

侧信息对偶攻击

毕 蕾^{1,2}, 路献辉^{1,2,3}, 罗俊杰⁴, 王鲲鹏^{1,2}

¹中国科学院信息工程研究所网络空间安全防御全国重点实验室 北京 中国 100085

²中国科学院大学网络空间安全学院 北京 中国 100049

³密码科学技术国家重点实验室 北京 中国 100878

⁴北京交通大学 北京 中国 100044

摘要 带错误学习(Learning with Errors, LWE)问题^[1]是构造格密码方案最常用的困难问题,在格密码方案设计中得到了广泛的应用。研究 LWE 问题的困难性对于分析这些格密码方案的安全性至关重要。原始攻击(Primal Attack)和对偶攻击(Dual Attack)是目前 LWE 问题实际安全性分析中最常用、效果最好的两种攻击方法^[2]。除了实际安全性分析中的攻击方法,2020 年, Dachman-Soled、Ducas、Gong 等人^[3]提出了利用从侧信道中得到信息改进原始攻击效果的基本框架,但并未考虑对偶攻击。最近,关于混合对偶攻击的研究^[4-7]结果显示,在许多情形下(混合)对偶攻击的效果比原始攻击更好,因此考虑如何在对偶攻击中利用侧信息是一个有意义的问题。本文研究了这一问题,给出了在对偶攻击中利用侧信息的方法并分析了它们的效果。具体地,本文考虑了 4 种类型的侧信息,结果表明,它们对于对偶攻击的影响主要体现在对于格的体积的影响上——当格的体积减小时,攻击变得容易。每种侧信息对于格的体积的影响程度不同,本文给出了在一定假设下,不同侧信息对于格体积的具体改变,据此,可分析得到它们对于对偶攻击的效果的最终影响。例如,在经典的 BKZ-core-SVP 模型下,每个完美提示的加入可将使用嵌入对偶攻击评估实际安全性的结果降低约 0.3 比特。

关键词 格;带错误学习问题;对偶攻击;侧信息

中图法分类号 TP309.7 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2026.05.20

Dual Attack with Side Information

BI Lei^{1,2}, LU Xianhui^{1,2,3}, LUO Junjie⁴, WANG Kunpeng^{1,2}

¹ SKLOIS, Institute of Information Engineering, CAS, Beijing 100085, China

² School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

³ State Key Laboratory of Cryptology, Beijing 100878, China

⁴ Beijing Jiaotong University, Beijing 100044, China

Abstract The Learning with Errors (LWE) problem^[1] is the most widely used problem in lattice-based cryptography and has been widely used in constructing lattice-based schemes. The study of the hardness of LWE is essential to analyze the security of these schemes. The primal attack and dual attack are the most common and effective attacks in the concrete security analysis of LWE^[2]. In addition to the attacks in the concrete security analysis, in 2020, Dachman-Soled, Ducas, Gong et al.^[3] pioneered a framework of using the information from side channel in the concrete security analysis and implemented it on primal attack, but they did not consider dual attack. Recently, the results of the studies on hybrid dual attack^[4-7] show that in many cases (hybrid) dual attack is more effective than primal attack, so it is an interesting open problem to study using side information in dual attack. In this paper, we study this problem. We give approaches to exploit side information in dual attack and analyze their effectiveness. Specifically, four types of side information are considered, and their effect on the dual attack is mainly on the volume of the lattice – when the volume of the lattice decreases, the attack becomes easier. Each type of side information has a different degree of influence on the volume of the lattice, and the specific changes of the lattice volume by different side information are also given in this paper under certain assumptions. Based on the changes in the lattice volume, the final impact on the effectiveness of dual attack can be analyzed. For instance, under the classical BKZ-core-SVP cost model, the integration of each perfect hint into embedded dual attack reduces the concrete security by about 0.3 bits.

Key words lattice; learning with errors problem; dual attack; side information

通讯作者: 毕蕾, 博士, Email: bilei@iie.ac.cn。

本课题得到国家自然科学基金(No. 61972391)、密码科学技术国家重点实验室开放课题项目(No. MMKFKT201810)资助。

收稿日期: 2021-04-05; 修改日期: 2021-05-31; 定稿日期: 2023-08-22

1 引言

格密码近年来广受关注, 由于其在安全性、参数尺寸、计算速度上的优势, 被认为是最有望成为后量子公钥密码算法标准的类型之一。带错误学习 (Learning with Errors, LWE) 问题^[1]是构造格密码方案最常用的困难问题, 在格密码方案设计中得到了广泛的应用。研究者利用 LWE 问题构造了一系列格密码方案, 如加密^[8]、密钥交换^[9]、数字签名^[10]、全同态加密^[11]等。

LWE 问题包括两个版本: 搜索-LWE(search-LWE)问题和判定-LWE(decision-LWE)问题, 其中搜索-LWE 问题是指, 给定 $(A, b = As + e \bmod q) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$, 求解秘密 s , 其中 s 服从 $\mathbb{Z}_q^n$ 上的某种秘密分布, 错误 e 服从某种错误分布; 判定-LWE 问题是指, 给定 $(A, b) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$, 判断 b 是通过 $b = As + e \bmod q$ 计算得到还是从 $\mathbb{Z}_q^m$ 上的均匀分布中抽取得到。

公钥密码方案的安全性基于底层问题的困难性, 因此在研究这些格密码方案的安全性时, 需要考虑 LWE 问题的困难性。目前, 格密码实际安全性分析中使用了多种攻击方法^[12], 如原始攻击(primal attack)^[13]、对偶攻击(dual attack)^[4]、解码攻击(decoding attack)^[14]、穷搜、BKW 算法^[15]、Araro-Ge 算法^[16]等, 其中原始攻击、对偶攻击、解码攻击由于用到了格基约化算法, 统称为格攻击。在所有的攻击方法中, 目前效果最好、最常用的是原始攻击和对偶攻击^[2]。

除了实际安全性分析方法外, 对基于 LWE 问题构造密码系统的安全性分析, 还有另一种更为实际的方法——侧信道攻击。美国国家标准与技术研究院^[17](National Institute of Standards and Technology, NIST)曾指出: “与那些受到侧信道攻击强烈影响的方案相比, 可以以最小的代价抵抗侧信道攻击的方案更为可取。因此, 分析方案对于主动和被动侧信道攻击的抵抗能力对于标准化进程至关重要。”

2020 年, Dachman-Soled、Ducas、Gong 等人^[3]提出了在使用原始攻击评估 LWE 问题实际安全性时利用侧信息(即从侧信道中得到的关于秘密和错误的信息)的基本框架。具体地, 原始攻击将 LWE 问题转化为有界距离解码(Bounded Distance Decoding, BDD)问题, 再归约为唯一最短向量问题(unique Shortest Vector Problem, uSVP), 之后利用 BKZ 算法进行求解。为了利用侧信息, 文献[3]将不同的侧信息形式化

为不同类型的提示(hint), 并定义了更一般的 BDD 问题版本——扭曲的有界距离解码(Distorted Bounded Distance Decoding, DBDD)问题, 然后将提示融入 DBDD 问题之中使得融入提示之后的 DBDD 问题归约得到的 uSVP 变得简单, 从而使原始攻击的效果变得更好。

文献[3]只考虑了原始攻击, 而没有考虑对偶攻击。然而, 最近的研究表明, 在许多情形下(混合)对偶攻击的效果比原始攻击更好^[4-7]。因此, 研究在对偶攻击中利用侧信息是一个有意义的问题。本文研究了这一问题, 主要研究内容及贡献如下。

1.1 研究内容及贡献

本文给出了在对偶攻击中利用侧信息形式化后得到不同类型提示的方法以及效果分析。具体地, 本文考虑了关于秘密 $s \in \mathbb{Z}_q^n$ 的四种提示, 其中前三种是文献[3]定义的, 最后一种是本文定义的:

1. 完美提示(perfect hint): $\langle u, s \rangle = h$,
2. 模提示(modular hint): $\langle u, s \rangle = h \bmod p$,
3. 近似提示(approximate hint): $\langle u, s \rangle + t = h$,
4. 模近似提示(modular approximate hint):

$\langle u, s \rangle + t = h \bmod p$,

其中, $u \in \mathbb{Z}^n$ 、 $h \in \mathbb{Z}$ 、 $p \in \mathbb{Z}$ 、 $t \in \mathbb{Z}$ 服从高斯分布 $\mathcal{G}_0$ 。

本文首先说明文献[3]中的框架不能直接用在在对偶攻击上, 主要原因在于该框架需将 LWE 问题转化为 DBDD 问题并在其中加入提示信息, 而对偶攻击无法求解 DBDD 问题。

本文选择直接利用提示词改造对偶攻击使用的格来使得攻击变得更有效。对偶攻击是通过区分分布来解决判定-LWE 问题的, 对偶攻击所使用的格的体积减小, 会使得攻击的区分优势变大, 使攻击变得更有效。因此, 本文研究了在不同的提示下, 如何构造对偶攻击所使用的格, 使格的体积尽可能小。具体地, 对于完美提示, 可将问题的维度减 1 来减小格的体积; 对于模提示, 可通过向格中加入一个向量, 使得格点变得更加密集, 来减小格的体积; 对于近似提示和模近似提示, 可以使用缩放技术^[4]来减小格的体积。四种提示对于格体积的减小程度不同, 本文在给出利用提示的方法的同时, 还分析了它们对格体积的具体影响。据此, 可分析得到对于对偶攻击最终效果的影响。

目前, 对偶攻击分为三种类型: 原始对偶攻击^[18]、嵌入对偶攻击^[9]、混合对偶攻击^[5]。对基于 LWE 问题的实用格密码算法, 混合对偶攻击最有效, 而混合对偶攻击是基于嵌入对偶攻击构造的, 因此本文

首先针对嵌入对偶攻击, 给出了利用四种提示的方法, 然后将这些方法推广到混合对偶攻击中。

1.2 组织结构

本文内容安排如下: 第2节给出预备知识, 第3、4、5、6节分别研究如何在嵌入对偶攻击中利用完美提示、模提示和近似提示、模近似提示, 第7节给出了将这些提示用于混合对偶攻击的方法, 第8节对比了不同提示在原始攻击和对偶攻击中的效果, 第9节是本文的总结和展望。

