{B}$ 解决 LWE 问题实例的优势至少是 $\lfloor\varepsilon/dQ_H^d\rfloor-negl(n)$. 证毕.

安全性. 本文标准模型下的 HIBE 方案的安全性由定理 3 刻画.

定理 3. 若 $(\mathbb{Z}_q,n,\bar{\Psi}_\alpha)$-LWE 的难解性成立,则本文在标准模型下 HIBE 方案是 INDr-sID-CPA 安全的.

证明. 假设攻击者 $\mathcal{A}$ 在区分定义 4 中预言机 $\mathcal{O}$ 的输出的具有不可忽略的优势,我们基于 $\mathcal{A}$ 的能力构造一个 LWE 算法 $\mathcal{B}$.

$\mathcal{B}$ 对预言机 $\mathcal{O}$ 进行询问并获取一组实例 $(\boldsymbol{u}_i,v_i)\in\mathbb{R}_q^n\times\mathbb{Z}_q$,其中 $i=1,2,\cdots,m$,要求 $\mathcal{B}$ 通过模拟游戏并基于 $\mathcal{A}$ 的能力区分出实例来自预言机 $\mathcal{O}_s$ 或 $\mathcal{O}_\$$. 模拟过程如下:

目标确定:攻击者 $\mathcal{A}$ 向模拟者 $\mathcal{B}$ 确定并宣布待攻击的目标身份 $\boldsymbol{id}^*=(\boldsymbol{id}_1^*,\boldsymbol{id}_2^*,\cdots,\boldsymbol{id}_\ell^*)\in\{0,1\}^\ell$. 当 $\ell<d$ 时,模拟过程相对简单,为此,我们直接假设攻击者 $\mathcal{A}$ 宣布的待攻击目标身份的深度 $|\boldsymbol{id}^*|$ 是系统可支持的最大分级深度,即 $\ell=d$,$\boldsymbol{id}^*=(\boldsymbol{id}_1^*,\boldsymbol{id}_2^*,\cdots,\boldsymbol{id}_d^*)\in\{0,1\}^d$.

系统建立:模拟者 $\mathcal{B}$ 首先利用实例 $(\boldsymbol{u}_i,v_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$ 生成随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,矩阵 $\boldsymbol{A}$ 的第 i 列是向量 $\boldsymbol{u}_i$,$i=1,2,\cdots,m$,将向量 $\boldsymbol{u}_0$ 作为公共随机向量 $\boldsymbol{u}_0\in\mathbb{R}_q^n$;然后利用 2.2 节优化的 SampleR 算法抽取 ℓ 个随机矩阵 $\boldsymbol{R}_{1,\boldsymbol{id}_1^*},\boldsymbol{R}_{2,\boldsymbol{id}_2^*},\cdots,\boldsymbol{R}_{\ell,\boldsymbol{id}_\ell^*}\in\mathbb{Z}^{m\times m}$,令 $\boldsymbol{A}_0=\boldsymbol{A}(\boldsymbol{R}_{1,\boldsymbol{id}_1^*})^{-1}(\boldsymbol{R}_{2,\boldsymbol{id}_2^*})^{-1}\cdots(\boldsymbol{R}_{\ell,\boldsymbol{id}_\ell^*})^{-1}$. 考虑如下 d 个矩阵

$$\boldsymbol{A}_i=\boldsymbol{A}_0(\boldsymbol{R}_{1,\boldsymbol{id}_1^*})^{-1}(\boldsymbol{R}_{2,\boldsymbol{id}_2^*})^{-1}\cdots(\boldsymbol{R}_{\ell,\boldsymbol{id}_\ell^*})^{-1},$$

其中 $i=0,1,\cdots,d-1$. 模拟者 $\mathcal{B}$ 为每一个矩阵 $\boldsymbol{A}_i$ 调用引理 4 中的 SampleRwithTrap 算法来生成随机矩阵 $\boldsymbol{R}_{i,1-\boldsymbol{id}_i^*}\in\mathbb{Z}^{m\times m}$ 和矩阵 $\boldsymbol{A}_i\cdot(\boldsymbol{R}_{i,1-\boldsymbol{id}_i^*})^{-1}$ 的陷门矩阵 $\boldsymbol{T}_{\boldsymbol{A}_i}$. 最后,模拟者 ℓ 将主公钥 $MPK=(\boldsymbol{A}_0,\boldsymbol{u}_0,\boldsymbol{R}_{1,0},\boldsymbol{R}_{1,1},\boldsymbol{R}_{2,0},\boldsymbol{R}_{2,1},\cdots,\boldsymbol{R}_{d,0},\boldsymbol{R}_{d,1})$ 发送给攻击者 $\mathcal{A}$.

