中国科学: 数学 2020 年 第 50 卷 第 10 期: 1417～1436
SCIENTIA SINICA Mathematica
创刊 70 周年特邀综述
《中国科学》杂志社
SCIENCE CHINA PRESS

格的计算和密码学应用

许光午[1,2], 王小云[3,1,2*]

1. 山东大学密码技术与信息安全教育部重点实验室, 青岛 266237;
2. 山东大学网络空间安全学院, 青岛 266237;
3. 清华大学高等研究院, 北京 100084
E-mail: gxu4sdq@sdu.edu.cn, xiaoyunwang@mail.tsinghua.edu.cn

收稿日期: 2020-06-03; 接受日期: 2020-08-18; 网络出版日期: 2020-09-18; * 通信作者
科技部国家重点研发计划 (批准号: 2018YFA0704702 和 2018YFA0704701) 资助项目

摘要 本文主要介绍格理论的一些基本计算问题和几个典型的密码学应用. 这个综述力求反映相关问题的数学本质并通过实例加以解释. 本文从格的基本概念、基本相关工具和格上几个重要计算问题的描述开始, 然后介绍和讨论几类著名的格论算法. 最后整理现代文献中格上密码学的几个重要构造并加以讨论.

关键词 格 短向量算法 格上密码学

MSC (2010) 主题分类 11H06, 11T71, 94A60

1 引言

整数格的研究是联系数论与几何的桥梁, 是数学历史上的一个优美篇章. 两个多世纪以来, 这个领域吸引了许多卓越的数学家, 例如, J.-L. Lagrange、C. F. Gauss、P. G. L. Dirichlet、C. Hermite 和 H. Minkowski. J.-L. Lagrange、C. F. Gauss 和 C. Hermite 关于正定二次型在整点取值的研究开创了数的几何. 二次型的算术理论甚至可以追溯到 17 世纪中期. 在 1654 年, P. de Fermat 曾证明形如 $8n+1$ 的素数可被表成 x^2+2y^2 (x 和 y 皆为整数) 的形式. 二次型的算术理论的系统阐述由 Gauss 在其巨著《算术研究》[1] 中给出. Gauss 的研究深刻地影响了后来代数数论的发展, 其处理方式被 Dirichlet 进一步简化. Minkowski[2] 注意到一个正定二次型确定了一个凸几何体和一个格, 他以天才的直觉证明了数的几何中里程碑式的基本结果: 如果 $\mathbb{R}^n$ 中的一个关于原点对称的紧致凸几何体 C 之体积不小于 2^n, 那么 C 必包含一个非平凡 (即非原点) 整点. 令 $\Lambda\subset\mathbb{R}^n$ 为一个 n 维格, 关于 Λ 的 Minkowski 基本定理可以导出 Λ 中最短 (非零) 向量长度 $\lambda_1(\Lambda)$ 满足 $\lambda_1(\Lambda)\leqslant R$, 如果以 R 为半径的球体积是 $2^n\det(\Lambda)$, 其中 $\det(\Lambda)$ 是 $\mathbb{R}^n/\Lambda$ 的体积. 当 n 充分大时, 这个上界近似于 $\sqrt{\frac{2n}{\pi\mathrm{e}}}(\det(\Lambda))^{\frac{1}{n}}$, 远优于 Hermite 的界 $(\frac{4}{3})^{\frac{n-1}{4}}(\det(\Lambda))^{\frac{1}{n}}$ [3]. 在 2 和 3 维的情形下分别有 Lagrange 和 Gauss 的短向量长度的估计 [1]. 历史上

英文引用格式: Xu G W, Wang X Y. Computational aspects of lattices and their cryptographic applications (in Chinese). Sci Sin Math, 2020, 50: 1417–1436, doi: 10.1360/SSM-2020-0174

© 2020《中国科学》杂志社

一些关于短向量的结果推导过程也提供了一个找出满足条件的非零格向量的算法. 如果不计维数, 这些算法能在多项式时间内完成计算任务. 然而, 当维数变量也被考虑时, 能否在多项式时间找到满足条件的非零格向量是个未知问题.

20 世纪 80 年代, Lenstra 等 [4] 发表了他们关于格基约化的 LLL (Lenstra-Lenstra-Lovász) 算法, 开启了真正的格计算时代. 格基约化是一个将给定格基转化成一个几乎正交格基的过程, 并且期望所得到的几乎正交格基使确定最短格向量的计算任务变得更加容易. LLL 算法是非平凡格基约化的第一个 (依赖维数和格基长度的) 多项式算法, 对于格 $\Lambda \subset \mathbb{R}^n$, 这个算法可以给出长度不超过 $2^{\frac{n-1}{2}}\lambda_1(\Lambda)$ 的非零格向量. LLL 算法在计算机代数、密码分析和编码理论等方面显示了巨大的应用潜力. 在公钥密码分析中, Adleman [5]、Brickell [6]、Lagarias 和 Odlyzko [7] 成功地将 LLL 算法用于各种背包密码体制的攻击中. Coppersmith [8, 9] 将 RSA (Rivest-Shamir-Adleman) 小加密指数的攻击转化为求解格中向量的问题, 并使用 LLL 算法在多项式时间内求解. LLL 算法还被用于研究 Diffie-Hellman 协议的安全性 (参见文献 [10, 11]).

另一方面, Ajtai [12] 关于基于数学困难问题的密码体系的安全性的创造性刻画开辟了格理论在密码学设计中的新天地. Ajtai 发现了一类随机格具有下面的性质: 从该类里选取一个随机格, 如果存在一个 (概率) 多项式算法能够解决其上最短向量问题 (shortest vector problem, SVP), 那么对任意格及某个近似因子必存在一个多项式算法能够解决其上的近似 SVP 问题. 这是史上第一个关于某个困难问题的最坏情形困难性与平均情形困难性 (worst-case/average-case) 等价的证明. 在仅依赖最坏情形困难性与平均情形困难性等价的前提下, 这个结果使得设计一个可以证明其安全性的密码体系成为可能. Ajtai 和 Dwork [13] 便给出了这样一个加密系统. 另一个意义深远的可证明困难性的格密码体制是 Regev [14] 的基于 LWE (learning with errors) 问题的加密体制, 其安全性归结为任意有效的求解 LWE 问题的多项式算法蕴涵一个多项式时间内解决最坏情形下 SVP 和 SIVP (shortest independent vectors problem) 的有效量子算法.

早期的基于格的密码体制还包括 Goldreich 等 [15] 的 GGH (Goldreich-Goldwasser-Halevi) 体制和 Hoffstein 等 [16] 的 NTRU (N-th degree truncated polynomial ring units) 体制, 其中后者因为令人满意的运算效率而一直受到高度关注.

格困难问题还被用于构造全同态加密体制. Gentry [17] 于 2009 年提出了用多项式商环的理想格来设计加 (解) 密函数, 使它们能够保持加法和乘法运算. Gentry 的结果完满地解决了人们长期以来一直寻求的能够用于密码检索和第三方计算等方面的安全方案.

1994 年, Shor [18] 证明了因子分解问题和离散对数问题在量子计算机模型下可在多项式时间内求解, 于是我们今天常用的公钥体系 (如 RSA、椭圆曲线密码学) 在量子计算的框架下不再提供安全保障. 由于近来量子算法和相关硬件发展进步, 如何设计能够抵御量子计算攻击的密码体系是当前备受关注的一个课题. 基于格困难问题的密码体系被认为是最具有潜在抗量子特性的一类密码体系, 格理论的研究在密码技术中的应用方兴未艾. 我们正在面对这个领域的又一个重要的转折点.

本文将主要介绍格理论的一些基本计算问题和几个典型的密码学应用. 我们在选材和描述上力求反映相关问题的数学本质, 通过实例加以解释. 篇幅的限制和我们的主要研究兴趣所在可能影响了本文内容的取舍, 我们建议有进一步兴趣的读者利用参考文献作更多的探索.

本文余下内容安排如下: 第 2 节介绍格的基本概念、基本相关工具和格上几个重要计算问题的描述与讨论. 第 3 节讨论一些著名的格论算法. 我们把格上密码学的几个重要构造及其讨论放在了第 4 节. 第 5 节给出本文的结束语.

2 格、相关计算问题和格上离散 Gauss 测度

一个秩为 n 的格 Λ 是 $\mathbb{R}^m$ 中的一个离散加法子群, 并且以 $\mathbb{R}^m$ 中 n 个线性无关的向量 $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n$ 为一组格基. 令 $\boldsymbol{B}$ 为 $m\times n$ 矩阵 $(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n)$, Λ 可被确切表成

$$\Lambda = L(\boldsymbol{B}) = \boldsymbol{B}\mathbb{Z}^n.$$

我们通常只考虑满秩格, 即 $m=n$. 也称 n 为格 Λ 的维数.

格 Λ 作为一个 $\mathbb{Z}$- 模, 其对偶格是 $\widehat{\Lambda}=\mathrm{Hom}(\Lambda,\mathbb{Z})$. 更确切地,

$$\widehat{\Lambda} = \{\boldsymbol{y}\in\mathbb{R}^n : \langle \boldsymbol{x},\boldsymbol{y}\rangle\in\mathbb{Z},\ \forall\,\boldsymbol{x}\in\Lambda\}$$

也是一个 n 维格.

易知, 对于格 Λ 的另一个格基 $\boldsymbol{B}'=(\boldsymbol{b}'_1,\ldots,\boldsymbol{b}'_n)$, 存在一个幺模矩阵 $\boldsymbol{U}\in\mathbb{Z}^{n\times n}$, 使得 $\boldsymbol{B}'=\boldsymbol{B}\boldsymbol{U}$. 给定格基 $\boldsymbol{B}=(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n)$, 其基本体是下述集合:

$$\mathcal{P}(\boldsymbol{B}) = \left\{\sum_{i=1}^n \alpha_i\boldsymbol{b}_i : 0\leqslant\alpha_i<1\right\}.$$

$\mathcal{P}(\boldsymbol{B})$ 还可写成 $\mathbb{R}^n/\Lambda$, 其体积 $\sqrt{\det(\boldsymbol{B}\boldsymbol{B}^\top)}$ 通常被记成 $\det(\Lambda)$.

格 Λ 的逐次最小长度 $\lambda_i(\Lambda)$ 定义为包含 i 个线性无关的格向量的以原点为球心的球的最小半径, 即

$$\lambda_i(\Lambda) = \min\{r>0 : \dim(\mathrm{span}(\Lambda\cap B(0,r)))\geqslant i\},$$

$i=1,2,\ldots,n$. 特别地, $\lambda_1(\Lambda)$ 是格 Λ 中最短非零向量的长度. 关于这些长度, Minkowski 给出的上界至今还是理论与计算中具有指导意义的重要参数. 下面两个基本结果通常分别被称为 Minkowski 第一和第二定理.

