软件学报 ISSN 1000-9825, CODEN RUXUEW
2025,36(10):4405−4416 [doi: 10.13328/j.cnki.jos.007388] [CSTR: 32375.14.jos.007388]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

半均匀 LWE 问题的紧致归约*

王 洋[1,2], 王明强[1]

[1](山东大学 数学学院, 山东 济南 250100)
[2](密码科学技术技术全国重点实验室, 北京 100878)
通信作者: 王明强, E-mail: wangmingqiang@sdu.edu.cn

摘 要: 在部分实用化的格密码协议设计和应用中, 需要用到公开矩阵服从特定分布的、非均匀的 LWE 问题的困难性来证明相应密码体制的安全性. 近期, 有研究工作给出了半均匀 LWE 问题的具体定义, 并采用类似证明熵 LWE 问题困难性的归约路线证明了欧氏格/理想格/模格上半均匀 LWE 问题的困难性. 但是, 已知的归约方法 (在维数和误差分布的高斯参数等方面) 会引入较大的归约损失, 同时需要引入额外的、非标准的困难性假设来证明环上的半均匀 LWE 问题的困难性. 利用 Hint-LWE 问题困难性的归约技巧, 给出了半均匀 LWE 问题困难性更紧致的归约. 采用的归约方法几乎不受代数结构的影响, 可以统一地应用到欧氏格/理想格/模格上定义的半均匀 LWE 问题. 可以基于标准的 LWE 假设证明对应欧氏格/理想格/模格上的半均匀 LWE 问题的困难性而无需引入任何额外的非标准困难性假设. 归约结果保持相应 LWE 问题的维数不变, 且归约过程中对应 LWE 问题的误差高斯参数的归约损失较小.

关键词: 基于格的密码学; 格中困难问题的归约; 半均匀 LWE 问题; Hint-LWE 问题; 离散高斯分布
中图法分类号: TP301

中文引用格式: 王洋, 王明强. 半均匀LWE问题的紧致归约. 软件学报, 2025, 36(10): 4405–4416. http://www.jos.org.cn/1000-9825/7388.htm
英文引用格式: Wang Y, Wang MQ. Tighter Reductions of LWE Problems with Semi-uniform Seeds. Ruan Jian Xue Bao/Journal of Software, 2025, 36(10): 4405–4416 (in Chinese). http://www.jos.org.cn/1000-9825/7388.htm

Tighter Reductions of LWE Problems with Semi-uniform Seeds

WANG Yang[1,2], WANG Ming-Qiang[1]

[1](School of Mathematics, Shandong University, Jinan 250100, China)
[2](State Key Laboratory of Cryptology, Beijing 100878, China)

Abstract: In certain designs and applications of practical lattice-based cryptography, the use of a specialized variant of LWE problems, where the public matrix is sampled from a non-uniform distribution, is required to establish the securities of corresponding cryptographic schemes. Recently, the formal definition of LWE problems with semi-uniform seeds was introduced in some work, in which the hardness of Euclidean, ideal, and module lattice-based LWE problems with semi-uniform seeds was proved through reduction roadmaps similar to those employed in the hardness proofs of entropic LWE problems. However, known reduction introduces significant losses in the Gaussian parameters of errors and dimensions. Moreover, additional non-standard assumptions are required to demonstrate the hardness of LWE problems with semi-uniform seeds over rings. In this study, a tighter reduction is proposed for LWE problems with semi-uniform seeds by incorporating modified techniques from the hardness proofs of Hint-LWE problems. The proposed reduction is largely unaffected by the algebraic structures of the underlying problems and can be uniformly applied to Euclidean, ideal, and module lattice-based LWE problems

* 基金项目: 国家重点研发计划 (2021YFB3100200); 保密通信全国重点实验室稳定支持计划 (2024, WD202402); 密码科学技术全国重点实验室开放课题 (MMKFKT202207); 山东省自然科学基金 (ZR2022QF039)
本文由“抗量子密码与区块链应用”专题特约编辑翁健教授、祝烈煌教授、赵运磊教授推荐.
收稿时间: 2024-06-25; 修改时间: 2024-09-05; 采用时间: 2024-12-30; jos 在线出版时间: 2025-01-20
CNKI 网络首发时间: 2025-08-12

with semi-uniform seeds. The hardness of these LWE problems can be established based on standard LWE assumptions without the need for any additional non-standard assumptions. Furthermore, the dimension of the corresponding LWE problems remains unchanged, and the reduction introduces only minimal losses in Gaussian parameters of errors.

Key words: lattice-based cryptography; reduction of lattice-based problem; LWE problems with semi-uniform seeds; Hint-LWE problem; discrete Gaussian distribution

欧氏格 LWE (learning with errors problem) 问题[1]及其 (代数) 变体环/模 LWE 问题[2,3]是目前格密码中应用最广泛的一类平均情形的数学困难问题, 基于欧氏格/环/模 LWE 问题及其适当形式的变体问题几乎可以设计已知的所有密码原语. 到目前为止, 关于 LWE 问题实用化变体问题的研究可以粗略地分为 3 类 (更具体的分类讨论可参考文献 [4]). 第 1 类是研究 LWE 问题的秘密或者误差分布为更一般的分布 (例如 $\{0,1\}$ 上的二元分布, 小区间 $[-\alpha,\alpha]$ 上的均匀分布, 熵 LWE 问题等) 时, 对应 LWE 问题的困难性[5–9]; 第 2 类是研究 LWE 问题的秘密或者误差存在部分泄露信息时, 对应的 LWE 问题 (即 Hint-LWE 问题) 的困难性[5,10–15]; 第 3 类是研究 LWE 问题的公开矩阵为非均匀分布时, 对应的 LWE 问题 (即非均匀 LWE 问题) 的困难性[4,16–18].

近期, Jia 等人[4,17,18] 系统地研究了一类特殊的非均匀 LWE 问题, 即半均匀 LWE 问题, 的困难性, 给出了半均匀 LWE 问题的形式化定义, 并采用类似证明熵 LWE 问题困难性的归约路线证明了欧氏格/理想格/模格上对应半均匀 LWE 问题的困难性. 以欧氏格为例, 称 $\mathbb{Z}_q^{m\times d}$ 上的分布 $\mathcal{D}$ 为 η-半均匀分布, 如果存在 $\mathbb{Z}^{m\times d}$ 上的一族可以有效取样的分布 $\{\phi_U\}_{U\in\mathbb{Z}_q^{m\times d}}$, 使得取样过程 $\{U+E_U : U \hookleftarrow \mathrm{U}\left(\mathbb{Z}_q^{m\times d}\right), E_U \hookleftarrow \phi_U\}$ 所输出的分布与 $\mathcal{D}$ 统计不可区分, 且以接近于 1 的概率有 E_U 的谱范数不超过 η 成立. 在本文中, 离散高斯分布一般使用 D; 当不引起歧义时, 我们使用 $\mathcal{D}$ 来表示对应 LWE 问题中的公开矩阵 A 服从的分布, 以突出半均匀 LWE 问题的公开矩阵. 对应地, 可以定义判定版本的非均匀 LWE 问题 $\mathrm{DLWE}^d_{\mathbb{Z},m,q,\chi_1}(\chi_2;\mathcal{D})$ 为区分如下分布.

(1) $\{(A, A\cdot \boldsymbol{s}+\boldsymbol{e} \bmod q\mathbb{Z}) : A \hookleftarrow \mathcal{D}, \boldsymbol{s} \hookleftarrow \chi_2, \boldsymbol{e} \hookleftarrow \chi_1\}$.

(2) $\{(A,\boldsymbol{u}) : A \hookleftarrow \mathcal{D}, \boldsymbol{u} \hookleftarrow \mathrm{U}(\mathbb{Z}_q^m)\}$.

值得注意的是, 对任意的 $U\in\mathbb{Z}_q^{m\times d}$, 当选取 ϕ_U 为特定的固定函数 $E_U=\left\lfloor \frac{q}{p}\cdot\left\lfloor \frac{p}{q}\cdot U\right\rceil\right\rceil - U$ 时, 对应的半均匀 LWE 问题即为区分如下分布.

(1) $\left\{\left(\left\lfloor \frac{q}{p}\cdot\left\lfloor \frac{p}{q}\cdot A\right\rceil\right\rceil, \left\lfloor \frac{q}{p}\cdot\left\lfloor \frac{p}{q}\cdot A\right\rceil\right\rceil\cdot \boldsymbol{s}+\boldsymbol{e} \bmod q\mathbb{Z}\right) : A \hookleftarrow \mathrm{U}\left(\mathbb{Z}_q^{m\times d}\right), \boldsymbol{s}\hookleftarrow\chi_2, \boldsymbol{e}\hookleftarrow\chi_1\right\}$.

(2) $\left\{\left(\left\lfloor \frac{q}{p}\cdot\left\lfloor \frac{p}{q}\cdot A\right\rceil\right\rceil, \boldsymbol{u}\right) : A \hookleftarrow \mathrm{U}\left(\mathbb{Z}_q^{m\times d}\right), \boldsymbol{u}\hookleftarrow \mathrm{U}(\mathbb{Z}_q^m)\right\}$.

值得指出的是, 由 A 可以很容易地计算 $\left\lfloor \frac{q}{p}\cdot\left\lfloor \frac{p}{q}\cdot A\right\rceil\right\rceil$. 利用这里一类特殊的半均匀 LWE 问题可以证明 NIST (National Institute of Standards and Technology) 后量子竞赛第 1 轮的候选算法 Kyber 采用的基础公钥加密方案的 IND-CPA (indistinguishability under chosen plaintext attack) 安全性[19,20]. 也就是说, 可以证明采用 LP 框架[21]和压缩公钥的方式来设计的高效公钥加密方案也是满足 IND-CPA 安全的. 早期, 由于缺乏对应非均匀 LWE 问题到标准 LWE 问题的严格归约, Kyber 设计团队从 NIST 第 2 轮竞选开始取消了方案中对公钥进行压缩的设计方式[22–24], 这导致对应方案的通信带宽的增加. 在实践应用中, 这一类特殊的半均匀 LWE 问题可以结合密钥共识等技术来设计非常高效的格密码方案[25–29].

虽然已知的半均匀 LWE 问题困难性的归约结果适用于一般的秘密分布 (即归约中仅要求秘密 $\boldsymbol{s}$ 的分布在特定条件下拥有足够的熵即可, $\boldsymbol{s}$ 所服从分布的具体形式可以不定). 但是由于采用的是类似证明熵 LWE 问题困难性的归约路线, 已知的半均匀 LWE 问题的归约在维数和高斯分布参数等方面的归约损失较大[4,17,18]. 具体来讲, 证明 d 维的半均匀 LWE 问题的困难性要用的 $\tilde{d}$ ($d=\mathrm{O}(\tilde{d}\cdot\log q)$) 维的标准 LWE 问题的困难性. 同时, 对于一般的 η-半均匀分布 $\mathcal{D}$, 归约过程中高斯误差参数的损失与样本数目有关 (特别是样本数为 $\mathrm{poly}(\lambda)$ 时, 误差参数的膨胀倍数较大). 另外, 在证明环中 (求解版本) 半均匀 LWE 问题的困难性时, 需要引入额外的、相对而言非标准的困难性假设, 即某种判定版本的 NTRU 问题对应的假设.

© 中国科学院软件研究所 http://www.jos.org.cn

在实用中, 一般采用的秘密/误差分布为离散高斯分布的 LWE 问题来进行密码协议的设计或者困难问题的归约讨论. 一个自然的问题是针对特定的离散高斯分布的情形, 能否给出非均匀 LWE 问题的更紧致的归约. 这也是本研究的主要出发点和研究动机所在.

在本文中, 我们推广了 Hint-LWE 问题困难性研究中用到的技巧并将其应用于半均匀 LWE 问题困难性的研究中, 给出了半均匀 LWE 问题困难性更紧致的归约方法. 本文采用的归约方法基本不受代数结构的限制, 可以统一地应用于欧氏格/理想格/模格上定义的半均匀 LWE 问题. 具体来讲, 本文的归约方式具有以下优势.

(1) 归约结果是保持维数的: 即 d 维的半均匀 LWE 问题的困难性仅需要用到 d 维的标准 LWE 问题的困难性来保证.

(2) 归约过程中的高斯参数损失较少, 且对于一般的 η-半均匀分布 $\mathcal{D}$, 归约中的高斯参数与样本数无关: 即高斯参数为 σ 的 d 维的半均匀 LWE 问题的困难性可以由高斯参数为 $\mathrm{O}(\eta\cdot\sigma)$ 的 d 维的标准 LWE 问题的困难性来保证.

