密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2014,1(1):13–27

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax:+86-10-81033101

格密码学研究*

王小云[1], 刘明洁[2]

1. 清华大学 高等研究院, 北京 100084
2. 北京大学 北京国际数学研究中心, 北京 100871
通讯作者: 王小云, E-mail: xiaoyunwang@tsinghua.edu.cn

摘 要: 格密码是一类备受关注的抗量子计算攻击的公钥密码体制. 格密码理论的研究涉及的密码数学问题很多, 学科交叉特色明显, 研究方法趋于多元化. 格密码的发展大体分为两条主线: 一是从具有悠久历史的格经典数学问题的研究发展到近 30 多年来高维格困难问题的求解算法及其计算复杂性理论研究; 二是从使用格困难问题的求解算法分析非格公钥密码体制的安全性发展到基于格困难问题的密码体制的设计. 本文从格困难问题的计算复杂性研究、格困难问题的求解算法、格密码体制的设计以及格密码分析四个方面较为全面地回顾了格密码领域 30 多年来的主要研究成果, 并试图体现四个研究领域方法的渗透与融合. 此外, 对与格密码理论研究有重要影响的一些格数学问题的经典研究方法与成果本文也进行了简单的描述.

关键词: 格理论; 密码分析; 格密码体制; 格困难问题; 计算复杂性
中图法分类号: TP309.7 **文献标识码:** A

中文引用格式: 王小云, 刘明洁. 格密码学研究[J]. 密码学报, 2014, 1(1): 13–27.
英文引用格式: Wang X Y, Liu M J. Survey of lattice-based cryptography[J]. Journal of Cryptologic Research, 2014, 1(1): 13–27.

Survey of Lattice-based Cryptography

WANG Xiao-Yun[1], LIU Ming-Jie[2]

1. Institute for Advanced Study, Tsinghua University, Beijing 100084, China
2. Beijing International Center for Mathematical Research, Peking University, Beijing 100871, China
Corresponding author: WANG Xiao-Yun, E-mail: xiaoyunwang@tsinghua.edu.cn

Abstract: Lattice-based cryptography is widely believed to resist quantum computer attacks, which involves many cryptographic mathematical problems and belongs to interdisciplinary study. The development of lattice-based cryptography follows two main lines: One is to study the computational complexity and searching algorithms for solving hard problems in high dimensional lattices based on the research of classical lattice problems. The other is to analyze the security of non-lattice-based public-key cryptosystems using the algorithms solving hard lattice problems, and further to design the lattice-based cryptosystems. This paper gives a survey of the main progress on lattice-based cryptography in recent 30 years, which covers the following concerns: computational complexity and searching algorithms relating to hard lattice problems, design and cryptanalysis of lattice-based cryptosystems. The paper tries to reflect the relationship of these four areas. In addition, some classical lattice problems and relative important results are described.

* 基金项目: 国家自然科学基金重点项目(61133013); 国家重点基础研究发展计划(973 计划)(2013CB834205)
收稿日期: 2013-12-15 定稿日期: 2014-01-04

Key words: lattice theory; cryptanalysis; lattice-based cryptosystem; hard lattice problems; computational complexity

1 前言

格理论的研究源于 1611 年开普勒提出的如下猜想: 在一个容器中堆放等半径的小球所能达到的最大密度是 $\pi/\sqrt{18}$. 1840 年前后, 高斯引进了格的概念并证明: 在三维空间堆球, 如果所有的球心构成一个格, 那么堆积密度所能达到的最大值是 $\pi/\sqrt{18}$. 在过去的一个半世纪中, Minkowski、Hermite、Bourgain、Hlawka、Kabatyansky、Levenstein、Lovasz、Mahler、Rogers 等著名数学家系统地发展了一般几何体的格堆积与覆盖理论. 在这一发展过程中, 确定一个给定几何体的最大格堆积密度和最小格覆盖密度一直是这一学科的核心问题.

格是 R^m 中一类具有周期性结构离散点的集合. 严格地说, 格是 m 维欧式空间 R^m 的 $n(m \geq n)$ 个线性无关向量组 $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n$ 的所有整系数线性组合, 即

$$\boldsymbol{L}(\boldsymbol{B}) = \left\{ \sum_{i=1}^{n} x_i \boldsymbol{b}_i : x_i \in Z, i = 1, \cdots, n \right\}$$

向量组 $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n$ 称为格的一组基. 同一个格可以用不同的格基表示. m 称为格的维数, n 称为格的秩. 满足 $m = n$ 的格称为满秩的. 通常我们只考虑满秩的格. 下面我们介绍格理论中一些基本概念和困难问题.

格的行列式: 格的行列式 $\det(\boldsymbol{L})$ 的值定义为格基本体 $\mathcal{P}(\boldsymbol{B}) = \left\{ \sum_{i=1}^{n} x_i \boldsymbol{b}_i, 0 \leq x_i < 1 \right\}$ 的体积, 容易证明有 $\det(\boldsymbol{L}) = \mathrm{vol}(\mathcal{P}(\boldsymbol{B})) = \sqrt{\boldsymbol{B}^{\mathrm{T}} \boldsymbol{B}}$, 其中 $\boldsymbol{B}$ 是以格基为列向量构成的矩阵.

对偶格: 对偶格与原格在同一个线性空间 R^m 中, 定义为 $\boldsymbol{L}^* = \left\{ \boldsymbol{x} \in R^m, \forall \boldsymbol{v} \in \boldsymbol{L}, \langle \boldsymbol{x}, \boldsymbol{v} \rangle \in Z \right\}$.

逐次最小长度: 第 i 个逐次最小长度 λ_i, 定义为以原点为球心, 包含 i 个线性无关格向量的最小球的半径, 即 $\lambda_i(\boldsymbol{L}) = \inf \left\{ r \middle| \dim\left(\mathrm{span}\left(\boldsymbol{L} \bigcap \boldsymbol{B}_n(r) \right) \right) \geq i \right\}, (i = 1, \cdots, n)$.

最短向量问题(Shortest Vector Problem, SVP): 给定格 $\boldsymbol{L}$, 找一个非零格向量 $\boldsymbol{v}$, 满足对任意非零向量 $\boldsymbol{u} \in \boldsymbol{L}, \|\boldsymbol{v}\| \leq \|\boldsymbol{u}\|$.

γ -近似最短向量问题(SVP-γ): 给定格 $\boldsymbol{L}$, 找一个非零格向量 $\boldsymbol{v}$, 满足对任意非零向量 $\boldsymbol{u} \in \boldsymbol{L}, \|\boldsymbol{v}\| \leq \gamma \|\boldsymbol{u}\|$.

逐次最小长度问题(Successive Minima Problem, SMP): 给定一个秩为 n 的格 $\boldsymbol{L}$, 找 n 个线性无关的向量 $\boldsymbol{s}_i$, 满足 $\lambda_i(\boldsymbol{L}) = \|\boldsymbol{s}_i\|, (i = 1, \cdots, n)$.

最短线性无关向量问题(Shortest Independent Vector Problem, SIVP): 给定一个秩为 n 的格 $\boldsymbol{L}$, 找 n 个线性无关的格向量 $\boldsymbol{s}_i$ 满足 $\|\boldsymbol{s}_i\| \leq \lambda_n(\boldsymbol{L}), (i = 1, \cdots, n)$.

唯一最短向量问题(Unique Shortest Vector Problem, uSVP-γ): 给定格 $\boldsymbol{L}$, 满足 $\lambda_2(\boldsymbol{L}) > \gamma \lambda_1(\boldsymbol{L})$, 找该格的最短向量.

最近向量问题(Closest Vector Problem, CVP): 给定一个格 $\boldsymbol{L}$ 和目标向量 $\boldsymbol{t} \in R^m$, 找一个非零格向量 $\boldsymbol{v}$, 满足对任意非零向量 $\boldsymbol{u} \in \boldsymbol{L}, \|\boldsymbol{v} - \boldsymbol{t}\| \leq \|\boldsymbol{u} - \boldsymbol{t}\|$.

有界距离解码问题(Bounded Distance Decoding, BDD-γ): 给定一个格 $\boldsymbol{L}$，目标向量 $\boldsymbol{t}$ 满足 $\mathrm{dist}(\boldsymbol{t},\boldsymbol{L})<\gamma\lambda_1(\boldsymbol{L})$，找一个非零格向量 $\boldsymbol{v}$，满足对任意非零向量 $\boldsymbol{u}\in\boldsymbol{L}$, $\|\boldsymbol{v}-\boldsymbol{t}\|\le\|\boldsymbol{u}-\boldsymbol{t}\|$.

判定版本 γ-近似最短向量问题(GapSVP-γ): 给定格 $\boldsymbol{L}$ 和一个有理数 r，如果 $\lambda_1(\boldsymbol{L})\le r$，则返回“是”; 如果 $\lambda_1(\boldsymbol{L})>\gamma r$，则返回“否”. 其他情况随机返回“是”或“否”.