2 预备知识

2.1 符号

在本文中, 符号 $\mathbb{Z}$ 和 $\mathfrak{R}$ 表示整数集合和实数集合。向量用小写黑体字母表示(例如 $\mathbf{x}$), 矩阵用大写黑体字母表示(例如 $\mathbf{X}$), $\mathbf{x}^T$ 和 $\mathbf{X}^T$ 表示向量和矩阵的转置。符号 $\|\cdot\|$ 表示向量的二范数 ℓ_2 , 或称欧氏范数。符号 $\gcd(a, b)$ 表示 a 和 b 的最大公约数。符号 $\oplus$ 表示对于两个向量的集合 S_1, S_2 , $S_1 \oplus S_2 = \{\mathbf{v} + \mathbf{w} : \mathbf{v} \in S_1, \mathbf{w} \in S_2\}$ 。

2.2 格和格上困难问题

定义 1(格, lattice). 已知 $\mathfrak{R}^m$ 中的 n 个线性无关的行向量 $\mathbf{b}_1, \dots, \mathbf{b}_n (m \geq n)$, 这组向量的所有整系数线性组合的集合称为 Λ , 记为

$$\Lambda = \left\{ \sum_{i=1}^n x_i \mathbf{b}_i, x_i \in \mathbb{Z} \right\},$$

其中线性无关的向量组 $\mathbf{b}_1, \dots, \mathbf{b}_n (m \geq n)$ 称为格 Λ 的一组基, n 为格的秩, m 为格的维数。当 $m = n$ 时, 称 Λ 为一个满秩格。格 Λ 上的最短向量的范数记为

$$\lambda_1(\Lambda) = \min_{\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}} \|\mathbf{v}\|$$

将格 Λ 的一组基 $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathfrak{R}^m$ 表示为 $\mathbf{B}$, 则 Λ 的体积表示为 $\det(\Lambda) = \sqrt{\det(\mathbf{B}\mathbf{B}^T)}$ 。

定义 2(对偶格, dual lattice). 给定格 Λ 和它的一组基 $\mathbf{B}$, Λ 的对偶格定义为

$$\Lambda^* = \{\mathbf{x} \in \text{Span}(\mathbf{B}) : \forall \mathbf{y} \in \Lambda, \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}\},$$

其中 $\text{Span}(\mathbf{B})$ 指由 $\mathbf{B}$ 的行向量张成的空间。根据定义有 $\det(\Lambda^*) = \frac{1}{\det(\Lambda)}$ 。

定义 3(q 元格, q -ary lattice). 令 $n, m, q \in \mathbb{Z}_+$, 给定矩阵 $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, 定义如下两种 q 元格:

$$\Lambda_q(\mathbf{A}) = \{\mathbf{v} \in \mathbb{Z}^m : \exists \mathbf{w} \in \mathbb{Z}^n \text{ s.t. } \mathbf{v} = \mathbf{w}\mathbf{A}^T \bmod q\},$$

$$\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{v} \in \mathbb{Z}^m : \mathbf{v}\mathbf{A} = \mathbf{0} \bmod q\}.$$

根据定义有

$$\Lambda_q^\perp(\mathbf{A}) = q \cdot \Lambda_q(\mathbf{A})^* \text{ 和 } \Lambda_q(\mathbf{A}) = q \cdot \Lambda_q^\perp(\mathbf{A})^{[14]}.$$

定义 4(小整数解问题, Short Integer Solution problem, SIS problem). 给定模数 $q \in \mathbb{Z}_+$, 常数 $c \in \mathfrak{R}$, $\mathbf{A} \in \mathbb{Z}_q^{m \times n}, m \geq n$, 寻找非零的 $\mathbf{v} \in \mathbb{Z}^m$ 满足 $\mathbf{v}\mathbf{A} = \mathbf{0} \bmod q$ 和 $\|\mathbf{v}\| \leq c$ 。

定义 5(带错误学习问题, Learning with Errors problem, LWE problem). 给定 $n, q \in \mathbb{Z}_+$ 和取自秘密分布 $\mathcal{S}$ 的秘密 $\mathbf{s} \in \mathbb{Z}_q^n$. χ 是一整数上的错误分布, 其标准差为 σ 。则令 $\text{LWE}_{n,q,\mathcal{S},\chi}$ 表示一 $\mathbb{Z}_q^n \times \mathbb{Z}_q$ 上的概率分布, 即从 $\mathbb{Z}_q^n$ 中均匀随机地抽取 $\mathbf{a}$, 从错误分布 χ 中抽取 e , 并返回 $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ 。

给定概率分布 $\text{LWE}_{n,q,\mathcal{S},\chi}$, 可定义 LWE 问题如下。

- 搜索-LWE(search LWE)问题: 给定 m 个取自分布 $\text{LWE}_{n,q,\mathcal{S},\chi}$ 的实例, 其中 $\mathbf{s} \leftarrow \mathcal{S}$, 求解 $\mathbf{s}$;
- 判定-LWE(decision LWE)问题: 给定 m 个实例, 区分它们是来自均匀分布 $\mathcal{U}(\mathbb{Z}_q^n \times \mathbb{Z}_q)$ 还是满足 $\mathbf{s} \leftarrow \mathcal{S}$ 的分布 $\text{LWE}_{n,q,\mathcal{S},\chi}$ 。

在本文中, m 个取自分布 $\text{LWE}_{n,q,\mathcal{S},\chi}$ 的 LWE 问题实例表示为如下矩阵形式:

$$(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q),$$

其中 $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{A} \leftarrow \mathbb{Z}_q^{m \times n}$, $\mathbf{e} \leftarrow \chi^m$, $\mathbf{b} \in \mathbb{Z}_q^m$ 。

2.3 格基约化算法

格基约化算法的主要目的是优化格基质量, 即将基向量约化得更短和更加相互正交。为了衡量格基的质量, Gama、Nguyen^[19]引入了埃尔米特因子(Hermite factor), 具体地, 给定一组格基 $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subset \mathfrak{R}^m$, 它的埃尔米特因子定义为

$$\delta_0^m = \frac{\|\mathbf{b}_1\|}{\det(\Lambda)^{\frac{1}{m}}} \quad (1)$$

目前最实用、应用最广泛的格基约化算法是 BKZ 算法。BKZ 算法中最重要的参数是块大小 β , β 越大则输出基质量越好, 但算法的时间复杂度也更高。块大小为 β 的 BKZ 输出基的根-埃尔米特因子为

$$\delta_0 \approx \left(\frac{\beta}{2\pi e} (\pi\beta)^\beta \right)^{\frac{1}{2(\beta-1)}}, \quad (2)$$

对于这一假设, Chen^[20]实验验证了它的合理性。

2.4 对偶攻击

目前文献中涉及三种对偶攻击形式: 原始对偶攻击^[14]、嵌入对偶攻击^[9]、混合对偶攻击^[5]。

2.4.1 原始对偶攻击

对偶攻击(dual attack)最初是由 Micciancio、Regev^[14]提出的, 本文将这种对偶攻击称为原始对偶

攻击, 其思想是将判定-LWE 问题归约到 SIS 问题, 即给定实例 $(A, b) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$, 构造格

$$\Lambda_{\text{dual}}^\perp(A) = \{w \in \mathbb{Z}^m : w \cdot A = 0 \bmod q\},$$

格 $\Lambda_{\text{dual}}^\perp(A)$ 的一组基为

$$\begin{pmatrix} qI_n & \\ -A_2A_1^{-1} & I_{m-n} \end{pmatrix},$$

其中 $A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} \in \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^{(m-n) \times n}$ 。从格 $\Lambda_{\text{dual}}^\perp(A)$ 中抽取短向量 w , 计算 $\langle w, b \rangle$, 如果 $(A, b) \leftarrow \text{LWE}_{n,q,s,\chi}$, 那么有

$$\begin{aligned} \langle w, b \rangle &= w \cdot (As + e) + \langle w, e \rangle \\ &= \langle w, e \rangle \bmod q \end{aligned}$$

是一个很小的值, 服从一定的高斯分布。而如果 $(A, b) \leftarrow U(\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m)$, 那么有 $\langle w, b \rangle \sim U(-\frac{q}{2}, \frac{q}{2})$ 。据此, 通过区分 $\langle w, b \rangle$ 的分布即可解决判定-LWE 问题。

值得注意的是, 对于对偶攻击而言, 需要考虑最优的实例数目, 即 m 的取值。由于在对偶攻击中 w 越短, 攻击的效果越好, 因此由埃尔米特因子的定义可得, 最优的 m 是使得

$$\|w\| = \delta_0^m \det(\Lambda_{\text{dual}}^\perp(A))^{\frac{1}{m}}$$

最小的 m 。由 $\det(\Lambda_{\text{dual}}^\perp(A)) = q^n$ 可得, 最优的 m 为

$$m = \sqrt{\frac{n \log q}{\log \delta_0}}$$

2.4.2 嵌入对偶攻击

之后, Alkim、Ducas、Pöppelmann 等人^[9]针对一般形式的 LWE 问题(即秘密服从错误分布)提出了另一种对偶攻击, 本文将其称为嵌入对偶攻击。具体地, 给定实例 $(A, b) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$, 嵌入对偶攻击构造格

$$\Lambda_{\text{dual}}^E(A) = \{(w, v) \in \mathbb{Z}^m \times \mathbb{Z}^n : w \cdot A = v \bmod q\},$$

格 $\Lambda_{\text{dual}}^E(A)$ 的一组基为

$$\begin{pmatrix} qI_n & & \\ -A_2A_1^{-1} & I_{m-n} & \\ A_1^{-1} & 0 & I_n \end{pmatrix} \quad (3)$$

其中 $A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} \in \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^{(m-n) \times n}$ 。从格 $\Lambda_{\text{dual}}^E(A)$ 中抽取短向量 (w, v) , 计算 $\langle w, b \rangle$, 如果 $(A, b) \leftarrow \text{LWE}_{n,q,s,\chi}$, 那么有

$$\begin{aligned} \langle w, b \rangle &= w \cdot (As + e) + \langle w, e \rangle \\ &= \langle v, s \rangle + \langle w, e \rangle \bmod q \end{aligned}$$