本文第 1 节介绍非均匀 LWE 问题的简单研究现状. 第 2 节介绍本文所需的基础知识, 包括欧氏格/理想格/模格、高斯分布、 LWE 问题/半均匀 LWE 问题的定义和一些有用的引理等. 第 3 节介绍本文的主要归约, 并将我们的归约结果与已知结果做简单比较. 最后, 在第 4 节总结全文.

1 非均匀 LWE 问题的相关工作

在初始 LWE 问题的样本中, 公开矩阵一般选自随机均匀分布, 即 $A \hookleftarrow \mathrm{U}\left(\mathbb{Z}_q^{m\times d}\right)$. 在已知的部分 LWE 问题的变体问题研究中, 经常需要将 A 换成所谓的 Lossy 形式 (即 $A = B\cdot C + E$, 使用多秘密的 LWE 样本来替换均匀矩阵) 来进行讨论[6–8]. 一般而言, $A = B\cdot C + E$ 对应的分布不是与均匀分布统计不可区分的. 但是在对应 LWE 问题困难这个计算假设下, 可以证明对应的“非均匀” LWE 问题也是困难的. 在本文中, 非均匀 LWE 问题指的是公开矩阵 A 服从的分布 $\mathcal{D}$ 与 $\mathrm{U}\left(\mathbb{Z}_q^{m\times d}\right)$ 不是统计或者计算不可区分的情况下对应的 LWE 问题.

据我们所知, 在不考虑某些 A 为特定的循环矩阵的情况下对应的 LWE 问题 (此类问题对应 A 的系数在某些环上均匀选择)[30] 时, Boneh 等人[16]首次讨论了非均匀 LWE 问题的困难性, 并证明了当公开矩阵 A 服从的分布为 (1) $\mathbb{Z}^d$ 上适当参数的离散高斯分布; (2) k 足够大时对应的 $\{0,1\}^k$ 上的均匀分布; (3) $\mathbb{Z}^d$ 的某些足够大的线性子空间上的均匀分布时, 对应的非均匀 LWE 问题的困难性可以由标准 LWE 问题的困难性来保证. 此外, Bruna 等人[31]提出的连续 LWE 问题 (continuous LWE problem) 对应的公开矩阵 A 服从适当的连续高斯分布, Gupte 等人[32]也证明了适当参数条件下, 此类问题的困难性可以由标准的 LWE 问题来保证.

但是, 上述几类非均匀 LWE 问题不适用于某些格密码应用 (例如压缩公钥的方式来设计的加密/密钥封装方案[25–29]). 近期, Jia 等人[4,17,18]形式化定义了半均匀 LWE 问题, 并采用类似证明熵 LWE 问题困难性的归约路线, 结合 Renyi 散度、格中正则性结论 (leftover hash lemma) 等工具证明了欧氏格/理想格/模格中适当参数的半均匀 LWE 问题是困难的.

2 基础知识

在本节中, 我们将给出符号说明, 并介绍在本文讨论过程中要经常用到的概念、定义和部分引理.

使用符号 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ 来依次表示全体整数/有理数/实数组成的集合. 对于给定的正整数 $q\in\mathbb{Z}$, 定义符号 $\mathbb{Z}_q := \mathbb{Z}/q\cdot\mathbb{Z}$ 并使用符号 $[q]$ 来表示集合 $\{1,2,\ldots,q\}$. 如无特殊说明, 我们默认 $\mathbb{Z}_q$ 中陪集的代表元取自集合 $\left[-\frac{q}{2},\frac{q}{2}\right)\cap\mathbb{Z}$. 本文使用粗体小写字母 $\boldsymbol{x}$ 来表示向量, 使用斜体大写字母 A 来表示矩阵或者集合. 如无特殊说明, 在本文中默认使用列向量, 并使用符号 A^{T} 来表示矩阵 A 的转置 (向量亦看为特殊的矩阵); 符号 I_d 表示 $d\times d$ 的单位矩阵. 对于向量 $\boldsymbol{x} = (x_1,\ldots,x_d)^{\mathrm{T}}\in\mathbb{R}^d$, 定义 $\|\boldsymbol{x}\| := \sum_{i=1}^{d} x_i^2$, $\|\boldsymbol{x}\|_1 := \sum_{i=1}^{d}|x_i|$, $\|\boldsymbol{x}\|_\infty := \max_{i\in[d]}|x_i|$. 对于矩阵 $A\in\mathbb{R}^{d\times d}$, 使用符号 $\mathfrak{s}_k(A), k\in[d]$ 来表示矩阵 A 的 d 个不同的奇异值. 我们默认对奇异值按照大小排序为 $\mathfrak{s}_d(A)\leqslant\ldots$

© 中国科学院软件研究所 http://www.jos.org.cn

$\leqslant \mathfrak{s}_2(A) \leqslant \mathfrak{s}_1(A)$, 此时 $\mathfrak{s}_1(A)$ 即为 A 的谱范数. 对于有限集合 S, 符号 $\mathrm{U}(S)$ 表示集合 S 上的均匀分布. 对于概率分布 $\mathcal{D}$, 使用符号 $x \hookleftarrow \mathcal{D}$ 来表示随机变量 x 服从分布 $\mathcal{D}$. 集合 S 上的离散概率分布 $\mathcal{D}_1$ 和 $\mathcal{D}_2$ 的统计距离 $\Delta(\mathcal{D}_1,\mathcal{D}_2)$ 定义为 $\Delta(\mathcal{D}_1,\mathcal{D}_2) := \frac{1}{2}\cdot\sum_{a\in S}\left|\Pr_{x\hookleftarrow\mathcal{D}_1}[x=a]-\Pr_{y\hookleftarrow\mathcal{D}_2}[y=a]\right|$. 我们使用符号 λ 来表示安全参数, 并称一个函数 $f(\lambda)$ 是可忽略的, 如果对任意的 $c>0$, 存在 λ_0, 使得对任意的 $\lambda \geqslant \lambda_0$, 不等式 $f(\lambda) \leqslant \frac{1}{\lambda^c}$ 恒成立. 当具体的函数形式对我们的讨论没有影响时, 一般使用符号 $negl(\lambda)$ 来表示 (某个或者某些不同的) 可忽略的函数. 如果 $\Delta(\mathcal{D}_1,\mathcal{D}_2) \leqslant negl(\lambda)$, 则称概率分布 $\mathcal{D}_1$ 和 $\mathcal{D}_2$ 是统计接近的/统计不可区分的.

2.1 格与离散高斯分布

本文仅讨论满秩的整数格. 更确切地说, 本文讨论的 d 维欧氏格 $\Lambda := \mathcal{L}(B)$ 可写成形如 $\mathbb{Z}\cdot\boldsymbol{b}_1+\ldots+\mathbb{Z}\cdot\boldsymbol{b}_d$ 的形式, 其中, $B := (\boldsymbol{b}_1|\ldots|\boldsymbol{b}_d) \in \mathbb{Z}^{d\times d}$, d 为任意正整数. 格 Λ 的对偶格 Λ^* 的定义为 $\Lambda^* := \{\boldsymbol{x}\in\mathbb{R}^d : <\boldsymbol{x},\boldsymbol{y}> \in \mathbb{Z}, \forall \boldsymbol{y}\in\Lambda\}$. 我们也关心特殊的理想/模格. 为了简化讨论, 本文固定正整数 $n=2^{\hat{n}}$, 并考虑特殊的分圆域 $\mathcal{K} := \mathbb{Q}[x]/(x^n+1)$ 及其代数整数环 $\mathcal{R} := \mathbb{Z}[x]/(x^n+1)$ (值得注意的是, 采用与本文类似的分析方法, 本文的结论可以推广到一般的代数数域中). 对于 $\mathcal{R}$ 中的多项式 $a = a_0+a_1\cdot x+\ldots+a_{n-1}\cdot x^{n-1}$, 我们采用系数嵌入 σ_{coef} 将其嵌入 $\mathbb{Z}^n$, 即 $\sigma_{\mathrm{coef}}(a) := (a_0,\ldots,a_{n-1})^{\mathrm{T}}$. 注意到 $\mathcal{R}$ 中两个元素的多项式乘法可以表示为矩阵乘以向量的形式. 对于给定的 $a = a_0+a_1\cdot x+\ldots+a_{n-1}\cdot x^{n-1}$ 和 $b = b_0+b_1\cdot x+\ldots+b_{n-1}\cdot x^{n-1}$, 经简单计算可知, $\sigma_{\mathrm{coef}}(a\cdot b) = M_{\mathrm{coef}}(a)\cdot\sigma_{\mathrm{coef}}(b) = M_{\mathrm{coef}}(b)\cdot\sigma_{\mathrm{coef}}(a)$. 其中,

$$M_{\mathrm{coef}}(a) := \begin{pmatrix} a_0 & -a_{n-1} & -a_{n-2} & \ldots & -a_1 \\ a_1 & a_0 & -a_{n-1} & \ldots & -a_2 \\ a_2 & a_1 & a_0 & \ldots & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \ldots & a_0 \end{pmatrix}.$$

易知, 对于 $\mathcal{R}$ 的任意理想 $\mathcal{J}$, $\sigma_{\mathrm{coef}}(\mathcal{J})$ 为一个满秩格.

对于任意给定的正实数 $s\in\mathbb{R}$ 和向量 $\boldsymbol{c}\in\mathbb{R}^d$, 定义以 s 为参数、以 $\boldsymbol{c}$ 为中心的 d 维高斯函数为 $\rho_{s,\boldsymbol{c}}(\boldsymbol{x}) := \mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2}}$. 对应地, 以 s 为参数、以 $\boldsymbol{c}$ 为中心的 d 维连续高斯分布 $D_{s,\boldsymbol{c}}$ 对应的概率密度函数为 $\frac{1}{s^d}\cdot\rho_{s,\boldsymbol{c}}(\boldsymbol{x})$, $\boldsymbol{x}\in\mathbb{R}^d$. 可以将对应的高斯分布限制在任意的格 (或者离散集合) Λ 上, 对应的离散高斯分布 $D_{\Lambda,s,\boldsymbol{c}}$ 的概率分布函数为 $\rho_{s,\boldsymbol{c}}(\boldsymbol{x})/\rho_{s,\boldsymbol{c}}(\Lambda)$, $\boldsymbol{x}\in\Lambda$. 这里, $\rho_{s,\boldsymbol{c}}(\Lambda) := \sum_{\boldsymbol{x}\in\Lambda}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})$. 当 $\boldsymbol{c}=0$ 或者 $s=1$ 时, 我们省略相关符号中对应的下标, 例如使用 $\rho_s(\boldsymbol{x})$, $\rho(\boldsymbol{x})$ 等. 给定任意非奇异的矩阵 $B\in\mathbb{R}^{d\times d}$, 矩阵 $\Sigma := B\cdot B^{\mathrm{T}}$ 是一个实对称正定矩阵 (记为 $\Sigma>0$). 定义 $\rho_B(\boldsymbol{x}) := \rho(B^{-1}\cdot\boldsymbol{x}) = \mathrm{e}^{-\pi\cdot\boldsymbol{x}^{\mathrm{T}}\cdot\Sigma^{-1}\cdot\boldsymbol{x}}$. 注意到 $\rho_B(\boldsymbol{x})$ 的取值仅仅与 Σ 和 $\boldsymbol{x}$ 相关, 因此我们记 $\rho_{\sqrt{\Sigma}}(\boldsymbol{x}) := \rho_B(\boldsymbol{x})$. 为了简化讨论, 这里的 $\sqrt{\Sigma}$ 选择为 Σ 的 Cholesky 分解 (即满足条件 $\Sigma = \sqrt{\Sigma}\cdot\sqrt{\Sigma}^{\mathrm{T}}$, $\sqrt{\Sigma}$ 为下三角矩阵). 事实上, 取 $\sqrt{\Sigma}$ 为任意满足条件 $\Sigma = B\cdot B^{\mathrm{T}}$ 的矩阵 B 并不会影响后续的讨论. 对于两个实对称正定矩阵 A,B, 如果 $A-B$ 仍为实对称正定矩阵, 则记 $A>B$.