堆积半径: 对 n 维格，以格点为球心，r 为半径做 n 维球，使得球两两不相交，最大的 r 称作堆积半径. 事实上这里 $r=\lambda_1(\boldsymbol{L})/2$.

覆盖半径: 对 n 维格，以格点为球心，r 为半径做 n 维球，能覆盖整个空间的最小 r 称作覆盖半径.

事实上，确定球的最大格堆积密度等价于求格的最短向量(SVP)的长度，确定球的最小格覆盖密度则等价于求到格点的最近距离(CVP). 因此格中困难问题既是经典数论也是计算复杂性理论的重要研究课题. 近 30 年来，在格中困难问题的复杂性与求解算法方面，国际上取得了许多重要成果. 随着对格困难问题算法研究的深入，研究人员发现格理论在密码分析与设计中都有很广泛的应用. 基于格的密码体制的安全性依赖于格中困难问题的难解程度，格中很多困难问题被证明是 NP 困难的，因此这类体制被普遍认为具有抗量子攻击的特性.

本文主要描述格的困难问题的计算复杂性研究，格困难问题的求解算法以及基于格的密码分析与设计. 本文剩余的内容安排如下: 第二章主要介绍格中计算问题困难性研究的主要成果，第三章就格中困难问题的搜索算法展开论述，第四章讨论了格中困难问题的算法在公钥密码分析中的几个重要成果，第五章针对基于格的密码体制的设计的主要成果做了回顾，最后在第六章中给出总结.

2 格中计算问题的困难性

格中最短向量问题是数论中的经典问题, 1850 年, Hermite 证明了对于任意一个 n 维格最短向量的长度小于 $\gamma_n\det(\boldsymbol{L})$，其中 γ_n 是 Hermite 常数. 1905 年 Minkowski 证明了 $n/2\pi e+O(n)\le\gamma_n\le 2n/\pi e$ [1,2]. 1978 年 Kabatyanskii 和 Levenshtein 将 γ_n 的上界改进到 $1.744n/2\pi e$ [3]. 这些结果给出了最短向量长度的一个上界，为密码学家在该问题的研究提供了重要的参考.

1981 年, Van Emde Boas[4]就证明了 l_∞ 范数下的精确 SVP 问题是 NP-hard 的，并猜测 l_2 范数下 SVP 同样是 NP-hard 的. 直到 1998 年，Ajtai[5]证明了 l_2 范数下近似因子小于 $\gamma=1+1/2^{n^\varepsilon}$ 的最短向量问题在随机归约下是 NP-Hard 的，即不存在有效的多项式算法求解近似因子为 $\gamma=1+1/2^{n^\varepsilon}$ 的 SVP 问题. 随后 Cai 与 Nerurkar[6]将 SVP 在随机归约下 NP-hard 的近似因子提高到 $\gamma=1+1/n^\varepsilon$. Miccinacio[7]考虑了一般范数度量下的最短向量问题，基于一个数论猜想将 $l_p(p\ge1)$ 下 SVP-γ问题的 NP-hard 因子提高到 $\gamma=\sqrt{2}$. 2005 年, Khot[8]指出在随机归约下任意常数近似因子的 SVP-γ是 NP-hard 的，并且在更强的复杂性假设 $\mathrm{NP}\not\subseteq\mathrm{RTIME}\left(2^{\mathrm{poly}(\log n)}\right)$ 下 SVP-γ($\gamma=2^{(\log n)^{1/2-\varepsilon}}$)是 NP-hard，在同样假设下，Haviv 与 Regev 利用基于张量积的格构造归约技术又将近似因子提高到 $\gamma=2^{(\log n)^{1-\varepsilon}}$. 进一步，若 $\mathrm{NP}\not\subseteq\mathrm{RSUBEXP}$，则 NP-hard 因子可达到 $n^{c/\log\log n}$，其中 $c>0$ 为一常数. 对 l_1 和 l_∞ 范数的 SVP 问题目前最好的结果分别是被证明在近似因子小于 $2-\varepsilon$ [7]和 $n^{c/\log\log n}$ [9]时，相应的近似 SVP 是 NP-hard 的. 到目前为止，具有 NP-hard 困难性的 SVP 问题不仅被广泛地用于格密码体制的设计，其快速求解算法也被计算机科学家与密码学家广泛研究.

CVP 问题的困难性研究方面, Van Emde Boas[4]首先指出精确 CVP 是 NP-C 问题. 利用 PCP 机器证明，Arora、Babai、Sweedyk 等指出任意常数近似因子的 CVP-γ问题是 NP-hard 的，并且在较强的复杂性假设 $\mathrm{NP}\not\subseteq\mathrm{RTIME}\left(2^{\mathrm{poly}(\log n)}\right)$ 下, NP-hard 的因子可以改进到 $\gamma=2^{(\log n)^{1-\varepsilon}}$. 目前最好的 CVP-γ复杂性结果

是 Dinur, Kindler 等[10]给出的，即 $\gamma = n^{c/\log\log n}$ 时的 CVP-γ 问题是 NP-hard 的.

对于 SIVP-γ 问题的复杂性, 1999 年, Blomer 与 Seifert[11]利用格嵌入构造技术，证明在复杂性假设 $NP \not\subseteq RP$ 下，任意常数近似因子的 SIVP 是 NP-hard 的. Regev 与 Rosen[12]研究了一般范数下该问题的困难性，基于范数嵌入技术，证明对任意的 $l_p(1 \le p \le \infty)$，在复杂性假设 $NP \not\subseteq RP$ 下，任意常数近似因子的 SIVP 是 NP-hard 的，在更强的复杂性假设 $NP \not\subseteq RTIME\left(2^{poly(\log n)}\right)$ 下, NP-hard 因子可以达到 $2^{(\log n)^{1-\varepsilon}}$.

一个自然的问题是：当近似因子继续增大时，格问题的困难性会怎样呢？显然 $\gamma = 2^{poly(n)}$ 时，由 LLL 算法可知格问题是容易求解的. 那么格问题 NP 困难性的近似因子的上界是怎样的？利用 Banaszczyk[13]给出的主对偶格的反转定理可知近似因子为 n 的 GapSVP 属于 coNP，因此若 $GapSVP_n$ 是 NP-hard 的，则 NP=coNP，这是不可能的. 1999 年 Goldreich 与 Goldwasser[14]采用交互证明协议证明了近似因子为 $O(\sqrt{n/\log n})$ 的 GapCVP，GapSVP 属于 CoAM . 2005 年 Aharonov 与 Regev[15]利用格上离散高斯测度理论研究了此问题，指出近似因子为 $O\left(\sqrt{n}\right)$ 的判定版本 CVP 属于 CoNP. 以上两个结果分别表明在不同的复杂性假设 $NP \not\subseteq CoAM$， $NP \not\subseteq CoNP$ 下， $GapCVP_{\sqrt{n/\log n}}$ 和 $GapCVP_{\sqrt{n}}$ 不是 NP-hard 的. 利用常规范数不等式可知，对一般 $l_p(1 \le p \le \infty)$ 范数下的 GapSVP 与 GapCVP 问题也有类似的结果.

同时，对于以上三个问题的难易程度，密码学家也进行了广泛研究. 这些问题之间关系的研究，帮助研究者提高了对基于这些困难问题的密码体制的安全性的认识. Goldreich, Miccinacio, Safra 等[16]首先指出 SVP-γ 不会难于 CVP-γ，2008 年，Miccinacio[17]证明了 SIVP-γ 可以归约为 CVP-γ，并且 $\gamma = 1$ 时 SIVP 与 CVP 是等价的，文献[18]中还给出了这些问题的变体 GapSVP-γ、uSVP-γ 与 BDD 问题在小多项式逼近因子内的等价性.

在格困难问题的归约中，反转定理是一个重要的工具. 它是数的几何的经典问题，其目的主要是研究原格与对偶格上某些不变量之间的关系，如逐次最小长度、覆盖半径以及最短基的长度等. 为了更精确地研究 Ajtai[19]提出的 worst-case 到 average-case 的归约因子, Cai 和 Micciancio 等人利用反转定理改进了其归约因子[20,21]; 2008 年, Micciancio 将其应用到 CVP 到 SIVP 的保持维数的归约中[17]; 1999 年, J. Blömer 等人证明了近似因子为 $O(n)$ 的 SVP、SIVP 以及 SBP 问题在 Karp-归约下不可能是 NP-hard 的除非 $NP = coNP$ [11]. 经典的反转定理主要研究 $\max_{1 \le i \le n} \lambda_i(\boldsymbol{L})\lambda_{n-i+1}\left(\boldsymbol{L}^*\right)$ 的上界问题，从最初的超指数上界到第一个多项式界的出现经历了半个世纪. 1939 年，Mahler 基于经典的数的几何学研究理论证明了 $(n!)^2$ 的上界，该结果于 1959 年被 Cassels 改进到 $n!$. 1990 年, Lagarias[22]等人利用 Korkin-Zolotarev 约化基的性质得到了第一个多项式上界 $n^2/6(n \ge 7)$. 直到 1993 年，Banaszczyk[13]证明了最优的上界为 $O(n)$. 2003 年，为了改进 Ajtai 的 worst-case 到 average-case 的归约因子, Cai 首次研究了带 gap 的格的反转定理，并得到了一些初步结果[23]. 2013 年，Wang 等解决了带 gap 的格的相关反转定理[24]. 此类问题的研究不仅在格困难问题的归约上有重要应用，而且在基于格的密码体制分析中也有潜在的作用，这是由于当前大部分格密码体制的密码格在连续短向量之间都有一定的 gap.