Minkowski 定理 对任意 n 维格 Λ, 有

(1) $\lambda_1(\Lambda)<\sqrt{n}\det(\Lambda)^{\frac{1}{n}}$;

(2) $(\prod_{i=1}^n\lambda_i(\Lambda))^{\frac{1}{n}}<\sqrt{n}\det(\Lambda)^{\frac{1}{n}}$.

2.1 格上困难问题

格的最短向量问题和最近向量问题, 作为具有内在价值的数学问题本身, 以及作为在纯粹数学、应用数学和密码学等领域有强烈背景和需求的格归约问题, 一个多世纪以来备受重视, 不断有深入的研究. 这两个问题属于计算上的困难问题, 其表述与所用的度量有关. 本文将采用通常的 Euclid 距离 (即 ℓ_2- 范数).

最短向量问题 (SVP): 给定格 Λ 的一组基 $\boldsymbol{B}$, 寻找一个非零格向量 $\boldsymbol{v}$ 使得 $\|\boldsymbol{v}\|=\lambda_1(\Lambda)$.

最近向量问题 (closest vector problem, CVP): 给定格 Λ 的一组基 $\boldsymbol{B}$ 和某个目标向量 $\boldsymbol{t}\in\mathbb{R}^n$, 寻找一个格向量 $\boldsymbol{v}_0$ 使得 $\|\boldsymbol{v_0}-\boldsymbol{t}\|=\min_{\boldsymbol{v}\in\Lambda}\|\boldsymbol{v}-\boldsymbol{t}\|$.

格的离散性保证了长度最短的非零向量的存在性. 但在构造的意义下, 上述问题属于格理论中的两类最基本的计算困难问题. 在此基础上, 还有许多衍生的格困难问题, 其中比较典型的问题包括:

γ- 近似最短向量问题 ($\mathbf{SVP}_\gamma$): 给定格 Λ 的一组基 $\boldsymbol{B}$ 和近似因子 $\gamma>1$, 寻找一个非零格向量 $\boldsymbol{v}$ 使得 $\|\boldsymbol{v}\|\leqslant\gamma\cdot\lambda_1(\Lambda)$.

最短线性无关向量问题 (SIVP): 给定格 Λ, 寻找 n 个线性无关的非零格向量 $\boldsymbol{v}_i$ 使得

$$\|\boldsymbol{v}_i\| \leqslant \lambda_n(\Lambda).$$

γ- 近似最近向量问题 ($\mathbf{CVP}_\gamma$): 给定格 Λ 的一组基 $\boldsymbol{B}$、某个目标向量 $\boldsymbol{t} \in \mathbb{R}^n$ 和近似因子 $\gamma > 1$, 寻找一个非零格向量 $\boldsymbol{v}$ 使得

$$\|\boldsymbol{v} - \boldsymbol{t}\| \leqslant \gamma \cdot \mathrm{dist}(\boldsymbol{t}, \Lambda).$$

γ- 有界距离解码问题 (γ-bounded distance decoding, $\mathbf{BDD}_\gamma$): 给定格 Λ 和某个目标向量 $\boldsymbol{t} \in \mathbb{R}^n$, 满足 $\mathrm{dist}(\boldsymbol{t}, \Lambda) < \gamma \cdot \lambda_1(\Lambda)$, 寻找一个非零格向量 $\boldsymbol{v}$, 使得 $\|\boldsymbol{v} - \boldsymbol{t}\| = \mathrm{dist}(\boldsymbol{t}, \Lambda)$.

在计算复杂性框架下, 我们现在知道最短向量问题在随机归约下是 NP- 困难的, 而精确的最近向量问题是 NP- 困难的. 从实用的角度, 近似因子为 $\gamma = O(n)$ 的 γ- 近似最短向量问题或 γ- 近似最近向量问题便可以考虑作为设计格密码体制的困难问题.

2.2 格上离散 Gauss 测度

给定实数 $s > 0$ 和向量 $\boldsymbol{c} \in \mathbb{R}^n$, 我们常用 $\rho_{s,\boldsymbol{c}}$ 来表示 Gauss 函数 $\rho_{s,\boldsymbol{c}}(\boldsymbol{x}) = \mathrm{e}^{-\pi \frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2}}$; 当 $s = 1$ 或 $\boldsymbol{c} = \boldsymbol{0}$ 时, 我们会省略 $\rho_{s,\boldsymbol{c}}$ 中的对应下标. Gauss 函数引出格 Λ 上一个自然的概率测度 $D_{\Lambda,s,\boldsymbol{c}}$, 其在格点 $\boldsymbol{v} \in \Lambda$ 的概率值被指定为

$$D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{v}) = \frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{v})}{\rho_{s,\boldsymbol{c}}(\Lambda)},$$

其中

$$\rho_{s,\boldsymbol{c}}(\Lambda) = \sum_{\boldsymbol{u} \in \Lambda} \rho_{s,\boldsymbol{c}}(\boldsymbol{u}).$$

函数 $\rho_{s,\boldsymbol{c}}$ 是 Schwartz 空间 (速降函数空间) 中最为典型的一类函数, 我们也看到每个格 Λ 都有一个自然的对偶格 $\widehat{\Lambda}$, 进而我们有了一个使用 Fourier 变换的极好框架. 特别地, Poisson 求和公式对于今天格的理论与计算有着本质的作用. 对于一个速降函数 $f : \mathbb{R}^n \to \mathbb{R}$ 和它的 Fourier 变换

$$\hat{f}(\boldsymbol{y}) = \int_{\mathbb{R}^n} \mathrm{e}^{-2\pi\sqrt{-1}\langle \boldsymbol{x}, \boldsymbol{y}\rangle} f(\boldsymbol{x}) d\boldsymbol{x},$$

Poisson 求和公式 [19] 指出

$$\sum_{\boldsymbol{v} \in \Lambda} f(\boldsymbol{v}) = \frac{1}{\det(\Lambda)} \sum_{\boldsymbol{y} \in \widehat{\Lambda}} \hat{f}(\boldsymbol{y}).$$

关于格上离散 Gauss 分布的研究最早源于 Banaszczyk [20, 21] 的工作. Banaszczyk 建立了几个著名的关于 Gauss 测度的不等式. 下面是 Banaszczyk 的两个基本不等式, 其中第一个是经过 Tian 等 [22] 改进了的结果.

Banaszczyk Gauss 测度不等式 对任意 n 维格 Λ 和向量 $\boldsymbol{u} \in \mathbb{R}^n$, 有

(1) 如果 $c > \frac{1}{\sqrt{2\pi}}$, 则[1)]

$$\frac{\rho(\Lambda + \boldsymbol{u} \setminus B(0, c\sqrt{n}))}{\rho(\Lambda)} < (c\sqrt{2\pi\mathrm{e}}\ \mathrm{e}^{-\pi c^2})^n;$$

1) Banaszczyk 的结论是, 如果 $\boldsymbol{u} \neq 0$, 则不等式的右端为 $2(c\sqrt{2\pi\mathrm{e}}\ \mathrm{e}^{-\pi c^2})^n$.

(2)

$$\sum_{\substack{\boldsymbol{x}\in\Lambda+\boldsymbol{u}\\ |x_k|\geqslant t}} \rho(\boldsymbol{x}) \leqslant 2\mathrm{e}^{-\pi t^2}\rho(\Lambda).$$

Poisson 求和公式在上述结论的推导中起了关键作用. Banaszczyk 的一些思想引发 Zheng 等 [23] 观察到一个关于格上 Gauss 测度的简单的测不准原理: 对任意 n 维格 Λ, 有

$$\sum_{\boldsymbol{x}\in\Lambda} \frac{\|\boldsymbol{x}\|^2\rho_s(\boldsymbol{x})}{\rho_s(\Lambda)} + s^4 \sum_{\boldsymbol{y}\in\widehat{\Lambda}} \frac{\|\boldsymbol{y}\|^2\widehat{\rho}_s(\boldsymbol{y})}{\widehat{\rho}_s(\widehat{\Lambda})} = \frac{ns^2}{2\pi}.$$

2.2.1 格上的反转定理

格上的反转关系是关于格上的逐次最小长度和其对偶格上逐次最小长度 (或覆盖半径) 之间的自然联系的刻画. 由于 Fourier 分析工具的应用, Banaszczyk [20] 极大地改进了格上的反转定理.

Banaszczyk 反转定理 对任意 n 维格 Λ 和整数 $i=1,\ldots,n$, 有

$$\lambda_i(\Lambda)\lambda_{n-i+1}(\widehat{\Lambda}) \leqslant n.$$

Cai [24] 强化了对逐次最小长度定义中线性无关格向量的要求, 得到了 Banaszczyk 反转定理的一个有意义的改进. 具体地, 文献 [24] 定义 n 个量 $g_1(\Lambda),\ldots,g_n(\Lambda)$ 如下:

$$g_i(\Lambda) = \min\{r>0 : \Lambda\cap B(0,r) \text{ 包含至少 } i \text{ 个可以扩充成 } \Lambda \text{ 的一组格基的线性无关格向量}\}.$$

显然对每个 $i=1,2,\ldots,n$, $\lambda_i(\Lambda)\leqslant g_i(\Lambda)$. Cai 证明了

$$g_i(\Lambda)\lambda_{n-i+1}(\widehat{\Lambda}) \leqslant Cn.$$

Cai 还首次研究了具有 n^{ε}- 唯一最短向量的格的反转定理, 改进了 Ajtai 的最坏情形困难性与平均情形困难性归约的近似因子. 对于具有 n^{ε}- 唯一最短向量的格, Wei 等 [25] 的工作解决了文献 [24] 中提出的相关问题, 也改进了 Cai 的结果. 例如, 文献 [25] 的一个结果证明了, 对于任意 $\varepsilon>0$, 如果 $\widehat{\Lambda}$ 具有 n^{ε}- 唯一最短向量, 则

$$1 \leqslant g_n(\Lambda)\lambda_1(\widehat{\Lambda}) \leqslant 1+4n^{1-\varepsilon}.$$

这个结果去掉了文献 [24] 中关于 $\varepsilon\leqslant\frac{1}{2}$ 的限制. 文献 [25] 还建立了这些反转定理的结论中的上界在相差常数因子的意义下的最优性结果.