当我们在 $\mathcal{R}$ 中讨论时, 我们使用符号 $f \hookleftarrow D_{\mathcal{R},s}$ 来表示多项式 f 的系数独立地取自参数为 s 的一维离散高斯分布 $D_{\mathbb{Z},s}$. 由于 $(D_{\mathbb{Z},s})^d = D_{\mathbb{Z}^d,s}$, 因此 $f \hookleftarrow D_{\mathcal{R},s}$ 等价于 f 的系数组成的向量服从分布 $D_{\mathbb{Z}^n,s}$, 即 $\sigma_{\mathrm{coef}}(f) \hookleftarrow D_{\mathbb{Z}^n,s}$. 特别地, 我们有 $D_{\mathcal{R}^d,s} = D_{\mathbb{Z}^{n\cdot d},s}$. 假设 $\varepsilon>0$ 为某正实数. 对任意的 d 维格 Λ, 定义格 Λ 的 (与 ε 相关的) 光滑参数 $\eta_\varepsilon(\Lambda)$ 为 $\min_{s>0}\{s : \rho_{1/s}(\Lambda^*\backslash\{0\}) \leqslant \varepsilon\}$. 类似地, 对于任意的实对称正定矩阵 $\Sigma>0$, 如果条件 $\eta_\varepsilon\left(\sqrt{\Sigma}^{-1}\cdot\Lambda\right) \leqslant 1$ 成立, 则记 $\sqrt{\Sigma} \geqslant \eta_\varepsilon(\Lambda)$. 根据定义, 条件 $\eta_\varepsilon\left(\sqrt{\Sigma}^{-1}\cdot\Lambda\right) \leqslant 1$ 等价于 $\rho\left(\sqrt{\Sigma}^{\mathrm{T}}\cdot\Lambda^*\backslash\{0\}\right) = \rho_{\sqrt{\Sigma}^{-1}}(\Lambda^*\backslash\{0\}) \leqslant 0$. 在本文后面的讨论中, 我们需要用到如下引理[1,8,10,33–35].

引理 1. 以下事实成立.

(1) 假设 Σ 是实对称正定矩阵, Λ 为某个格, 实数 $\varepsilon\in\left(0,\frac{1}{2}\right)$. 如果 $\mathfrak{s}_1(\Sigma) \leqslant \eta_\varepsilon(\Lambda)^{-2}$, 则有 $\sqrt{\Sigma} \geqslant \eta_\varepsilon(\Lambda)$.

(2) 对于 d 维格 $\mathbb{Z}^d$, 存在可忽略的 $\varepsilon = \varepsilon(\lambda)$ 使得 $\eta_\varepsilon(\mathbb{Z}^d) \leqslant \omega\left(\sqrt{\log d}\right)$.

(3) 假设已知 d 维格 $\Lambda = \mathcal{L}(B)$ 的一组格基 B, 实数 $r = \omega\left(\sqrt{\log d}\right)$. 则对任意的向量 $\boldsymbol{c}\in\mathbb{R}^d$ 和满足条件

© 中国科学院软件研究所 http://www.jos.org.cn

$\Sigma > r^2 \cdot B \cdot B^{\mathrm{T}}$ 的实对称正定矩阵 Σ, 存在利用 B 的多项式时间的取样算法从一个与分布 $D_{\Lambda,\sqrt{\Sigma},\boldsymbol{c}}$ 统计接近的分布中抽取样本.

注意到在 σ_{coef} 的作用下, $\mathcal{R}$ 对应 $\mathbb{Z}^n$. 根据引理 1, 对任意的向量 $\boldsymbol{c} \in \mathbb{R}^{n\cdot d}$ 和满足条件 $\Sigma > \omega\left(\sqrt{\log n \cdot d}\right)$ 的实对称正定矩阵 Σ, 我们可以有效地从一个与 $D_{\mathcal{R}^d,\sqrt{\Sigma},\boldsymbol{c}}$ 统计不可区分的分布中进行抽样.

引理 2. 假设实数 $\varepsilon \in \left(0,\frac{1}{2}\right)$, Σ_1,Σ_2 为实对称正定矩阵, $\Sigma_3^{-1} := \Sigma_2^{-1} + \Sigma_2^{-1}$ 且满足条件 $\sqrt{\Sigma_3} \geqslant \eta_\varepsilon(\mathbb{Z}^d)$. 则对任意的向量 $\boldsymbol{c} \in \mathbb{R}^d$, 分布 $\{\boldsymbol{x}_1 + \boldsymbol{x}_2 : \boldsymbol{x}_1 \hookleftarrow D_{\mathbb{Z}^d,\sqrt{\Sigma_1}}, \boldsymbol{x}_2 \hookleftarrow D_{\mathbb{Z}^d,\sqrt{\Sigma_2},\boldsymbol{c}}\}$ 与 $D_{\mathbb{Z}^d,\sqrt{\Sigma_1+\Sigma_2},\boldsymbol{c}}$ 的统计距离不超过 $2\cdot\varepsilon$.

利用引理 2, 我们可以将某个离散高斯分布拆分为某两个适当参数的离散高斯分布的和.

2.2 LWE 问题

LWE 问题最早由 Regev[1]提出, 是目前格密码设计中应用最广泛的一类平均情形的格中困难问题.

本文用符号 $\mathfrak{R}$ 来表示环 $\mathbb{Z}$ 或者 $\mathcal{R}$, 并定义 $\mathfrak{R}_q := \mathfrak{R}/q\cdot\mathfrak{R}$. 在系数嵌入 σ_{coef} 的作用下, $\mathcal{R}$ 中元素的加法和乘法可以使用 $\mathbb{Z}^n$ 中向量的加法, 以及对应矩阵和向量的乘法来表示. 注意到 σ_{coef} 可以平凡地扩展到以 $\mathcal{R}$ 中的元素为元素的向量或者矩阵上. 为了讨论方便, 定义 $\mathbb{Z}$ 上的 σ_{coef} 作用为恒等映射. 这样, σ_{coef} 可以视为 $\mathfrak{R}$ 上的 $\mathbb{Z}$-模同态, 或者视为 $\mathfrak{R}_q$ 上的 $\mathbb{Z}_q$-模同态.

对于正整数 m,d,q 以及 $\mathfrak{R}^m$ 上的概率分布 χ_1, $\mathfrak{R}^d$ 上的概率分布 χ_2, $\mathfrak{R}_q^{m\times d}$ 上的概率分布 $\mathcal{D}$, 定义环 $\mathfrak{R}$ 相关的判定版本的 LWE 问题 (记为 $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}(\chi_2;\mathcal{D})$) 为如下问题: 区分分布 $(A, A\cdot\boldsymbol{s}+\boldsymbol{e} \bmod q\cdot\mathfrak{R})$ 与分布 $(A,\boldsymbol{u})$. 这里, $A \hookleftarrow \mathcal{D}$, $\boldsymbol{s} \hookleftarrow \chi_2$, $\boldsymbol{e} \hookleftarrow \chi_1$, $\boldsymbol{u} \hookleftarrow \mathrm{U}\left(\mathfrak{R}_q^m\right)$. 注意到在上述定义中, 参数 m 对应的是 LWE 问题的样本数; $\mathcal{D}$ 即为 LWE 问题公开矩阵服从的分布; χ_1 和 χ_2 分别为 LWE 问题的误差向量和秘密向量服从的分布. 为了下文讨论方便, 当样本形式为 $(A, A\cdot\boldsymbol{s}+\boldsymbol{e} \bmod q\cdot\mathfrak{R})$ 时, 我们称对应的样本取自 $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}(\chi_2;\mathcal{D})$ 问题的分布. 对于任意的 (量子) 概率多项式时间的敌手 $\mathfrak{A}$, 定义其解决 $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}(\chi_2;\mathcal{D})$ 问题的优势为:

$$\mathrm{Adv}_{\mathfrak{A}}\left(\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}(\chi_2;\mathcal{D})\right) := |\Pr[\mathfrak{A}(A, A\cdot\boldsymbol{s}+\boldsymbol{e} \bmod q\cdot\mathfrak{R}) = 1] - \Pr[\mathfrak{A}(A,\boldsymbol{u}) = 1]|.$$

当 $\mathfrak{R} = \mathbb{Z}$ 时, 上述判定版本 LWE 问题对应欧氏格上的 LWE 问题. 此时, 参数 d 为对应的 (格的) 维数. 而当 $\mathfrak{R} = \mathcal{R}$ 时, 上述判定版本 LWE 问题对应现实中最常用的、扩张次数为 2 的幂次的分圆域上定义的相应 LWE 问题. 此时, 对应的 (格的) 维数为 $n\cdot d$. 当 $d = 1$ 时对应环 LWE 问题, 而当 $d \geqslant 2$ 时对应模 LWE 问题.

一般而言,LWE 问题的公开矩阵的分布为 $\mathcal{D} = \mathrm{U}\left(\mathfrak{R}_q^{m\times d}\right)$. 当 $\mathcal{D} \neq \mathrm{U}\left(\mathfrak{R}_q^{m\times d}\right)$ 时, 我们称对应的 LWE 问题为非均匀 LWE 问题. 本文关心的是非均匀 LWE 问题中的一类特殊的半均匀 LWE 问题, 即 $\mathcal{D}$ 为下面定义的 η-半均匀分布[4,17,18].

定义 1. 假设 m,d 为正整数. 对于任意的正实数 $\eta > 0$, 我们称分布 $\mathcal{D}$ 为 $\mathfrak{R}_q^{m\times d}$ 上的 η-半均匀分布, 如果存在 $\mathfrak{R}^{m\times d}$ 上的一族可以有效取样的概率分布 $\{\phi_U\}_{U\in\mathfrak{R}^{m\times d}}$ 使得对任意随机取样的 $A \hookleftarrow \mathcal{D}, U \hookleftarrow \mathrm{U}\left(\mathfrak{R}_q^{m\times d}\right)$ 和 $E_U \hookleftarrow \phi_U$, 下面两个条件成立:

(1) 随机变量 A 与 $U + E_U \bmod q\cdot\mathfrak{R}$ 统计不可区分.

(2) $\Pr_{U\hookleftarrow\mathrm{U}(\mathfrak{R}_q^{m\times d}),E_U\hookleftarrow\phi_U}\left[\mathfrak{s}_1(\sigma_{\mathrm{coef}}(E_U)) \leqslant \eta\right] \geqslant 1 - negl(\lambda)$.

3 半均匀 LWE 问题的困难性研究

本节将给出半均匀 LWE 问题相关的更紧的归约方法. 在给出具体的归约之前, 我们需要用到下面这个关键引理. 引理 3 的证明所采用到的方法与文献 [10] 中的方法类似.

引理 3. 假设 σ_1,σ_2 为正实数, $\tilde{m},\tilde{n}$ 为正整数, $F \in \mathbb{Z}^{\tilde{m}\times\tilde{n}}$ 为任意一个使得矩阵 $\Sigma_0 := \left(\frac{1}{\sigma_1{}^2}\cdot I_{\tilde{n}} + \frac{1}{\sigma_2{}^2}\cdot F^{\mathrm{T}}\cdot F\right)^{-1}$ 存在的矩阵. 则以下两个取样过程输出的分布相同.

(1) 先取样 $\boldsymbol{s} \hookleftarrow D_{\mathbb{Z}^{\tilde{n}},\sigma_1}$ 和 $\boldsymbol{e} \hookleftarrow D_{\mathbb{Z}^{\tilde{m}},\sigma_2}$, 再计算 $\boldsymbol{z} = F\cdot\boldsymbol{s}+\boldsymbol{e}$, 最后输出 $(\boldsymbol{s},\boldsymbol{z}) \in \mathbb{Z}^{\tilde{n}} \times \mathbb{Z}^{\tilde{m}}$.

(2) 先取样 $\boldsymbol{s} \hookleftarrow D_{\mathbb{Z}^{\tilde{n}},\sigma_1}$ 和 $\boldsymbol{e} \hookleftarrow D_{\mathbb{Z}^{\tilde{m}},\sigma_2}$, 再计算 $\boldsymbol{z} = F\cdot\boldsymbol{s}+\boldsymbol{e}$ 和 $\boldsymbol{c} = \frac{1}{\sigma_2{}^2}\cdot\Sigma_0\cdot F^{\mathrm{T}}\cdot\boldsymbol{z}$; 随后采样 $\tilde{\boldsymbol{s}} \hookleftarrow D_{\mathbb{Z}^{\tilde{n}},\sqrt{\Sigma_0},\boldsymbol{c}}$; 最后输

© 中国科学院软件研究所 http://www.jos.org.cn

出 $(\tilde{\boldsymbol{s}},\boldsymbol{z})\in\mathbb{Z}^{\tilde{n}}\times\mathbb{Z}^{\tilde{m}}$.