3 求解格中困难问题的算法

在格的复杂性理论不断取得突破的同时，密码学家在求解 SVP、CVP 的算法方面也做了很多突破性的工作. 求解最短向量问题的算法可以分为两类：精确算法和近似算法. 精确算法可以证明能找到最短向量，近似算法的输出是一个满足长度小于某个界的非零的短向量. 由于求解最短向量问题是 NP-Hard 的，在高维情况下，实际中只能使用近似算法. 但这两类算法是互为补充，不可分割的. 近似

算法往往需要低维的精确算法作为子程序, 选择不同维数的低维格对应不同的近似因子和时间复杂度. 另一方面, 现在所有的精确求解最短向量的算法, 都需要调用近似算法作为预处理, 得到一组约化基或者初始输入格点. 在实际中, 预处理的好坏对精确算法的效率有很大的影响.

3.1 近似算法

在近似算法方面, 目前多项式时间内仅能解决近似因子为 $2^{O(n\log\log n/\log n)}$ 的短向量和近似最近向量问题[25,26].

第一个也是最著名的求解近似 SVP 问题的算法是由 H. Lenstra, A. Lenstra, Lovasz 在 1982 年提出的 LLL 算法[27]. 该算法在多项式时间内, 输出近似因子为 $((1+\varepsilon)\sqrt{4/3})^{(n-1)/2}$ 的短向量, ε 是一个正常数. LLL 算法的提出对格理论的研究, 特别是公钥密码算法分析起到了很大的推动作用, 不仅是在密码领域, LLL 算法在计算代数、计算数论等领域也有广泛的应用, 已被公认为是 20 世纪最重要的算法之一. 在 LLL 算法提出 25 周年的 2007 年, 密码学家在法国卡昂大学举行了纪念大会, 研究人员就 14 个与 LLL 密切相关的研究课题 25 年来的进展在大会上做了报告, 并出版了纪念论文集. 该书已成为研究格密码学的重要参考文献.

1987 年 Schnorr[28]利用分块约化的方法推广了 LLL 算法, 算法需要多项式次调用求解 k 维格最短向量的算法, 近似因子降为 $O\left(\left(6k^2\right)^{n/k}\right)$, 使得近似因子和时间复杂度实现了部分的平衡. 目前理论上最好的求解近似短向量算法是 Gama 和 Nguyen 在 2008 年提出的[29], 该算法在分块约化的基础上结合了对偶格的约化, 算法的复杂度仍是多项式次调用求解 k 维格的 SVP 算法, 近似因子降到 $\left((1+\varepsilon)\gamma_k\right)^{(n-k)/(k-1)}$, 这里 γ_k 为 Hermite 常数[1,2]. 最实用的基约化算法是 Schnorr 和 Euchner 在 1994 年提出的 BKZ 算法[30]. 2011 年, Chen 和 Nguyen[31]提出了新版本的 BKZ 算法, 在实际中大大提高了基约化算法的效率, 并且给出了精确的模拟算法, 可以估计高维情况下算法输出格基的性质和运行时间. 关于基约化算法的详细综述可以参考文献[32].

实际上, 格基约化算法的实验数据比理论结果好很多[33], 但目前还没有找到合理的解释, 一些问题仍有待进一步研究.

3.2 精确算法

精确求解最短向量问题的算法有确定性算法和随机算法两类.

最早的也是研究最多的确定性算法是枚举算法, 主要思想是先对格基进行 QR 分解, 利用正交变换不改变向量的欧氏范数长度, 把格基转化为对角线元素为 Gram-Schmidt 正交化向量长度的上三角矩阵, 进而列举出所有小于某个界的向量. 算法的效率在很大程度上依赖于格基的好坏. 枚举算法的空间复杂度都是多项式的.

最早的枚举算法是 1981 年计算数论学家 Pohst 和 Fincke[34,35]提出的, 时间复杂度是 $2^{O(n^2)}$. 1983 年 Kannan[36]提出了时间复杂度是 $2^{O(n\log n)}$ 的枚举算法, Helfrich 对该算法的复杂度做了更精确的分析得到 $n^{n/2+O(n)}$ 的界[37]. 2007 年, Hanrot 和 Stehle 给出 Kannan 算法更紧的复杂度上界 $n^{n/2e+o(n)}$ [38]. 随后, 他们利用 Ajtai 对 KZ 约化基的构造技巧, 证明存在一类输入基, 使得 Kannan 算法的复杂度至少是 $n^{n/2e+o(n)}$ [39].

实际中的枚举算法[30,40], 通常都利用裁剪技术, 以牺牲成功概率为代价降低时间复杂度. 2010 年 EUROCRYPT 上, Gama 等人系统地研究了极度裁剪技术[41], 在理论上指数阶地降低了枚举算法的复杂度, 但没有改变复杂度的主项. 同时该技术在实验中也有效地提高了枚举算法的效率.

2010 年 Micciancio 和 Voulgaris 提出了一种新的确定性算法[42], 是目前理论上最好的求解 SVP、CVP 的确定算法. 该算法把求解相关向量和 CVP 问题结合起来, 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. 算法在 $2^{2n+O(n)}$ 时间内解决了 SVP、CVP、SIVP 等格中主要困难问题, 但其空间复杂度也是指数的, 约为 $2^{n+O(n)}$.

另一类求解 SVP 问题的算法是随机算法. 2001 年 Ajtai 等提出的 AKS 筛法[26], 在当时第一次把求解最短向量问题的时间复杂度降到单指数的 $2^{O(n)}$. 2004 年 Regev[43], 2008 年 Nguyen 和 Vidick[44]先后对这个筛法的复杂度给出了更准确的估计. 2010 年, Micciancio 和 Voulgaris 利用更精确的估点方法估计该算法的时间和空间复杂度上界分别是 $2^{3.4n+O(n)}$ 和 $2^{1.97n+O(n)}$ [45]. 该改进基于数论中 1978 年 Kabatiansky 和 Levenshtein[3]提出的关于球面覆盖问题的经典结论. 同时文献[45]还提出了一种新的筛法 ListSieve, 时间和空间复杂度分别为 $2^{3.199n+O(n)}$ 和 $2^{1.325n+O(n)}$. 结合生日攻击最好的筛法可在 $2^{2.465n+O(n)}$ 的时间内找到最短向量[46].

随机筛法与枚举算法相比, 虽然在理论上有更好的时间上界, 但在实际中不如枚举算法有效. 除了存储空间的限制以外, 主要原因是为了实现算法的可证明性, 随机算法不是直接对格点进行筛, 而是对扰动点进行筛的. 扰动技术的使用大大增加了算法的复杂度, 但这种技术在实际中的作用一直不明确. 因此, 研究不带扰动的筛法更具有实际意义.

一类较为有效的随机算法是启发式算法, 该类算法基于某种随机假设, 可以直接对格点进行处理, 大大降低了算法的复杂度上界. 2008 年 Nguyen 和 Vidick[44]提出了第一个随机启发式筛法, 基于 AKS 筛法, 时间复杂度和空间复杂度分别为 $2^{0.415n+O(n)}$ 和 $2^{0.2075n+O(n)}$. ListSieve 的启发式版本[45]在实际中更为有效, 但遗憾的是它的复杂度上界没有估计. 2011 年, Wang 等提出一个两层筛的启发式随机筛法[47], 将时间复杂度降到 $2^{0.3836n+O(n)}$, 算法的空间复杂度是 $2^{0.2557n+O(n)}$. 该算法与之前的筛法不同, 利用两层筛的技术, 先用第一层中心点将格点分到不同的大球中, 再利用每个大球中的第二层中心点分别进行第二层筛, 达到压缩格点长度的目的. 这种技术减少了比较次数, 对时间和空间实现了部分平衡. 其复杂度的估计的主要工具为经典球覆盖和多重积分理论. 2013 年, Zhang 等利用这种技术进一步的提出了三层筛法[48], 时间复杂度和空间复杂度分别是 $2^{0.3778n+O(n)}$ 和 $2^{0.2833n+O(n)}$.