模拟私钥派生:模拟者 $\mathcal{B}$ 利用系统建立阶段调用引理 4 中的 SampleRwithTrap 生成的陷门矩阵 $\boldsymbol{T}_{\boldsymbol{A}_i}$ 来回应攻击者 $\mathcal{A}$ 的私钥询问. 要求攻击者 $\mathcal{A}$ 询问的用户身份不能是目标身份 $\boldsymbol{id}^*$ 的父身份. 模拟者调用 2.4 节 HIBE 方案中的 Derive$(MPK,\boldsymbol{T}_{\boldsymbol{A}_i},\boldsymbol{id})$ 算法,利用攻击者所查询身份的父身份的陷门矩阵 $\boldsymbol{T}_{\boldsymbol{A}_i}$ 派生出所查询身份的陷门矩阵. 如果 $i=d$,直接运行引理 1 中的 RandBasis$(\boldsymbol{T}_{\boldsymbol{A}_i},\sigma_d)$ 算法. 输出并发送 $\boldsymbol{id}$ 的陷门矩阵至攻击者 $\mathcal{A}$.

挑战阶段. 攻击者 $\mathcal{A}$ 向模拟者 $\mathcal{B}$ 发送一个消息比特 $b^*\in\{0,1\}$,$\mathcal{B}$ 将从预言机 $\mathcal{O}$ 获取到的一组实例中的 $v_1,\cdots,v_m\in\mathbb{Z}_q$ 设为 $\boldsymbol{v}^*=\begin{pmatrix}v_1\\v_2\\\vdots\\v_m\end{pmatrix}$,并令 $\boldsymbol{c}_1^*=\boldsymbol{v}^*\in\mathbb{Z}_q^m$;利用 v_0 盲化消息位得 $c_0^*=v_0+b^*\lfloor q/2\rfloor\in\mathbb{Z}_q$;选取一个随机位 $r\leftarrow\{0,1\}$,如果 $r=0$,发送挑战密文 $CT^*=(c_0^*,\boldsymbol{c}_1^*)$ 至攻击者 $\mathcal{A}$,如果 $r=1$,选取一个随机的 $CT^*=(c_0,\boldsymbol{c}_1)\in\mathbb{Z}_q\times\mathbb{Z}_q^m$ 发送给攻击者.

容易看出,当定义 4 中的预言机 $\mathcal{O}$ 输出是伪随机的(即 $\mathcal{O}=\mathcal{O}_s$ 时),$v_0=\boldsymbol{u}_0^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x}$ 与挑战密文中的 c_0^* 部分是相同的,且 $\boldsymbol{v}^*=\boldsymbol{A}_0^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{y}$ 与挑战密文中的 $\boldsymbol{c}_1^*$ 部分是相同的,$\boldsymbol{x}$ 和 $\boldsymbol{y}$ 分别是选自 $\bar{\Psi}_\alpha$ 和 $\bar{\Psi}_\alpha^m$ 分布的容错值和容错向量. 因此,挑战密文 $CT^*=(c_0^*,\boldsymbol{c}_1^*)$ 的分布与预言机 $\mathcal{O}_s$ 的输出是统计不可区分的;当 $\mathcal{O}=\mathcal{O}_\$$ 时,v_0 在 $\mathbb{Z}_q$ 上和 $\boldsymbol{v}^*$ 在 $\mathbb{Z}_q^m$ 上都是均匀的,则挑战密文 $CT^*=(c_0,\boldsymbol{c}_1)$ 在 $\mathbb{Z}_q\times\mathbb{Z}_q^m$ 总是均匀的.