证明: 记输出的第 1 个随机变量为 $\boldsymbol{x}$, 第 2 个随机变量为 $\boldsymbol{y}$. 注意到对任意的 $(\boldsymbol{v},\boldsymbol{w})\in\mathbb{Z}^{\tilde{n}}\times\mathbb{Z}^{\tilde{m}}$:

$$\Pr[\boldsymbol{x}=\boldsymbol{v}\wedge\boldsymbol{y}=\boldsymbol{w}]=\Pr[\boldsymbol{y}=\boldsymbol{w}]\cdot\Pr[\boldsymbol{x}=\boldsymbol{v}|\boldsymbol{y}=\boldsymbol{w}].$$

同时, 在两个取样过程中, $\Pr[\boldsymbol{y}=\boldsymbol{w}]=\Pr[\boldsymbol{z}=F\cdot\boldsymbol{s}+\boldsymbol{e}=\boldsymbol{w}]$ 相同. 因此, 为了证明这两个取样过程最后输出的分布相同, 只需证明在取样过程 (1) 中, 在已知 $F\cdot\boldsymbol{s}+\boldsymbol{e}$ 的情况下, $\boldsymbol{s}$ 服从的条件分布为 $D_{\mathbb{Z}^{\tilde{n}},\sqrt{\Sigma_0},\boldsymbol{c}}$ 即可.

为此, 任取 $(\boldsymbol{v},\boldsymbol{w})\in\mathbb{Z}^{\tilde{n}}\times\mathbb{Z}^{\tilde{m}}$. 在取样过程 (1) 中, 我们有:

$$\begin{aligned}&\Pr[\boldsymbol{x}=\boldsymbol{v}\wedge\boldsymbol{y}=\boldsymbol{w}]=\Pr[\boldsymbol{s}=\boldsymbol{v}\wedge F\cdot\boldsymbol{s}+\boldsymbol{e}=\boldsymbol{w}]=\Pr[\boldsymbol{s}=\boldsymbol{v}\wedge\boldsymbol{e}=\boldsymbol{w}-F\cdot\boldsymbol{v}]\\&=\frac{1}{\rho_{\sigma_1}(\mathbb{Z}^{\tilde{n}})\cdot\rho_{\sigma_2}(\mathbb{Z}^{\tilde{m}})}\cdot\mathrm{e}^{-\pi\left(\frac{1}{\sigma_1^2}\cdot\boldsymbol{v}^{\mathrm{T}}\cdot\boldsymbol{v}+\frac{1}{\sigma_2^2}\cdot(\boldsymbol{w}-F\cdot\boldsymbol{v})^{\mathrm{T}}\cdot(\boldsymbol{w}-F\cdot\boldsymbol{v})\right)}=\frac{1}{\rho_{\sigma_1}(\mathbb{Z}^{\tilde{n}})\cdot\rho_{\sigma_2}(\mathbb{Z}^{\tilde{m}})}\cdot\mathrm{e}^{-\pi\left((\boldsymbol{v}-\boldsymbol{c})^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot(\boldsymbol{v}-\boldsymbol{c})-\boldsymbol{c}^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot\boldsymbol{c}+\frac{1}{\sigma_2^2}\boldsymbol{w}^{\mathrm{T}}\cdot\boldsymbol{w}\right)}.\end{aligned}$$

这里, 我们用到了条件 $\Sigma_0^{-1}=\Sigma_0^{-\mathrm{T}}$. 注意到:

$$\Pr[\boldsymbol{y}=\boldsymbol{w}]=\Pr[\boldsymbol{z}=\boldsymbol{w}]=\sum_{\boldsymbol{a}\in\mathbb{Z}^{\tilde{n}}}\Pr[\boldsymbol{s}=\boldsymbol{a}]\cdot\Pr[\boldsymbol{e}=\boldsymbol{w}-F\cdot\boldsymbol{s}|\boldsymbol{s}=\boldsymbol{a}]=\frac{1}{\rho_{\sigma_1}(\mathbb{Z}^{\tilde{n}})\cdot\rho_{\sigma_2}(\mathbb{Z}^{\tilde{m}})}\cdot\sum_{\boldsymbol{a}\in\mathbb{Z}^{\tilde{n}}}\mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{a}\|^2}{\sigma_1^2}}\cdot\mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{w}-F\cdot\boldsymbol{a}\|^2}{\sigma_2^2}},$$

我们可以得到:

$$\Pr[\boldsymbol{x}=\boldsymbol{v}|\boldsymbol{y}=\boldsymbol{w}]=\Pr[\boldsymbol{s}=\boldsymbol{v}|\boldsymbol{z}=\boldsymbol{w}]=\frac{\Pr[\boldsymbol{s}=\boldsymbol{v}\wedge\boldsymbol{z}=\boldsymbol{w}]}{\Pr[\boldsymbol{z}=\boldsymbol{w}]}=\frac{\mathrm{e}^{-\pi\left(-\boldsymbol{c}^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot\boldsymbol{c}+\frac{1}{\sigma_2^2}\boldsymbol{w}^{\mathrm{T}}\cdot\boldsymbol{w}\right)}}{\sum_{\boldsymbol{a}\in\mathbb{Z}^{\tilde{n}}}\mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{a}\|^2}{\sigma_1^2}}\cdot\mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{w}-F\cdot\boldsymbol{a}\|^2}{\sigma_2^2}}}\cdot\mathrm{e}^{-\pi\cdot(\boldsymbol{v}-\boldsymbol{c})^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot(\boldsymbol{v}-\boldsymbol{c})}.$$

因为公式 $\dfrac{\mathrm{e}^{-\pi\left(-\boldsymbol{c}^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot\boldsymbol{c}+\frac{1}{\sigma_2^2}\boldsymbol{w}^{\mathrm{T}}\cdot\boldsymbol{w}\right)}}{\sum_{\boldsymbol{a}\in\mathbb{Z}^{\tilde{n}}}\mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{a}\|^2}{\sigma_1^2}}\cdot\mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{w}-F\cdot\boldsymbol{a}\|^2}{\sigma_2^2}}}$ 与 $\boldsymbol{v}$ 无关, 且有概率等式 $\sum_{\boldsymbol{v}\in\mathbb{Z}^{\tilde{n}}}\Pr[\boldsymbol{s}=\boldsymbol{v}|\boldsymbol{z}=\boldsymbol{w}]=1$ 成立, 所以我们有:

$$\frac{\mathrm{e}^{-\pi\left(-\boldsymbol{c}^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot\boldsymbol{c}+\frac{1}{\sigma_2^2}\boldsymbol{w}^{\mathrm{T}}\cdot\boldsymbol{w}\right)}}{\sum_{\boldsymbol{a}\in\mathbb{Z}^{\tilde{n}}}\mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{a}\|^2}{\sigma_1^2}}\cdot\mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{w}-F\cdot\boldsymbol{a}\|^2}{\sigma_2^2}}}=\left(\sum_{\boldsymbol{v}\in\mathbb{Z}^{\tilde{n}}}\mathrm{e}^{-\pi\cdot(\boldsymbol{v}-\boldsymbol{c})^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot(\boldsymbol{v}-\boldsymbol{c})}\right)^{-1}=\frac{1}{\rho_{\sqrt{\Sigma_0},\boldsymbol{c}}(\mathbb{Z}^{\tilde{n}})}.$$

因此,

$$\Pr[\boldsymbol{s}=\boldsymbol{v}|\boldsymbol{z}=\boldsymbol{w}]=\frac{1}{\rho_{\sqrt{\Sigma_0},\boldsymbol{c}}(\mathbb{Z}^{\tilde{n}})}\cdot\mathrm{e}^{-\pi\cdot(\boldsymbol{v}-\boldsymbol{c})^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot(\boldsymbol{v}-\boldsymbol{c})}.$$

也就是说, 在已知 $\boldsymbol{z}=F\cdot\boldsymbol{s}+\boldsymbol{e}=\boldsymbol{w}$ 的情况下, $\boldsymbol{s}$ 服从的条件分布为 $D_{\mathbb{Z}^{\tilde{n}},\sqrt{\Sigma_0},\boldsymbol{c}}$. 证毕.

3.1 半均匀 LWE 问题的归约

本文的主要定理如下.

定理 1. 假设 $\varepsilon=negl(\lambda)$ 为某可忽略的函数, m,q,d 为正整数, $\mathcal{D}$ 为 $\mathfrak{R}_q^{m\times d}$ 上的 η-半均匀分布, 正实数 $\sigma_1,\sigma_2,\sigma_3,\sigma_4,\gamma\geqslant\omega\left(\max\left\{\sqrt{\log m\cdot n},\sqrt{\log d\cdot n}\right\}\right)$ 且满足条件 $\dfrac{\gamma\cdot\sigma_3}{\sqrt{\gamma^2+\sigma_3^2}}\geqslant\eta_\varepsilon(\mathfrak{R}^m)$, $\sigma_1=\sqrt{\gamma^2+\sigma_3^2}$, $\dfrac{1}{\sigma_2^2}+\dfrac{\eta^2}{\gamma^2}<\dfrac{1}{2\cdot\sigma_4^2}$. 记 $\chi_1=D_{\mathfrak{R}^m,\sigma_1}$, $\chi_2=D_{\mathfrak{R}^d,\sigma_2}$, $\chi_3=D_{\mathfrak{R}^m,\sigma_3}$, $\chi_4=D_{\mathfrak{R}^d,\sigma_4}$. 如果存在一个 (量子) 概率多项式时间的敌手 $\mathfrak{A}$ 可以以 δ 的概率解决 $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}(\chi_2;\mathcal{D})$ 问题, 则存在一个 (量子) 概率多项式时间的敌手 $\mathfrak{B}$ 可以以 $\delta-negl(\lambda)$ 的概率解决 $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_3}(\chi_4;\mathrm{U}\left(\mathfrak{R}_q^{m\times d}\right))$ 问题.

证明: 根据假设, $\mathcal{D}$ 为 $\mathfrak{R}_q^{m\times d}$ 上的 η-半均匀分布. 由定义 1, 存在 $\mathfrak{R}^{m\times d}$ 上的一族可以有效取样的概率分布 $\{\phi_U\}_{U\in\mathfrak{R}^{m\times d}}$ 使得对任意随机取样的 $A\hookleftarrow\mathcal{D}$, $U\hookleftarrow\mathrm{U}\left(\mathfrak{R}_q^{m\times d}\right)$ 和 $E_U\hookleftarrow\phi_U$, 随机变量 A 与 $U+E_U \bmod q\cdot\mathfrak{R}$ 统计不可区分. 同时, 有 $\Pr_{U\hookleftarrow\mathrm{U}(\mathfrak{R}_q^{m\times d}),E_U\hookleftarrow\phi_U}[\mathfrak{s}_1(\sigma_{\mathrm{coef}}(E_U))\leqslant\eta]\geqslant 1-negl(\lambda)$ 成立.

对任意 (量子) 概率多项式时间的敌手 $\mathfrak{A}$, 我们定义一系列区分游戏 Game_i, 并定义 $p_i:=\Pr_{\mathrm{Game}_i}[\mathfrak{A}(A,\boldsymbol{b})=1]$. 这里, $i\in[6]$, $(A,\boldsymbol{b})\in\mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$.

- Game_1: 取样 $A\hookleftarrow\mathcal{D}$, $\boldsymbol{s}\hookleftarrow\chi_2$, $\boldsymbol{e}\hookleftarrow\chi_1$; 计算 $\boldsymbol{b}=A\cdot\boldsymbol{s}+\boldsymbol{e} \bmod q\cdot\mathfrak{R}$; 最后输出 $(A,\boldsymbol{b})\in\mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ 给 $\mathfrak{A}$.

注意到 Game_1 中输出的样本 $(A,\boldsymbol{b})$ 即为 $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}(\chi_2;\mathcal{D})$ 问题的原始分布.

- Game_2: 取样 $U\hookleftarrow\mathrm{U}\left(\mathfrak{R}_q^{m\times d}\right)$, $E_U\hookleftarrow\phi_U$, $\boldsymbol{s}\hookleftarrow\chi_2$, $\boldsymbol{e}\hookleftarrow\chi_1$; 如果 $\mathfrak{s}_1(\sigma_{\mathrm{coef}}(E_U))>\eta$, 则输出 $\perp$ (代表采样出错, 游

© 中国科学院软件研究所 http://www.jos.org.cn

戏终止); 否则, 计算 $A = U + E_U \bmod q\cdot\mathfrak{R}$, $\boldsymbol{b} = A\cdot\boldsymbol{s}+\boldsymbol{e} \bmod q\cdot\mathfrak{R}$; 最后输出 $(A,\boldsymbol{b})\in\mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ 给 $\mathfrak{A}$.

根据定义 1, 在 Game_2 中输出 $\perp$ 的概率是可忽略的. 当 Game_2 正常输出 $(A,\boldsymbol{b})$ 时, Game_2 中输出的 A 与 Game_1 中输出的 A 统计不可区分. 因此, 我们有 $|p_1-p_2|\leqslant negl(\lambda)$.