2013 年 Becker 等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. 时间复杂度和空间分别是 $2^{0.377n+O(n)}$ 和 $2^{0.292n+O(n)}$.

由于实用的算法通常是启发式的, 衡量他们的好坏很困难. 因此, 密码学家针对两类格设置了求最短向量的挑战[49], 鼓励研究人员寻找实际中更有效的求解最短向量的方法. 目前对 q-ary 格的挑战做到了 825 维, 背包类格做到了 128 维. SVP 挑战的提出使得研究人员对该类密码问题的难度和体制的安全强度有了更深入的认识, 也吸引了更多的研究人员从事该课题的研究.

3.3 求解 CVP 问题的算法

求解最近向量问题的算法与求解最短向量问题的算法密切相关. 对基约化算法来说, 有了一组约化基, 最直观的方法就是利用 Babai 的最近平面算法[50]求解 CVP 问题, 得到的解与该约化基 Gram-Schmidt 的性质密切相关, 一般会与求解 SVP 问题有相同阶的近似因子. 对枚举算法, 由于复杂度由枚举数量决定, 因此依赖于约化基的性质, 用枚举求解 CVP 与 SVP 也有相同阶的复杂度. 目前理论上最好的, 利用细胞结构(Voronoi Cell)求解 SVP 的算法[42], 也可在相同的时间复杂度上界内, 解决 CVP 问题. 但对求解 SVP 问题的随机算法 AKS 筛法, 若将其推广到求最近向量[51], 目前只能解决 $1+\varepsilon$ 近似的 CVP 问题, 这里 $\varepsilon>0$, 复杂度是 $2^{O((1+1/\varepsilon)n)}$, 随着 ε 的减小复杂度增大. 这个结果在文献[52]中, 被进一步推广到 l_p 范数.

BDD 问题是目标向量距格比较近的最近向量问题. 很多解码问题就是 BDD 问题. 2000 年 Klein 指出如果目标向量与格的距离小于 $O(1/n)\lambda_1$, 那么存在一个带预处理的多项式时间算法可以求解该问

题[53]. 后来利用 Aharonov 和 Regev[15]提出的离散高斯变换构造函数, 判定与格点距离的方法, 这个结果被改进到 $O\left(\sqrt{(\log n)/n}\right)$[54].

4 基于格的密码分析

事实上, 格理论第一次在密码学中应用, 是作为一种分析工具出现的. 很多非基于格的密码体制的安全性分析, 可以归约到求解格中困难问题, 进而利用求解这些困难问题的算法进行分析. 这些研究从一开始就将基于经典数学难题—分解因子问题与离散对数问题的公钥密码体制的安全性分析的研究方法进行了跨学科的思维转换,从而让人们意识到格理论的研究对公钥密码分析的重要性.

Shamir[55]在 1982 年第一次提出破解基本的 Merkel-Hellman 背包密码体制的多项式时间算法. 其主要思想是利用 H. W. Lenstra 等人[56]的理论, 即利用多项式时间内求解关于固定数量变元的整数规划解决背包密码算法中的问题. 该方法是 LLL 算法的雏形. 随后, Lagarias[57]将背包问题归约为找格中的短向量问题, 通过更有效的 LLL 算法求解. 1985 年, Lagarias 和 Odlyzko 构造了一类格, 利用 LLL 算法求解格的短向量, 从而破解了密度小于 0. 6463 的背包体制[58]. 后来通过构造不同的背包格, 该结果被改进到 0.9408[59].

4.1 基于格的 RSA 安全性分析

在 RSA 体制及其变体的分析方面, 格基约化算法也得到一些很好的分析结果. RSA 是第一个公钥密码体制, 1977 年由麻省理工学院的 Rivest, Shamir 和 Aldeman[60]设计, 可以同时用于数据加密和数字签名, 是迄今为止最著名的公钥密码算法之一. RSA 公钥密码算法的安全性依赖于 Z_N 环中求解 e 次根的(平均)困难性. 其中 $N=pq$, p 和 q 是两个大素数. 通常把求解 e 次根问题简称为 RSA 问题. 如果 N 的分解已知则计算解密密钥 d 容易, 因此求解 RSA 问题不比求解 d 和分解 N 困难.

虽然直接求解 RSA 问题是困难的, 但在知道一些额外信息的情况下, 破解 RSA 体制可以转化成求解格中困难问题, 进而利用 LLL 算法来求解. 这方面开创性的工作是 Coppersmith 在 1996 年提出的. 他的工作是通过构造格求解单变元模方程的小值解[61]和两个变元整系数方程的小值解[62]. 这两个重要定理的提出, 使得 RSA 体制的分析得到非常多的结果. 这里我们只介绍其中几个重要的结果.

注意到, 因子分解问题可以很容易的转化成求解一个二元方程的根的问题 $f(x,y)=N-xy$. Coppersmith[62]的结果表明, 对于二元方程满足 $|x|\le X, |y|\le Y, XY\le\sqrt{N}$ 的根, 可以在多项式时间能找到. 即, 如果已知 p 的高一半比特 $\tilde{p}$, 计算 $\tilde{q}=N/\tilde{p}$, 这里 $|p-\tilde{p}|\le N^{0.25}, |q-\tilde{q}|\le N^{0.25}$, 这样得到一个二元方程 $f(x,y)=N-(\tilde{p}+x)(\tilde{q}+y)$, 求它的小根 $(p-\tilde{p},q-\tilde{q})$ 即可分解 N. 也就是说已知 p 或 q 的高一半比特, 可以在多项式时间内分解 N, 这个结果也可以通过构造单变元模多项式求解[63], 并且比双变元构造方法更有效.

为了提高加密的速度, 加密者希望选择小的加密指数 e. Coppersmith[61]著名的一个结果是针对加密指数 $e=3$ 的 RSA 体制的攻击: 如果知道明文的 2/3, 即可以恢复整个明文.

小解密指数也存在格攻击, 第一个攻击是 Weiner 利用连分数方法给出的. 利用双变元模方程的小解结果, Boneh 和 Durfee 改进 Weiner 的界, 指出当 $d<N^{1-\sqrt{2}/2}\approx N^{0.292}$ 时, 可以在多项式时间内恢复 d [64]. Weiner 在给出连分数攻击的同时, 建议用中国剩余定理形式的 RSA 即 CRT-RSA 来实现 RSA 的解密或签名, 以抵抗小解密指数攻击. 但是, Bleichenbacher 和 May[65]证明当 $d_p, d_q<\min\left\{N^{1/4},(N/e)^{2/5}\right\}$ 时, 有一个启发式的算法可以利用求解格中最短向量来分解 N. 2007 年, Jechemsz 和 May 补充和改进了上述

攻击结果, 得出 $d_p, d_q < N^{0.073}$ 时可以在多项式时间内分解 N. 这种攻击的 CRT-RSA 弱密钥界跟前面的界不同, 是与加密指数 e 无关的.

Boneh 等人[66]首次提出了部分私钥泄露攻击的概念, 同时指出当加密指数 e 很小时, 泄露 d 的低 1/4 比特, 攻击者可以在以 e 和 $\log N$ 为多项式的时间内分解 N. 这些结果是 Coppersmith 的定理的直接应用. May 等相继改进了这个结果, 把公钥 e 的范围扩大到 $\phi(N)$, 并推广和改进了 Coppersmith 的格构造技术.

另外, 求解私钥 d 与分解 N 的等价性问题也是通过转化成模方程的小根问题利用 Coppersmith 的方法证明的[67,68].

4.2 其他密码体制的分析

除了上面介绍的对背包密码体制和 RSA 密码体制的结果以外, 格在 DSA 和 ECDSA 类的算法的分析方面也有很好的结果.

DSA 是美国国家标准与技术研究院(NIST)公布的签名算法的标准, 它的安全性基于有限域上的离散对数问题. ECDSA 是 DSA 的椭圆曲线版本, 安全性基于椭圆曲线上的离散对数问题.

在这两个算法中, 每一次签名都需要一个随机数 nonce, 已知这个 nonce 就可以恢复秘密密钥. 2001 年, Howgrave-Graham 和 Smart 在 DSA 部分 nonce 已知的情况下[69], 给出了一个基于格的启发式攻击. 后来, Nguyen 和 Shparlinski 改进了这个结果[70], 利用格基约化算法的界, 得到一个可证明的多项式时间攻击. 实验结果可在已知 nonce 的低 3 比特, 100 个签名的情况下恢复密钥. 这个结果可以推广到 ECDSA[71]. 2013 年, Liu 和 Nguyen 利用裁剪枚举求解 BDD 问题进一步改进了这个结果, 将 nonce 泄露的比特数降到 2 比特[72].

对 RSA 加密填充标准 PKCS#1 的选择密文攻击也可以转化成格中最近向量问题来解决[73].