猜测阶段. 在攻击者 $\mathcal{A}$ 完成又一轮的私钥询问后,攻击者 $\mathcal{A}$ 猜测收到的挑战密文 CT^* 是来自伪随机预言机 $\mathcal{O}_s$ 还是是真随机的预言机 $\mathcal{O}_\$$. 模拟者 $\mathcal{B}$ 输出 $\mathcal{A}$ 的猜测结果作为对 LWE 问题的求解.

综上,模拟者 $\mathcal{B}$ 解决 LWE 实例的优势和攻击者 $\mathcal{A}$ 猜测与之交互的是 $\mathcal{O}_s$ 还是 $\mathcal{O}_\$$ 的优势相同. 因此不存在 PPT 算法有效求解 $(\mathbb{Z}_q, n, \overline{\Psi}_\alpha)$-LWE 问题,本方案是 INDr-sID-CPA 安全的. 模拟完成.

证毕.

4　效率分析

本节对随机预言模型下和标准模型下的 HIBE 方案分别进行效率分析. 为更好地体现本文 HIBE 方案的优越性,我们将 HIBE 陷门派生前的参数和计算效率与派生后的分开进行对比. 为简单直观,我们将派生前和派生后的分级深度设为 $\ell=1$ 和 $\ell=2$.

4.1　随机预言模型下的 HIBE 方案效率分析

我们选择 2 个随机预言模型下的 HIBE 方案作为参照对象:Cash 等人[18] 于 EUROCRYPT 2010 提出的随机预言模型下适应性安全的首个格上 HIBE 方案(简称 CHKP 方案);Agrawal 等人[19] 于 CRYPTO 2010 上提出的一种具有较短密文尺寸且可固定维数派生的随机预言模型下适应性安全的 HIBE 方案(简称 ABBa 方案). 设安全参数 $n=284$, $q=2$ 的 24 次方. 对比结果如表 4 和表 5 所示,其中 RO-adaptive 表示该方案满足随机预言模型下 INDr-aID-CPA 安全性.

Table 4　Efficiency Comparison of HIBE Schemes Before Trapdoor Delegation Under Random Oracle Model

表 4　随机预言模型下的 HIBE 方案陷门派生前效率对比

Scheme (RO-adaptive)	The Dimension of Lattice	The Size of Trapdoor /MB	The Size of User's Public Key /MB	The Size of User's Private Key /KB	Ciphertext Expansion Rate	Computational Cost (multiplications and additions in $\mathbb{Z}_q$)		
						Trapdoor Generation	Preimage Sample	Encryption & Decryption
CHKP's	40 896	199.38	66.48	9.98	1 963 032	$\approx 15.31\times10^{12}$ mults $\approx 15.30\times10^{12}$ adds	$\approx 50.17\times10^{8}$ mults $\approx 66.90\times10^{8}$ adds	$\approx 49.94\times10^{8}$ mults $\approx 49.94\times10^{8}$ adds
ABBa's	34 080	138.46	27.69	4.16	817 944	$\approx 15.86\times10^{13}$ mults $\approx 19.82\times10^{13}$ adds	$\approx 34.84\times10^{8}$ mults $\approx 46.46\times10^{8}$ adds	$\approx 32.99\times10^{10}$ mults $\approx 32.98\times10^{10}$ adds
Ours	13 632	5.54	11.08	1.66	327 192	$\approx 39.07\times10^{11}$ mults $\approx 39.07\times10^{11}$ adds	$\approx 96.87\times10^{6}$ mults $\approx 96.87\times10^{6}$ adds	$\approx 52.78\times10^{9}$ mults $\approx 52.77\times10^{9}$ adds

Table 5　Efficiency Comparison of HIBE Schemes After Trapdoor Delegation Under Random Oracle Model