- Game_3: 取样 $U\hookleftarrow \mathrm{U}\left(\mathfrak{R}_q^{m\times d}\right)$, $E_U\hookleftarrow\phi_U$, $\boldsymbol{s}\hookleftarrow\chi_2$; 如果 $\mathfrak{s}_1(\sigma_{\mathrm{coef}}(E_U))>\eta$, 则输出 $\perp$; 否则继续取样 $\boldsymbol{e}_1\hookleftarrow D_{\mathfrak{R}^m,\gamma}$, $\boldsymbol{e}_2\hookleftarrow D_{\mathfrak{R}^m,\sigma_3}$; 再计算 $\boldsymbol{z}=E_U\cdot\boldsymbol{s}+\boldsymbol{e}_1$, $A=U+E_U \bmod q\cdot\mathfrak{R}$, $\boldsymbol{b}=U\cdot\boldsymbol{s}+\boldsymbol{z}+\boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}$; 最后输出 $(A,\boldsymbol{b})\in\mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ 给 $\mathfrak{A}$.

下面当 $\mathfrak{R}=\mathbb{Z}$ 时取 $N=m$, $\tilde{N}=d$; 而当 $\mathfrak{R}=\mathcal{R}$ 时取 $N=m\cdot n$, $\tilde{N}=n\cdot d$. 如果令 $\Sigma_1:=\gamma^2\cdot I_N$, $\Sigma_2:=\sigma_3^2\cdot I_N$ 并取 $\Sigma_3:=\dfrac{\gamma^2\cdot\sigma_3^2}{\gamma^2+\sigma_3^2}\cdot I_N$, 则根据假设 $\dfrac{\gamma\cdot\sigma_3}{\sqrt{\gamma^2+\sigma_3^2}}\geqslant\eta_\varepsilon(\mathfrak{R}^m)=\eta_\varepsilon(\mathbb{Z}^N)$ 以及引理 2 可知, 概率分布 $D_{\mathfrak{R}^m,\gamma}+D_{\mathfrak{R}^m,\sigma_3}$ 与概率分布 $D_{\mathfrak{R}^m,\sqrt{\gamma^2+\sigma_3^2}}=\chi_1$ 的统计距离不超过 $2\cdot\varepsilon$. 在 Game_3 中, 我们有:

$$\boldsymbol{b}=U\cdot\boldsymbol{s}+\boldsymbol{z}+\boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}=U\cdot\boldsymbol{s}+E_U\cdot\boldsymbol{s}+\boldsymbol{e}_1+\boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}=(U+E_U)\cdot\boldsymbol{s}+(\boldsymbol{e}_1+\boldsymbol{e}_2) \bmod q\cdot\mathfrak{R}=A\cdot\boldsymbol{s}+(\boldsymbol{e}_1+\boldsymbol{e}_2) \bmod q\cdot\mathfrak{R}.$$

所以, 根据上述分析, 我们可以得到 $|p_2-p_3|\leqslant negl(\lambda)$.

- Game_4: 取样 $U\hookleftarrow \mathrm{U}\left(\mathfrak{R}_q^{m\times d}\right)$, $E_U\hookleftarrow\phi_U$, $\boldsymbol{s}\hookleftarrow\chi_2$; 如果 $\mathfrak{s}_1(\sigma_{\mathrm{coef}}(E_U))>\eta$, 则输出 $\perp$; 否则继续取样 $\boldsymbol{e}_1\hookleftarrow D_{\mathfrak{R}^m,\gamma}$, $\boldsymbol{e}_2\hookleftarrow D_{\mathfrak{R}^m,\sigma_3}$; 再计算 $A=U+E_U \bmod q\cdot\mathfrak{R}$, $\boldsymbol{z}=E_U\cdot\boldsymbol{s}+\boldsymbol{e}_1$, 并取 $\Sigma_0:=\left(\dfrac{1}{\sigma_2^2}\cdot I_{\tilde{N}}+\dfrac{1}{\gamma^2}\cdot\sigma_{\mathrm{coef}}(E_U)^{\mathrm{T}}\cdot\sigma_{\mathrm{coef}}(E_U)\right)^{-1}$, $\boldsymbol{c}=\dfrac{1}{\gamma^2}\cdot\Sigma_0\cdot\sigma_{\mathrm{coef}}(E_U)^{\mathrm{T}}\cdot\boldsymbol{z}$; 随后取样 $\tilde{\boldsymbol{s}}\hookleftarrow D_{\mathfrak{R}^d,\sqrt{\Sigma_0},\boldsymbol{c}}$, 并利用二元组 $(\tilde{\boldsymbol{s}},\boldsymbol{z})$ 来计算 $\boldsymbol{b}=U\cdot\tilde{\boldsymbol{s}}+\boldsymbol{z}+\boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}$; 最后输出 $(A,\boldsymbol{b})\in\mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ 给 $\mathfrak{A}$.

我们先来分析 Game_4 中所需要的分布是否可以有效地取样. 注意到 $\Sigma_0^{-1}=\dfrac{1}{\sigma_2^2}\cdot I_{\tilde{N}}+\dfrac{1}{\gamma^2}\cdot\sigma_{\mathrm{coef}}(E_U)^{\mathrm{T}}\cdot\sigma_{\mathrm{coef}}(E_U)$, 根据参数选择, 我们有 $\mathfrak{s}_1(\Sigma_0^{-1})\leqslant\dfrac{1}{\sigma_2^2}+\dfrac{\eta^2}{\gamma^2}<\dfrac{1}{2\cdot\sigma_4^2}$. 所以, 可以得到 $\mathfrak{s}_{\tilde{N}}(\Sigma_0)>2\cdot\sigma_4^2$, 进而有 $\Sigma_0>\sigma_4^2\cdot I_{\tilde{N}}$ 成立. 由引理 1 以及我们选择的参数条件 $\sigma_4\geqslant\omega\left(\sqrt{\log n\cdot d}\right)$ 可知, 可以有效地从一个与 $D_{\mathfrak{R}^d,\sqrt{\Sigma_0},\boldsymbol{c}}$ 统计不可区分的分布中采样 $\tilde{\boldsymbol{s}}$. 当所有的分布均可以有效采样时, Game_3 与 Game_4 的区别仅仅在于用于计算 $\boldsymbol{b}$ 的 $(\boldsymbol{s},\boldsymbol{z})$ 与 $(\tilde{\boldsymbol{s}},\boldsymbol{z})$ 的不同. 根据引理 3, 在我们的参数选择下, $(\boldsymbol{s},\boldsymbol{z})$ 与 $(\tilde{\boldsymbol{s}},\boldsymbol{z})$ 的分布统计不可区分. 因此, 我们有 $|p_3-p_4|\leqslant negl(\lambda)$.

- Game_5: 取样 $U\hookleftarrow \mathrm{U}\left(\mathfrak{R}_q^{m\times d}\right)$, $E_U\hookleftarrow\phi_U$, $\boldsymbol{s}\hookleftarrow\chi_2$; 如果 $\mathfrak{s}_1(\sigma_{\mathrm{coef}}(E_U))>\eta$, 则输出 $\perp$; 否则继续取样 $\boldsymbol{e}_1\hookleftarrow D_{\mathfrak{R}^m,\gamma}$, $\boldsymbol{e}_2\hookleftarrow D_{\mathfrak{R}^m,\sigma_3}$; 再计算 $A=U+E_U \bmod q\cdot\mathfrak{R}$, $\boldsymbol{z}=E_U\cdot\boldsymbol{s}+\boldsymbol{e}_1$, 并取 $\Sigma_0:=\left(\dfrac{1}{\sigma_2^2}\cdot I_{\tilde{N}}+\dfrac{1}{\gamma^2}\cdot\sigma_{\mathrm{coef}}(E_U)^{\mathrm{T}}\cdot\sigma_{\mathrm{coef}}(E_U)\right)^{-1}$, $\boldsymbol{c}=\dfrac{1}{\gamma^2}\cdot\Sigma_0\cdot\sigma_{\mathrm{coef}}(E_U)^{\mathrm{T}}\cdot\boldsymbol{z}$; 随后取样 $\boldsymbol{s}_1\hookleftarrow D_{\mathfrak{R}^d,\sqrt{\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}}},\boldsymbol{c}}$ 和 $\boldsymbol{s}_2\hookleftarrow D_{\mathfrak{R}^d,\sigma_4}$ 并计算 $\tilde{\boldsymbol{s}}=\boldsymbol{s}_1+\boldsymbol{s}_2 \bmod q\cdot\mathfrak{R}$; 再利用二元组 $(\tilde{\boldsymbol{s}},\boldsymbol{z})$ 来计算 $\boldsymbol{b}=U\cdot\tilde{\boldsymbol{s}}+\boldsymbol{z}+\boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}$; 最后输出 $(A,\boldsymbol{b})\in\mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ 给 $\mathfrak{A}$.

我们已经知道 $\mathfrak{s}_{\tilde{N}}(\Sigma_0)>2\cdot\sigma_4^2$, 所以 $\mathfrak{s}_{\tilde{N}}(\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}})>\sigma_4^2$. 根据引理 1 和我们的参数选择, 可以有效地从一个与 $D_{\mathfrak{R}^d,\sqrt{\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}}},\boldsymbol{c}}$ 统计接近的分布进行采样. 如果现在取 $\Sigma_1^{-1}=\dfrac{1}{\sigma_4^2}\cdot I_{\tilde{N}}$, $\Sigma_2^{-1}=(\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}})^{-1}$ 并令 $\Sigma_3^{-1}=\Sigma_1^{-1}+\Sigma_2^{-1}$, 简单计算即知 $\mathfrak{s}_1(\Sigma_3^{-1})\leqslant\dfrac{1}{\sigma_4^2}+\mathfrak{s}_1(\Sigma_2^{-1})<\dfrac{2}{\sigma_4^2}\leqslant(\eta_\varepsilon(\mathfrak{R}^d))^{-2}$ 成立. 由引理 1 可知, $\sqrt{\Sigma_3}\geqslant\eta_\varepsilon(\mathfrak{R}^d)$. 进而根据引理 2, 分布 $D_{\mathfrak{R}^d,\sqrt{\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}}},\boldsymbol{c}}+D_{\mathfrak{R}^d,\sigma_4}$ 与分布 $D_{\mathfrak{R}^d,\sqrt{\Sigma_0},\boldsymbol{c}}$ 的统计距离不超过 $2\cdot\varepsilon$, 即 Game_4 和 Game_5 中对应的 $\tilde{\boldsymbol{s}}$ 的分布统计不可区分. 所以, 我们可以得到 $|p_4-p_5|\leqslant negl(\lambda)$.

- Game_6: 取样 $U\hookleftarrow \mathrm{U}\left(\mathfrak{R}_q^{m\times d}\right)$, $E_U\hookleftarrow\phi_U$, $\boldsymbol{s}\hookleftarrow\chi_2$ 和 $\boldsymbol{e}_1\hookleftarrow D_{\mathfrak{R}^m,\gamma}$; 如果 $\mathfrak{s}_1(\sigma_{\mathrm{coef}}(E_U))>\eta$, 则输出 $\perp$; 否则计算 $A=U+E_U \bmod q\cdot\mathfrak{R}$ 和 $\boldsymbol{z}=E_U\cdot\boldsymbol{s}+\boldsymbol{e}_1$; 令 $\Sigma_0:=\left(\dfrac{1}{\sigma_2^2}\cdot I_{\tilde{N}}+\dfrac{1}{\gamma^2}\cdot\sigma_{\mathrm{coef}}(E_U)^{\mathrm{T}}\cdot\sigma_{\mathrm{coef}}(E_U)\right)^{-1}$, $\boldsymbol{c}=\dfrac{1}{\gamma^2}\cdot\Sigma_0\cdot\sigma_{\mathrm{coef}}(E_U)^{\mathrm{T}}\cdot\boldsymbol{z}$; 随后取样 $\boldsymbol{s}_1\hookleftarrow D_{\mathfrak{R}^d,\sqrt{\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}}},\boldsymbol{c}}$ 和 $\boldsymbol{u}\hookleftarrow \mathrm{U}\left(\mathfrak{R}_q^m\right)$; 计算 $\boldsymbol{b}=U\cdot\boldsymbol{s}_1+\boldsymbol{z}+\boldsymbol{u} \bmod q\cdot\mathfrak{R}$; 最后输出 $(A,\boldsymbol{b})\in\mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ 给 $\mathfrak{A}$.

在 Game_6 中, 由于 $\boldsymbol{u}$ 是独立随机地取自分布 $\mathrm{U}\left(\mathfrak{R}_q^m\right)$, 因此有 $\boldsymbol{b}\hookleftarrow \mathrm{U}\left(\mathfrak{R}_q^m\right)$ 成立. 根据 η-半均匀分布, A 服从的分布与 $\mathcal{D}$ 统计不可区分. 根据假设, $\mathfrak{A}$ 可以以 δ 的概率解决 $\mathrm{DLWE}_{\mathfrak{R},m,q,\chi_1}^d(\chi_2;\mathcal{D})$ 问题. 所以我们可以得到 $|p_1-p_6|\geqslant\delta-negl(\lambda)$. 综合 $\mathrm{Game}_1-\mathrm{Game}_5$ 的分析, 我们有 $|p_5-p_6|\geqslant\delta-negl(\lambda)$.