是一个很小的值, 服从一定的高斯分布。而如果

$(A, b) \leftarrow U(\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m)$, 那么有 $\langle w, b \rangle \sim U(-\frac{q}{2}, \frac{q}{2})$ 。据此, 通过区分 $\langle w, b \rangle$ 的分布即可解决判定-LWE 问题。

文献[9]指出, 当从格 $\Lambda_{\text{dual}}^E(A)$ 中抽取向量有 $\|(w, v)\| = \ell$ 时, 嵌入对偶攻击的成功优势为

$$\varepsilon = 4\exp(-2\pi^2\tau^2), \quad (4)$$

其中 $\tau = \frac{\ell\sigma}{q}$, σ 是错误分布 χ 的标准差。当使用 $\frac{1}{\varepsilon^2}$ 个这样的短向量时, 可将成功概率放大到约为 1。

2.4.3 混合对偶攻击

2017 年, Albrecht^[4]提出了混合对偶攻击, 将嵌入对偶攻击和猜测相结合。具体地, 给定实例 $(A, b) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$, 如果 $(A, b) \leftarrow \text{LWE}_{n,q,s,\chi}$, 则混合对偶攻击将 s 和 A 分别分成两部分

$$s = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} \in \mathbb{Z}_q^r \times \mathbb{Z}_q^{n-r},$$

$$A = (A_1, A_2) \in \mathbb{Z}_q^{m \times r} \times \mathbb{Z}_q^{m \times (n-r)},$$

其中 $s_1 \in \mathbb{Z}_q^r$ 用于猜测, A_2 用于构造对偶格:

$$\Lambda_{\text{dual}}^E(A_2) = \{(w, v) \in \mathbb{Z}^m \times \mathbb{Z}^{n-r} : w \cdot A_2 = v \bmod q\}$$

从其中抽取短向量 (w, v) , 计算

$$\begin{aligned} \langle w, b \rangle &= w \cdot As + \langle w, e \rangle \\ &= wA_1s_1 + \langle v, s_2 \rangle + \langle w, e \rangle \bmod q, \end{aligned}$$

之后, 对于候选猜测 $\tilde{s}_1$, 区分 $\langle v, s_2 \rangle + \langle w, e \rangle = \langle w, b \rangle - wA_1\tilde{s}_1 \bmod q$ 的分布和 $\mathbb{Z}_q$ 上的均匀分布即可判断猜测是否正确。

2.5 侧信息对应的提示

文献[3]在利用侧信息时, 将侧信息形式化为 4 种类型, 本文用到了其中 3 种, 定义如下。

定义 6(完美提示, perfect hint^[3]). 关于 $s \in \mathbb{Z}^n$ 的一个完美提示是指 $u \in \mathbb{Z}^n$ 和 $h \in \mathbb{Z}$ 使得

$$\langle u, s \rangle = h$$

定义 7(模提示, modular hint^[3]). 关于 $s \in \mathbb{Z}^n$ 的一个模提示是指 $u \in \mathbb{Z}^n, p \in \mathbb{Z}_+$ 和 $h \in \mathbb{Z}$ 使得

$$\langle u, s \rangle = h \bmod p$$

定义 8(近似提示, approximate hint^[3]). 关于 $s \in \mathbb{Z}^n$ 的一个近似提示是指 $u \in \mathbb{Z}^n, t \in \mathbb{Z}$ 和 $h \in \mathbb{Z}$ 使得

$$\langle u, s \rangle + t = h,$$

其中 t 服从高斯分布 $\mathcal{G}_q$ 且与 s 互相独立。

除文献[3]给出的提示之外, 本文还定义了如下模近似提示。

定义 9(模近似提示, modular approximate hint). 关于 $s \in \mathbb{Z}^n$ 的一个模近似提示是指 $u \in \mathbb{Z}^n, t \in \mathbb{Z}$,

$h \in \mathbb{Z}$ 和 $p \in \mathbb{Z}_+$ 使得

$$\langle \mathbf{u}, \mathbf{s} \rangle + t = h \bmod p,$$

其中 t 服从高斯分布 $\mathcal{G}_q$ 且与 $\mathbf{s}$ 互相独立。

2.6 需要用到的定义和结论

定义 10(原始向量, primitive vector [3]). 一组向量 $\mathbf{v}_1, \dots, \mathbf{v}_k$ 关于 Λ 是原始的, 如果 $\Lambda \cap \text{Span}(\mathbf{v}_1, \dots, \mathbf{v}_k)$ 等于由 $\mathbf{v}_1, \dots, \mathbf{v}_k$ 生成的格。这相当于 $\mathbf{v}_1, \dots, \mathbf{v}_k$ 可以被扩展为 Λ 的一组基。如果 $k = 1$, 那么 $\mathbf{v}_1$ 是原始的意味着对于任意的整数 $i \geq 2$, 有 $\frac{\mathbf{v}_1}{i} \notin \Lambda$ 。

引理 1. 令 Λ 为一个格, Λ^* 表示它的对偶格, $p \in \mathbb{Z}_+$ 。如果 $\mathbf{v} \in \Lambda^*$ 是格 Λ^* 中的一个原始向量, 那么 $\Lambda' = \{\mathbf{x} \in \Lambda : \langle \mathbf{x}, \mathbf{v} \rangle = 0 \bmod p\}$ 是 Λ 的子格, 且满足 $\det(\Lambda') = p \cdot \det(\Lambda)$ 。

下面引理 2 给出了当 $\mathbf{v} \in \Lambda^*$ 不是原始向量时, 与引理 1 类似的结论。

引理 2. 令 Λ 为一个格, Λ^* 表示它的对偶格, $k_1, k_2 \in \mathbb{Z}_+$ 。令 $\frac{1}{k_1} \cdot \mathbf{v} \in \Lambda^*$ 表示格 Λ^* 中的一个原始向量。令 $\Lambda' = \{\mathbf{x} \in \Lambda : \langle \mathbf{x}, \mathbf{v} \rangle = 0 \bmod k_1 k_2\}$ 是 Λ 的子格, 那么有 $\det(\Lambda') = k_2 \cdot \det(\Lambda)$ 。

证明. 令 $\Lambda_{k_1} = \frac{1}{k_1} \cdot \Lambda$, 那么有 $\Lambda_{k_1}^* = k_1 \cdot \Lambda^* = k_1 \cdot \Lambda^*$ 。由 $\frac{1}{k_1} \mathbf{v} \in \Lambda^*$ 是 Λ^* 中的原始向量可知 $\mathbf{v} \in \Lambda_{k_1}^*$ 是 $\Lambda_{k_1}^*$ 中的原始向量。令 $\Lambda'_{k_1} = \{\mathbf{x} \in \Lambda_{k_1} : \langle \mathbf{x}, \mathbf{v} \rangle = 0 \bmod k_2\}$ 。根据引理 1 可知 $\det(\Lambda'_{k_1}) = k_2 \cdot \det(\Lambda_{k_1})$ 。结合 $\Lambda_{k_1} = \frac{1}{k_1} \cdot \Lambda$ 以及

$$\begin{aligned} \Lambda_2^* &= \left\{ \frac{1}{q} \cdot \mathbf{v} \in \left(\frac{1}{q} \cdot \mathbb{Z} \right)^{d_1} : \mathbf{v} = \mathbf{z} \mathbf{C}^T \bmod q \text{ for some } \mathbf{z} \in \mathbb{Z}^{d_2} \text{ and } \left\langle \frac{1}{q} \cdot \mathbf{v}, \mathbf{p} \right\rangle \in \mathbb{Z} \right\} \\ &= \left\{ \frac{1}{q} \cdot \mathbf{v} \in \left(\frac{1}{q} \cdot \mathbb{Z} \right)^{d_1} : \mathbf{v} = \mathbf{z} \mathbf{C}^T \bmod q \text{ for some } \mathbf{z} \in \mathbb{Z}^{d_2} \text{ and } \langle \mathbf{v}, \mathbf{p} \rangle = 0 \bmod q \right\} \\ &= \frac{1}{q} \cdot \{ \mathbf{v} \in \Lambda_q(\mathbf{C}) : \langle \mathbf{v}, \mathbf{p} \rangle = 0 \bmod q \} \end{aligned}$$

由 $\mathbf{p} \in \frac{1}{q} \cdot \Lambda_1 = \Lambda_q(\mathbf{C})^*$ 是 $\Lambda_q(\mathbf{C})^*$ 中的一个原始向量, 根据引理 1 有

$$\begin{aligned} \det(\{ \mathbf{v} \in \Lambda_q(\mathbf{C}) : \langle \mathbf{v}, \mathbf{p} \rangle = 0 \bmod q \}) \\ = q \cdot \det(\Lambda_q(\mathbf{C})), \end{aligned}$$

因此有 $\det(\Lambda_2^*) = q \cdot \det(\Lambda_1^*)$ 。从而有 $\det(\Lambda_2) = \frac{1}{q} \cdot \det(\Lambda_1)$ 。

2.7 文献[3]中的框架及分析

文献[3]给出了在原始攻击中使用各种不同提示的框架。这一框架基于有界距离解码(Bounded Distance Decoding, BDD)问题的变形版本——扭曲

$$\begin{aligned} \Lambda'_{k_1} &= \{ \mathbf{x} \in \Lambda_{k_1} : \langle \mathbf{x}, \mathbf{v} \rangle = 0 \bmod k_2 \} \\ &= \{ \mathbf{x} \in \frac{1}{k_1} \cdot \Lambda : \langle \mathbf{x}, \mathbf{v} \rangle = 0 \bmod k_2 \} \\ &= \frac{1}{k_1} \cdot \{ k_1 \cdot \mathbf{x} \in \Lambda : \langle \mathbf{x}, \mathbf{v} \rangle = 0 \bmod k_2 \} \\ &= \frac{1}{k_1} \cdot \{ \mathbf{x} \in \Lambda : \langle \mathbf{x}, \mathbf{v} \rangle = 0 \bmod k_1 k_2 \} \\ &= \frac{1}{k_1} \cdot \Lambda' \end{aligned}$$