表 5　随机预言模型下的 HIBE 方案派生后效率对比

Scheme (RO-adaptive)	The Dimension of Lattice	The Size of Trapdoor /MB	The Size of User's Public Key /MB	The Size of User's Private Key /KB	Ciphertext Expansion Rate	Computational Cost (multiplications and additions in $\mathbb{Z}_q$)		
						Trapdoor Generation	Preimage Sample	Encryption & Decryption
CHKP's	81 792	797.50	99.69	14.98	2 944 536	$\approx 16.42\times10^{14}$ mults $\approx 21.89\times10^{14}$ adds	$\approx 20.07\times10^{9}$ mults $\approx 26.76\times10^{9}$ adds	$\approx 66.78\times10^{8}$ mults $\approx 66.78\times10^{8}$ adds
ABBa's	34 080	138.46	27.69	4.16	817 944	$\approx 11.87\times10^{13}$ mults $\approx 15.83\times10^{13}$ adds	$\approx 34.84\times10^{8}$ mults $\approx 46.46\times10^{8}$ adds	$\approx 39.91\times10^{12}$ mults $\approx 39.90\times10^{12}$ adds
Ours	13 632	5.54	11.08	1.66	327192	$\approx 13.21\times10^{11}$ mults $\approx 13.21\times10^{11}$ adds	$\approx 96.87\times10^{6}$ mults $\approx 96.87\times10^{6}$ adds	$\approx 25.86\times10^{11}$ mults $\approx 25.86\times10^{11}$ adds

由表 4 和表 5 对比可以看出,相比 CHKP 方案,ABBa 方案和本文方案的主要优势在于陷门派生前后格的维数保持不变,因此效率参数如陷门尺寸、用户公私钥尺寸、明文-密文扩展率以及计算效率上的原像采样算法的复杂度均保持不变. 但是,基于固定维数陷门派生技术的 HIBE 方案存在的主要缺点是加密复杂度较大,原因是:当加密者向分级深度为 ℓ 的用户发送消息时,需要计算 ℓ 个 $m\times m$ 矩阵的连续乘积. 但优点是该运算对于每个用户身份只需进行 1 次,且与发送的消息是无关的.

相比同是固定维数陷门派生的 ABBa 方案,本文方案的优势在于具有较低的格的维数. 原因在于

所采用的 MP12 陷门生成算法(见引理 7)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是安全参数 n 的可忽略函数. 且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.

在陷门生成复杂度上,相比 ABBa 方案,本文方案具有明显的优势. 原因在于本文方案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 1 次乘运算;在原像采样复杂度上,本文方案是 ABBa 方案的 5/13 倍,原因在于原像采样算法使用小整数作为输入项且支持并行化运算,而不是使用输入项是高精度实数的正交化迭代运算;在陷门派生上,本文方案比其他方案高效的原因在于,陷门派生算法复杂度主要取决于所调用的 SampleR 算法(见引理 6)和 RandBasis 算法(见引理 1),而它们效率的根本都取决于所调用的原像采样算法. 在 2.2 节我们分析所调用的原像采样算法的时间复杂度相比通常原像采样算法的 $\Omega(n^2\,\mathrm{lb}^2\,n)$ 可降至 $O(n\,\mathrm{lb}^c\,n)$,且基于固定维数派生陷门算法的 HIBE 方案的陷门派生复杂度不会随系统分级深度的增长而变高.

4.2 标准模型下的 HIBE 方案效率分析

我们选择 3 个标准模型下的 HIBE 方案作为参照对象:Agrawal 等人[19]在 EUROCRYPT 2010 上提出的一种高效的标准模型下选择性安全的 HIBE 方案(简称 ABBb 方案);Agrawal 等人[20]在 CRYPTO 2010 上提出的可固定维数派生的标准模型下选择性安全的 HIBE 方案(简称 ABBa 方案);2016 年 Wang 等人[24]提出的一种标准模型下高效的选择性安全的 HIBE 方案(简称 WWL 方案). 与 4.1 节相同,设安全参数 $n=284$,$q=2$ 的 24 次方. 此外,在 ABBa,WWL 和本文方案中,设 $\bar{k}=60$ 是每个分级中用户身份的二进制长度. 对比结果如表 6 和表 7 所示,表中 SM-selective 表示该方案满足标准模型下 INDr-sID-CPA 安全性.