2.2.2 格上的光滑参数

随机采样, 特别是离散 Gauss 采样是基于格的密码体制构造中的一个关键步骤, 与系统的安全性密切相关. 具体的方法是从给定格 Λ 中选取向量, 并使得选中的向量的分布服从由 $\rho_{s,\boldsymbol{c}}(\boldsymbol{x}) = \mathrm{e}^{-\pi\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2}}$ 确定的离散 Gauss 分布 $D_{\Lambda,s,\boldsymbol{c}}$, 这里参数 s 的确定影响着安全性和系统效率. 当 s 足够大时, 离散 Gauss 分布 $D_{\Lambda,s,\boldsymbol{c}}$ 更加接近由密度函数 $\frac{1}{s^n}\mathrm{e}^{-\pi\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2}}$ 给出的连续 Gauss 分布, 且在模 Λ 的意义下与平均分布的统计距离足够小. Micciancio 和 Regev [26] 定义了光滑参数来决定这样 s 的下界. 关于给定的 $\varepsilon>0$, n 维格 Λ 的光滑参数 $\eta_{\varepsilon}(\Lambda)$ 定义为

$$\eta_{\varepsilon}(\Lambda) = \min\{s : \rho_{\frac{1}{s}}(\widehat{\Lambda}) \leqslant 1+\varepsilon\}.$$

数学上, 如果 $s \geqslant \eta_\varepsilon(\Lambda)$, 那么在 $\mathbb{R}^n/\Lambda$ 上, 平均分布与由密度函数 $d(\boldsymbol{x}) = \frac{1}{s^n}\rho_s(\Lambda+\boldsymbol{x})$ 定义的概率分布的统计距离为

$$\begin{aligned}
&\frac{1}{2}\int_{\mathbb{R}^n/\Lambda}\left|U(\boldsymbol{x}) - \frac{1}{s^n}\rho_s(\Lambda+\boldsymbol{x})\right|d\boldsymbol{x}\\
&\quad= \frac{1}{2}\int_{\mathbb{R}^n/\Lambda}\left|\frac{1}{\det(\Lambda)} - \frac{1}{s^n}\rho_s(\Lambda+\boldsymbol{x})\right|d\boldsymbol{x}\\
&\quad= \frac{1}{2}\int_{\mathbb{R}^n/\Lambda}\frac{1}{\det(\Lambda)}\left|1 - \sum_{\boldsymbol{y}\in\widehat{\Lambda}}\mathrm{e}^{2\pi\sqrt{-1}\langle\boldsymbol{y},\boldsymbol{x}\rangle}\rho_{\frac{1}{s}}(\boldsymbol{y})\right|d\boldsymbol{x}\\
&\quad\leqslant \frac{1}{2}(\rho_{\frac{1}{s}}(\widehat{\Lambda}) - 1)\\
&\quad\leqslant \frac{\varepsilon}{2}.
\end{aligned}$$

光滑参数 $\eta_\varepsilon(\Lambda)$ 的第一个非平凡估计是文献 [26] 给出的, 依赖于格 Λ 的逐次最小长度中的最大者:

$$\eta_\varepsilon(\Lambda) \leqslant \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}}\lambda_n(\Lambda).$$

Peikert [27] 给出的估计与关于对偶格 ℓ_∞- 范数下最短向量长度相关:

$$\eta_\varepsilon(\Lambda) \leqslant \frac{\sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}}}{\lambda_1^\infty(\widehat{\Lambda})}.$$

我们知道, $\lambda_n(\Lambda)$ 和 $\lambda_1^\infty(\widehat{\Lambda})$ 的估计通常是很难精确做到的. 我们考虑另一个选择. 对每一个 Λ 的格基 $\boldsymbol{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$, 我们用 $\{\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \ldots, \boldsymbol{b}_n^*\}$ 表示该格基的 Gram-Schmidt 正交基. 取

$$\tilde{bl}(\Lambda) = \min\Big\{\max_j \|\boldsymbol{b}_j^*\| : \boldsymbol{B}\ \text{是一个格基}\Big\}.$$

$\eta_\varepsilon(\Lambda)$ 依赖于 $\tilde{bl}(\Lambda)$ 的估计出自文献 [28]:

$$\eta_\varepsilon(\Lambda) \leqslant \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}}\tilde{bl}(\Lambda).$$

这个估计被 Zheng 等 [23] 加细为

$$\eta_\varepsilon(\Lambda) \leqslant \sqrt{\frac{\ln(n-1+\frac{2n}{\varepsilon})}{\pi}}\tilde{bl}(\Lambda).$$

上述结果的证明需要条件 $\varepsilon < \min\{1, 0.086435n\}$, 但在应用中我们自然假定 ε 很小, 这样的条件通常总能满足. 文献 [23] 还给出了一维格上十分接近其确切值的 $\eta_\varepsilon(\mathbb{Z})$ 的上界; 证明了当 $\varepsilon < 0.086435$ 时,

$$\eta_\varepsilon(\mathbb{Z}) \leqslant \sqrt{\frac{\ln(\frac{\varepsilon}{44}+\frac{2}{\varepsilon})}{\pi}}.$$

3 经典格问题的计算

本节主要介绍几类有影响的计算格的短向量算法. 我们看到大部分算法都是指数时间的, 有的甚至是指数空间的. 本节的最后一部分将描述 Ajtai 的归约理论, 它是可证明安全的格密码体制的一个基石.

3.1 LLL 约化算法

Lenstra 等 [4] 的格基约化算法能够在多项式时间内把一组格基约化成一个包含短向量的新格基. 在无法得到最短向量的情形下, LLL 算法给出的短向量在很多应用中可以导致足够好的结果.

直观上, 如果能够找到一个接近正交的格基, 那么寻求最短向量的任务就变得简单. 于是, Gram-Schmidt 正交化过程在 LLL 算法里起着重要作用. 设有格 Λ 的一组基 $\boldsymbol{B}=(\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n)$, 我们用 $\boldsymbol{B}^*=(\boldsymbol{b}_1^*,\boldsymbol{b}_2^*,\ldots,\boldsymbol{b}_n^*)$ 表示该格基的 Gram-Schmidt 正交基. 熟知, 矩阵 $\boldsymbol{B}$ 可被分解为 $\boldsymbol{B}=\boldsymbol{B}^*\tilde{\boldsymbol{R}}$, 其中

$$\tilde{\boldsymbol{R}}=\begin{pmatrix}1 & \mu_{21} & \cdots & \mu_{n1}\\ 0 & 1 & \cdots & \mu_{n2}\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1\end{pmatrix},$$

对于 $j>i$, $\mu_{ji}=\frac{\langle \boldsymbol{b}_j,\boldsymbol{b}_i^*\rangle}{\|\boldsymbol{b}_i^*\|^2}$. 输入一个格基, LLL 算法输出一个约化基 $\boldsymbol{B}$, 其 Gram-Schmidt 正交化满足

(1) (尺度约化) 对所有的 $j>i$, $|\mu_{ji}|\leqslant\frac{1}{2}$;

(2) (Lovász 条件) 对所有的 i, $\frac{3}{4}\|\boldsymbol{b}_i^*\|^2\leqslant\|\boldsymbol{b}_{i+1}^*\|^2+\mu_{i+1,i}^2\|\boldsymbol{b}_i^*\|^2$.

为满足上述条件, LLL 算法不断更新格基 $\{\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n\}$ (同时更新 Gram-Schmidt 正交基 $\{\boldsymbol{b}_1^*,\boldsymbol{b}_2^*,\ldots,\boldsymbol{b}_n^*\}$). 例如, 对于固定的 j, 若存在某个 $i<j$ 使得 $|\mu_{ji}|>\frac{1}{2}$, 则需要把原来格基中的 $\boldsymbol{b}_j$ 换成 $\boldsymbol{b}_j-\lfloor\mu_{ji}\rceil\boldsymbol{b}_i$. 这样的步骤按 i 从大到小的次序施行便可做到尺度约化. 我们称之为格基 $\boldsymbol{B}$ 的正规化. 尺度约化还不足以得到较理想的格基, 如果一个格基接近正交, 或接近以长度排序, Lovász 条件便可满足, 也使长度归约更加有效. 在 LLL 算法中, 如果 Lovász 条件在第 i 步得不到满足, 则需要交换 $\boldsymbol{b}_i$ 和 $\boldsymbol{b}_{i+1}$, 然后对置换后的新基再重新施行各个步骤.

LLL 算法的具体描述如下:

算法 1 LLL 算法

输入格 Λ 的一组基 $\boldsymbol{B}=(\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n)$.

1: 计算 Gram-Schmidt 正交基 $\boldsymbol{B}^*$;

2: 计算 $\boldsymbol{B}$ 的正规化;

3: 如果存在 $i<n$ 使 $\frac{3}{4}\|\boldsymbol{b}_i^*\|^2>\|\boldsymbol{b}_{i+1}^*\|^2+\mu_{i+1,i}^2\|\boldsymbol{b}_i^*\|^2$

  交换 $\boldsymbol{b}_i$ 和 $\boldsymbol{b}_{i+1}$;

  返回第一步;

4: 输出 $\boldsymbol{B}$.

设输入基满足 $\max_i\|\boldsymbol{b}_i\|\leqslant B$, 则 LLL 算法在大小为 $O(n+\log B)$ 的有理数中需要算术运算的个数为 $O(n^5\log B)$. LLL 算法所产生的约化基有下面的基本性质:

定理 (Lenstra、Lenstra 和 Lovász) 设 $\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n$ 是 n 维格 Λ 的一组 LLL- 约化基, 则

(1) $\det(\Lambda)\leqslant\prod_{i=1}^n\|\boldsymbol{b}_i\|\leqslant 2^{\frac{n(n-1)}{4}}\det(\Lambda)$;

(2) $\|\boldsymbol{b}_j\|\leqslant 2^{\frac{i-1}{2}}\|\boldsymbol{b}_i^*\|$, $1\leqslant j<i\leqslant n$;

(3) $\|\boldsymbol{b}_1\|\leqslant 2^{\frac{n-1}{4}}\det(\Lambda)^{\frac{1}{n}}$;

(4) 对 Λ 中任一线性无关向量组 $\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t$, 一定有

$$\|\boldsymbol{b}_j\|\leqslant 2^{\frac{n-1}{2}}\max\{\|\boldsymbol{x}_1\|,\|\boldsymbol{x}_2\|,\ldots,\|\boldsymbol{x}_t\|\},\quad 1\leqslant j\leqslant t.$$

特别地, $\|\boldsymbol{b}_1\| \leqslant 2^{\frac{n-1}{2}}\lambda_1(\Lambda)$.

关于格基约化, Korkine-Zolotareff 约化算法及其扩展在解最短向量问题中十分有用.

格 Λ 的一组基 $\boldsymbol{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ 在被 Korkine-Zolotareff 约化算法更新后满足

(1) 对所有的 $j > i$, $|\mu_{ji}| \leqslant \frac{1}{2}$;

(2) 对所有的 i, $\|\boldsymbol{b}_i^*\| = \lambda_1(\pi_i(\Lambda))$,

其中 $\pi_i : \mathbb{R}^n \to (\mathbb{R}\boldsymbol{b}_1 + \cdots + \mathbb{R}\boldsymbol{b}_{i-1})^{\perp}$ 是正交投射, 特别地, $\pi_i(\boldsymbol{b}_j) = \boldsymbol{b}_j^* + \sum_{k=i}^{j-1}\mu_{jk}\boldsymbol{b}_k^*$ 且 $\boldsymbol{b}_1$ 是 Λ 的一个最短向量 (参见文献 [29]). Korkine-Zolotareff 约化算法是指数时间的. LLL 算法则是将复杂的过程 $\|\boldsymbol{b}_i^*\| = \lambda_1(\pi_i(\Lambda))$ 换成两个基向量的对换.