可得 $\det(\Lambda') = k_2 \cdot \det(\Lambda)$ 。

下面引理 3 给出了当往一个 q 元格的格基中加入一个向量时格体积的变化。引理 3 将被用于分析模提示对于对偶攻击的影响中。

引理 3. 给定 $\mathbf{C} \in \mathbb{Z}^{d_1 \times d_2}$, 定义 $\Lambda_1 = \Lambda_q^{\perp}(\mathbf{C})$, $\Lambda_2 = \Lambda_1 \oplus \mathbb{Z} \cdot \mathbf{p} = \{ \mathbf{z} = \mathbf{v} + i \cdot \mathbf{p} : \mathbf{v} \in \Lambda_1, i \in \mathbb{Z} \}$, 其中 $\mathbf{p}$ 是 $\frac{1}{q} \cdot \Lambda_1$ 中的一个原始向量, 那么有 $\det(\Lambda_2) = \frac{1}{q} \cdot \det(\Lambda_1)$ 。

证明. 为比较格 Λ_1 与格 Λ_2 的体积, 考虑它们的对偶格。令 Λ_1^* 表示 Λ_1 的对偶格, 根据定义有 $\Lambda_1^* = \frac{1}{q} \cdot \Lambda_q(\mathbf{C})$ 。考虑格

$$\Lambda_2^* = \{ \mathbf{v} \in \Lambda_1^* : \langle \mathbf{v}, \mathbf{p} \rangle = 0 \}$$

容易验证, Λ_2 与 Λ_2^* 互为对偶格。下面证明 $\det(\Lambda_2^*) = q \cdot \det(\Lambda_1^*)$, 从而有 $\det(\Lambda_2) = \frac{1}{q} \cdot \det(\Lambda_1)$ 。由

$$\Lambda_1^* = \frac{1}{q} \cdot \Lambda_q(\mathbf{C})$$

可知

的有界距离解码(Distorted Bounded Distance Decoding, DBDD)问题, 其目标是找到目标点周围椭圆体(而不是 BDD 问题中的球体)中的格向量。原始攻击首先将 LWE 问题转化为 BDD 问题, 然后将其归约到唯一最短向量问题(unique-Shortest Vector Problem, uSVP), 再通过格基约化算法进行求解, 如图 1 所示。文献[3]中加入提示后的原始攻击, 首先将 LWE 问题视为 DBDD 问题的特殊实例, 之后将提示信息合并到 DBDD 问题的实例中。接下来, 再将包含提示信息的新 DBDD 问题实例转化为 uSVP, 这一 uSVP 比没有提示信息的原始攻击中的 uSVP 更容易求解。最后, 利用格基约化算法求解这个更容易的 uSVP, 如图 2 所示。

LWE/BDD $\longrightarrow$ uSVP $_{\Lambda'}$ $\longrightarrow$ Lattice reduction

图 1 没有提示时的原始攻击

Figure 1 Primal attack without hints

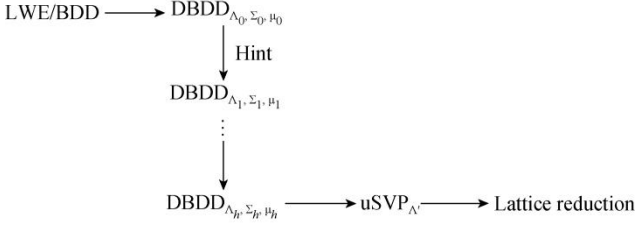


图 2 文献[3]中加入提示的原始攻击

Figure 2 Primal attack with hints in Ref.[3]

文献[3]提到该框架可以用在对偶攻击上, 然而并没有给出相关细节。事实上, 该框架不能直接用于对偶攻击, 这是因为对偶攻击不能用于求解 BDD 问题。在对偶攻击中, 需要在对偶格中寻找短向量, 如果仍然使用 DBDD 问题来合并提示信息, 转化后的包含提示信息的 DBDD 实例无法转换回 LWE 实例。因此, 此时只能通过求解 DBDD 问题(或 BDD 问题或 uSVP)来求解给定的 LWE 问题, 而该实例无法使用对偶攻击来处理。

此外, 提示对原始攻击和对偶攻击的影响也不相同。以模提示为例, 在原始攻击中加入模提示会使得原始攻击所用的格变得更加稀疏, 这是因为转化后的格是由原格与一系列平行的超平面相交形成的子格。但是, 在对偶攻击中, 以嵌入对偶攻击为例, 攻击使用的是对偶格 $\Lambda_{\text{dual}}^E(\mathbf{A}) = \{(\mathbf{w}, \mathbf{v}) \in \mathbb{Z}^m \times \mathbb{Z}^n : \mathbf{w} \cdot \mathbf{A} = \mathbf{v} \bmod q\}$, 此时模提示的作用并不是将对偶格与一系列超平面做交。事实上, 在第 4 节中可以看到, 模提示对于对偶攻击的影响是在对偶格上添加了一个新向量。

3 完美提示

本节给出将完美提示加入嵌入对偶攻击中的方法并分析产生的影响。给定一个完美提示 $\langle \mathbf{u}, \mathbf{s} \rangle = h$, 可将其展开为 $u_1 s_1 + \dots + u_n s_n = h$, 不失一般性, 此处假设 $u_1 \neq 0$, 那么有

$$s_1 = \frac{1}{u_1} (h - u_2 s_2 - \dots - u_n s_n). \quad (5)$$

即 s_1 可以用 $s_2, \dots, s_n$ 线性表示, 因此 LWE 问题 $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q)$ 的规模可减小 1 维。

具体地, 令 $\mathbf{A} = (\mathbf{A}_1 \ \dots \ \mathbf{A}_n)$, 其中 $\mathbf{A}_i$ 表示 $\mathbf{A}$ 的第 i 列。如果 $(\mathbf{A}, \mathbf{b}) \leftarrow \text{LWE}_{n,q,s,\chi}$, 那么有

$$\mathbf{A}_1 s_1 + \dots + \mathbf{A}_n s_n + \mathbf{e} = \mathbf{b} \bmod q. \quad (6)$$

将式(5)和式(6)相结合可得

$$\begin{aligned} & \left(\mathbf{A}_2 - \frac{u_2}{u_1} \mathbf{A}_1 \right) s_2 + \dots + \left(\mathbf{A}_n - \frac{u_n}{u_1} \mathbf{A}_1 \right) s_n + \mathbf{e} \\ &= \mathbf{b} - \frac{h}{u_1} \mathbf{A}_1 + q\mathbf{k}, \end{aligned}$$

其中 $\mathbf{k} \in \mathbb{Z}^m$ 。这可以看作一个新的 $n-1$ 维的 LWE 问题实例

$$\begin{aligned} \bar{\mathbf{A}} &= \left(\mathbf{A}_2 - \frac{u_2}{u_1} \mathbf{A}_1 \ \dots \ \mathbf{A}_n - \frac{u_n}{u_1} \mathbf{A}_1 \right), \\ \bar{\mathbf{s}} &= (s_2, \dots, s_n), \\ \bar{\mathbf{b}} &= \mathbf{b} - \frac{h}{u_1} \mathbf{A}_1. \end{aligned}$$

接下来需要对这个新的 LWE 问题实例使用嵌入对偶攻击, 问题的关键在于如何构造对偶格。注意到, 此时矩阵 $\bar{\mathbf{A}}$ 中的元素可能不再是整数。

3.1 失败的尝试

对这个新的 LWE 实例构造格

$$\Lambda_{\text{dual}}^E(\bar{\mathbf{A}}) = \left\{ (\mathbf{w}, \mathbf{v}) \in \mathbb{Z}^m \times \mathbb{Z}^{n-1} : \begin{aligned} & \mathbf{w} \cdot \bar{\mathbf{A}} = \mathbf{v} \bmod q \end{aligned} \right\}$$

按照式(3)中嵌入对偶攻击的格基的一般形式可尝试构造一组基为

$$\begin{pmatrix} q\mathbf{I}_{n-1} \\ -\bar{\mathbf{A}}_2 \bar{\mathbf{A}}_1^{-1} & \mathbf{I}_{m-n+1} \\ \bar{\mathbf{A}}_1^{-1} & \mathbf{0} & \mathbf{I}_{n-1} \end{pmatrix}, \quad \begin{pmatrix} q\mathbf{I}_{n-1} \\ -\bar{\mathbf{A}}_2 \bar{\mathbf{A}}_1^{-1} & \mathbf{I}_{m-n+1} \\ \bar{\mathbf{A}}_1^{-1} & \mathbf{0} & \mathbf{I}_{n-1} \end{pmatrix},$$

其中 $\bar{\mathbf{A}} = \begin{pmatrix} \bar{\mathbf{A}}_1 \\ \bar{\mathbf{A}}_2 \end{pmatrix} \in \left(\frac{1}{u_1} \mathbb{Z} \right)^{(n-1) \times (n-1)} \times \left(\frac{1}{u_1} \mathbb{Z} \right)^{(m-n+1) \times (n-1)}$ 。根据格 $\Lambda_{\text{dual}}^E(\bar{\mathbf{A}})$ 的定义, 这组基应该满足

$$\begin{pmatrix} q\mathbf{I}_{n-1} \\ -\bar{\mathbf{A}}_2 \bar{\mathbf{A}}_1^{-1} & \mathbf{I}_{m-n+1} \\ \bar{\mathbf{A}}_1^{-1} & \mathbf{0} & \mathbf{I}_{n-1} \end{pmatrix} \begin{pmatrix} \bar{\mathbf{A}}_1 \\ \bar{\mathbf{A}}_2 \\ -\mathbf{I}_{n-1} \end{pmatrix} = \mathbf{0} \bmod q. \quad (7)$$

式(7)的前 $n-1$ 行要求 $q\mathbf{I}_{n-1} \bar{\mathbf{A}}_1 = \mathbf{0} \bmod q$, 这等价于要求 $\bar{\mathbf{A}}_1 \in \mathbb{Z}^{(n-1) \times (n-1)}$, 而根据 $\bar{\mathbf{A}}$ 的构造可知这一点并不满足, 因为 $\bar{\mathbf{A}}_1 \in \left(\frac{1}{u_1} \mathbb{Z} \right)^{(n-1) \times (n-1)}$ 中可能包含非整数的元素。因此这个 $n-1$ 维的实例不能直接用嵌入对偶攻击如上求解。