利用格基约化算法, Nguyen 和 Stern 在 1998 年给出了 Ajtai-Dwork 密码体制的分析结果[74], 使得该体制在实用的参数范围内不安全; 1999 年 GGH 密码体制的 5 个挑战密文中的 4 个也被 Nguyen 利用格基约化算法成功破解[75].

NTRU 加密体制由 Hoffstein, Pipher 和 Silverman 于 1998 年提出[76], 被认为很可能是后量子时代 RSA 和椭圆曲线加密算法的替代者. 该体制的破解可以转化成求解格中最短向量或最近向量问题. 与 RSA 体制相比, NTRU 加密体制加解密速度更快, 而且随着安全参数的提高, NTRU 的速度优势更加明显. 2008 年 IEEE 标准 1363.1 制定了基于格的密码体制, 主要是NTRU 加密体制的标准. 作为基于格的密码体制, NTRU 的很多分析结果是基于格中困难问题的算法得到的, 包括直接利用格中求解最短向量的算法求秘密密钥[77], 中间相遇攻击和格攻击的混合攻击[78]等.

除此以外格理论在计算代数等领域也有很多应用. 一些数学问题可以通过转化为格基约化算法可求解的问题而得到解决. 比如, 有理数域上单变元多项式的分解问题[27], 变量个数固定的整数规划问题[56], 有限域上单变元稀疏多项式解的存在性判定[79]等.

5 基于格密码体制的设计

5.1 陷门函数的构造

1996 年 Ajtai 在他的开创性论文[19]中, 给出了一种方法构造一类随机格, 求解这个格中的短向量至少与求解最坏情况的近似最短向量一样难. 关于 average-case 到 worst-case 的归约结果将在下一节介绍.

自从 Ajtai 的工作之后, 这一类的随机格被用做许多密码元件的基础, 包括单向函数、抗碰撞的 hash 函数、公钥加密、数字签名、基于身份的加密等. 比如文献[80,81].

Ajtai 的工作还表明一个困难的随机格可以和一个相对短的格向量一起生成, 这个短向量可以作

为密码系统里的秘密密钥, 但是它的应用很少[82].

第一个基于格的密码体制是 1997 年提出的 Ajtai-Dwork 密码体制[83]. 该体制的安全性基于 Ajtai 的 average-case 到 worst-case 的归约. 之后, Goldreich, Goldwasser 和 Halevi[84]提出了更实用的 GGH 密码体制. 设计者先选择一组短的格基, 生成格, 然后将短的格基随机化生成另一组格基作为公开密钥, 短的格基是秘密密钥. 但是这种方法生成的格不是 Ajtai 提出的那类随机困难格. 虽然后来 Micciancio[85]对 GGH 的格基生成算法进行了改进, 这个体制的安全性仍然没有证明.

1999 年 Ajtai 提出了一种构造随机格和它的短格基的方法[86]. 这种生成方案有一个很重要的优势, 这类随机格服从合适的分布而且是 Ajtai 于 1996 年提出的那一类具有可证明安全性的随机格. 具体地说, 给出了一种构造随机格 $\boldsymbol{A}\in Z_q^{m\times n}$ 和它对应的垂直格 $\Lambda^{\perp}(\boldsymbol{A})=\{\boldsymbol{x}\in Z^m \mid \boldsymbol{xA}\equiv 0(\bmod q)\}$ 的线性无关短向量组 $\boldsymbol{S}\in Z^{m\times m}$ 的方法: 对奇数 $q=\mathrm{poly}(n)$, 整数 $m\geq 5n\log q$, 可以在多项式时间内构造 $(\boldsymbol{A},\boldsymbol{S})$, 其中 $\boldsymbol{A}\in Z_q^{m\times n}$ 是随机均匀的, $\boldsymbol{S}\in Z^{m\times m}$ 是对应的 $\Lambda^{\perp}(\boldsymbol{A})=\{\boldsymbol{x}\in Z^m \mid \boldsymbol{xA}\equiv 0(\bmod q)\}$ 的一个线性无关短向量组, 有 $\boldsymbol{SA}\equiv 0(\bmod q)$, 且 $\|\boldsymbol{S}\|=O(m^{2.5})$.

但是直到 2008 年 Gentry, Peikert 和 Vaikuntanathan[81]才开始用这种构造作为陷门设计密码体制. 他们在论文中提出了一种基于格困难问题 SIS_{β} 的单向陷门函数. 核心思想是给出了一种原像取样的方法. 具体地说, 使用高斯采样使得在拥有陷门的情况下求得原像. 文中提出一种有效算法, 在格基给定的情况下, 按离散高斯分布取格点, 标准差由格基施密特正交化的长度决定. 这里构造的单向陷门函数是基于 $\mathrm{SIS}_{s\sqrt{m}}$ 的. 平均情况的 SIS 问题可以多项式时间归约到最坏情况的格困难问题 SIVP. 可用于设计数字签名, 基于身份的加密方案等.

2009 年, Alwen 和 Peikert 进一步优化了 Ajtai 的结果[87], 构造出更短的格基, 在实际应用中使得归约中近似因子变小, 高斯取样中方差也变小.

具体地说给出如下两个结论: 对整数 $q=\mathrm{poly}(n)$, 整数 $m\geq 3n\log q$, 可以在多项式时间内构造 $(\boldsymbol{A},\boldsymbol{S})$, 其中 $\boldsymbol{A}\in Z_q^{m\times n}$ 是随机均匀的, $\boldsymbol{S}\in Z^{m\times m}$ 是对应的 $\Lambda^{\perp}(\boldsymbol{A})=\{\boldsymbol{x}\in Z^m \mid \boldsymbol{xA}\equiv 0(\bmod q)\}$ 的一个短格基, 有 $\boldsymbol{SA}\equiv 0(\bmod q)$, 且 $\|\boldsymbol{S}\|=O(m)$.

对于整数 $q=\mathrm{poly}(n)$, 整数 $m\geq 2n\log^2 q$, 可以在多项式时间内构造 $(\boldsymbol{A},\boldsymbol{S})$, 其中, $\boldsymbol{A}\in Z_q^{m\times n}$ 是随机均匀的, $\boldsymbol{S}\in Z^{m\times m}$ 是对应的 $\Lambda^{\perp}(\boldsymbol{A})=\{\boldsymbol{x}\in Z^m \mid \boldsymbol{xA}\equiv 0(\bmod q)\}$ 的一个短格基, 有 $\boldsymbol{SA}\equiv 0(\bmod q)$, 且 $\|\boldsymbol{S}\|=O(m^{0.5})$.

2012 年, Micciancio 等人改进了文献[81]中基于格问题的单向陷门函数生成方法[88]. 新的生成方案更快, 更简洁, 生成的单向函数困难性更高. 该方法主要用来生成 LWE 的单向陷门函数. 不仅如此, 该方法在经过一些矩阵变换之后, 可以和文献[81]的方法相类似, 生成ISIS 问题的单向函数和陷门. 这里的陷门就是对偶格的一组短格基. 所不同的是, 新的方案生成的短格基在经过施密特正交化之后, 长度更短, 因此从某种意义上来说, 新方法生成的陷门更好. 从参数方面具体来说, 两个衡量指标, m 约为 $2n\log q$, s 约为 $1.6\sqrt{n\log q}$, 均比文献[81]的方法优化了. 文中优化了以往的高斯采样技术, 使得采样过程可以并行化进行, 时间复杂度更低. 同时也使得 s 更小. 主要的优化手段是使用了 sub-Gaussian 分布的相关性质. 之所以采用高斯采样求得原像, 而不是采用确定性的 nearest-plane 算法, 是为了保证不泄露陷门的信息.

5.2 worst-case 到 average-case 的归约

1996 年 Ajtai 首次提出格的陷门单向函数的思想[19], 并开创性地给出了格中困难问题的 worst-case

到 average-case 的归约证明[83], 即格问题在最坏情况下的困难性可以归约为一类随机格中问题的困难性, 使得基于格的密码体制具有了可证明安全的性质.

5.2.1 SIS 问题

基于格的密码学中, 两类重要的 average-case 问题是模线性方程组的小整数解问题(the Small Integer Solutions problem, SIS)和机器学习理论中的 Learning With Errors problem(LWE)问题. SIS 问题的具体定义如下:

小整数解问题: 给定整数 m 、 n 、 q , Z_q 表示模 q 的剩余类群, 随机选取矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$ 和适当的界定参数 β, 求解一非零整数向量 $\boldsymbol{z}\in Z^m\setminus\{0\}$, 使得 $\boldsymbol{Az}=0 \bmod q$ 且 $\|\boldsymbol{z}\|\le\beta$.