由表 4 和表 5 对比可以看出,与 4.1 节随机预言模型下的对比结果相似,相比非固定维数派生的 ABBb 方案,其他方案的主要优势在于陷门派生前后格的维数保持不变,因此效率参数如陷门尺寸、用户公私钥尺寸、明文-密文扩展率以及计算效率上的原像采样算法的复杂度均保持不变. 但是,基于固定维数陷门派生技术的 HIBE 方案存在的主要缺陷仍然是加密的复杂度,且该复杂度比 4.1 节随机预言模型下的要高,原因是在无随机预言模型的情况下,标准模型下的 HIBE 方案将每一级的用户身份设置为长度为 $\bar{k}$ 的二进制向量的形式,在加密者向分级深度为 ℓ 的用户发送消息时,需要计算 $\ell\bar{k}$ 个 $m\times m$ 矩阵的连续乘积,且不排除 $\ell=1$ 的情况. 但优点是该运算对于每个用户身份只需进行 1 次,且与发送的消息是无关的.

在陷门派生上,对于固定维数派生的 HIBE 方案,由于 ABBa 和 WWL 方案均基于 ABBa 中提出的时间复杂度是 $\Omega(n^3\,\mathrm{lb}^3\,n)$ 的 SampleR 算法,本文方案采用 2.2 节优化后的 SampleR 算法可将算法时间复杂度降至 $O(n^2\,\mathrm{lb}^c\,n)$,c 为常数;对于非固定

Table 6 Efficiency Comparison of HIBE Schemes Before Trapdoor Delegation Under Standard Model

表 6 标准模型下的 HIBE 方案派生前效率对比

Scheme (SM-selective)	The Dimension of Lattice	The Size of Trapdoor /MB	The Size of User's Public Key /MB	The Size of User's Private Key /KB	Ciphertext Expansion Rate	Computational Cost (multiplications and additions in $\mathbb{Z}_q$)		
						Trapdoor Generation	Preimage Sample	Encryption & Decryption
ABBb's	34 080	138.46	55.44	8.32	1 635 864	$\approx 12.75\times10^{12}$ mults $\approx 12.74\times10^{12}$ adds	$\approx 34.84\times10^{8}$ mults $\approx 46.46\times10^{8}$ adds	$\approx 39.30\times10^{8}$ mults $\approx 39.30\times10^{8}$ adds
ABBa's	34 080	138.46	27.69	4.16	817 944	$\approx 12.75\times10^{12}$ mults $\approx 12.74\times10^{12}$ adds	$\approx 34.84\times10^{8}$ mults $\approx 46.46\times10^{8}$ adds	$\approx 23.75\times10^{14}$ mults $\approx 23.74\times10^{14}$ adds
WWL's	40 896	199.38	33.23	4.99	981 528	$\approx 15.31\times10^{12}$ mults $\approx 15.30\times10^{12}$ adds	$\approx 50.17\times10^{8}$ mults $\approx 66.90\times10^{8}$ adds	$\approx 41.04\times10^{14}$ mults $\approx 41.03\times10^{14}$ adds
Ours	13 632	5.54	11.08	1.66	327 192	$\approx 13.74\times10^{9}$ mults $\approx 13.73\times10^{9}$ adds	$\approx 96.87\times10^{6}$ mults $\approx 96.87\times10^{6}$ adds	$\approx 15.20\times10^{14}$ mults $\approx 15.19\times10^{14}$ adds

Table 7　Efficiency Comparison of HIBE Schemes After Trapdoor Delegation Under Standard Model