3.2 正确的方法

考虑降格 $\Lambda_{\text{dual}}^E(\bar{\mathbf{A}})$ 重写作新形式

$$\Lambda_{\text{dual}}^E(\bar{\mathbf{A}}) = \left\{ (\mathbf{v}, \mathbf{w}) \in \mathbb{Z}^n \times \mathbb{Z}^m : \begin{aligned} & \mathbf{v} = \mathbf{w} \cdot \bar{\mathbf{A}} \bmod q \end{aligned} \right\}, \quad (8)$$

即 $(\mathbf{v}, \mathbf{w})$ 满足

$$(\mathbf{v} \ \mathbf{w}) \begin{pmatrix} \mathbf{I}_{n-1} \\ -\bar{\mathbf{A}} \end{pmatrix} = \mathbf{0} \bmod q$$

据此可构造格 $\Lambda_{\text{dual}}^E(\bar{\mathbf{A}})$ 的一组基为

$$\begin{pmatrix} q\mathbf{I}_{n-1} \\ \bar{\mathbf{A}} \quad \mathbf{I}_m \end{pmatrix}$$

容易验证, 这组基满足

$$\begin{pmatrix} q\mathbf{I}_{n-1} \\ \bar{\mathbf{A}} \quad \mathbf{I}_m \end{pmatrix} \begin{pmatrix} \mathbf{I}_{n-1} \\ -\bar{\mathbf{A}} \end{pmatrix} = \mathbf{0} \bmod q$$

因此, 这个 $n-1$ 维的实例可以用式(8)中的嵌入对偶攻击的格的新形式进行求解。

从格基可以看出, 格 $\Lambda_{\text{dual}}^E(\bar{\mathbf{A}})$ 的体积为

$$\det(\Lambda_{\text{dual}}^E(\bar{\mathbf{A}})) = q^{n-1},$$

与没有加入提示信息的嵌入对偶攻击的格 $\Lambda_{\text{dual}}^E(\mathbf{A})$ 相比, 有

$$\det(\Lambda_{\text{dual}}^E(\bar{\mathbf{A}})) = \frac{1}{q} \cdot \det(\Lambda_{\text{dual}}^E(\mathbf{A})),$$

即加入一个完美提示后得到的嵌入对偶攻击的格的体积降低为原来的 $\frac{1}{q}$ 。因此根据式(1)和式(2), 当使用相同块大小 β 的 BKZ 算法在这两个格中寻找短向量时, 从格 $\Lambda_{\text{dual}}^E(\bar{\mathbf{A}})$ 中抽取的短向量长度比从 $\Lambda_{\text{dual}}^E(\mathbf{A})$ 中的更短, 因此攻击也会更加有效。

注 2. 上述方法不能用于原始对偶攻击, 原因与上面失败的尝试中的原因相同。事实上, 如果用上述方法得到新的 $n-1$ 维的 LWE 问题实例, 原始对偶攻击使用格 $\Lambda_{\text{dual}}^1(\bar{\mathbf{A}}) = \{\mathbf{w} \in \mathbb{Z}^m: \mathbf{w} \cdot \bar{\mathbf{A}} = \mathbf{0} \bmod q\}$, 其中 $\bar{\mathbf{A}} \in (\frac{1}{u_1}\mathbb{Z})^{m \times (n-1)}$ 。容易验证格 $\Lambda_{\text{dual}}^1(\bar{\mathbf{A}})$ 的格基不能写作如下形式

$$\begin{pmatrix} q\mathbf{I}_{n-1} \\ -\bar{\mathbf{A}}_2\bar{\mathbf{A}}_1^{-1} \quad \mathbf{I}_{m-n+1} \end{pmatrix}.$$

因此在原始对偶攻击中利用完美提示需要其他的方法。事实上, 在原始对偶攻击中使用完美提示, 可通过将完美提示看作下一节中的 q -模提示加以利用, 通过下一节的分析可知, 这样的利用方式可将格的体积降低为 $\frac{1}{q}$, 与上述嵌入对偶攻击利用完美提示的效果相同。

4 模提示

本节给出将模提示加入嵌入对偶攻击中的方法及产生的影响。给定模提示 $\langle \mathbf{u}, \mathbf{s} \rangle = h \bmod p$, 本章按照 p 的不同分情况讨论:

1. $p = q$ 时, 称这一模提示为 q -模提示,
2. $p \neq q$ 时, 称这一模提示为 p -模提示。

4.1 q -模提示

没有加入提示信息的嵌入对偶攻击的格 $\Lambda_{\text{dual}}^E(\mathbf{A})$ 可写作

$$\Lambda_{\text{dual}}^E(\mathbf{A}) = \{(\mathbf{v}, \mathbf{w}) \in \mathbb{Z}^n \times \mathbb{Z}^m: \mathbf{v} = \mathbf{w} \cdot \mathbf{A} \bmod q\},$$

攻击需要从格 $\Lambda_{\text{dual}}^E(\mathbf{A})$ 中寻找短向量 $(\mathbf{v}, \mathbf{w}) \in \Lambda_{\text{dual}}^E(\mathbf{A})$, 使得

$$\mathbf{v} - \mathbf{w} \cdot \mathbf{A} = \mathbf{0} \bmod q,$$

得到一个 q -模提示 $\langle \mathbf{u}, \mathbf{s} \rangle = h \bmod q$ 之后, 目标可转化为寻找短向量 $(\mathbf{v}, \mathbf{w})$ 使得

$$\mathbf{v} - \mathbf{w} \cdot \mathbf{A} = \mathbf{c} \cdot \mathbf{u} \bmod q, \mathbf{c} \in \mathbb{Z}, \quad (9)$$

此时有

$$\begin{aligned} \langle \mathbf{w}, \mathbf{b} \rangle &= \mathbf{w} \cdot (\mathbf{A}\mathbf{s} + \mathbf{e}) \\ &= -\mathbf{c} \cdot \langle \mathbf{u}, \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle \\ &= -\mathbf{c} \cdot h + \langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle \bmod q, \end{aligned}$$

因此通过区分

$$\langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle = \langle \mathbf{w}, \mathbf{b} \rangle + \mathbf{c} \cdot h \bmod q$$

的分布和 $\mathbb{Z}_q$ 上的均匀分布即可解决判定-LWE 问题。因此, 当前的目标可转化为从格

$$\Lambda(\mathbf{A}, \mathbf{u}) = \left\{ \begin{pmatrix} \mathbf{v} & \mathbf{w} & c \end{pmatrix} \begin{pmatrix} \mathbf{I}_n \\ -\mathbf{A} \\ -\mathbf{u} \end{pmatrix} = \mathbf{0} \bmod q, \mathbf{c} \in \mathbb{Z} \right\}$$

中抽取短向量。接下来的问题是如何从上面的格中高效地抽取短向量。

4.1.1 简单的尝试

一个简单的寻找满足式(9)的短向量 $(\mathbf{v}, \mathbf{w})$ 的方法是将 c 视作一个变量。之后可将式(9)重写作

$$(\mathbf{v} \ \mathbf{w} \ c) \begin{pmatrix} \mathbf{I}_n \\ -\mathbf{A} \\ -\mathbf{u} \end{pmatrix} = \mathbf{0} \bmod q, \mathbf{c} \in \mathbb{Z},$$

据此可构造格

$$\Lambda_{\text{dual-side}}^E(\mathbf{A}, \mathbf{u}) = \left\{ \begin{pmatrix} \mathbf{v}, \mathbf{w}, c \end{pmatrix} \in \mathbb{Z}^n \times \mathbb{Z}^m \times \mathbb{Z}: \begin{pmatrix} \mathbf{v} & \mathbf{w} & c \end{pmatrix} \begin{pmatrix} \mathbf{I}_n \\ -\mathbf{A} \\ -\mathbf{u} \end{pmatrix} = \mathbf{0} \bmod q \right\},$$

那么当找到一个 $\Lambda_{\text{dual-side}}^E(\mathbf{A}, \mathbf{u})$ 中的短向量时, 取前 $n+m$ 位即可得到 $(\mathbf{v}, \mathbf{w})$ 满足式(9)。

这个方法等同于将 q -模提示看作一个特殊的 LWE 实例 $\langle \mathbf{u}, \mathbf{s} \rangle + \mathbf{e} = h \bmod q$, 其中错误 $\mathbf{e} = \mathbf{0}$ 。与没有添加 q -模提示的嵌入对偶攻击相比, 这样做的优势是将 τ 从 $\frac{\ell\sigma}{q}$ 降低至 $\sqrt{\frac{m-1}{m}} \cdot \frac{\ell\sigma}{q}$, 其中 τ 的含义见式(4)。然而, 由于 $\sqrt{\frac{m-1}{m}}$ 非常接近 1, 这样做的优化效果十分有限。例如, 当有 $\frac{m}{2}$ 个这样的模提示时,

仅能将 τ 降低为 $\frac{1}{\sqrt{2}}\tau$ 。

这个方法的一个弊端是将式(4)中的 c 看作目标短向量的一部分, 从而无法利用 c 可为任意大小的整数这一特点(c 不必是一个比较小的值)。根据这一特点, 下面 4.1.2 节给出了一个更高效的方法。

4.1.2 高效的方法

本节给出一个更高效的方法得到格 $\Lambda(\mathbf{A}, \mathbf{u})$ 中的短向量 $(\mathbf{v}, \mathbf{w})$ 。为此, 再次考虑格 $\Lambda_{\text{dual-side}}^E(\mathbf{A}, \mathbf{u})$, 它的一组基为

$$\mathbf{B} = \begin{pmatrix} q\mathbf{I}_n & & \\ \mathbf{A} & \mathbf{I}_m & \\ -\mathbf{u} & \mathbf{0} & 1 \end{pmatrix}$$

令 $\mathbf{B}_{n+m} \in \mathbb{Z}^{(n+m+1) \times (n+m)}$ 表示 $\mathbf{B}$ 的前 $n+m$ 列构成的矩阵, 即

$$\mathbf{B}_{n+m} = \begin{pmatrix} q\mathbf{I}_n & & \\ \mathbf{A} & \mathbf{I}_m & \\ -\mathbf{u} & \mathbf{0} & \end{pmatrix}$$