注意到在 Game_5 中,

$$\boldsymbol{b}=U\cdot\tilde{\boldsymbol{s}}+\boldsymbol{z}+\boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}=U\cdot\boldsymbol{s}_1+\boldsymbol{z}+U\cdot\boldsymbol{s}_2+\boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}.$$

© 中国科学院软件研究所 http://www.jos.org.cn

现在, 我们可以利用敌手 $\mathfrak{A}$ 的能力来构造敌手 $\mathfrak{B}$ 以解决 $\mathrm{DLWE}^{d}_{\mathfrak{R},m,q,\chi_3}(\chi_4;\mathrm{U}(\mathfrak{R}_q^{m\times d}))$ 问题. 假设敌手 $\mathfrak{B}$ 获得的样本为 $(U,\tilde{\boldsymbol{b}})$, 其中 $U\hookleftarrow \mathrm{U}(\mathfrak{R}_q^{m\times d})$, $\boldsymbol{s}_2\hookleftarrow D_{\mathfrak{R}^d,\sigma_4}$, $\boldsymbol{e}_2\hookleftarrow D_{\mathfrak{R}^m,\sigma_3}$, $\tilde{\boldsymbol{b}}=U\cdot\boldsymbol{s}_2+\boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}$ 或者 $U\hookleftarrow \mathrm{U}(\mathfrak{R}_q^{m\times d})$, $\tilde{\boldsymbol{b}}\hookleftarrow \mathrm{U}(\mathfrak{R}_q^{m})$. 则 $\mathfrak{B}$ 进行如下操作.

(1) 取样 $E_U\hookleftarrow\phi_U$, $\boldsymbol{s}\hookleftarrow\chi_2$; 如果 $\mathfrak{s}_1(\sigma_{\mathrm{coef}}(E_U))>\eta$, 则输出 $\perp$; 否则继续取样 $\boldsymbol{e}_1\hookleftarrow D_{\mathfrak{R}^m,\gamma}$.

(2) 计算 $A=U+E_U \bmod q\cdot\mathfrak{R}$ 和 $\boldsymbol{z}=E_U\cdot\boldsymbol{s}+\boldsymbol{e}_1$, 随后取 $\Sigma_0:=\left(\frac{1}{\sigma_2^2}\cdot I_{\tilde{N}}+\frac{1}{\gamma^2}\cdot\sigma_{\mathrm{coef}}(E_U)^{\mathrm{T}}\cdot\sigma_{\mathrm{coef}}(E_U)\right)^{-1}$, $\boldsymbol{c}=\frac{1}{\gamma^2}\cdot\Sigma_0\cdot\sigma_{\mathrm{coef}}(E_U)^{\mathrm{T}}\cdot\boldsymbol{z}$.

(3) 取样 $\boldsymbol{s}_1\hookleftarrow D_{\mathfrak{R}^d,\sqrt{\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}}},\boldsymbol{c}}$, 随后计算 $\boldsymbol{b}=U\cdot\boldsymbol{s}_1+\boldsymbol{z}+\tilde{\boldsymbol{b}} \bmod q\cdot\mathfrak{R}$.

(4) 输出 $(A,\boldsymbol{b})\in\mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^{m}$ 给 $\mathfrak{A}$.

最后 $\mathfrak{B}$ 输出 $\mathfrak{A}$ 的输出即可.

显然, 根据我们的参数选择, 上述 $\mathfrak{B}$ 的操作可以在概率多项式时间内完成. 下面来分析所构造的敌手 $\mathfrak{B}$ 可以成功解决 $\mathrm{DLWE}^{d}_{\mathfrak{R},m,q,\chi_3}(\chi_4;\mathrm{U}(\mathfrak{R}_q^{m\times d}))$ 问题的概率. 易知, 当 $(U,\tilde{\boldsymbol{b}})$ 来自均匀分布时, $\mathfrak{B}$ 给 $\mathfrak{A}$ 的样本 $(A,\boldsymbol{b})$ 所服从的分布与 Game_6 的输出所服从的分布相同. 否则, $\mathfrak{B}$ 给 $\mathfrak{A}$ 的样本 $(A,\boldsymbol{b})$ 所服从的分布与 Game_5 的输出所服从的分布相同. 因此,

$$\mathrm{Adv}_{\mathfrak{B}}\left(\mathrm{DLWE}^{d}_{\mathfrak{R},m,q,\chi_3}(\chi_4;\mathrm{U}(\mathfrak{R}_q^{m\times d}))\right)=|p_5-p_6|\geqslant\delta-negl(\lambda).$$

证毕.

注意到定理 1 中的条件 $\sigma_1,\sigma_2,\sigma_3,\sigma_4,\gamma\geqslant\omega\left(\max\left\{\sqrt{\log m\cdot n},\sqrt{\log d\cdot n}\right\}\right)$ 是为了对 $\mathfrak{R}$ 进行统一分析. 当 $\mathfrak{R}=\mathbb{Z}$ 时, 相应的条件可以改为 $\sigma_1,\sigma_2,\sigma_3,\sigma_4,\gamma\geqslant\omega\left(\max\left\{\sqrt{\log m},\sqrt{\log d}\right\}\right)$. 我们对定理 1 中所选择的参数条件进行一些简单的说明. 条件 $\frac{\gamma\cdot\sigma_3}{\sqrt{\gamma^2+\sigma_3^2}}\geqslant\eta_\varepsilon(\mathfrak{R}^m)$ 和 $\sigma_1=\sqrt{\gamma^2+\sigma_3^2}$ 是为了保证从 Game_2 到 Game_3 的过程中, 我们可以对 Game_2 中的原始误差 $\boldsymbol{e}$ 进行拆分; 条件 $\frac{1}{\sigma_2^2}+\frac{\eta^2}{\gamma^2}<\frac{1}{2\cdot\sigma_4^2}$ 是为了保证我们可以应用关键引理 3; 本质上讲, 条件 $\sigma_1,\sigma_2,\sigma_3,\sigma_4,\gamma\geqslant\omega\left(\max\left\{\sqrt{\log m\cdot n},\sqrt{\log d\cdot n}\right\}\right)$ 保证了证明过程中对应的离散高斯分布均可以有效地取样. 同时, 此条件连同条件 $\frac{1}{\sigma_2^2}+\frac{\eta^2}{\gamma^2}<\frac{1}{2\cdot\sigma_4^2}$ 也保证了从 Game_4 到 Game_5 的过渡中可以对 Game_4 中的原始误差 $\boldsymbol{s}$ 进行拆分. 最后得到的 Game_5 (以及 Game_6) 即为所期望的分布形式, 非常便于我们来构造概率多项式时间的算法 (归约) 来嵌入 $\mathrm{DLWE}^{d}_{\mathfrak{R},m,q,\chi_3}(\chi_4;\mathrm{U}(\mathfrak{R}_q^{m\times d}))$ 问题的实例.

3.2 与已知结果的对比分析

利用定理 1, 可以得到半均匀的 (欧氏格/环/模) LWE 问题的困难性结果. 在本节中, 对任意的整数 $x\in\mathbb{Z}$, 使用符号 $\lfloor x\rceil$ 来表示不超过 x 的最大整数, 并定义 $\lfloor x\rceil:=\left\lfloor x+\frac{1}{2}\right\rfloor$. 相应的取整符号可以平凡的推广到向量 (多项式) 或者矩阵上.

当 $\mathfrak{R}=\mathbb{Z}$ 时, 可以得到 d 维欧氏格对应的半均匀 LWE 问题的困难性归约.

推论 1. 假设 $\varepsilon=negl(\lambda)$ 为某可忽略的函数, m,q,d 为正整数, $\mathcal{D}$ 为 $\mathbb{Z}_q^{m\times d}$ 上的 η-半均匀分布, 正实数 $\sigma_1,\sigma_2,\sigma_3,\sigma_4,\gamma\geqslant\sqrt{2}\cdot\omega\left(\max\left\{\sqrt{\log m},\sqrt{\log d}\right\}\right)$ 且满足条件 $\frac{\gamma\cdot\sigma_3}{\sqrt{\gamma^2+\sigma_3^2}}\geqslant\eta_\varepsilon(\mathbb{Z}^m)$, $\sigma_1=\sqrt{\gamma^2+\sigma_3^2}$, $\frac{1}{\sigma_2^2}+\frac{\eta^2}{\gamma^2}<\frac{1}{2\cdot\sigma_4^2}$. 记 $\chi_1=D_{\mathbb{Z}^m,\sigma_1}$, $\chi_2=D_{\mathbb{Z}^d,\sigma_2}$, $\chi_3=D_{\mathbb{Z}^m,\sigma_3}$, $\chi_4=D_{\mathbb{Z}^d,\sigma_4}$. 如果存在一个 (量子) 概率多项式时间的敌手 $\mathfrak{A}$ 可以以 δ 的概率解决 $\mathrm{DLWE}^{d}_{\mathbb{Z},m,q,\chi_1}(\chi_2;\mathcal{D})$ 问题, 则存在一个 (量子) 概率多项式时间的敌手 $\mathfrak{B}$ 可以以 $\delta-negl(\lambda)$ 的概率解决 $\mathrm{DLWE}^{d}_{\mathbb{Z},m,q,\chi_3}(\chi_4;\mathrm{U}(\mathbb{Z}_q^{m\times d}))$ 问题.

如果选择 $\sigma_2=2\sqrt{2}\cdot\sigma_4$, $\gamma=2\sqrt{2}\cdot\sigma_4\cdot\eta$, 则 $\frac{1}{\sigma_2^2}+\frac{\eta^2}{\gamma^2}=\frac{1}{4\cdot\sigma_4^2}<\frac{1}{2\cdot\sigma_4^2}$. 由引理 1, $\eta_\varepsilon(\mathbb{Z}^m)\leqslant\omega\left(\sqrt{\log m}\right)$. 而 $\frac{\gamma\cdot\sigma_3}{\sqrt{\gamma^2+\sigma_3^2}}=\frac{\gamma}{\sqrt{1+\left(\frac{\gamma}{\sigma_3}\right)^2}}=\frac{\sigma_3}{\sqrt{1+\left(\frac{\sigma_3}{\gamma}\right)^2}}$, 所以在上述参数设置下, 当 $\sigma_3,\gamma\geqslant\sqrt{2}\cdot\omega\left(\sqrt{\log m}\right)$ 时, 不等式 $\frac{\gamma\cdot\sigma_3}{\sqrt{\gamma^2+\sigma_3^2}}\geqslant$

© 中国科学院软件研究所 http://www.jos.org.cn

$\eta_\varepsilon(\mathbb{Z}^m)$ 恒成立.

注意到 $\sigma_1=\sqrt{\gamma^2+\sigma_3^2}$, 因此当选取参数 $\sigma_3=\sigma_4=:\sigma$ 时, 可以将标准 (即秘密与误差服从相同参数的离散高斯分布) 的 $\mathrm{DLWE}^d_{\mathbb{Z},m,q,D_{\mathbb{Z}^m,\sigma}}\left(D_{\mathbb{Z}^d,\sigma};\mathrm{U}\left(\mathbb{Z}_q^{m\times d}\right)\right)$ 问题归约到公开矩阵服从任意 η-半均匀分布 $\mathcal{D}$ 的半均匀 $\mathrm{DLWE}^d_{\mathbb{Z},m,q,\chi_1}(\chi_2;\mathcal{D})$ 问题. 其中, $\chi_1=D_{\mathbb{Z}^m,\sigma_1}$, $\sigma_1=\mathrm{O}(\eta\cdot\sigma)$; $\chi_2=D_{\mathbb{Z}^d,\sigma_2}$, $\sigma_2=\mathrm{O}(\sigma)$.

值得指出的是, 在不计多项式规模样本数的情况下, 误差 $\boldsymbol{e}$ 所服从的高斯分布的参数大小决定了对应 LWE 问题的困难程度 (例如, 采用文献 [36] 的方法可以将秘密取自均匀分布的 LWE 问题归约到秘密取自与误差相同参数的离散高斯分布的 LWE 问题, 即所谓的标准形式 (normal form) 的 LWE 问题; 而秘密取自均匀分布的 LWE 问题是同等条件下最难的一类问题). 因此, 我们在这里仅举例说明 $\sigma_3=\sigma_4$ 的情形.