1987 年, Schnorr [30] 在 LLL 算法的基础上引入了分块约化的思想, 进而产生了 BKZ (block Korkine-Zolotareff) 算法. 给定分块大小 β 和 $\varepsilon > 0$, 这个算法所生成的格基 $\boldsymbol{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ 满足

(1) 这个基在 ε 因子下是 LLL 归约的 (即对所有的 i, $(1-\varepsilon)\|\boldsymbol{b}_i^*\|^2 \leqslant \|\boldsymbol{b}_{i+1}^*\|^2 + \mu_{i+1,i}^2\|\boldsymbol{b}_i^*\|^2$);

(2) 对所有的 $i, \|\boldsymbol{b}_i^*\| = \lambda_1(\Lambda_{[i,k]})$, 其中 $k = \min\{i+\beta-1, n\}$, $\Lambda_{[i,k]} = \sum_{j=i}^{k}\mathbb{Z}\pi_i(\boldsymbol{b}_j)$.

BKZ2.0 [31] 是 BKZ 算法的一个结合 Gama 等 [32] 裁剪技术的实现, 具有实用性.

3.2 求解最短向量的枚举算法

枚举算法是求解最短向量问题的精确算法. 给定一组格基, 遍历在一定界限之内的所有整系数线性组合, 从而找到最短向量. 显然, 枚举算法的效率取决于格基的质量.

1983 年, Kannan [33] 提出了著名的最短向量枚举算法. 本质上, Kannan 的枚举算法算出一个 n 维格的 Korkine-Zolotareff 约化基. 这个算法从准 Korkine-Zolotareff 约化基 (即 $\pi_1(\boldsymbol{b}_2), \ldots, \pi_1(\boldsymbol{b}_n)$ 为 $\pi_1(\Lambda)$ 的 Korkine-Zolotareff 约化基, 且 $\|\pi_1(\boldsymbol{b}_2)\| \geqslant \frac{1}{2}\|\boldsymbol{b}_1\|$) 开始, 通过枚举所有长度小于第一个向量的格点找到其中的最短向量. 该算法的最佳时间复杂度为 $2^{O(n\log n)}$. Helfrich [34] 改进了 Kannan 枚举算法, 其时间复杂度降为 $n^{\frac{n}{2}+O(n)}$. Hanrot 和 Stehlé [35] 把复杂度进一步改进到 $n^{\frac{n}{2e}+O(n)}$.

基于 LLL 约化基的枚举算法包括 Fincke 和 Pohst 的工作 [36] 和 Schnorr 和 Euchner 的工作 [37]. Schnorr-Euchner 算法在解决实际问题的过程中十分有效, 尽管其时间复杂度高于 Kannan 的枚举算法. Schnorr-Euchner 算法基于 LLL 约化基, 通过逐次枚举目标向量在 Gram-Schmidt 正交基中每个分量的值来遍历所有长度小于某个上界的格点. 该算法的时间复杂度由文献 [32] 给出, 约为 $\sum_{i=1}^{n} q^{(n-i)i/2}2^{O(n)}$ (q 对应于 GSA (geometric series assumption) 中由约化基所决定的常数).

Gama 等 [32] 应用裁剪技术来减少全枚举算法所需格点的个数, 证明了在选择合适的界函数的情形下: (1) 线性裁剪在枚举点数的期望上比全枚举算法提升约 1.189^n; (2) 极限裁剪在枚举点数的期望上比全枚举算法提升约 1.414^n.

给定格 Λ 的一个基 $\boldsymbol{B}$, 每个格向量关于 Gram-Schmidt 正交基 $\boldsymbol{B}^*$ 的分量的整数部分叫作该格向量的一个正交整数表示. 观察表明, 最短向量的正交整数表示显示稀疏性. Schnorr [38] 的随机采样算法用到了正交整数表示. 最近正交整数表示方法被 Ding 等 [39] 用于解最短向量的遗传算法中. Fukase [40] 用正交整数表示结合扩张采样算法来求解最短向量.

Zheng 等 [41] 应用正交整数表示技术, 提出了求最短向量的正交枚举算法. 该算法较好地使用了随机格中短向量近似服从均匀分布的条件, 对比经典的全枚举算法以及极限裁剪枚举算法, 在输出短向量时所需要枚举格点数的期望上比全枚举算法有更显著的提升, 约提升至 1.512^n. 此外, 正交枚举算法还具有参数选取灵活、适用范围广以及枚举格点个数的上界可被精确估计的特点. 正交枚举技术

还在文献 [41] 中进一步发展, 形成了混合 BKZ 算法 (MBKZ (mixed BKZ) 算法). 这个算法通过将正交枚举技术应用到 BKZ 算法中提高了枚举效率; 同时, 使用了记录中间结果的技术来显著减少枚举失败的概率. 此外, 通过结合正交枚举和传统枚举的优点, 避免了 BKZ 算法中的随机化带来的冗余, 进一步提高了算法的效率.

3.3 求解最短向量的随机筛法

随机筛法是精确计算 SVP 的主要随机算法, 其基本思想是将大量随机选取的采样点按照某种方式相互约化.

Ajtai 等[42] 在 2001 年提出 AKS (Ajtai-Kumar-Sivakumar) 筛法, 其主要思想可被总结如下. 设 Λ 为 n 维格, $\gamma < 1$. 令 S 为从半径为 $R = 2^{O(n)}\lambda_1(\Lambda)$ 的球内所采的格点的集合. 如果 S 含有足够多的格点, 那么其中应有两个格点 $\boldsymbol{v}$ 和 $\boldsymbol{u}$ 使得 $\|\boldsymbol{u}-\boldsymbol{v}\| \leqslant \gamma R$, 于是得到了 Λ 的一个短向量 $\boldsymbol{u}-\boldsymbol{v}$. 这个算法的主要步骤是一个筛选子集 $C \subset S$ 的过程, 要求 C 满足 (1) $|C|$ 不要过大; (2) 对每个 $\boldsymbol{u} \in S$, 可以找到 $\boldsymbol{v} \in C$ 使得 $\|\boldsymbol{u}-\boldsymbol{v}\| \leqslant \gamma R$. 将其用于生成 $S' \subset \Lambda \cap B(0, \gamma R)$ 使得 $|S'| = |S| - |C|$. 当使用多项式次筛选过程后, 便可得到一个长度小于 $r\lambda_1(\Lambda)$ ($r \geqslant 1$ 为常数) 的格点.

在空间复杂度是 $2^{O(n)}$ 的情形下, AKS 筛法第一次把求解最短向量问题的时间复杂度降到单指数 $2^{O(n)}$. Nguyen 和 Vidick[43] 给出了一个更具体的复杂度的分析, 证明了 AKS 筛法的时间花费为 $\tilde{O}(2^{5.9n})$, 存储空间为 $\tilde{O}(2^{2.95n})$. Nguyen 和 Vidick 还提出了一个随机启发式 AKS 筛法, 复杂度的分析变得更加精确: 算法需用 $(\frac{4}{3}+\varepsilon)^n$ 多项式时间运算、$(\frac{4}{3}+\varepsilon)^{\frac{n}{2}}$ 多项式比特的空间. Wang 等[44] 提出了二重筛法的思想并对上述结果给予改进, 把时间复杂度降至 $2^{0.3836n+o(n)}$, 空间复杂度变成 $2^{0.2557n+o(n)}$. Micciancio 和 Voulgaris[45] 利用更精确的求覆盖方法估计 AKS 筛法, 证明了时间和空间复杂度可分别为 $2^{3.4n+o(n)}$ 和 $2^{1.97n+o(n)}$. 文献 [45] 还设计了一个名为 ListSieve 的新筛法, 使得寻找最短向量可在 $2^{3.199n+o(n)}$ 时间内和 $2^{1.325n+o(n)}$ 空间内完成. 在 ListSieve 的基础上, Pujol 和 Stehlé[46] 把生日攻击的思想引进了筛法, 建议了 ListSieve-Birthday 算法, 改进的时间和空间复杂度可分别为 $2^{2.465n+o(n)}$ 和 $2^{1.233n+o(n)}$. 2013 年, Becker 等[47] 给出了一种新的启发式随机筛法, 算法针对目标格构造了一系列的格, 通过逐个求解其中的短向量, 逐步找到原格中的最短向量, 时间和空间复杂度分别是 $2^{0.377n+o(n)}$ 和 $2^{0.2925n+o(n)}$.

当前已知最高效的经典计算机模型下的启发式筛法是由 Becker 等[48] 提出的, 该算法实现了时间和空间复杂度的平衡, 两者均为 $2^{0.292n+o(n)}$. 在量子计算模型下, Laarhoven 等[49] 通过 Grover 算法将上述筛法的时间复杂度进一步改进为 $2^{0.265n+o(n)}$.

3.4 求解最短向量的其他算法

Voronoi 细胞是计算几何中的一个重要构造, 是解决很多实际问题的一个有用工具. 关于格 Λ 的 (开) Voronoi 细胞是下面的集合:

$$\mathcal{V}(\Lambda) = \{\boldsymbol{x} \in \mathbb{R}^n : \forall\, \boldsymbol{v} \in \Lambda \setminus \{0\}, \|\boldsymbol{v}-\boldsymbol{x}\| > \|\boldsymbol{x}\|\}.$$

目前理论上最好的求解 SVP 和 CVP 的确定算法是由 Micciancio 和 Voulgaris[50] 发展的 Voronoi 细胞算法. 这个算法的主要思想是用有限个不等式来描述 $\mathcal{V}(\Lambda)$, 即找到一个相关向量的有限集 V, 使得 $\mathcal{V}(\Lambda) = \bigcap_{\boldsymbol{v}\in V} H_{\boldsymbol{v}}$, 其中 $H_{\boldsymbol{v}} = \{\boldsymbol{x} \in \mathbb{R}^n : \|\boldsymbol{v}-\boldsymbol{x}\| > \|\boldsymbol{x}\|\}$. 注意到最短相关向量也是一个最短格向量. Voronoi 细胞算法把求解相关向量和 CVP 问题结合在一起. 利用格点的 Voronoi 细胞结构, 将求

解相关向量问题作为预处理来求解最近向量问题, 在求相关向量的过程中使用了递归调用的方法, 并且巧妙地调用带预处理的求最近向量问题的算法. 这个确定性算法可在 $2^{2n+o(n)}$ 时间内解决几个格中主要困难问题 (如 SVP、CVP 和 SIVP). 此算法所用空间也是指数的, 约为 $2^{n+o(n)}$.