SIS 问题是 1996 年 Ajtai 在文献[19]中提出的. 在这篇基于格的密码体制开创性的文献中, Ajtai 证明了任意 n 维格的近似因子为 γ 的 SIVP 问题(SIVP)、GapSVP 问题和 uSVP 问题可以多项式时间归约到 SIS 问题, 这里 $\gamma=n^c$. 即如果存在有效的算法解决 SIS 问题, 就可以解决 n 维最坏格的 SIVP 和 GapSVP 问题, 这两个算法的时间至多相差多项式倍. 显然, 这里的近似因子决定了 SIS 问题的困难程度, 相应的决定了基于它的密码体制的安全性. 很多密码学家为降低这个近似因子做了大量工作.

2003 年, Cai[23]等基于 Ajtai 的思想, 通过利用更精细的随机采样格点技术并将主对偶格的反转定理引入归约因子的证明, 将 SIVP 的近似因子降低到 $n^{3+\varepsilon}$, GapSVP 的近似因子降到 $n^{4+\varepsilon}$. 2004 年, Micciancio 把这两个近似因子分别降到 $n^{2.5+\varepsilon}$ 和 $n^{3+\varepsilon}$, 并且将近似因子为 $n^{2.5+\varepsilon}$ 的覆盖半径问题归约到了 SIS 问题. 目前最好的归约因子 2007 年 Micciancio 和 Regev[89]给出的, 通过引入格上的离散高斯测度这一强有力的工具, 给出了一种更有效的随机采样格点技术, 把 SIVP 和 GapSVP 的近似因子都降到 $\tilde{O}(n)$. 这里 $g(n)=\tilde{O}(f(n))$ 表示存在常数 $a,c\ge 0$ 使得 $g(n)\le af(n)\log^c f(n)$. 2007 年, Peikert 利用 Banaszczyk[90]给出的格上一般范数的高斯测度不等式, 在几乎相同归约因子 $\tilde{O}(n)$ 的情况下, 将 l_p 范数下的 SIVP 与 GapSVP 问题归约到 SIS 问题. 最近, Micciancio 与 Peikert[91]在保持 SIS 困难性不变的情况下降低了参数 q 的规模尺寸, 使其能更有效地应用于密码体制的设计. 此外, Peikert 与 Rosen 还考虑了某些特殊格的 SIVP 与 SIS 的关系, 得到了更好的归约因子. 但这些特殊格计算问题的困难性还有待进一步研究.

5.2.2 LWE 问题

LWE 问题是 2005 年 Regev[80]提出的, 具体定义如下: LWE 问题的输入是矩阵 $\boldsymbol{A}$ 和向量 $\boldsymbol{v}$, $\boldsymbol{v}=\boldsymbol{As}+\boldsymbol{e}$, 其中 $\boldsymbol{A}\in Z_q^{m\times n}$, $\boldsymbol{s}\in Z_q^n$ 分别在 $Z_q^{m\times n}$ 和 Z_q^n 中依均匀分布随机选择, 扰动变量 $\boldsymbol{e}$ 在 Z_q^m 上服从某种公开的分布. 判定版本的LWE是指区分真正的LWE实例中的 $\boldsymbol{v}$ 和在 Z_q^m 中按均匀分布随机选择的 $\boldsymbol{v}$. 搜索版本 LWE 要求恢复 $\boldsymbol{s}$.

LWE 问题的困难性也是 Regev 在 2005 年第一次研究的, 他证明了在量子归约下, LWE 至少与 worst-case 的近似因子为 $\tilde{O}(n/\alpha)$ 的 SVP, SIVP 的变体一样困难, 其中 α 是LWE实例中与扰动分布的方差有关的参数. 具体地, 若存在求解 LWE 问题的有效算法, 那么便可找到近似因子为 $\tilde{O}(n/\alpha)$ 的求解 GapSVP 与 SIVP 问题的有效量子算法.

LWE 问题的提出在基于格的密码学中引起了广泛关注, 尤其是在格密码体制的设计中有重要应用. 但起初, 该问题的困难性归约算法为量子算法, 如何去量子化成为 LWE 问题研究一个重要公开问题. 2009 年, Peikert[92]在保持近似因子不变的情况下, 给出了 $q\ge 2^{O(n)}$ 时, GapSVP 到 LWE 一个经典归约, 但此时的参数 q 很大, 使得密码体制的实用性遇到很大的障碍. 最近, Brakerski 等人[93]取得了重大突破, 证明了多项式模 q 下 LWE 问题的经典困难性, 向可证明安全的实用化格密码体制的设计迈出了

重要一步.

实际上搜索版本的 LWE 可以看做一个 m 维 q-ary 格 $\left\{\boldsymbol{y}\in Z^m \middle| \boldsymbol{y}=\boldsymbol{A}\boldsymbol{s} \bmod q, \boldsymbol{s}\in Z_q^n\right\}$ 上, 以 $\boldsymbol{v}$ 为目标向量的最近向量问题, 而该目标向量与格的距离实际上是扰动变量 $\boldsymbol{e}$ 的长度, 通常很小, 因此是一个 BDD 问题. 由于很多体制是基于 LWE 问题设计的, 特别是在现在备受关注的同态加密体制中也有很广泛的应用. 因此研究求解 LWE 问题的算法是目前很热门的研究课题, 许多求解 LWE 问题的算法相继出现.

2008 年, Micciancio 和 Regev 给出了一个对判定 LWE 问题的区分攻击[94], 区分概率是 $\exp\left(-\pi\left(\|\boldsymbol{w}\|\alpha\right)^2\right)$, 其中 $\boldsymbol{w}$ 是在 LWE 格的 q- 对偶格中找到的短向量. 2011 年在 CT-RSA 上, Linder 和 Peikert 提出了一种广义化的最近平面算法[95], 对成功概率和时间复杂度做了部分平衡. 2013 年 Liu 和 Nguyen 提出了一种随机化的多最近平面算法, 并利用裁剪枚举求解 LWE 问题, 大大改进了多最近平面算法的效率[72]. Arora 和 Ge 提出了一种代数线性化的方法, 算法关于维数是指数的, 但对扰动较小的情况可以降到亚指数的[96].

基于 LWE 问题许多密码学家设计了不同用途的格密码体制, 比如文献[92,97,98]等. 另外, 值得注意的是目前受到广泛关注的全同态加密体制很多也是基于格中困难问题设计的, 比如文献[98,99]等.

6 结论

本文从格中计算问题的困难性, 求解格中困难问题的算法, 基于格的密码分析以及格密码体制的设计四个方面, 对格密码学的主要研究进展进行了较为详细的总结. 过去 30 年来该领域丰富的研究成果表明了该领域受关注的程度. 它的学科交叉所带来的许多数学问题不仅成为密码领域重点研究的内容, 也被数学领域与计算机科学领域所关注. 格密码体制由于其运算具有线性特性比 RSA 等经典公钥密码体制具有更快的实现效率. 又由于该类密码体制安全性基于NP-Hard或者NP-C问题, 使得格密码体制成为抗量子攻击的密码体制中最核心研究领域. 此外, 由于格运算具有同态特性, 因此设计格同态加密密码体制对于解决安全云计算环境下的密文检索, 加密数据处理等方面具有潜在的应用价值. 尽管如此, 格密码理论还待于完善与发展, 无论是理论研究还是实用化密码体制的设计都具有很大的理论价值和实际意义.

References

[1] Conway J H, Sloane N J A. Sphere packings, lattices and groups[M]. Springer Berlin Heidelberg, 1999.

[2] Milnor J W, Husemoller D. Symmetric bilinear forms[M]. New York: Springer-Verlag, 1973.

[3] Kabatiansky G A, Levenshtein V I. On bounds for packings on a sphere and in space[J]. Problemy Peredachi Informatsii, 1978, 14(1): 3–25.

[4] Van Emde-Boas P. Another NP-complete partition problem and the complexity of computing short vectors in a lattice[M]. University of Amsterdam, 1981, 81(4).

[5] Ajtai M. The shortest vector problem in L2 is NP-hard for randomized reductions[C]. In: Proceedings of the 30th Annual ACM Symposium on Theory of Computing. New York: ACM, 1998: 10–19.

[6] Cai J Y, Nerurkar A. Approximating the SVP to within a factor (1-1/dim$^{\varepsilon}$) is NP-hard under randomized reductions[J]. Journal of Computer and System Sciences, 1999, 59(2): 221–239.

[7] Micciancio D. The shortest vector in a lattice is hard to approximate to within some constant[C]. In: Proceedings of 39th Annual Symposium on Foundations of Computer Science. Los Alamitos: IEEE Comp Soc, 1998: 92–98.

[8] Khot S. Hardness of approximating the shortest vector problem in lattices[J]. Journal of the ACM (JACM), 2005, 52(5): 789–808.

[9] Dinur I. Approximating SVP infinity to within almost-polynomial factors is NP-hard[J]. Theoretical Computer Science, 2002, 285(1): 55–71.

[10] Dinur I, KindlerG, Raz R, Safra S. Approximating CVP to within almost-polynomial factors is NP-hard[J]. Combinatorica, 2003, 23(2): 205–243.