与文献 [4] 的归约结果相比, 本文的归约结果是保持格的维数 d 的, 但是文献 [4] 中的归约结果需要依赖于相应的低维 LWE 问题的困难性. 同时, 在我们的归约结果中, 在渐进意义下两个问题的误差参数大小的归约损失为 η, 与样本数目无关. 但是文献 [4] 中的归约结果在渐进意义下两个问题的误差参数大小的归约损失与样本数相关 (约为 $\sigma_1=\tilde{\mathrm{O}}\left(\sqrt{m}\cdot\sigma+\eta\right)$). 不过值得注意的是, 本文的归约结果仅仅局限于秘密/误差服从离散高斯分布的情形, 且仅适用于判定版本 LWE 问题的归约. 而文献 [4] 的归约同时适用于求解和判定版本问题的归约, 但是对于判定版本的对应问题, 需要额外限制 q 为素数或者要求秘密 $\boldsymbol{s}$ 取自 $\{0,1\}$ 上的、特定条件下熵足够大的二元分布.

假设 $0<p\leqslant q$ 为正整数, 对任意的矩阵 $U\in\mathbb{Z}_q^{m\times d}$, 可以定义固定函数 $E_U=\left\lfloor\frac{q}{p}\cdot\left\lfloor\frac{p}{q}\cdot U\right\rceil\right\rceil-U$. 对任意的 $x\in\mathbb{Z}_q$, 简单计算知 $\left\|x-\left\lfloor\frac{q}{p}\cdot\left\lfloor\frac{p}{q}\cdot x\right\rceil\right\rceil\right\|\leqslant\left\lfloor\frac{q}{2p}\right\rceil$. 因此, 我们有 $\mathfrak{s}_1(E_U)\leqslant\sqrt{m\cdot d}\cdot\left\lfloor\frac{q}{2p}\right\rceil$. 定义分布 $\mathcal{D}_{p,q,m,d}$ 为: 取样 $U\in\mathbb{Z}_q^{m\times d}$, 输出 $\left\lfloor\frac{q}{p}\cdot\left\lfloor\frac{p}{q}\cdot U\right\rceil\right\rceil$, 则 $\mathcal{D}_{p,q,m,d}$ 为特殊的 $\sqrt{m\cdot d}\cdot\left\lfloor\frac{q}{2p}\right\rceil$-半均匀分布. 上述讨论的结论可以自然地应用到 $\mathcal{D}_{p,q,m,d}$ 对应的半均匀 LWE 问题.

当 $\mathfrak{R}=\mathcal{R}$ 时, 可以得到对应的判定版本的环/模半均匀 LWE 问题的困难性归约.

推论 2. 假设 $\varepsilon=negl(\lambda)$ 为某可忽略的函数, m, q, d 为正整数, $\mathcal{D}$ 为 $\mathcal{R}_q^{m\times d}$ 上的 η-半均匀分布, 正实数 σ_1, σ_2, σ_3, σ_4, $\gamma\geqslant\sqrt{2}\cdot\omega\left(\max\left\{\sqrt{\log m\cdot n},\sqrt{\log d\cdot n}\right\}\right)$ 且满足条件 $\frac{\gamma\cdot\sigma_3}{\sqrt{\gamma^2+\sigma_3^2}}\geqslant\eta_\varepsilon(\mathcal{R}^m)$, $\sigma_1=\sqrt{\gamma^2+\sigma_3^2}$, $\frac{1}{\sigma_2^2}+\frac{\eta^2}{\gamma^2}<\frac{1}{2\cdot\sigma_4^2}$. 记 $\chi_1=D_{\mathcal{R}^m,\sigma_1}$, $\chi_2=D_{\mathcal{R}^d,\sigma_2}$, $\chi_3=D_{\mathcal{R}^m,\sigma_3}$, $\chi_4=D_{\mathcal{R}^d,\sigma_4}$. 如果存在一个 (量子) 概率多项式时间的敌手 $\mathfrak{A}$ 可以以 δ 的概率解决 $\mathrm{DLWE}^d_{\mathcal{R},m,q,\chi_1}(\chi_2;\mathcal{D})$ 问题, 则存在一个 (量子) 概率多项式时间的敌手 $\mathfrak{B}$ 可以以 $\delta-negl(\lambda)$ 的概率解决 $\mathrm{DLWE}^d_{\mathcal{R},m,q,\chi_3}(\chi_4;\mathrm{U}\left(\mathcal{R}_q^{m\times d}\right))$ 问题.

类似于欧氏格中的半均匀 LWE 问题的参数分析, 可以推出以下结论. 当选取参数 $\sigma_3=\sigma_4=:\sigma$ 时, 可以将标准的 $\mathrm{DLWE}^d_{\mathcal{R},m,q,D_{\mathcal{R}^m,\sigma}}(D_{\mathcal{R}^d,\sigma};\mathrm{U}\left(\mathcal{R}_q^{m\times d}\right))$ 问题归约到公开矩阵服从任意 η-半均匀分布 $\mathcal{D}$ 的半均匀 $\mathrm{DLWE}^d_{\mathcal{R},m,q,\chi_1}(\chi_2;\mathcal{D})$ 问题. 其中, $\chi_1=D_{\mathcal{R}^m,\sigma_1}$, $\sigma_1=\mathrm{O}(\eta\cdot\sigma)$; $\chi_2=D_{\mathcal{R}^d,\sigma_2}$, $\sigma_2=\mathrm{O}(\sigma)$.

注意到当 $d=1$ 时, 上述结果即为对应的环上的半均匀 LWE 问题的困难性归约结果. 与文献 [17] 的结论相比, 我们可以将标准的环 LWE 问题归约到对应的半均匀环 LWE 问题, 而不需要使用额外的困难性假设 (例如某些特定形式的 DSPR (decisional small polynomial ratio) 假设, 即对应为判定版本的 NTRU 假设). 当 $d\geqslant 2$ 时, 与文献 [4] 的结果相比, 在渐近的意义下, 我们的误差参数的归约损失仅为 η, 与其余参数无关. 特别地, 我们的归约也是保持格的维数的, 不需要像文献 [4,17,18] 那样基于低维度 (更确切地说, 低秩数) 的模 LWE 问题的困难性.

当定义分布 $\mathcal{D}_{p,q,m,d}$ 为: 取样 $U\in\mathcal{R}_q^{m\times d}$, 输出 $\left\lfloor\frac{q}{p}\cdot\left\lfloor\frac{p}{q}\cdot U\right\rceil\right\rceil$ 时, 简单计算易知, $\mathcal{D}_{p,q,m,d}$ 为特殊的 $n\cdot\sqrt{m\cdot d}\cdot\left\lfloor\frac{q}{2p}\right\rceil$-半均匀分布. 利用分布 $\mathcal{D}_{p,q,m,d}$ 对应的半均匀模 LWE 问题可以证明, 当采用类似 NIST 第 1 轮候选算法 Kyber 那种压缩公钥的设计方式时, 对应的底层加密方案也满足 IND-CPA 安全性. 具体方案的构造如下. 由于相关方案的 IND-CPA 安全性的证明是标准的, 我们仅给出大概解释, 证明的具体细节可以参考文献 [4,25–29].

- $\mathrm{KeyGen}(1^\lambda)$: 给定安全参数 λ, 密钥生成算法采样 $A\hookleftarrow\mathrm{U}\left(\mathcal{R}_q^{d\times d}\right)$, $\boldsymbol{s}\hookleftarrow D_{\mathcal{R}^d,\sigma_2}$, $\boldsymbol{e}\hookleftarrow D_{\mathcal{R}^d,\sigma_1}$. 计算 $\boldsymbol{b}=A\cdot\boldsymbol{s}+\boldsymbol{e}$,

© 中国科学院软件研究所 http://www.jos.org.cn

并返回公钥 $pk=\left(A,\left\lfloor\frac{p}{q}\cdot\boldsymbol{b}\right\rceil\right)$ 和私钥 $sk=\boldsymbol{s}$.

● $\mathrm{Enc}(pk,m)$: 假设 $pk=\left(A,\left\lfloor\frac{p}{q}\cdot\boldsymbol{b}\right\rceil\right)$, 要加密消息 $\sigma_{\mathrm{coef}}(m)\in\{0,1\}^n$, 加密算法先计算 $\tilde{\boldsymbol{b}}=\left\lfloor\frac{q}{p}\cdot\left\lfloor\frac{p}{q}\cdot\boldsymbol{b}\right\rceil\right\rceil$. 随后, 采样 $\boldsymbol{r}\hookleftarrow D_{\mathcal{R}^d,\sigma_2}$, $\boldsymbol{e}_1\hookleftarrow D_{\mathcal{R}^d,\sigma_2}$, $e_2\hookleftarrow D_{\mathcal{R},\sigma_1}$, 并计算 $\boldsymbol{c}_1=A^{\mathrm{T}}\cdot\boldsymbol{r}+\boldsymbol{e}_1$ 和 $c_2=\tilde{\boldsymbol{b}}^{\mathrm{T}}\cdot\boldsymbol{r}+e_2$. 最后返回密文 $ct=(\boldsymbol{c}_1,c_2)$.

● $\mathrm{Dec}(sk,ct)$: 假设 $ct=(\boldsymbol{c}_1,c_2)$, $sk=\boldsymbol{s}$. 解密算法计算并返回 $m=\left\lfloor\frac{2}{q}\cdot(c_2-\boldsymbol{s}^{\mathrm{T}}\cdot\boldsymbol{c}_1)\right\rceil$.

简单计算可知, 对于适当选择的参数, 上述方案可以正确解密. 为证明方案的 IND-CPA 安全性, 需要用到两次相应判定版本的 LWE 假设. 第 1 次是将 $(A,\boldsymbol{b})$ 替换为均匀随机的 $(A,\boldsymbol{u})$, 用到的假设是 $\mathrm{DLWE}^d_{\mathcal{R},d,q,D_{\mathcal{R}^d,\sigma_1}}(D_{\mathcal{R}^d,\sigma_2};\mathrm{U}(\mathcal{R}_q^{d\times d}))$ 问题是困难的; 第 2 次是将密文替换为随机均匀的元素, 其中替换密文 $\boldsymbol{c}_1$ 用到的假设仍是 $\mathrm{DLWE}^d_{\mathcal{R},d,q,D_{\mathcal{R}^d,\sigma_1}}(D_{\mathcal{R}^d,\sigma_2};\mathrm{U}(\mathcal{R}_q^{d\times d}))$ 问题是困难的. 但是, 替换密文 c_2 需要用到的困难性假设是 $\mathrm{DLWE}^d_{\mathcal{R},1,q,D_{\mathcal{R},\sigma_1}}(D_{\mathcal{R}^d,\sigma_2};\mathcal{D}_{p,q,1,d})$. 这里, $\mathcal{D}_{p,q,1,d}$ 对应的分布为: 取样 $\boldsymbol{u}\hookleftarrow\mathrm{U}(\mathcal{R}_q^d)$, 输出 $\left\lfloor\frac{q}{p}\cdot\left\lfloor\frac{p}{q}\cdot\boldsymbol{u}\right\rceil\right\rceil$. 注意到分布 $\mathcal{D}_{p,q,1,d}$ 是 $n\cdot\sqrt{d}\cdot\left\lfloor\frac{q}{2p}\right\rceil$-半均匀分布, 采用本文的归约结果可知, $\mathrm{DLWE}^d_{\mathcal{R},1,q,D_{\mathcal{R},\sigma_1}}(D_{\mathcal{R}^d,\sigma_2};\mathcal{D}_{p,q,1,d})$ 问题的困难性可以由 $\mathrm{DLWE}^d_{\mathcal{R},1,q,D_{\mathcal{R},\sigma}}(D_{\mathcal{R}^d,\sigma};\mathrm{U}(\mathcal{R}_q^d))$ 问题的困难性来保证. 对应的参数关系是 $\sigma_1=\mathrm{O}\left(n\cdot\sqrt{d}\cdot\left\lfloor\frac{q}{2p}\right\rceil\cdot\sigma\right)$, $\sigma_2=\mathrm{O}(\sigma)$. 为兼顾解密错误率和安全强度, 参数 p,q 相差的比特数一般为 $\mathrm{O}(1)$. 采用文献 [27] 的经验估计, 非对称 LWE 问题的困难性与误差参数约为 $\sqrt{\sigma_1\cdot\sigma_2}=\mathrm{O}(n^{1/2}\cdot d^{1/2})\cdot\sigma$ 的对称 LWE 问题的困难性相当. 因此, 当将本文的归约结果应用于 Kyber 类采用压缩公钥的设计方式来设计的公钥加密方案时, 对应的理论归约损失约为 $\mathrm{O}(n^{1/2}\cdot d^{1/4})$. 值得指出的是, 本文的归约方式对于参数 d (和 q) 的限制很小. 可以选择 $d=\mathrm{O}(1)$, 此时对应的理论归约损失约为 $\mathrm{O}(n^{1/2})$.