2015 年, Aggarwal 等 [51] 报告了一个求解 SVP 的随机算法, 这是一个通过离散 Gauss 采样的空间和时间复杂度皆为 $2^{n+o(n)}$ 的算法. 具体地, 给定一个格 Λ, 对于任意 "宽度" 参数 $s>0$, 文献 [51] 中的算法可在 $2^{n+o(n)}$ 时间和空间内输出 $2^{\frac{n}{2}}$ 个服从分布 $D_{\Lambda,s}$ 的相互独立的格向量. 如果要求宽度参数 s 大于光滑参数, 那么算法的空间与时间复杂度可以降低为 $2^{\frac{n}{2}+o(n)}$.

3.5 Ajtai 的随机格构造

1996 年 Ajtai [12] 给出了第一个具体关于著名的格的最短向量问题的最坏情形和平均情形计算复杂性的关联. Ajtai 建立了一个最坏情况下困难性意义下的逼近短格基问题到依平均分布在某种格的随机类里选取的格中寻找一个短向量 $\boldsymbol{v}$ 的问题的概率归约. 现在来定义 Ajtai 随机类 $\mathcal{A}$. 给定一个正整数 n, Ajtai 随机类依赖于两个固定的常数 $c_1>1$ 和 $c_2>0$. 取 $m=\lfloor c_1 n\rfloor$, $q=\lfloor n^{c_2}\rfloor$. 取 m 个 n 维整向量

$$\boldsymbol{v}_j=(v_{1j},\ldots,v_{nj}),\quad 0\leqslant v_{ij}<q,\quad 1\leqslant j\leqslant m. \tag{*}$$

由此, 定义随机变量 $z=z(n,m,q)$ 依平均分布在下面 m 个模 q 整向量序列的集合中取值:

$$\{(\boldsymbol{v}_1,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_m):\boldsymbol{v}_j \text{ 满足条件 } (*)\}.$$

现在定义 Ajtai 格 $\Lambda(z,q)$ 如下:

$$\Lambda(z,q)=\left\{(h_1,h_2,\ldots,h_m)\in\mathbb{Z}^m:\sum_{j=1}^m h_j\boldsymbol{v}_j\equiv 0 \pmod q\right\}.$$

注意到对于 $\mathbb{R}^m$ 的标准基 $\boldsymbol{e}_1,\ldots,\boldsymbol{e}_m$, $\Lambda(z,q)$ 包含 m 个线性无关的格向量 $q\boldsymbol{e}_1,\ldots,q\boldsymbol{e}_m$, 所以, $\Lambda(z,q)$ 是 m 维的.

Ajtai 证明了, 如果对关于 n 的 Ajtai 随机类 $\mathcal{A}$ 的任一个随机选取的格, 存在一个多项式时间概率算法计算其 SVP, 那么也存在多项式时间概率算法解决下述 3 个问题:

(1) 在模去多项式因子 n^{k_1} 的意义下, 确定 n 维格的一个非零最短向量的长度;

(2) 对一个满足 $\lambda_2(\Lambda)\geqslant n^{k_2}\lambda_1(\Lambda)$ 的 n 维格 Λ, 求解 Λ 的 SVP;

(3) 在模去多项式因子 n^{k_3} 的意义下, 找出一个 n 维格 Λ 的一组基 $\{\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n\}$ 使 $\max_i\|\boldsymbol{b}_i\|$ 在所有可能的基中最小.

Ajtai 算法的归约因子被不断改进, 参见文献 [24,52,53].

Ajtai 随机类 $\mathcal{A}$ 中随机格的个数以及随机格基本体的体积平均值的计算可见参见文献 [54]. 关于随机格基本体的体积的一个简单情形是, 如果 q 为素数且 z 的取值为 $(\boldsymbol{v}_1,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_m)$, 那么

$$\det(\Lambda(z,q))=q^r,$$

其中

$$r=\dim(\operatorname{span}(\boldsymbol{v}_1,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_m)).$$

4 格的密码学应用

本节首先描述格在密码学分析中两个有深刻数学影响的应用实例. 然后讨论几个当前受到关注的基于格的密码体制, 包括一些后量子时代公钥密码标准化的候选算法, 类型有密钥交换、公钥加密和数字签名等.

4.1 格在密码分析中的两个应用

4.1.1 背包加密系统的密码分析

关于 Merkle-Hellman 背包加密体制 [55] 的密码分析是密码学中的一个经典例子, 特别是 LLL 算法的应用. 下面是 Merkle-Hellman 背包加密体制的公钥/私钥对的产生过程: 生成一个超递增序列 $\boldsymbol{b}=(b_1,\ldots,b_n)\in\mathbb{N}^n$ $(b_j>\sum_{k=1}^{j-1}b_k)$, 随机选取模数 $M>\sum_{k=1}^{n}b_k$ 及正整数 W 使得 $\gcd(W,M)=1$. 令 π 为 $\{1,\ldots,n\}$ 上的一个随机置换. 对每个 j, 计算

$$a_j=Wb_{\pi(j)} \pmod M.$$

系统的公钥是 $\boldsymbol{a}=(a_1,\ldots,a_n)$; 私钥是 $(\pi,M,W,\boldsymbol{b})$.

今有 n 比特明文 $m=m_1\cdots m_n\in\{0,1\}^n$, 将其加密得到密文 $c=\sum_{j=1}^{n}m_ja_j$. 用私钥 $(\pi,M,W,\boldsymbol{b})$ 对 c 解密, 我们只需计算 $W^{-1}c \pmod M$. 事实上,

$$W^{-1}c \pmod M=\sum_{j=1}^{n}m_jb_{\pi(j)}=\sum_{j=1}^{n}m_{\pi^{-1}(j)}b_j,$$

于是 $\boldsymbol{b}$ 的超递增性使我们容易解出比特 $m_{\pi^{-1}(j)}$ $(j=1,\ldots,n)$ 的具体值.

尽管这个系统试图利用子集和问题的困难性来导出安全性, 但 $\boldsymbol{b}$ 的超递增假设无法保证隐匿性. 这个系统在 1984 年被 Shamir [56] 攻破. 这里将描述 Lagarias 和 Odlyzko [7] 使用某类格中短向量的办法对 Merkle-Hellman 背包加密体制的攻击. 假设有密文 $c=\sum_{j=1}^{n}m_ja_j$ 和公钥 $\boldsymbol{a}$. 必要时可用 $\sum_{j=1}^{n}a_j-c$ 代替 c, 假定至多有一半的 $m_1,\ldots,m_n$ 非零. 用下面格基 (矩阵的列) 生成 ($n+1$ 维) 格 Λ:

$$\begin{pmatrix} I_n & 0 \\ \boldsymbol{a} & -c \end{pmatrix}.$$

注意到 $(m_1,\ldots,m_n,0)^\top$ 是一个长度不大于 $\sqrt{\frac{n}{2}}$ 的 (未知) 格向量, 我们对上面的格基施行 LLL 约化以期得到这个短向量. Lagarias 和 Odlyzko 证明了下述结论:

(1) 设 $\beta>1.54725$. 如果 $\max_j a_j\leqslant 2^{\beta n}$, 则以很高概率, $(m_1,\ldots,m_n,0)^\top$ 为格 Λ 中的最短向量.

(2) 设 $\beta>0$, $B>2^{(\frac{1}{2}+\beta)n^2}$. 如果 $\max_j a_j\leqslant B$, 则以很高概率, $(m_1,\ldots,m_n,0)^\top$ 可以通过 LLL 算法得到.

上面第二个结论的条件要求 $\boldsymbol{a}$ 的密度为

$$d(\boldsymbol{a}):=\frac{n}{\log_2(\max_j a_j)}\leqslant\frac{1}{\frac{1}{2}+\beta}\frac{1}{n}.$$

Lagarias 和 Odlyzko 的方法更一般, 能够攻击多次迭代的背包加密体制. 他们的方法被 Coster 等 [57] 及 Nguyen 和 Stern [58] 进一步改进.

4.1.2 Coppersmith 方法

作为格基约化的应用, Coppersmith[8,9,59,60] 开创了确定一般多项式同余方程小整数解的研究. 这个理论在密码分析, 特别是 RSA 体制分析中的几个问题中得到了有效的应用. Coppersmith 方法所关心的问题是, 给定多项式 $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$, 已知

$$f(x_0) \equiv 0 \pmod{M}, \quad |x_0| \leqslant M^{\frac{1}{d}},$$

求解 x_0. Coppersmith 证明了下述结论.

Coppersmith 定理 设 $0 < \varepsilon < \min\{0.18, \frac{1}{d}\}$. 如果存在 $|x_0| \leqslant \frac{1}{2}M^{\frac{1}{d}-\varepsilon}$ 使得 $f(x_0) \equiv 0 \pmod{M}$, 那么 x_0 可以在 (关于 d、$\frac{1}{\varepsilon}$、$\log M$ 的) 多项式时间内被求得.

我们结合一个与 RSA 体制安全性相关的问题来解释 Coppersmith 的构造.

设有两个素数满足 $q < p < 2q$, 且 $N = pq$. 在 RSA 中, N 是公开信息, 而 p 和 q 需要保密. 假如攻击者得到了 p 的一半多一点的高有效位, 即已知 $\tilde{p}$ 使得 $\tilde{p} < p$ 且 $p - \tilde{p} < N^{\frac{1}{4}-\varepsilon}$, 那么 Coppersmith 方法可以在多项式时间内计算 $p - \tilde{p}$, 进而得到 p 和 q. 具体过程如下: 令

$$f(x) = x + \tilde{p} \quad \text{和} \quad x_0 = p - \tilde{p}.$$

于是有

$$f(x_0) \equiv 0 \pmod{N}.$$

设 m 和 t 为两个待定的正整数. 构造下列多项式:

$$\begin{aligned}
&u_0(x) = N^m, \quad u_1(x) = N^{m-1}f(x), \quad u_2(x) = N^{m-2}f^2(x), \quad \ldots, \quad u_{m-1}(x) = Nf^{m-1}(x),\\
&u_m(x) = f^m(x), \quad u_{m+1}(x) = xf^m(x), \quad u_{m+2}(x) = x^2f^m(x), \quad \ldots, \quad u_{m+t-1}(x) = x^{t-1}f^m(x).
\end{aligned}$$

记 $n = m + t$, $X = N^{\frac{1}{4}-\varepsilon}$. 假设 $u_j(x) = c_0 + c_1x + \cdots + c_kx^k$, 则多项式 $u_j(xX)$ 的系数向量便是

$$(c_0, c_1X, c_2X^2, \ldots, c_kX^k).$$

设 Λ 为由 n 个多项式 $\{u_0(xX), u_1(xX), u_2(xX), \ldots, u_{n-1}(xX)\}$ 的系数向量生成的格, 其基的矩阵形式为

$$\begin{pmatrix}
N^m & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0\\
N^{m-1}\tilde{p} & N^{m-1}X & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0\\
N^{m-2}\tilde{p}^2 & 2N^{m-2}\tilde{p}X & N^{m-2}X^2 & 0 & \cdots & \cdots & \cdots & \cdots & 0\\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\
N\tilde{p}^{m-1} & (m-1)N\tilde{p}^{m-2}X & \frac{(m-1)(m-2)}{2}N\tilde{p}^{m-3}X^2 & \cdots & NX^{m-1} & 0 & \cdots & \cdots & 0\\
\tilde{p}^m & m\tilde{p}^{m-1}X & \frac{m(m-1)}{2}\tilde{p}^{m-2}X^2 & \cdots & m\tilde{p}X^{m-1} & X^m & 0 & \cdots & 0\\
0 & \tilde{p}^mX & m\tilde{p}^{m-1}X^2 & \cdots & \cdots & m\tilde{p}X^m & X^{m+1} & \cdots & 0\\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\
0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & m\tilde{p}X^{n-2} & X^{n-1}
\end{pmatrix}.$$

我们可以看出

$$\det(\Lambda) = N^{\frac{m(m-1)}{2}} X^{\frac{n(n-1)}{2}}.$$

所以, LLL 算法可以计算出 Λ 中长度小于 $2^{\frac{n-1}{4}} N^{\frac{m(m-1)}{2n}} X^{\frac{(n-1)}{2}}$ 的短向量 $\boldsymbol{v}$. 设 $\boldsymbol{v}$ 对应多项式 $g(x)$ (次数至多为 $n-1$).