[11] Blömer J, Seifert J P. On the complexity of computing short linearly independent vectors and short bases in a lattice[C]. In: Proceedings of the 31st annual ACM symposium on Theory of Computing. New York: ACM, 1999: 711–720.

[12] Regev O, Rosen R. Lattice problems and norm embeddings[C]. In: Proceedings of the 38th annual ACM Symposium on Theory of Computing. New York: ACM, 2006: 447–456.

[13] Banaszczyk W. New bounds in some transference theorems in the geometry of numbers[J]. Mathematische Annalen, 1993, 296(1): 625–635.

[14] Goldreich O, Goldwasser S. On the limits of nonapproximability of lattice problems[J]. Journal of Computer and System Sciences, 2000, 60(3): 540–563.

[15] Aharonov D, Regev O. Lattice problems in NP∩coNP[J]. Journal of the ACM (JACM), 2005, 52(5): 749–765.

[16] Goldreich O, Micciancio D, Safra S, et al. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors[J]. Information Processing Letters, 1999, 71(2): 55–61.

[17] Micciancio D. Efficient reductions among lattice problems[C]. In: Proceedings of the 19th Annual ACM-SIAM Symposium on Discrete Algorithms. Society for Industrial and Applied Mathematics, 2008: 84–93.

[18] Lyubashevsky V, Micciancio D. On bounded distance decoding, unique shortest vectors, and the minimum distance problem[C]. In: Wagner D ed. Advances in Cryptology-CRYPTO 2009. Springer Berlin Heidelberg, 2009: 577–594.

[19] Ajtai M. Generating hard instances of lattice problems[C]. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing. New York: ACM, 1996: 99–108.

[20] Cai J Y, Nerurkar A P. An improved worst-case to average-case connection for lattice problems[C]. In: Proceedings of 38th Annual Symposium on Foundations of Computer Science. IEEE Computer Society Press, 1997(38): 468–477.

[21] Micciancio D. Improved cryptographic hash functions with worst-case/average-case connection[C]. In: Proceedings of the 34th Annual ACM Symposium on Theory of Computing. New York: ACM, 2002: 609–618.

[22] Lagarias J C, Lenstra Jr H W, Schnorr C P. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice[J]. Combinatorica, 1990, 10(4): 333–348.

[23] Cai J Y. A new transference theorem in the geometry of numbers and new bounds for Ajtai's connection factor[J]. Discrete Applied Mathematics, 2003, 126(1): 9–31.

[24] Wei W, Tian C L, Wang X Y, New transference theorems on lattices possessing N^{ε}-unique shortest vectors[J]. Discrete Mathematics. 2014, 315-316: 144–155.

[25] Schnorr C P. Block reduced lattice bases and successive minima[J]. Combinatorics, Probability and Computing, 1994, 3(4): 507–522.

[26] Ajtai M, Kumar R, Sivakumar D. A sieve algorithm for the shortest lattice vector problem[C]. In: Proceedings of the 33rd Annual ACM Symposium on Theory of Computing. New York: ACM, 2001: 601–610.

[27] Lenstra A K, Lenstra H W, Lovász L. Factoring polynomials with rational coefficients[J]. Mathematische Annalen, 1982, 261(4): 515–534.

[28] Schnorr C P. A hierarchy of polynomial time lattice basis reduction algorithms[J]. Theoretical Computer Science, 1987, 53(2): 201–224.

[29] Gama N, Nguyen P Q. Finding short lattice vectors within mordell's inequality[C]. In: Dwork C ed. Proceedings of the 40th Annual ACM Symposium on Theory of Computing. New York: ACM, 2008: 207–216.

[30] Schnorr C P, Euchner M. Lattice basis reduction: improved practical algorithms and solving subset sum problems[J]. Mathematical Programming, 1994, 66(1–3): 181–199.

[31] Chen Y, Nguyen P Q. BKZ 2.0: better lattice security estimates[C]. In: Lee D H, Wang X Y eds. Advances in Cryptology-ASIACRYPT 2011. Springer Berlin Heidelberg, 2011: 1–20.

[32] Nguyen P Q, Valle B. The LLL algorithm: survey and applications[M]. Springer Berlin Heidelberg, 2009.

[33] Gama N, Nguyen P Q. Predicting lattice reduction[C]. In: Advances in Cryptology-EUROCRYPT 2008. Springer Berlin Heidelberg, 2008: 31–51.

[34] Fincke U, Pohst M. A procedure for determining algebraic integers of given norm[C]. In: Hulzen J A ed. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1983: 194–202.

[35] Pohst M. On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications[J]. ACM Sigsam Bulletin, 1981, 15(1): 37–44.

[36] Kannan R. Improved algorithms for integer programming and related lattice problems[C]. In: Proceedings of the 15th Annual ACM Symposium on Theory of Computing. New York: ACM, 1983: 193–206.

[37] Helfrich B. Algorithms to construct Minkowski reduced and Hermite reduced lattice bases[J]. Theoretical Computer Science, 1985, 41: 125–139.

[38] Hanrot G, Stehlé D. Improved analysis of Kannan's shortest lattice vector algorithm[C]. In: Menezes A ed. Advances in Cryptology-CRYPTO 2007. Springer Berlin Heidelberg, 2007: 170–186.

[39] Hanrot G, Stehlé D. Worst-case Hermite-Korkine-Zolotarev reduced lattice bases[J]. arXiv preprint arXiv:0801.3331, 2008.

[40] Stehlé D, Watkins M. On the extremality of an 80-dimensional lattice[M]. In: Hanrot G, Morain F, Thomé E eds. Algorithmic Number Theory. Springer Berlin Heidelberg, 2010: 340–356.

[41] Gama N, Nguyen P Q, Regev O. Lattice enumeration using extreme pruning[C]. In: Gilbert H ed. Advances in Cryptology-EUROCRYPT 2010. Springer Berlin Heidelberg, 2010: 257–278.

[42] Micciancio D, Voulgaris P. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations[J]. Siam Journal on Computing, 2013, 42(3): 1364–1391.

[43] Regev O. Lecture Notes on Lattices in Computer Science[EB/OL]. http://www.cs.tau.ac.il/odedr/teaching/lattices fall 2004/index. html. 2004.

[44] Nguyen P Q, Vidick T. Sieve algorithms for the shortest vector problem are practical[J]. Journal of Mathematical Cryptology, 2008, 2(2): 181–207.

[45] Micciancio D, Voulgaris P. Faster exponential time algorithms for the shortest vector problem[C]. In: Charikar M ed. Proceedings of the 21st Annual ACM-SIAM Symposium on Discrete Algorithms. Society for Industrial and Applied Mathematics, 2010: 1468–1480.

[46] Pujol X, Stehlé D. Solving the shortest lattice vector problem in Time $2^{2.465n}$[J]. IACR Cryptology ePrint Archive, 2009, 2009: 605.

[47] Wang X Y, Liu M J, Tian C L, et al. Improved Nguyen-Vidick heuristic sieve algorithm for shortest vector problem[C]. In: Bruce S N, Cheung L, Chi Kwong Hui, eds. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2011. New York: ACM, 2011: 1–9.

[48] Zhang F, Pan Y B, Hu G R. A three-level sieve algorithm for the shortest vector problem[C]. In: SAC 2013-20th International Conference on Selected Areas in Cryptography, 2013.

[49] R. Lindner, M. Ruckert. The Lattice Challenge Homepage[EB/OL], http://www. latticechallenge.org/.

[50] Babai L. On Lovász' lattice reduction and the nearest lattice point problem[J]. Combinatorica, 1986, 6(1): 1–13.

[51] Ajtai M, Kumar R, Sivakumar D. Sampling short lattice vectors and the closest lattice vector problem[C]. In: Martin D C ed. Proceedings of 17th IEEE Annual Conference on Computational Complexity. IEEE, 2002: 41–45.

[52] Blomer J, Naewe S. Sampling methods for shortest vectors, closest vectors and successive minima[J]. Theoretical Computer Science, 2009, 410(18): 1648–1665.

[53] Klein P. Finding the closest lattice vector when it's unusually close[C]. In: Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms. San Francisco: Society for Industrial and Applied Mathematics, 2000: 937–941.

[54] Liu Y K, Lyubashevsky V, Micciancio D. On bounded distance decoding for general lattices[C]. In: Díaz J, K. Jansen, Rolim J D P eds. Ninth International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2006 and Tenth International Workshop on Randomization and Computation, RANDOM 2006. Springer Berlin Heidelberg, 2006: 450–461.

[55] Shamir A. A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem[J]. IEEE Transactions on Information Theory, 1984, 30(5): 699–704.

[56] Lenstra Jr H W. Integer programming with a fixed number of variables[J]. Mathematics of Operations Research, 1983, 8(4): 538–548.