我们采用文献 [4] 第 5.2 节的定理来估计采用上述设计方式的公钥加密方案 IND-CPA 安全性的理论归约损失. 此时, $\mathrm{DLWE}^d_{\mathcal{R},1,q,D_{\mathcal{R},\sigma_1}}(D_{\mathcal{R}^d,\sigma_2};\mathcal{D}_{p,q,1,d})$ 问题的困难性可以由 $\mathrm{DLWE}^k_{\mathcal{R},1,q,D_{\mathcal{R},\sigma}}(\mathrm{U}(\mathcal{R}_q^k);\mathrm{U}(\mathcal{R}_q^k))$ 问题的困难性和 $\mathrm{DLWE}^d_{\mathcal{R},1,q,D_{\mathcal{R},\sigma_1}}(\mathrm{U}(\mathcal{R}_q^d);\mathrm{U}(\mathcal{R}_q^d))$ 问题的困难性来保证. 这里, $\sigma_1=\mathrm{O}\left(n\cdot\sqrt{d}\cdot\left\lfloor\frac{q}{2p}\right\rceil\cdot\sigma+\sigma^2\right)$. 如果我们也选择 $\sigma_2=\mathrm{O}(\sigma)$ 的话, 根据离散高斯的性质大致估计文献 [4] 中的熵不等式条件可以得到对应模 LWE 问题的秩至少应该满足 $d\geqslant\mathrm{O}(k\cdot\log q+\log n+\omega(\log\lambda))$ (注意到即使是将 $D_{\mathcal{R}^d,\sigma_2}$ 替换为随机均匀分布, 这个条件也应该满足). 因此严格来讲, 文献 [4] 的归约结果不适用于 $d=\mathrm{O}(1)$ 的情形. 此外, 文献 [4] 的归约结果对于参数 q 以及秘密分布也有额外的限制. 例如要求 q 为分裂性质良好的素数, 且要求秘密的分布模 $q\mathcal{R}$ 的每一个素理想均具有足够大的熵. 如果加上这些限制, 文献 [4] 的归约结果将更加受限.

4 总 结

在本文中, 我们将 Hint-LWE 相关问题研究中的方法进行改进并应用到半均匀 LWE 问题的研究之中, 给出了非均匀 LWE 问题更简单、更紧致的困难性归约. 具体来讲, 本文的归约方法几乎不受代数结构的影响, 可以一致地应用到对应的欧氏格/环/模上的半均匀 LWE 问题的归约. 相比于已知的半均匀 LWE 问题的归约结果, 本文给出的归约是保持对应 LWE 问题的维数的, 归约损失小且归约损失 (对应的 LWE 问题的误差所服从的离散高斯参数) 与样本数等条件无关. 当将本文的归约应用到环 LWE 问题时, 对应的归约方法可以基于标准的环 LWE 问题给出非均匀环 LWE 问题的困难性证明, 归约结论无需用到 DSPR 等额外的 (相对而言非标准的) 困难性假设.

References:

[1] Regev O. On lattices, learning with errors, random linear codes, and cryptography. In: Proc. of the 37th Annual ACM SIGACT Symp. on Theory of Computing. Baltimore: ACM, 2005. 84–93. [doi: 10.1145/1060590.1060603]

[2] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. In: Gilbert H, ed. Proc. of the 29th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. French: Springer, 2010. 1–23. [doi: 10.1007/978-3-642-13190-5_1]

[3] Langlois A, Stehlé D. Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography, 2015, 75(3): 565–599. [doi: 10.1007/s10623-014-9938-4]

[4] Jia WJ, Zhang J, Xiang BW, Wang BC. Hardness of (M)LWE with semi-uniform seeds. Theoretical Computer Science, 2024, 994:

© 中国科学院软件研究所 http://www.jos.org.cn

114481. [doi: 10.1016/j.tcs.2024.114481]

[5] Brakerski Z, Langlois A, Peikert C, Regev O, Stehlé D. Classical hardness of learning with errors. In: Proc. of the 45th Annual ACM Symp. on Theory of Computing. Palo Alto: ACM, 2005. 575–584. [doi: 10.1145/2488608.2488680]

[6] Goldwasser S, Kalai YT, Peikert C, Vaikuntanathan V. Robustness of the learning with errors assumption. In: Innovations in Computer Science—ICS 2010. Beijing: Tsinghua University Press, 2010. 230–240.

[7] Micciancio D. On the hardness of learning with errors with binary secrets. Theory of Computing, 2018, 14: 13. [doi: 10.4086/toc.2018.v014a013]

[8] Brakerski Z, Döttling N. Hardness of LWE on general entropic distributions. In: Canteaut A, Ishai Y, eds. Proc. of the 39th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Zagreb: Springer, 2020. 551–575. [doi: 10.1007/978-3-030-45724-2_19]

[9] Boudgoust K, Jeudy C, Roux-Langlois A, Wen WQ. On the hardness of module learning with errors with short distributions. Journal of Cryptology, 2023, 36(1): 1. [doi: 10.1007/s00145-022-09441-3]

[10] Kim D, Lee D, Seo J, Song Y. Toward practical lattice-based proof of knowledge from Hint-MLWE. In: Handschuh H, Lysyanskaya A, eds. Proc. of the 43rd Annual Int'l Cryptology Conf. on Advances in Cryptology (CRYPTO 2023). Santa Barbara: Springer, 2023. 549–580. [doi: 10.1007/978-3-031-38554-4_18]

[11] Dottling N, Kolonelos D, Lai RWF, Lin CW, Malavolta G, Rahimi A. Efficient laconic cryptography from learning with errors. In: Hazay C, Stam M, eds. Proc. of the 42nd Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Lyon: Springer, 2023. 417–446. [doi: 10.1007/978-3-031-30620-4_14]

[12] Agrawal S, Libert B, Stehlé D. Fully secure functional encryption for inner products, from standard assumptions. In: Robshaw M, Katz J, eds. Proc. of the 36th Annual Int'l Cryptology Conf. on Advances in Cryptology (CRYPTO 2016). Santa Barbara: Springer, 2023. 333–362. [doi: 10.1007/978-3-662-53015-3_12]

[13] Mera JMB, Karmakar A, Marc T, Soleimanian A. Efficient lattice-based inner-product functional encryption. In: Hanaoka G, Shikata J, Watanabe Y, eds. Proc. of the 25th IACR Int'l Conf. on Practice and Theory of Public-key Cryptography. Springer, 2022. 163–193. [doi: 10.1007/978-3-030-97131-1_6]

[14] Alperin-Sheriff J, Peikert C. Circular and KDM security for identity-based encryption. In: Fischlin M, Buchmann J, Manulis M, eds. Proc. of the 15th Int'l Conf. on Practice and Theory in Public Key Cryptography. Darmstadt: Springer, 2012. 334–352. [doi: 10.1007/978-3-642-30057-8_20]

[15] O'Neill A, Peikert C, Waters B. Bi-deniable public-key encryption. In: Rogaway P, ed. Proc. of the 31st Annual Cryptology Conf. on Advances in Cryptology (CRYPTO 2011). Santa Barbara: Springer, 2011. 525–542. [doi: 10.1007/978-3-642-22792-9_30]

[16] Boneh D, Lewi K, Montgomery H, Raghunathan A. Key homomorphic PRFs and their applications. In: Canetti R, Garay JA, eds. Proc. of the 33rd Annual Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2013. 410–428. [doi: 10.1007/978-3-642-40041-4_23]

[17] Jia WJ, Zhang J, Wang BC. Hardness of module-LWE with semiuniform seeds from module-NTRU. IET Information Security, 2023, 2023: 2969432. [doi: 10.1049/2023/2969432]

[18] Jia WJ, Wang BC. Hardness of (Semiuniform) MLWE with short distributions using the Rényi divergence. IET Information Security, 2023, 2023: 2104380. [doi: 10.1049/2023/2104380]

[19] National Institute of Standards and Technology. Post-quantum cryptography—Round 1 submissions. 2024. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions

[20] Bos J, Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schanck JM, Schwabe P, Seiler G, Stehle D. CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In: Proc. of the 2018 IEEE European Symp. on Security and Privacy (EuroS&P). London: IEEE, 2018. 353–367. [doi: 10.1109/EuroSP.2018.00032]

[21] Lindner R, Peikert C. Better key sizes (and attacks) for LWE-based encryption. In: Kiayias A, ed. Topics in Cryptology—CT-RSA 2011. Berlin, Heidelberg: Springer, 2011. 319–339. [doi: 10.1007/978-3-642-19074-2_21]

[22] National Institute of Standards and Technology. Post-quantum cryptography—Round 2 submissions. 2024. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions

[23] National Institute of Standards and Technology. Post-quantum cryptography—Round 3 submissions. 2024. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

[24] National Institute of Standards and Technology. Post-quantum cryptography—Selected algorithms 2022. 2024. https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

[25] Jin ZZ, Zhao YL. Optimal key consensus in presence of noise. arXiv:1611.06150, 2017.

© 中国科学院软件研究所 http://www.jos.org.cn

[26] Jin ZZ, Zhao YL. Generic and practical key establishment from lattice. In: Deng RH, Gauthier-Umana V, Ochoa M, Yung M, eds. Proc. of the 17th Int'l Conf. on Applied Cryptography and Network Security. Bogota: Springer, 2019. 302–322. [doi: 10.1007/978-3-030-21568-2_15]

[27] Zhang J, Yu Y, Fan SQ, Zhang ZF, Yang K. Tweaking the asymmetry of asymmetric-key cryptography on lattices: KEMs and signatures of smaller sizes. In: Kiayias A, Kohlweiss M, Wallden P, Zikas V, eds. Proc. of the 23rd IACR Int'l Conf. on Practice and Theory of Public-key Cryptography. Edinburgh: Springer, 2020. 37–65. [doi: 10.1007/978-3-030-45388-6_2]

[28] Chinese Association for Cryptologic Research. Public key algorithms selected to the second round competition of national cryptographic algorithm competitions. 2020 (in Chinese). http://sfjs.cacrnet.org.cn/site/term/list_77_1.html

[29] Chinese Association for Cryptologic Research. Announcement of the selection results of the national cryptographic algorithm competition. 2020 (in Chinese). https://www.cacrnet.org.cn/site/content/854.html

[30] Micciancio D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. Computational Complexity, 2007, 16(4): 365–411. [doi: 10.1007/s00037-007-0234-9]

[31] Bruna J, Regev O, Song MJ, Tang Y. Continuous LWE. In: Proc. of the 53rd Annual ACM SIGACT Symp. on Theory of Computing. ACM, 2021. 694–707. [doi: 10.1145/3406325.3451000]

[32] Gupte A, Vafa N, Vaikuntanathan V. Continuous LWE is as hard as LWE & applications to learning Gaussian mixtures. In: Proc. of the 63rd IEEE Annual Symp. on Foundations of Computer Science. Denver: IEEE, 2022. 1162–1173. [doi: 10.1109/FOCS54457.2022.00112]

[33] Peikert C. An efficient and parallel Gaussian sampler for lattices. In: Rabin T, ed. Proc. of the 30th Annual Cryptology Conf. on Advances in Cryptology (CRYPTO 2010). Santa Barbara: Springer, 2010. 80–97. [doi: 10.1007/978-3-642-14623-7_5]

[34] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Proc. of the 40th Annual ACM Symp. on Theory of Computing. Victoria: ACM, 2008. 197–206. [doi: 10.1145/1374376.1374407]

[35] Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. SIAM Journal on Computing, 2007, 37(1): 267–302. [doi: 10.1137/S0097539705447360]

[36] Applebaum B, Cash D, Peikert C, Sahai A. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Halevi S, ed. Proc. of the 29th Annual Int'l Cryptology Conf. on Advances in Cryptology (CRYPTO 2009). Santa Barbara: Springer, 2009. 595–618. [doi: 10.1007/978-3-642-03356-8_35]

附中文参考文献:

[28] 中国密码学会. 全国密码算法设计竞赛进入第 2 轮公钥算法. 2020. http://sfjs.cacrnet.org.cn/site/term/list_77_1.html

[29] 中国密码学会. 关于全国密码算法设计竞赛算法评选结果的公示. 2020. https://www.cacrnet.org.cn/site/cont-ent/854.html

王洋(1990－), 男, 博士, 助理研究员, 主要研究领域为格密码, 量子信息, 量子计算.

王明强(1970－), 男, 博士, 教授, 博士生导师, 主要研究领域为公钥密码算法的分析与设计, 椭圆曲线, 格密码, 量子信息, 量子计算.

© 中国科学院软件研究所 http://www.jos.org.cn