由于 $u_j(x_0) \equiv 0 \pmod{N^m}$, 所以, $g(x_0) \equiv 0 \pmod{N^m}$. 我们选取的 m 和 t 只要满足

$$2^{\frac{n-1}{4}} N^{\frac{m(m-1)}{2n}} X^{\frac{(n-1)}{2}} \leqslant \frac{N^m}{\sqrt{n}}$$

即可. 总结一下, 有

(1) $|x_0| \leqslant X$;

(2) $g(x_0) \equiv 0 \pmod{N^m}$;

(3) $\|\boldsymbol{v}\| \leqslant \frac{N^m}{\sqrt{n}}$.

由 Howgrave-Graham 引理 [61, 62] 可知 $g(x_0) = 0$, 于是 (整数) x_0 可被计算出来. Coppersmith 方法的更多信息可参见文献 [62].

4.2 基于格的密码学的几个例子

基于格的密码学是一个成熟的研究与应用领域, 有许许多多的新思想、新设计. 格密码学的潜在的抵抗来自量子计算机的攻击的特性更是为相关算法协议的研究与实现提供了新的动力, 使之蓬勃发展. 著名的基于格的密码学设计包括 Ajtai-Dwork 格密码体制、Goldreich-Goldwasser-Halevi 公钥加密和签名系统, NTRU 系统、基于 SIS (short integer solution) 的密码系统、基于 LWE 的密码系统、基于身份的加密系统和全同态加密系统等 (参见文献 [63]).

本节将介绍目前人们关心的几个格密码系统.

4.2.1 NTRU

著名的公钥系统 NTRU 由 Hoffstein 等 [16, 64] 于 20 世纪 90 年代发明并不断加工, 成为今天运算效率最高的格上密码系统之一, 并被认为是量子时代替换 RSA 和 ECC (elliptic curve cryptography) 的一个选项.

NTRU 加密系统的工作对象是环 $R = \mathbb{Z}[x]/(x^N - 1)$, 并取 p 和 q 满足 $\gcd(p, q) = 1$. 具体描述如下. 公钥/私钥对的产生过程: 选取小系数多项式 $f, g \in R$, 并计算

$$F_q = f^{-1} \pmod{q}, \quad F_p = f^{-1} \pmod{p}, \quad h = gF_q \pmod{q}.$$

系统的公钥是 h, 私钥是 (f, F_p).

加密: 将明文编码成一个 $\pmod{p}$ 的多项式 m, 随机取一个小系数多项式 r, 得到密文

$$c = prh + m \pmod{q}.$$

解密: 用私钥 (f, F_p) 对 c 解密的过程如下: 先计算 $a = cf \pmod{q}$, 再选取适当的 A 使 a 的系数皆在区间 $[A, A+q)$ 内. 最后 $aF_p \pmod{p}$ 即为明文 m.

现在考虑 NTRU 加密系统的格论解释. 将公钥 h 写成 $h = h_0 + h_1 x + \cdots + h_{N-1}x^{N-1}$, 记

$$H = \begin{pmatrix} h_0 & h_{N-1} & \cdots & h_1 \\ h_1 & h_0 & \cdots & h_2 \\ \vdots & \vdots & \ddots & \vdots \\ h_{N-1} & h_{N-2} & \cdots & h_0 \end{pmatrix},$$

并考虑 $2N \times 2N$ 矩阵

$$\boldsymbol{B}_h = \begin{pmatrix} I_N & 0 \\ H & qI_N \end{pmatrix}.$$

设 Λ_h 为由 $\boldsymbol{B}_h$ (列向量) 生成的格. 设 f 和 g 的系数为 $f_0, \ldots, f_{N-1}$, $g_0, \ldots, g_{N-1}$, 我们看到

$$(f_0, \ldots, f_{N-1}, g_0, \ldots, g_{N-1})^\top = \boldsymbol{B}_h (f_0, \ldots, f_{N-1}, u_0, \ldots, u_{N-1})^\top,$$

其中 $u_0, \ldots, u_{N-1}$ 为多项式

$$u(x) = \frac{g(x) - f(x)h(x)}{q} \pmod{x^N - 1}$$

的系数. 这表明 $(f_0, \ldots, f_{N-1}, g_0, \ldots, g_{N-1})^\top$ 是格 Λ_h 中的短向量 (f 和 g 的系数皆很小). 所以, 若能计算 Λ_h 的 SVP, 便有可能求出密钥 (f, F_p). 另外, 给定公钥和密文, 求解明文的问题可以归结为 Λ_h 的 CVP 问题.

我们需要指出的是, NTRU 的设计不是建立在最坏情况困难性与平均情况困难性归约基础上的, 缺少严格意义上的安全性证明. 2011 年, Stehlé 和 Steinfeld [65] 在形如 $\mathbb{Z}[x]/(x^{2^m}+1)$ 的环上建立了可证明安全的 NTRU, 这个构造的抗量子性质目前也受到关注. 在更一般分圆环上可证明安全的 NTRU 的构造由 Yu 等 [66]、Wang 和 Wang [67] 给出.

4.2.2 LWE 问题及相关的格上加密体系

首先给出 Regev [14] 的 LWE 问题的定义. 给定二元组

$$(\boldsymbol{A}, \boldsymbol{b}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m,$$

其中 $\boldsymbol{A}$ 依平均分布取自 $\mathbb{Z}_q^{m\times n}$, 且有依平均分布取自 $\mathbb{Z}_q^n$ 的 $\boldsymbol{s}$ 和依 (独立的取整的) Gauss 分布取自 $\mathbb{Z}_q^m$ 的 $\boldsymbol{e}$ 使得 $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e}$. 我们的任务如下:

- (判定形式的 LWE) 以不可忽略的概率区分 $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e}$ 和依平均分布取自 $\mathbb{Z}_q^m$ 的向量 $\boldsymbol{b}'$;
- (搜索形式的 LWE) 求解 $\boldsymbol{s}$.

Regev 证明了两种形式的等价性, 且在量子归约下, 一个求解 LWE 的有效算法可以导致近似因子为 $\tilde{O}(\frac{n}{\alpha})$ (Gauss 分布中的宽度为 αq, 且 $\alpha q > \sqrt{n}$) 的 GapSVP 和 SIVP 的有效量子算法. 在经典意义下 LWE 到 GapSVP 的归约由 Peikert [68] 和 Brakerski 等 [69] 给出.

下面介绍 Regev [14] 的基于 LWE 的公钥加密系统. 取素数 p 满足 $n^2 < p < 2n^2$,

$$m = (1+\varepsilon)(n+1)\log p, \quad \alpha(n) = o\left(\frac{1}{\sqrt{n}\log n}\right).$$

定义 $\mathbb{Z}_p$ 上的分布 χ 为

$$\chi(k)=\int_{\frac{k-\frac{1}{2}}{p}}^{\frac{k+\frac{1}{2}}{p}}\sum_{j\in\mathbb{Z}}\frac{1}{\alpha(n)}\rho\left(\frac{x-j}{\alpha(n)}\right)dx.$$

公钥/私钥对的产生过程: 首先在 $\mathbb{Z}_p^{m\times n}$ 中依平均分布随机选取 $\boldsymbol{A}$, 在 $\mathbb{Z}_p^n$ 中依平均分布随机选取 $\boldsymbol{s}$. 再取 $\boldsymbol{e}\in\mathbb{Z}_p^m$ 使其分量相互独立地服从分布 χ. 计算 $\boldsymbol{b}=\boldsymbol{A}\boldsymbol{s}+\boldsymbol{e}$. 系统的公钥是 $(\boldsymbol{A},\boldsymbol{b})$, 私钥是 $\boldsymbol{s}$.

加密: 明文 b 是一个比特. 加密者随机选取 $\boldsymbol{x}\in\{0,1\}^m$ (看成列向量), 计算密文

$$c=\left(\boldsymbol{A}^\top\boldsymbol{x},\left\lfloor\frac{p}{2}\right\rfloor\cdot b+\boldsymbol{x}^\top\boldsymbol{b}\right).$$

解密: 用私钥 $\boldsymbol{s}$ 对 $c=(\boldsymbol{r},t)$ 解密如下: 计算 $y=(t-\boldsymbol{r}^\top\boldsymbol{s})\pmod p$. 明文由下式给出:

$$b=\begin{cases}0, & \text{如果 } y \text{ 接近 } 0,\\ 1, & \text{如果 } y \text{ 接近 } \left\lfloor\dfrac{p}{2}\right\rfloor.\end{cases}$$

Regev 加密体系的安全性是建立在 LWE 问题的困难性基础上的, 有经典意义上的安全性证明.

利用 LWE (以及环上 LWE) 构造 Diffie-Hellman 类型的密钥交换协议于 2011 年由 Ding 提出. 2012 年, Ding 等 [70] 给出了详细描述. 相似的思想在文献 [71] 中给出并由 Alkim 等 [72] 实现.