令 $\Lambda(\mathbf{B}_{n+m})$ 表示由 $\mathbf{B}_{n+m}$ 的行向量生成的格。那么寻找短向量 $(\mathbf{v}, \mathbf{w}) \in \Lambda(\mathbf{A}, \mathbf{u})$ 等价于寻找短向量 $(\mathbf{v}, \mathbf{w}) \in \Lambda(\mathbf{B}_{n+m})$ 。注意到, 每个 $(\mathbf{v}, \mathbf{w}) \in \Lambda(\mathbf{B}_{n+m})$ 都对应一个 $(\mathbf{v}, \mathbf{w}, c) \in \Lambda_{\text{dual-side}}^E(\mathbf{A}, \mathbf{u})$, 即存在 $c \in \mathbb{Z}$ 使得

$$(\mathbf{v} \quad \mathbf{w}) \begin{pmatrix} \mathbf{I}_n \\ -\mathbf{A} \end{pmatrix} = c \cdot \mathbf{u} \bmod q$$

成立, 因此这个 $(\mathbf{v}, \mathbf{w})$ 是格 $\Lambda(\mathbf{A}, \mathbf{u})$ 中的向量。

寻找 $(\mathbf{v}, \mathbf{w}) \in \Lambda(\mathbf{A}, \mathbf{u})$ 的过程如算法 1 所示, 相关结论见引理 4。

算法 1. 利用 q -模信息的嵌入对偶攻击

输入: $(\mathbf{A}, \mathbf{u})$

输出: $(\mathbf{v}, \mathbf{w})$

1. $\mathbf{P} \leftarrow$ 置换矩阵;
2. 构造格 $\Lambda_{\text{dual-side}}^E(\mathbf{A}, \mathbf{u})$ 和它的一个基 $\mathbf{B}$;
3. $\mathbf{B}_{n+m} \in \mathbb{Z}^{(n+m+1) \times (n+m)} \leftarrow$ 取 $\mathbf{B}$ 的前 $n+m$ 列;
4. $\mathbf{B}'_{n+m} \in \mathbb{Z}^{(n+m) \times (n+m)} \leftarrow$ 使用 LLL 算法消除 $\mathbf{B}_{n+m}$ 行的线性相关性, 并去掉第一行 $\mathbf{0}$ 行;
5. $(\mathbf{v}, \mathbf{w}) \leftarrow$ 在格 $\Lambda(\mathbf{B}_{n+m}) = \Lambda(\mathbf{B}'_{n+m})$ 上 1 执行 BKZ 算法, 输出基中的最短向量。

引理 4. 算法 1 输出的任意 $(\mathbf{v}, \mathbf{w})$, 都存在 $c \in \mathbb{Z}$ 使得

$$\mathbf{v} - \mathbf{w} \cdot \mathbf{A} = c \cdot \mathbf{u} \bmod q$$

证明. 对于算法 1 输出的任意一个 $(\mathbf{v}, \mathbf{w})$, 存在 $\mathbf{x} = (x_1, \dots, x_{n+m+1})$ 使得

$$(\mathbf{v}, \mathbf{w}) = \mathbf{x} \cdot \mathbf{B}_{n+m} = \mathbf{x} \cdot \begin{pmatrix} q\mathbf{I}_n & & \\ \mathbf{A} & \mathbf{I}_m & \\ -\mathbf{u} & \mathbf{0} & 1 \end{pmatrix},$$

那么用这组系数 $\mathbf{x}$ 对格 $\Lambda_{\text{dual-side}}^E(\mathbf{A}, \mathbf{u})$ 的基 $\mathbf{B}$ 进行线性组合可得到

$$\begin{aligned} \mathbf{x} \cdot \mathbf{B} &= \mathbf{x} \cdot \begin{pmatrix} q\mathbf{I}_n & & \\ \mathbf{A} & \mathbf{I}_m & \\ -\mathbf{u} & \mathbf{0} & 1 \end{pmatrix} \\ &= (\mathbf{v}, \mathbf{w}, x_{n+m+1}), \end{aligned}$$

按照格 $\Lambda_{\text{dual-side}}^E(\mathbf{A}, \mathbf{u})$ 的定义可知 $(\mathbf{v}, \mathbf{w}, x_{n+m+1})$ 满足

$$\mathbf{v} - \mathbf{w} \cdot \mathbf{A} = x_{n+m+1} \cdot \mathbf{u} \bmod q$$

即对于算法 1 输出的任意一个 $(\mathbf{v}, \mathbf{w})$, 都存在一个 $c = x_{n+m+1}$ 使得

$$\mathbf{v} - \mathbf{w} \cdot \mathbf{A} = c \cdot \mathbf{u} \bmod q$$

成立。□

4.1.3 效果预测

本节分析在嵌入对偶攻击中加入 q -模提示的效果。这一效果主要体现在对格的体积的影响上, 因此本节的目标是分析在加入 q -模提示前后嵌入对偶攻击构造格的体积变化。

当没有提示时, 需要从格 $\Lambda_{\text{dual}}^E(\mathbf{A})$ 中抽取短向量, 而当加入一个 q -模提示后, 上一节的分析说明只需从 $\Lambda(\mathbf{B}_{n+m})$ 中抽取短向量。注意到格 $\Lambda_{\text{dual}}^E(\mathbf{A})$ 和 $\Lambda(\mathbf{B}_{n+m})$ 的维度均为 $n+m$, 但它们的体积不同。根据定义可知, $\Lambda_{\text{dual}}^E(\mathbf{A})$ 是由 $\mathbf{B}_{n+m}$ 的前 $n+m$ 行生成的, 而 $\Lambda(\mathbf{B}_{n+m})$ 是由 $\mathbf{B}_{n+m}$ 的所有 $n+m+1$ 行生成的。令 $\mathbf{p} = (-\mathbf{u}, \mathbf{0})$ 表示 $\mathbf{B}_{n+m}$ 的最后一行, 那么有

$$\Lambda(\mathbf{B}_{n+m}) = \Lambda_{\text{dual}}^E(\mathbf{A}) \oplus \{i \cdot \mathbf{p} : i \in \mathbb{Z}\}$$

直接比较 $\Lambda_{\text{dual}}^E(\mathbf{A})$ 和 $\Lambda(\mathbf{B}_{n+m})$ 的体积比较困难, 但可通过比较它们的对偶格的体积来对原格的体积进行比较。根据引理 3 可知, 如果 $\mathbf{p}$ 是

$$\frac{1}{q} \cdot \Lambda_{\text{dual}}^E(\mathbf{A}) = \frac{1}{q} \cdot \Lambda_q^\perp \left(\begin{pmatrix} \mathbf{I}_n \\ -\mathbf{A} \end{pmatrix} \right)$$

中的原始向量, 那么有

$$\det(\Lambda(\mathbf{B}_{n+m})) = \frac{1}{q} \cdot \det(\Lambda_{\text{dual}}^E(\mathbf{A})),$$

即加入一个 q -模提示可以将嵌入对偶攻击的格体积降低为原来的 $\frac{1}{q}$ 。

4.2 p -模提示

一个 p -模提示可以首先转化为一个 q -模提示, 即

$$\langle \mathbf{s}, \mathbf{u} \rangle = h \bmod p \Leftrightarrow \langle \mathbf{s}, \frac{q}{p} \cdot \mathbf{u} \rangle = h \bmod q,$$

然后使用与上述 q -模提示同样的方法进行利

用。但是 p -模提示取得的效果不同。注意到, 上节中有结论: 如果 $\mathbf{p} = (-\mathbf{u}, \mathbf{0})$ 是 $\frac{1}{q} \cdot \Lambda_{\text{dual}}^E(\mathbf{A})$ 中的原始向量, 那么一个 q -模提示可以使格的体积降低为原来的 $\frac{1}{q}$ 。但一个 p -模提示对应的向量

$$\mathbf{p}_p = \frac{q}{p} \cdot \mathbf{p}$$

一定不是 $\frac{1}{q} \cdot \Lambda_{\text{dual}}^E(\mathbf{A})$ 中的原始向量。这是因为, $\frac{1}{q} \cdot \Lambda_{\text{dual}}^E(\mathbf{A})$ 的一组基为

$$\begin{pmatrix} \mathbf{I}_n \\ \frac{1}{q} \cdot \mathbf{A} & \frac{1}{q} \cdot \mathbf{I}_m \end{pmatrix},$$

如果 $p \neq q$, 那么依据定义可知, $\mathbf{p}_p$ 不是 $\Lambda_{\text{dual}}^E(\mathbf{A})$ 中的原始向量。

在嵌入对偶攻击中加入一个 p -模提示的效果与 p 和 q 的最大公约数 $\phi = \gcd(p, q)$ 有关。令 $q' = \frac{q}{\phi}$, $p' = \frac{p}{\phi}$, 那么有

$$\mathbf{p}_p = \frac{q}{p} \cdot \mathbf{p} = \frac{q'}{p'} \cdot \mathbf{p}$$

根据引理 2, 如果 $\frac{1}{p'} \cdot \mathbf{p}$ 是 $\frac{1}{q'} \cdot \Lambda_{\text{dual}}^E(\mathbf{A})$ 中的原始向量, 那么这个 p -模提示的效果为将格的体积降低为原来的 $\frac{1}{p} \cdot p' = \frac{1}{\phi}$ 。特别地, 如果 q 可以被 p 整除, 那么有 $\phi = p$, 即格的体积降低为原来的 $\frac{1}{p}$, 如果 q 和 p 是互素的, 那么有 $\phi = 1$, 即格的体积不发生变化。

5 近似提示

本节给出将近似提示加入嵌入对偶攻击中的方法以及产生的影响。一个近似提示 $\langle \mathbf{u}, \mathbf{s} \rangle + t = h, t \sim \mathcal{G}_q$ 可看作一个特殊的 LWE 实例。如果 t 的标准差 q 比给定的 LWE 实例中的错误 $\mathbf{e}$ 的标准差 σ 大, 这个近似提示即可视为一个无效的提示。因此, 本节接下来的部分均假设 $q < \sigma$ 。