[57] Lagarias J C. Knapsack public key cryptosystems and Diophantine approximation[C]. In: Advances in Cryptology-CRYPTO '83. New York: Springer, 1984: 3–23.

[58] Lagarias J C, Odlyzko A M. Solving low-density subset sum problems[J]. Journal of the ACM, 1985, 32(1): 229–246.

[59] Coster M J, LaMacchia B A, Odlyzko A M, et al. An improved low-density subset sum algorithm[C]. In: Advances in Cryptology-EUROCRYPT '91. Workshop on the Theory and Application of Cryptographic Techniques Proceedings. Springer Berlin Heidelberg, 1991: 54–67.

[60] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120–126.

[61] Coppersmith D. Finding a small root of a univariate modular equation[C]. In: U.M. Maurer ed. Proceedings of the 1996 International Conference on the Theory and Application of Cryptographic Techniques, EUROCRYPT '96. Springer Berlin Heidelberg, 1996: 155–165.

[62] Coppersmith D. Finding a small root of a bivariate integer equation; factoring with high bits known[C]. In: U.M. Maurer ed. Proceedings of the 1996 International Conference on the Theory and Application of Cryptographic Techniques, EUROCRYPT '96. Springer Berlin Heidelberg, 1996: 178–178.

[63] Coppersmith D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities[J]. Journal of Cryptology, 1997, 10(4): 233–260.

[64] Boneh D, Durfee G. Cryptanalysis of RSA with private key d less than $N^{0.292}$[J]. IEEE Transactions on Information Theory, 2000, 46(4): 1339–1349.

[65] Bleichenbacher D, May A. New attacks on RSA with small secret CRT-exponents[C]. In: Public Key Cryptography-PKC 2006. Springer Berlin Heidelberg, 2006: 1-13.

[66] Boneh D, Durfee G, Frankel Y. An attack on RSA given a small fraction of the private key bits[C]. In: Advances in Cryptology-ASIACRYPT '98. Springer Berlin Heidelberg, 1998: 25–34.

[67] Coron J S, May A. Deterministic polynomial-time equivalence of computing the RSA secret key and factoring[J]. Journal of Cryptology, 2007, 20(1): 39–50.

[68] May A. Computing the RSA secret key is deterministic polynomial time equivalent to factoring[C]. In: Advances in Cryptology-CRYPTO 2004. Springer Berlin Heidelberg 2004: 213–219.

[69] Howgrave-Graham N A, Smart N P. Lattice attacks on digital signature schemes[J]. Designs, Codes and Cryptography, 2001, 23(3): 283–290.

[70] Nguyen P Q, Shparlinski I E. The insecurity of the digital signature algorithm with partially known nonces[J]. Journal of Cryptology, 2002, 15(3): 15–176.

[71] Nguyen P Q, Shparlinski I E. The insecurity of the elliptic curve digital signature algorithm with partially known nonces[J]. Designs, Codes and Cryptography, 2003, 30(2): 201–217.

[72] Liu M, Nguyen P Q. Solving BDD by enumeration: an update[C]. In: Dawson E ed. Cryptographers' Track at the RSA Conference 2013, CT-RSA 2013. Springer Berlin Heidelberg, 2013. 293–309.

[73] Bleichenbacher D. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS#1[C]. In: H. Krawczyk ed. Advances in Cryptology-CRYPTO '98. Springer Berlin Heidelberg, 1998: 1–12.

[74] Nguyen P, Stern J. Cryptanalysis of the Ajtai-Dwork cryptosystem[C]. In: Krawczyik H ed. Advances in Cryptology-CRYPTO '98. Springer Berlin Heidelberg, 1998: 223–242.

[75] Nguyen P. Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from Crypto '97[C]. In: Wiener M J ed. Advances in Cryptology-CRYPTO '99. Springer Berlin Heidelberg, 1999: 288–304.

[76] Hoffstein J, Pipher J, Silverman J H. NTRU: a ring-based public key cryptosystem[M]. In: Buhler J ed. Algorithmic Number Theory. Springer Berlin Heidelberg, 1998: 267–288.

[77] Coppersmith D, Shamir A. Lattice attacks on NTRU[C]. In: Proceedings of the 1997 International Conference on the Theory and Application of Cryptographic Techniques, EUROCRYPT '97. Springer Berlin Heidelberg, 1997: 52–61.

[78] Howgrave-Graham N. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU[C]. In: Advances in Cryptology-CRYPTO 2007. Springer Berlin Heidelberg, 2007: 150–169.

[79] Bi J, Cheng Q, Rojas J M. Sub-Linear Root Detection, and New Hardness Results, for Sparse Polynomials Over Finite Fields[C]. In: Monagan M B, Cooperman G, Giesbrecht M eds. 38th International Symposium on Symbolic and Algebraic Computation, ISSAC 2013. New York: ACM, 2013: 61–68.

[80] Regev O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM (JACM), 2009, 56(6): 34.

[81] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[C]. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing. New York: ACM, 2008: 197–206.

[82] Micciancio D, Vadhan S P. Statistical zero-knowledge proofs with efficient provers: lattice problems and more[C]. In: Advances in Cryptology-CRYPTO 2003. Springer Berlin Heidelberg, 2003:282–298.

[83] Ajtai M, Dwork C. A public-key cryptosystem with worst-case/average-case equivalence[C]. In: Proceedings of the 29th Annual ACM Symposium on Theory of Computing. New York: ACM, 1997: 284–293.

[84] Goldreich O, Goldwasser S, Halevi S. Public-key cryptosystems from lattice reduction problems[C]. In: Advances in Cryptology-CRYPTO '97. Springer Berlin Heidelberg, 1997: 112–131.

[85] Micciancio D. Improving lattice based cryptosystems using the Hermite normal form[M]. In: Cryptography and Lattices. Springer Berlin Heidelberg, 2001: 126–145.

[86] Ajtai M. Generating hard instances of the short basis problem[C]. In Wiedermann J, Boas P v E, Nielsen M eds. 26th International Colloquium on Automata, Languages and Programming, ICALP 1999. Springer Berlin Heidelberg, 1999: 1–9.

[87] Alwen J, Peikert C. Generating shorter bases for hard random lattices[J]. Theory of Computing Systems, 2011, 48(3): 535–553.

[88] Micciancio D, Peikert C. Trapdoors for lattices: simpler, tighter, faster, smaller[C]. In: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2012. Springer Berlin Heidelberg, 2012: 700–718.

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

[90] Banaszczyk W. Inequalities for convex bodies and polar reciprocal lattices in R^N[J]. Discrete & Computational Geometry, 1995, 13(1): 217–231.

[91] Micciancio D, Peikert C. Hardness of SIS and LWE with small parameters[C]. In: 33rd Annual International Cryptology Conference, CRYPTO 2013. Springer Berlin Heidelberg, 2013: 21–39.

[92] Peikert C. Public-key cryptosystems from the worst-case shortest vector problem[C]. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM, 2009: 333–342.

[93] Brakerski Z, Langlois A, Peikert C, et al. Classical hardness of learning with errors[C]. In: Proceedings of the 45th Annual ACM Symposium on Symposium on Theory of Computing. New York: ACM, 2013: 575–584.

[94] Micciancio D, Regev O, Lattice-based cryptography[C]. In Bernstein D J, Buchmann J, Dahmen E eds. Proceedings of Post-Quantum Cryptography. Springer Berlin Heidelberg, 2009: 147–191.

[95] Lindner R, Peikert C. Better key sizes (and attacks) for LWE-based encryption[C]. In: Kiayias A ed. Topics in Cryptology-CT-RSA 2011. Springer Berlin Heidelberg, 2011: 319–339.

[96] Arora S, Ge R. New algorithms for learning in presence of errors[M]. In: Aceto L, Henzinger M, Sgall J eds. Automata, Languages and Programming. Springer Berlin Heidelberg, 2011: 403–415.

[97] Agrawal S, Boneh D, Boyen X. Efficient lattice (H) IBE in the standard model[C]. In: Advances in Cryptology–EUROCRYPT 2010. Springer Berlin Heidelberg: 553–572.

[98] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE[C]. In: Ostrovsky R ed. 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS). New York: ACM, 2011: 97–106.

[99] Gentry C. Fully homomorphic rncryption using ideal lattices[C]. In: Proceedings of the 2009 ACM Symposium on Theory of Computing. New York: ACM, 2009: 169–178.

作者信息

王小云(1966–), 山东省诸城人, 博士, 教授, 博士生导师, 中国密码学会副理事长, 清华大学杨振宁讲座教授. 教育部长江学者特聘教授, 国家杰出青年基金获得者, 清华大学密码理论与技术研究中心主任. 主要研究领域为密码学.
E-mail: xiaoyunwang@tsinghua.edu.cn

刘明洁(1985–), 山东省济南市人, 博士后. 主要研究领域为基于格的密码学.
E-mail: liumj9705@pku.edu.cn