表 7　标准模型下的 HIBE 方案派生后效率对比

Scheme (SM-selective)	The Dimension of Lattice	The Size of Trapdoor /MB	The Size of User's Public Key /MB	The Size of User's Private Key /KB	Ciphertext Expansion Rate	Computational Cost (multiplications and additions in $\mathbb{Z}_q$)		
						Trapdoor Generation	Preimage Sample	Encryption & Decryption
ABBb's	68 160	553.82	83.04	12.48	2 453 784	$\approx 95.00\times10^{13}$ mults $\approx 12.67\times10^{14}$ adds	$\approx 13.94\times10^{9}$ mults $\approx 18.58\times10^{9}$ adds	$\approx 51.01\times10^{8}$ mults $\approx 51.01\times10^{8}$ adds
ABBa's	34 080	138.46	27.69	4.16	817 944	$\approx 24.94\times10^{14}$ mults $\approx 25.34\times10^{14}$ adds	$\approx 34.84\times10^{8}$ mults $\approx 46.46\times10^{8}$ adds	$\approx 47.50\times10^{14}$ mults $\approx 47.49\times10^{14}$ adds
WWL's	40 896	199.38	33.23	4.99	981 528	$\approx 43.10\times10^{14}$ mults $\approx 43.78\times10^{14}$ adds	$\approx 50.17\times10^{8}$ mults $\approx 66.90\times10^{8}$ adds	$\approx 82.08\times10^{14}$ mults $\approx 82.07\times10^{14}$ adds
Ours	13 632	5.54	11.08	1.66	327 192	$\approx 15.34\times10^{13}$ mults $\approx 15.34\times10^{13}$ adds	$\approx 96.87\times10^{6}$ mults $\approx 96.87\times10^{6}$ adds	$\approx 30.40\times10^{14}$ mults $\approx 30.38\times10^{14}$ adds

维数派生的 HIBE 方案,其时间复杂度与格的维数紧密相关.由表 7 可以看出,在系统分级深度仅为 2 时,本文方案相比 ABBb 方案已有 6 倍的提升,且基于固定维数派生的 HIBE 方案因为格的维数在陷门派生前后不变,因此陷门派生的时间复杂度不受系统分级深度的影响.

综上所述,相比同类方案,本文方案在随机预言模型和标准模型下的陷门派生复杂度有效降低,且方案的效率参数和计算效率整体有所提高.因此,本文方案总体上是较高效的.

5　总　　结

为解决格上基于固定维数陷门派生技术的 HIBE 方案中陷门派生复杂度过高的问题,本文提出一种高效的$\mathbb{Z}_q$可逆矩阵提取算法,并基于该算法结合固定维数的陷门派生算法和 MP12 陷门函数分别在随机预言模型和标准模型下给出 2 种改进方案.方案安全性均归约至 LWE 问题的难解性,其中基于随机预言模型的 HIBE 方案的安全性满足 IND-aID-CPA 安全,基于标准模型的 HIBE 方案安全性满足 IND-sID-CPA 安全.对比分析表明,格上基于固定维数派生技术 HIBE 方案中陷门派生复杂度过高的问题得到有效解决,且在其他效率参数和计算效率上整体提升.

本文方案的不足在于标准模型下方案安全性仅满足 IND-sID-CPA 安全,如何构造标准模型下 IND-aID-CPA 安全的格上 HIBE 方案是值得进一步研究的问题.

参　考　文　献

[1] Shamir A. Identity-based crypto systems and signature schemes [C] //Proc of CRYPTO 1984. Berlin: Springer, 1984: 47-53

[2] Boneh D, Franklin M. Identity-based encryption from the weil pairing [C] //Proc of CRYPTO 2001. Berlin: Springer, 2001: 213-229

[3] Waters B. Efficient identity-based encryption without random oracles [C] //Proc of EUROCRYPT 2005. Berlin: Springer, 2005: 114-127

[4] Lai Junzuo, Deng R H, Liu Shengli, et al. Identity-based encryption secure against selective opening chosen-ciphertext attack [C] //Proc of EUROCRYPT 2012. Berlin: Springer, 2012: 77-92

[5] Yamada S. Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters [C] //Proc of EUROCRYPT 2016. Berlin: Springer, 2016: 32-62

[6] Wang Fenghe, Liu Zhenhua, Wang Chunxiao. Full secure identity-based encryption scheme with short public key size over lattices in the standard model [J]. International Journal of Computer Mathematics, 2016, 93(6): 854-863

[7] Regev O. On lattices, learning with errors, random linear codes, and cryptography [J]. Journal of the ACM, 2009, 56(6): 84-93

[8] Nguyen P, Zhang Jiang, Zhang Zhenfeng. Simpler efficient group signatures from lattices [C] //Proc of Public-Key Cryptography. Berlin: Springer, 2015: 401-426

[9] Libert B, Ling San, Nguyen K, et al. Zero-knowledge arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors [C] //Proc of EUROCRYPT 2016. Berlin: Springer, 2016: 1-31