4.2.3 基于 LWE 的全同态加密体制

全同态加密是由 Rivest 等 [73] 在 1978 年提出的关于隐私保护的设想. 数学上的要求是数据的运算与加密运算可以交换, 这样加密了的用户数据可以在不必解密的情形下被服务提供方 (如云) 进行计算, 其结果还是密文, 而用户只需对结果施行解密便能得到数据的实际运算值. 以全同态公钥体制为例, 其形式定义如下: 设 pk 和 sk 分别为体制的公钥和私钥, 我们称该体制是一个全同态加密体制, 如果存在一个求值算法 Eval, 使得对每个函数 $f:\{0,1\}^*\to\{0,1\}$ 和每个长度适当的字符串 $x\in\{0,1\}^*$, 加密函数 Enc 和解密函数 Dec 满足

$$\mathrm{Dec}_{sk}(\mathrm{Eval}(f,\mathrm{Enc}_{pk}(x)))=f(x),$$

或运算 f 和 Enc 可交换:

$$\mathrm{Eval}(f,\mathrm{Enc}_{pk}(x))=\mathrm{Enc}_{pk}(f(x)).$$

这个方面的重大突破发生在 2009 年. Gentry [17] 第一个构造出了全同态公钥加密系统, 所使用的数学对象是理想格. 一个有效的全同态加密通常由某个有扰动的线性函数给出, 解密的条件要求随机扰动项很小. 一般情形下, 全同态体制需要多个解密运算, 常导致扰动误差急剧增大而无法正确解密. Gentry 提出了一个极其巧妙的想法, 把解密函数和密钥当成一般函数和数据看待, 利用同态性质不断解密进而降低误差增长的速率. 这个思想叫作 Bootstrapping 过程. Gentry 的创造性工作引发了一系列后续研究, 可参见文献 [74–81]. 这里简要介绍 Gentry 等 [82] 和 Shai [83] 在 2013 年提出的基于 LWE 的全同态体制.

我们需要先介绍 Gadget 陷门. 设 q 为 LWE 中的模数, 令 $\ell=\lceil\log_2 q\rceil$. 定义 Gadget 矩阵 $\boldsymbol{G}$ 如下:

$$\boldsymbol{g}=(1,2,\ldots,2^{\ell-1})^\top\in\mathbb{Z}_q^\ell,\quad \boldsymbol{G}=\boldsymbol{I}_n\otimes\boldsymbol{g}^\top\in\mathbb{Z}_q^{n\times n\ell}.$$

我们将 $\mathbb{Z}_q$ 中的元数 u 表成二进制, 即 $u = b_0 + 2b_1 + \cdots + 2^{\ell-1}b_{\ell-1}$, 其中 $b_i \in \{0,1\}$. 记

$$\mathbf{bin}(u) = (b_0, b_1, \ldots, b_{\ell-1}).$$

定义映射

$$\begin{aligned}&\boldsymbol{G}^{-1} : \mathbb{Z}^n \to \mathbb{Z}^{n\ell},\\&(u_1, \ldots, u_n)^\top \mapsto (\mathbf{bin}(u_1), \ldots, \mathbf{bin}(u_n))^\top.\end{aligned}$$

$\boldsymbol{G}^{-1}$ 的作用还可以自然地推广到矩阵上. 我们有

$$\boldsymbol{G}\boldsymbol{G}^{-1}(u_1, \ldots, u_n)^\top = (u_1, \ldots, u_n)^\top.$$

矩阵 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ 的以可逆 (或零) 矩阵 $\boldsymbol{H} \in \mathbb{Z}_q^{n\times n}$ 为标签的陷门是任意一个充分 "短" 的矩阵 $\boldsymbol{R} \in \mathbb{Z}^{n\times n\ell}$ 使得

$$\boldsymbol{A}\boldsymbol{R} \equiv \boldsymbol{H}\boldsymbol{G} \pmod q.$$

陷门的质量由 $\boldsymbol{R}$ 的最大奇异值 $s_1(\boldsymbol{R}) = \max_{\|\boldsymbol{u}\|=1} \|\boldsymbol{R}(\boldsymbol{u})\|$ 决定, $s_1(\boldsymbol{R})$ 越小, 表示 $\boldsymbol{R}$ 的质量越高. 例如, 当 $\boldsymbol{R}$ 的元素服从参数为 s 的离散 Gauss 分布时, $s_1(\boldsymbol{R})$ 以高概率约等于 $O(s(\sqrt{m} + \sqrt{n\ell}))$.

GSW (Gentry-Sahai-Waters) 的全同态加密系统的公钥是

$$\boldsymbol{A} = \begin{pmatrix}\boldsymbol{B}\\ \boldsymbol{b}^\top\end{pmatrix},$$

其中我们依平均概率随机选取 $\boldsymbol{B} \in \mathbb{Z}_q^{(n-1)\times m}$, $\boldsymbol{b} = \boldsymbol{B}^\top\boldsymbol{t} + \boldsymbol{e}$ ($\boldsymbol{e}$ 为以某种分布随机选取的小扰动), 而私钥为 $\boldsymbol{s} = \binom{-\boldsymbol{t}}{1}$. 我们注意到 $\boldsymbol{A}^\top\boldsymbol{s} = \boldsymbol{e} \approx \boldsymbol{0}$.

对比特 $x \in \{0,1\}$ 进行加密, 首先随机选取小系数矩阵 $\boldsymbol{R} \in \mathbb{Z}^{m\times n\ell}$, 所得密文为下面的矩阵 $\boldsymbol{C} \in \mathbb{Z}_q^{n\times n\ell}$:

$$\boldsymbol{C} = x\boldsymbol{G} - \boldsymbol{A}\boldsymbol{R}.$$

这表明, $\binom{\boldsymbol{R}}{\boldsymbol{I}}$ 是矩阵 $[\boldsymbol{A}|\boldsymbol{C}]$ 的以 $x\boldsymbol{I}$ 为标签的陷门. 直接计算 $\boldsymbol{s}^\top\boldsymbol{C}$, 便可用密钥 $\boldsymbol{s}$ 对密文 $\boldsymbol{C}$ 进行解密.

关于基本同态性质, 加法同态是平凡的. 现设 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 分别为 x_1 和 x_2 的密文, 考虑 $\boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)$:

$$\boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) = (x_1\boldsymbol{G} - \boldsymbol{A}\boldsymbol{R}_1)\boldsymbol{G}^{-1}(\boldsymbol{C}_2) = x_1\boldsymbol{C}_2 - \boldsymbol{A}\boldsymbol{R}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) = x_1x_2\boldsymbol{G} - \boldsymbol{A}\boldsymbol{R}',$$

其中

$$\boldsymbol{R}' = \boldsymbol{R}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) + x_1\boldsymbol{R}_2.$$

值得注意的是 $\boldsymbol{G}^{-1}$ 变换可将 (低维) 长向量变成平缓的 (高维) 短向量, 又因 $\boldsymbol{R}_1$ 有较好的质量, 所以 $\boldsymbol{R}'$ 是小系数矩阵, 进而 $\boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)$ 是乘积 x_1x_2 的密文. 同理, 解密后的扰动误差的上界也能得到较好的控制. 这使得对任意层次的布尔电路施行 Bootstrapping 成为可能, 于是得到一个全同态加密.

我们通常只需核验可表示任意布尔电路的 NAND 运算的同态性质, 其中 $\mathrm{NAND}(x_1, x_2) = 1 - x_1x_2$. 它所对应的密文记为 $\mathrm{homNAND}(\boldsymbol{C}_1, \boldsymbol{C}_2)$, 其表达式为 $\mathrm{homNAND}(\boldsymbol{C}_1, \boldsymbol{C}_2) = \boldsymbol{G} - \boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) \pmod q$.

5 结束语

格理论的发展过程一直是与数学内部和外部对它的需要紧密相连的. 对格论中重要的未决问题展开研究, 进一步发掘格论与数学和计算科学等方面的非平凡联系将是长期的有意义的科学方向, 也是日益增长的实践需求. 今天我们似乎更加需要了解格论问题的广阔的计算前景和多样的密码学应用潜力. 同时, 来自计算机科学和密码学的促进也会使格理论愈加丰富.

致谢 作者感谢审稿人对本文提出的有益意见, 也感谢郑中翔博士在本文的写作过程中所提供的协助.

参考文献

1 Gauss C F. Disquisitiones Arithmeticae. New York-Berlin-Heidelberg-Tokyo: Springer-Verlag, 1966
2 Minkowski H. Geometrie der Zahlen. Leipzig: Teubner, 1896
3 Hermite C. Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objects de la théorie des nombres. J Reine Angew Math, 1850, 1850: 279–315
4 Lenstra A K, Lenstra Jr H W, Lovász L. Factoring polynomials with rational coefficients. Math Ann, 1982, 261: 515–534
5 Adleman L M. On breaking the iterated Merkle-Hellman public-key cryptosystem. In: Advances in Cryptology. Boston: Springer, 1982, 303–308
6 Brickell E F. Breaking iterated knapsacks. In: Advances in Cryptology. Lecture Notes in Computer Science, vol. 196. Berlin: Springer, 1984, 342–358
7 Lagarias J C, Odlyzko A M. Solving low-density subset sum problems. J ACM, 1985, 32: 229–246
8 Coppersmith D. Finding a small root of a univariate modular equation. In: Proceedings of the 15th Annual International Conference on Theory and Application of Cryptographic Techniques. Berlin-Heidelberg: Springer-Verlag, 1996, 155–165
9 Coppersmith D. Finding a small root of a bivariate integer equation; factoring with high bits known. In: Advances in Cryptology. Lecture Notes in Computer Science, vol. 1070. Berlin-Heidelberg: Springer, 1996, 178–189
10 Boneh D, Venkatesan R. Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes. In: Advances in Cryptology. Lecture Notes in Computer Science, vol. 1109. Berlin-Heidelberg: Springer, 1996, 129–142
11 Boneh D, Shparlinski I E. On the unpredictability of bits of the elliptic curve Diffie-Hellman scheme. In: Advances in Cryptology. Lecture Notes in Computer Science, vol. 2139. Berlin-Heidelberg: Springer, 2001, 201–212
12 Ajtai M. Generating hard instances of lattice problems (extended abstract). In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. New York: Association for Computing Machinery, 1996, 99–108
13 Ajtai M, Dwork C. A public-key cryptosystem with worst-case/average-case equivalence. In: Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing. New York: Association for Computing Machinery, 1997, 270–299
14 Regev O. On lattices, learning with errors, random linear codes, and cryptography. In: Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing. New York: Association for Computing Machinery, 2005, 84–93
15 Goldreich O, Goldwasser S, Halevi S. Public-key cryptosystems from lattice reduction problems. In: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology. Berlin-Heidelberg: Springer-Verlag, 1997, 112–131
16 Hoffstein J, Pipher J, Silverman J H. NTRU: A ring-based public key cryptosystem. In: Proceedings of the Third International Symposium on Algorithmic Number Theory. Berlin-Heidelberg: Springer-Verlag, 1998, 267–288
17 Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: Association for Computing Machinery, 2009, 169–178
18 Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Washington: IEEE Computer Society, 1994, 124–134
19 Serre J P. A Course in Arithmetic. Graduate Texts in Mathematics, vol. 7. New York: Springer, 1973
20 Banaszczyk W. New bounds in some transference theorems in the geometry of numbers. Math Ann, 1993, 296: 625–635
21 Banaszczyk W. Inequalities for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$. Discrete Comput Geom, 1995, 13: 217–231
22 Tian C, Liu M, Xu G. Measure inequalities and the transference theorem in the geometry of numbers. Proc Amer