近似提示 $\langle \mathbf{u}, \mathbf{s} \rangle + t = h, t \sim \mathcal{G}_q$ 与完美提示十分类似。实际上, 一个完美提示可以看作一个特殊情况的近似提示, 即当 $t = 0$ 时的近似提示。因此, 与完美提示类似, 可将近似提示 $\langle \mathbf{u}, \mathbf{s} \rangle + t = h$ 展开为 $u_1 s_1 + \dots + u_n s_n + t = h$, 不失一般性, 此处假设 $u_1 \neq 0$, 那么有

$$s_1 = \frac{1}{u_1} (h - u_2 s_2 - \dots - u_n s_n) - \frac{1}{u_1} t \quad (10)$$

令 $\mathbf{A} = (\mathbf{A}_1 \ \dots \ \mathbf{A}_n)$, 其中 $\mathbf{A}_i$ 表示 $\mathbf{A}$ 的第 i 列, 那么

$$\mathbf{A}_1 s_1 + \dots + \mathbf{A}_n s_n + \mathbf{e} = \mathbf{b} \bmod q \quad (11)$$

将式(10)和式(11)相结合可得

$$-\frac{1}{u_1} \mathbf{A}_1 t + \left(\mathbf{A}_2 - \frac{u_2}{u_1} \mathbf{A}_1 \right) s_2 + \dots + \left(\mathbf{A}_n - \frac{u_n}{u_1} \mathbf{A}_1 \right) s_n + \mathbf{e} = \mathbf{b} - \frac{h}{u_1} \mathbf{A}_1 + q \mathbf{k},$$

其中 $\mathbf{k} \in \mathbb{Z}^m$ 。这可以看作一个新的 LWE 实例 $(\bar{\mathbf{A}}, \bar{\mathbf{b}} = \bar{\mathbf{A}} \bar{\mathbf{s}} + \mathbf{e} \bmod q)$, 其中

$$\begin{aligned} \bar{\mathbf{A}} &= \begin{pmatrix} -\frac{1}{u_1} \mathbf{A}_1 & \mathbf{A}_2 - \frac{u_2}{u_1} \mathbf{A}_1 & \dots & \mathbf{A}_n - \frac{u_n}{u_1} \mathbf{A}_1 \end{pmatrix}, \\ \bar{\mathbf{s}} &= (t, s_2, \dots, s_n), \\ \bar{\mathbf{b}} &= \mathbf{b} - \frac{h}{u_1} \mathbf{A}_1 \end{aligned}$$

注意到, 与完美提示不同, 近似提示中有变量 t , 因此新的 LWE 实例中 t 代替了 s_1 成为新的变量。据此可构造相应的嵌入对偶攻击的格 $\Lambda_{\text{dual}}^E(\bar{\mathbf{A}})$ 。由于 t 和 $\mathbf{s}$ 的标准差不同, 使用缩放因子 $\gamma = \frac{\sigma_s}{q}$ 可使攻击的效果更好, 其中 σ_s 是 $\mathbf{s}$ 的标准差, 具体地,

$$\Lambda_{\text{dual}}^E(\bar{\mathbf{A}}, \gamma) = \left\{ \left(\frac{1}{\gamma} \cdot \mathbf{v}, \mathbf{v}, \mathbf{w} \right) \in \left(\frac{1}{\gamma} \cdot \mathbb{Z} \right) \times \mathbb{Z}^{n-1} \times \mathbb{Z}^m : \right. \\ \left. (\mathbf{v}, \mathbf{v}) = \mathbf{w} \cdot \bar{\mathbf{A}} \bmod q \right\}$$

格 $\Lambda_{\text{dual}}^E(\bar{\mathbf{A}}, \gamma)$ 的一组基为

$$\begin{pmatrix} \frac{q}{\gamma} \\ \mathbf{q} \cdot \mathbf{I}_{n-1} \\ \mathbf{A} & \mathbf{I}_m \end{pmatrix}$$

则 $\det(\Lambda_{\text{dual}}^E(\bar{\mathbf{A}}, \gamma)) = \frac{1}{\gamma} \cdot q^n$, 是没有加入提示信息的嵌入对偶攻击的格体积的 $\frac{1}{\gamma}$, 即

$$\det(\Lambda_{\text{dual}}^E(\bar{\mathbf{A}}, \gamma)) = \frac{1}{\gamma} \cdot \det(\Lambda_{\text{dual}}^E(\mathbf{A}))$$

综上, 一个近似提示可以使嵌入对偶攻击的格体积降为原来的 $\frac{1}{\gamma}$, 其中 $\gamma = \frac{\sigma}{q}$, 从而使攻击的效果更好。

6 模近似提示

本节给出将模近似提示加入嵌入对偶攻击中的方法以及产生的影响。与模提示类似, 根据模近似提示 $\langle \mathbf{u}, \mathbf{s} \rangle + t = h \bmod p$ 中模数 p 的不同将提示进行分类: 当 $p = q$ 时称为 q -模近似提示, 当 $p \neq q$ 时称为 p -模近似提示。由于一个 p -模近似提示可以通过乘以一定的倍数转化为一个 q -模近似提示, 本章主要考虑 q -模近似提示。一个 q -模近似提示可以看作作为一个特殊的 LWE 实例, 与近似提示类似, 本节假设 t 的标准差 q 小于 LWE 实例中的错误 $\mathbf{e}$ 的标准差 σ 。下面首先说明 q -模提示的方法不能用于 q -模近似提示,

然后对 q -模近似提示给出一个与近似提示类似的利用缩放因子的方法。

如果用和 q -模提示类似的方法, 即在格

$$\Lambda(\mathbf{A}, \mathbf{u}) = \left\{ \begin{array}{l} (\mathbf{v}, \mathbf{w}) \in \mathbb{Z}^n \times \mathbb{Z}^m: \\ (\mathbf{v} \quad \mathbf{w}) \begin{pmatrix} \mathbf{I}_n \\ -\mathbf{A} \end{pmatrix} = \mathbf{c} \cdot \mathbf{u} \bmod q, \mathbf{c} \in \mathbb{Z} \end{array} \right\}$$

中寻找短向量 $(\mathbf{v}, \mathbf{w})$, 那么对于 $(\mathbf{A}, \mathbf{b}) \leftarrow \text{LWE}_{n,q,s,\chi}$, 有

$$\begin{aligned} \langle \mathbf{w}, \mathbf{b} \rangle &= \mathbf{w} \cdot \mathbf{A}\mathbf{s} + \langle \mathbf{w}, \mathbf{e} \rangle \\ &= -\mathbf{c} \cdot \langle \mathbf{u}, \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle \\ &= -\mathbf{c} \cdot \mathbf{h} + \mathbf{c} \cdot \mathbf{t} + \langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle \bmod q, \end{aligned}$$

此时需要区分

$\langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle + \mathbf{c} \cdot \mathbf{t} = \langle \mathbf{w}, \mathbf{b} \rangle + \mathbf{c} \cdot \mathbf{h} \bmod q$ 的分布和 $\mathbb{Z}_q$ 上的均匀分布。注意到此处除 $\langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle$ 还有一个额外的 $\mathbf{c} \cdot \mathbf{t}$, 因此需确保 $\mathbf{c}$ 也是一个较小的数字, 否则将 $\langle \mathbf{w}, \mathbf{b} \rangle + \mathbf{c} \cdot \mathbf{h} \bmod q$ 的分布和 $\mathbb{Z}_q$ 上的均匀分布区分。 q -模提示的方法不能保证 $\mathbf{c}$ 较小, 因此不能用于 q -模近似提示。

下面考虑使用格 $\Lambda_{\text{dual-side}}^E(\mathbf{A}, \mathbf{u})$, 并使用缩放技术使得攻击的效果更好。具体地, 构造格

$$\Lambda_{\text{dual-side}}^E(\mathbf{A}, \mathbf{u}, \gamma) = \left\{ \begin{array}{l} (\mathbf{v}, \mathbf{w}, \frac{1}{\gamma} \cdot \mathbf{c}) \in \mathbb{Z}^n \times \mathbb{Z}^m \times \left(\frac{1}{\gamma} \cdot \mathbb{Z}\right): \\ (\mathbf{v} \quad \mathbf{w} \quad \mathbf{c}) \begin{pmatrix} \mathbf{I}_n \\ -\mathbf{A} \\ \mathbf{u} \end{pmatrix} = \mathbf{0} \bmod q \end{array} \right\}$$

其中 $\gamma = \frac{\sigma_s}{q}$ 是缩放因子。 $\Lambda_{\text{dual-side}}^E(\mathbf{A}, \mathbf{u}, \gamma)$ 的一组基为

$$\begin{pmatrix} q\mathbf{I}_n & & \\ \mathbf{A} & \mathbf{I}_m & \\ -\mathbf{u} & \mathbf{0} & \frac{1}{\gamma} \end{pmatrix}$$

那么对于 $(\mathbf{v}, \mathbf{w}, \mathbf{c}) \in \Lambda_{\text{dual-side}}^E(\mathbf{A}, \mathbf{u}, \gamma)$, 有

$$\begin{aligned} \langle \mathbf{w}, \mathbf{b} \rangle &= \gamma \cdot \langle \mathbf{c} \cdot \mathbf{u}, \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle \\ &= \gamma \cdot \mathbf{c} \cdot \mathbf{h} + \gamma \cdot \mathbf{c} \cdot \mathbf{t} + \langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle \bmod q \end{aligned}$$

接下来只需区分

$$\begin{aligned} \gamma \cdot \mathbf{c} \cdot \mathbf{t} + \langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle \\ = \langle \mathbf{w}, \mathbf{b} \rangle - \gamma \cdot \mathbf{c} \cdot \mathbf{h} \bmod q \end{aligned}$$

的分布和 $\mathbb{Z}_q$ 上的均匀分布即可解决判定-LWE 问题。

容易看到, 一个 q -模近似提示的效果是将格的体积减少为原来的 $\frac{1}{\gamma}$, 从而使攻击的效果更好。

7 利用侧信息的混合对偶攻击

对于实用性的密码方案, 混合对偶攻击比嵌入对偶攻击更有效。本节给出如何将嵌入对偶攻击的方法推广到混合对偶攻击。如第 2 节所述, 混合对偶

攻击将 $\mathbf{s}$ 和 $\mathbf{A}$ 分别分成两部分

$$\mathbf{s} = \begin{pmatrix} \mathbf{s}_1 \\ \mathbf{s}_2 \end{pmatrix} \in \mathbb{Z}_q^r \times \mathbb{Z}_q^{n-r},$$

$$\mathbf{A} = (\mathbf{A}_1, \mathbf{A}_2) \in \mathbb{Z}_q^{m \times r} \times \mathbb{Z}_q^{m \times (n-r)},$$