[10] Brakerski Z, Perlman R. Lattice-based fully dynamic multi-key FHE with short ciphertexts [C] //Proc of CRYPTO 2016. Berlin: Springer, 2016: 190-213

[11] Zhang Yanhua, Hu Yupu. A new verifiable encrypted signature from lattices [J]. Journal of Computer Research and Development, 2017, 54(2): 305-312 (in Chinese)
(张彦华, 胡予濮. 新的基于格的可验证加密签名方案[J]. 计算机研究与发展, 2017, 54 (2): 305-312

[12] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions [C] //Proc of the 40th ACM Symp on Theory of Computing. New York: ACM, 2008: 197-206

[13] Ajtai M. Generating hard instances of the short basis problem [C] //Proc of Int Colloquium on Automata, Languages and Programming. Berlin: Springer, 1999: 1-9

[14] Agrawal S, Boyen X, Vaikuntanathan V, et al. Functional encryption for threshold functions (or fuzzy IBE) from lattices [C] //Proc of Public Key Cryptography. Berlin: Springer, 2012: 280-297

[15] Ducas L, Lyubashevsky V, Prest T. Efficient identity-based encryption over NTRU lattices [C] //Proc of ASIACRYPT 2014. Berlin: Springer, 2014: 22-41

[16] Katsumata S, Yamada S. Partitioning via non-linear polynomial functions: More compact IBEs from ideal lattices and bilinear maps [C] //Proc of ASIACRYPT 2016, Berlin: Springer, 2016: 682-712

[17] Zhang Jiang, Chen Yu, Zhang Zhenfeng. Programmable hash functions from lattices: Short signatures and IBEs with small key sizes [C] //Proc of CRYPTO 2016. Berlin: Springer, 2016: 302-332

[18] Cash D, Hofheinz D, Kiltz E, et al. Bonsai trees, or how to delegate a lattice basis [C] //Proc of EUROCRYPT 2010. Berlin: Springer, 2010: 523-552

[19] Agrawal S, Boneh D, Boyen X. Efficient lattice (H) IBE in the standard model [C] //Proc of EUROCRYPT 2010. Berlin: Springer, 2010: 553-572

[20] Agrawal S, Boneh D, Boyen X. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE [C] // Proc of CRYPTO 2010. Berlin: Springer, 2010: 98-115

[21] Micciancio D, Peikert C. Trapdoors for lattices: Simpler, tighter, faster, smaller [C] //Proc of EUROCRYPT 2012. Berlin: Springer, 2012: 700-718

[22] Alwen J, Peikert C. Generating shorter bases for hard random lattices [C] //Proc of the 26th Int Symp on Theoretical Aspects of Computer Science. Berlin: Springer, 2009: 535-553

[23] Micciancio D, Goldwasser S. Complexity of Lattice Problems: A Cryptographic Perspective [G] //The International Series in Engineering and Computer Science: 671. Berlin: Springer, 2002

[24] Wang Fenghe, Wang Chunxiao, Liu Zhenhua. Efficient hierarchical identity based encryption scheme in the standard model over lattices [J]. Frontiers of Information Technology & Electronic Engineering, 2016, 17(8): 781-791

Ye Qing, born in 1981. Associate professor at Henan Polytechnic University. Received her PhD degree from Beijing University of Posts and Telecommunications. Her main research interests include lattice cryptography and algebra.

Hu Mingxing, born in 1994. Master candidate in School of Computer Science and Technology, Henan Polytechnic University. His main research interests include information security and lattice cryptography.

Tang Yongli, born in 1972. Professor at Henan Polytechnic University. Senior member of CCF. Received her PhD degree from Beijing University of Posts and Telecommunications. His main research interests include information security and cryptography.

Liu Kun, born in 1978. Associate professor at Henan Polytechnic University. Received her MSc degree from Chongqing University of Posts and Telecommunications. Her main research interests include cryptography and number theory.

Yan Xixi, born in 1985. Associate professor at Henan Polytechnic University. Received her PhD degree from Beijing University of Posts and Telecommunications. Her main research interests include lattice cryptography and algebra.