Math Soc, 2014, 142: 47–57
23 Zheng Z, Zhao C, Xu G. Discrete Gaussian measures and new bounds of the smoothing parameter for lattices. Appl Algebra Engrg Comm Comput, 2020, doi: 10.1007/s00200-020-00417-z
24 Cai J. A new transference theorem in the geometry of numbers and new bounds for Ajtai's connection factor. Discrete Appl Math, 2003, 126: 9–31
25 Wei W, Tian C, Wang X. New transference theorems on lattices possessing n^{ε}-unique shortest vectors. Discrete Math, 2014, 315–316: 144–155
26 Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. SIAM J Comput, 2007, 37: 267–302
27 Peikert C. Limits on the hardness of lattice problems in ℓ_p norms. Comput Complexity, 2008, 17: 300–351
28 Gentry C, Peikert C, Vaikuntanathan V. How to use a short basis: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing. New York: Association for Computing Machinery, 2008, 197–206
29 Lagarias J C, Lenstra Jr H W, Schnorr C P. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. Combinatorica, 1990, 10: 333–348
30 Schnorr C P. A hierarchy of polynomial time lattice basis reduction algorithms. Theoret Comput Sci, 1987, 53: 201–224
31 Chen Y, Nguyen P Q. BKZ 2.0: Better lattice security estimates. In: Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security. Berlin-Heidelberg: Springer-Verlag, 2011, 1–20
32 Gama N, Nguyen P Q, Regev O. Lattice enumeration using extreme pruning. In: Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin-Heidelberg: Springer-Verlag, 2010, 257–278
33 Kannan R. Improved algorithms for integer programming and related problems. In: Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing. New York: Association for Computing Machinery, 1983, 193–206
34 Helfrich B. Algorithms to construct Minkowski reduced and Hermite reduced lattice bases. Theoret Comput Sci, 1985, 41: 125–139
35 Hanrot G, Stehlé D. Improved analysis of Kannan's shortest lattice vector algorithm. In: Proceedings of the 27th Annual International Cryptology Conference on Advances in Cryptology. Berlin-Heidelberg: Springer-Verlag, 2007, 170–186
36 Fincke U, Pohst M. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. Math Comp, 1985, 44: 463–471
37 Schnorr C P, Euchner M. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. Math Program, 1994, 66: 181–199
38 Schnorr C P. Lattice reduction by random sampling and birthday methods. In: Proceedings of the 20th Annual Symposium on Theoretical Aspects of Computer Science. Berlin-Heidelberg: Springer-Verlag, 2003, 145–156
39 Ding D, Zhu G, Wang X. A genetic algorithm for searching the shortest lattice vector of SVP challenge. In: Proceedings of the 2015 Annual Conference on Genetic and Evolutionary Computation. New York: Association for Computing Machinery, 2015, 823–830
40 Fukase K M. An accelerated algorithm for solving SVP based on statistical analysis. J Inf Process, 2015, 23: 67–80
41 Zheng Z, Wang X, Xu G, et al. Orthogonalized lattice enumeration for solving SVP. Sci China Inf Sci, 2018, 61: 032115
42 Ajtai M, Kumar R, Sivakumar M. A sieve algorithm for the shortest lattice vector problem. In: Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing. New York: Association for Computing Machinery, 2001, 601–610
43 Nguyen P Q, Vidick T. Sieve algorithms for the shortest vector problem are practical. J Math Cryptol, 2008, 2: 181–207
44 Wang X, Liu M, Tian C, et al. Improved Nguyen-Vidick heuristic sieve algorithm for shortest vector problem. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. New York: Association for Computing Machinery, 2011, 1–9
45 Micciancio D, Voulgaris P. Faster exponential time algorithms for the shortest vector problem. In: Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms. Philadelphia: SIAM, 2010, 1468–1480
46 Pujol X, Stehlé D. Solving the shortest lattice vector problem in time $2^{2.465n}$. Https://eprint.iacr.org/2009/605, 2009
47 Becker A, Gama N, Joux A. Solving shortest and closest vector problems: The decomposition approach. Https://eprint.iacr.org/2013/685, 2013
48 Becker A, Ducas L, Gama N, et al. New directions in nearest neighbor searching with applications to lattice sieving. In: Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms. Philadelphia: SIAM,

2016, 10–24
49 Laarhoven T, Mosca M, van de Pol J. Solving the shortest vector problem in lattices faster using quantum search. In: Post-Quantum Cryptography. Lecture Notes in Computer Science, vol. 7932. Berlin-Heidelberg: Springer, 2013, 83–101
50 Micciancio D, Voulgaris P. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. SIAM J Comput, 2013, 42: 1364–1391
51 Aggarwal D, Dadush D, Regev O, et al. Solving the shortest vector problem in 2^n time using discrete Gaussian sampling. In: Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing. New York: Association for Computing Machinery, 2015, 733–742
52 Cai J, Nerurkar A. An improved worst-case to average-case connection for lattice problems. In: Proceedings of the 38th Annual Symposium on Foundations of Computer Science. Washington: IEEE Computer Society, 1997, 468–477
53 Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. In: Proceedings of the 45th Annual Symposium on Foundations of Computer Science. Washington: IEEE Computer Society, 2004, 372–381
54 Cusick T W. The Ajtai random class of lattices. Theoret Comput Sci, 1999, 226: 29–36
55 Merkle R C, Hellman M E. Hiding information and signatures in trapdoor knapsacks. IEEE Trans Inform Theory, 1978, 24: 525–530
56 Shamir A. A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. IEEE Trans Inform Theory, 1984, 30: 699–704
57 Coster M J, Joux A, LaMacchia B A, et al. An improved low-density subset sum algorithm. In: Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques. Berlin-Heidelberg: Springer-Verlag, 1991, 54–67
58 Nguyen P Q, Stern J. The two faces of lattices in cryptology. In: Cryptography and Lattices. Lecture Notes in Computer Science, vol. 2146. Berlin-Heidelberg: Springer, 2001, 146–180
59 Coppersmith D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J Cryptology, 1997, 10: 233–260
60 Coppersmith D. Finding small solutions to small degree polynomials. In: Cryptography and Lattices. Lecture Notes in Computer Science, vol. 2146. Berlin-Heidelberg: Springer, 2001, 20–31
61 Howgrave-Graham N. Finding small roots of univariate modular equations revisited. In: Proceedings of Cryptography and Coding. Lecture Notes in Computer Science, vol. 1355. Berlin-Heidelberg: Springer, 1997, 131–142
62 May A. Using LLL-reduction for solving RSA and factorization problems: A survey. In: The LLL Algorithm. Berlin-Heidelberg: Springer, 2010, 315–348
63 Peikert C. A decade of lattice cryptography. Found Trends Theor Comput Sci, 2014, 10: 283–424
64 Hoffstein J, Pipher J, Silverman J H. NTRU: A new high speed public key cryptosystem. Https://web.securityinnovation.com/hubfs/files/ntru-orig.pdf, 1996
65 Stehlé D, Steinfeld R. Making NTRU as secure as worst-case problems over ideal lattices. In: Advances in Cryptology. Lecture Notes in Computer Science, vol. 6632. Berlin-Heidelberg: Springer-Verlag, 2011, 27–47
66 Yu Y, Xu G, Wang X. Provably secure NTRU instances over primecyclotomic rings. In: Public-Key Cryptography–PKC 2017. Lecture Notes in Computer Science, vol. 10174. Berlin-Heidelberg: Springer, 2017, 409–434
67 Wang Y, Wang M. Provably secure NTRUEncrypt over any cyclotomic field. In: Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 11349. Cham: Springer, 2018, 391–417
68 Peikert C. Public-key cryptosystems from the worst-case shortest vector problem. In: Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing. New York: Association for Computing Machinery, 2009, 333–342
69 Brakerski Z, Langlois A, Peikert C, et al. Classical hardness of learning with errors. In: Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing. New York: Association for Computing Machinery, 2013, 575–584
70 Ding J, Xie X, Lin X. A simple provably secure key exchange scheme based on the learning with errors problem. Https://eprint.iacr.org/2012/688, 2012
71 Peikert C. Lattice cryptography for the internet. In: Post-Quantum Cryptography. Lecture Notes in Computer Science, vol. 8772. Cham: Springer, 2014, 197–219
72 Alkim E, Ducas L, Pöppelmann T, et al. Post-quantum key exchange: A new hope. In: Proceedings of the 25th USENIX Conference on Security Symposium. Berkeley: USENIX Association, 2016, 327–343
73 Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms. Found Secure Comput, 1978, 4: 169–180
74 van Dijk M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers. In: Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin-Heidelberg: Springer-Verlag, 2010, 24–43

75 Gentry C. Toward basing fully homomorphic encryption on worst-case hardness. In: Proceedings of the 30th Annual Conference on Advances in Cryptology. Berlin-Heidelberg: Springer-Verlag, 2010, 116–137
76 Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. In: Proceedings of the 52nd Annual Symposium on Foundations of Computer Science. Washington: IEEE Computer Society, 2011, 97–106
77 Coron J-S, Mandal A, Naccache D, et al. Fully homomorphic encryption over the integers with shorter public keys. In: Proceedings of the 31st Annual Conference on Advances in Cryptology. Berlin-Heidelberg: Springer-Verlag, 2011, 487–504
78 Brakerski Z. Fully homomorphic encryption without modulus switching from classical GapSVP. In: Proceedings of the 32nd Annual Cryptology Conference on Advances in Cryptology. Berlin-Heidelberg: Springer-Verlag, 2012, 868–886
79 Gentry C, Halevi S, Smart N P. Fully homomorphic encryption with polylog overhead. In: Proceedings of the 31st Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin-Heidelberg: Springer-Verlag, 2012, 465–482
80 Cheon J H, Coron J-S, Kim J, et al. Batch fully homomorphic encryption over the integers. In: Proceedings of the 32nd Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin-Heidelberg: Springer-Verlag, 2013, 315–335
81 Smart N P, Vercauteren F. Fully homomorphic SIMD operations. Des Codes Cryptogr, 2014, 71: 57–81
82 Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In: Advances in Cryptology. Lecture Notes in Computer Science, vol. 8042. Berlin-Heidelberg: Springer, 2013, 75–92
83 Shai H. Homomorphic encryption. In: Tutorials on the Foundations of Cryptography Dedicated to Oded Goldreich. Cham: Springer, 2017, 219–276

Computational aspects of lattices and their cryptographic applications

Guangwu Xu & Xiaoyun Wang

Abstract This paper surveys some fundamental computational lattice problems and several classical primitives of lattice based cryptography. The paper tries to reflect some mathematical insights of the related problems. The paper starts with basic concepts and basic tools for lattice theory, followed by more detailed description of several classes of lattice algorithms. Some important cryptographic constructions of lattice cryptography are described in the last part of the paper.

Keywords **lattices, short vector algorithms, lattice based cryptography**

MSC(2010) **11H06, 11T71, 94A60**

doi: 10.1360/SSM-2020-0174