其中 $\mathbf{s}_1 \in \mathbb{Z}_q^r$ 用于猜测, $\mathbf{A}_2$ 用于构造对偶格

$$\Lambda_{\text{dual}}^E(\mathbf{A}_2) = \left\{ \begin{array}{l} (\mathbf{v}, \mathbf{w}) \in \mathbb{Z}^{n-r} \times \mathbb{Z}^m: \\ (\mathbf{v} \quad \mathbf{w}) \begin{pmatrix} \mathbf{I}_{n-r} \\ -\mathbf{A}_2 \end{pmatrix} = \mathbf{0} \bmod q \end{array} \right\}$$

可以看出混合对偶攻击中对偶格的构造方式与嵌入对偶攻击相同, 区别仅在于将 $\mathbf{A}$ 替换为 $\mathbf{A}_2$ 。因此, 前文所给出的在嵌入对偶攻击中利用提示的方法可直接用于混合对偶攻击中。

以 q -模提示为例, 当给定 q -模提示 $\langle \mathbf{u}, \mathbf{s} \rangle = \mathbf{h} \bmod q$ 时, 混合对偶攻击构造格

$$\Lambda_{\text{dual-side}}^E(\mathbf{A}_2, \mathbf{u}_2) = \left\{ \begin{array}{l} (\mathbf{v}, \mathbf{w}) \in \mathbb{Z}^{n-r} \times \mathbb{Z}^m: \\ (\mathbf{v} \quad \mathbf{w}) \begin{pmatrix} \mathbf{I}_{n-r} \\ -\mathbf{A}_2 \end{pmatrix} = \mathbf{c} \cdot \mathbf{u}_2 \bmod q, \mathbf{c} \in \mathbb{Z} \end{array} \right\},$$

并从其中得到短向量 $(\mathbf{v}, \mathbf{w})$ 。如果 $(\mathbf{A}, \mathbf{b}) \leftarrow \text{LWE}_{n,q,s,\chi}$, 那么

$$\begin{aligned} \langle \mathbf{w}, \mathbf{b} \rangle &= \mathbf{w} \cdot \mathbf{A}\mathbf{s} + \langle \mathbf{w}, \mathbf{e} \rangle \\ &= \mathbf{w}\mathbf{A}_1\mathbf{s}_1 - \mathbf{c} \cdot \langle \mathbf{u}_2, \mathbf{s}_2 \rangle + \langle \mathbf{v}, \mathbf{s}_2 \rangle + \langle \mathbf{w}, \mathbf{e} \rangle \\ &= \mathbf{w}\mathbf{A}_1\mathbf{s}_1 - \mathbf{c} \cdot \mathbf{h} + \langle \mathbf{u}_1, \mathbf{s}_1 \rangle + \langle \mathbf{v}, \mathbf{s}_2 \rangle \\ &\quad + \langle \mathbf{w}, \mathbf{e} \rangle \bmod q, \end{aligned}$$

之后, 对于候选猜测 $\tilde{\mathbf{s}}_1$, 区分

$$\begin{aligned} \langle \mathbf{v}, \mathbf{s}_2 \rangle + \langle \mathbf{w}, \mathbf{e} \rangle &= \\ \langle \mathbf{w}, \mathbf{b} \rangle - \mathbf{w}\mathbf{A}_1\tilde{\mathbf{s}}_1 + \mathbf{c} \cdot \mathbf{h} - \mathbf{c} \cdot \langle \mathbf{u}_1, \tilde{\mathbf{s}}_1 \rangle \bmod q \end{aligned}$$

的分布和 $\mathbb{Z}_q$ 上的均匀分布即可判断猜测是否正确。

8 原始攻击和对偶攻击利用侧信息的对比

本节对比各种提示在原始攻击和对偶攻击中的效果。不同的提示对于攻击的影响主要体现在三个方面: 格的维度、格的体积、秘密的标准差。对于原始攻击而言, 格的维度降低、体积增大或者秘密标准差降低都会使得攻击变得容易。而对于对偶攻击而言, 格的体积降低或者秘密标准差降低会使得攻击变得容易, 而由于对偶攻击存在最优的格的维度, 且在实例数目足够的情况下可以对格的维度进行自

表 1 不同因素对攻击困难程度的影响

Table 1 The effects of different factors on the hardness of attacks

	原始攻击	对偶攻击
↑		
维度	↑	先 ↑ 后 ↓
体积	↓	↑
标准差	↑	↑

由选择, 所以在对偶攻击中无需考虑格的维度的影响。另外, 需注意的, 格的体积对攻击效果的影响在原始攻击和对偶攻击中是相反的。接下来比较不同提示对于两种攻击的影响(见表 2)。简单起见, 表 2 中的数据假设模提示的模数 p 满足 $\gcd(q, p) = p$, 并且假设提示所对应的向量 $\mathbf{u}$ (以及 $\mathbf{p}$) 都是它们相应的格中的原始向量。从表 2 可以看出, 这些提示对于两种攻击都有益处, 但提升效果不同。将完美提示加入原始攻击, 会使得格的维度减 1, 体积增加为原来的 $\|\mathbf{u}\|$ 倍; 而对于对偶攻击, 加入一个完美提示会使得格的体积减小为原来的 $\frac{1}{q}$ 。将一个模数为 p 的模提示加入两种攻击, 格的体积均向有益于攻击的方向变化, 变化均为 p 倍。将近似提示加入原始攻击, 格中最短向量(即秘密)的标准差减小, 而对于对偶攻击, 格的体积减小为原来的 $\frac{1}{\gamma}$, γ 定义见第 6 节。模近似提示是本文定义的, 因此并未用于原始攻击。将模近似提示加入对偶攻击会使得格的体积减小为原来的 $\frac{1}{\gamma}$ 。

表 2 不同提示对攻击的影响

Table 2 The effects of different hints on attacks

提示	原始攻击	对偶攻击
完美提示	维度 -1 体积 * $\ \mathbf{u}\ $	维度 -1 体积 / q
模提示	体积 * p	体积 / p
近似提示	标准差 ↓	体积 / γ
模近似提示	-	体积 / γ

最后, 为了直观展示提示对于实际安全性的影响, 本文以完美提示为例, 选择 Kyber512^[21]这一方案, 展示不同数量的完美提示词对于 Kyber512 在使用原始攻击和对偶攻击评估所得到的实际安全性的影响。方案参数及提示信息如表 3 所示, 评估结果使用经典的 BKZ-core-SVP 模型^[9], 即 $T_{\text{BKZ}} = 2^{0.292\beta}$ 。结果如图 3 所示。从图中可以看出, 完美提示在两种攻击中的效果基本一致, 两种攻击的评估结果随着提示数目的增加而降低, 并且每多出一个完美提示时, 评估结果下降约 0.3 比特(对应于 BKZ 算法的参数 β 减小 1)。

9 总结与展望

本文研究了在对偶攻击中如何利用侧信息提升攻击的效果。具体地, 本文考虑了关于秘密 $\mathbf{s}$ 的侧信息对应的四种类型的提示, 给出了这些提示在对偶攻击中不同的使用方式, 分析了这些提示对于对

偶攻击中格体积的影响, 最后对比了这些提示在原始攻击以及对偶攻击中的效果。

表 3 Kyber512 方案参数及提示信息

Table 3 The parameters of Kyber512 and the hints

Kyber512 参数		
$n=512$	$Q=3329$	$\sigma=1.2$
提示 $\mathbf{u}$ 是一个汉明重量为 5 的三元向量		

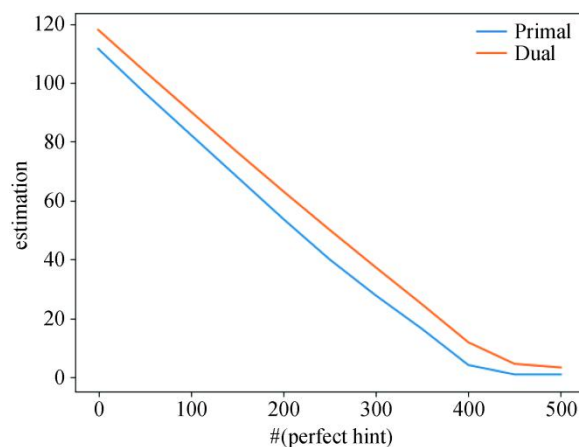


图 3 完美提示对于原始攻击和对偶攻击在 Kyber512 上的影响

Figure 3 primal attack and dual attack with perfect hints on Kyber512

基于目前的研究结果, 未来我们还需要在以下几个方面进行更加深入的研究:

1. 侧信息除了影响对偶攻击的格的体积, 还会直接影响对偶攻击中 $\langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle \bmod q$ 的分布及其标准差。在加入侧信息前, 这一分布可由高斯分布近似, 在加入侧信息后, 这一分布变得难以描述。然而, 这一分布的描述对于选择对偶攻击所用的参数 β 至关重要, 而参数 β 的选择直接影响对偶攻击的效果。因此, 考虑侧信息的加入如何影响 $\langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle \bmod q$ 的分布是下一步值得研究的工作。

2. 除了关于秘密 $\mathbf{s}$ 的提示, 还可考虑在对偶攻击中加入关于错误 $\mathbf{e}$ 的提示。与上一点类似, 关于 $\mathbf{e}$ 的提示对于对偶攻击的影响也主要体现在 $\langle \mathbf{v}, \mathbf{s} \rangle + \langle \mathbf{w}, \mathbf{e} \rangle \bmod q$ 的分布的变化上。

3. 由第 8 节的对比(表 2)可以看出, 侧信息对于原始攻击和对偶攻击效果的提升程度不同。研究效果的差异所产生的原因, 以及侧信息的效果在两种攻击中是否可以进一步提升, 是十分有意义的工作。

参考文献

- [1] Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography[C]. *The thirty-seventh annual ACM symposium on Theory of computing*, 2005: 84-93.
- [2] Albrecht M R, Curtis B R, Deo A, et al. Estimate all the {LWE, NTRU} Schemes![C]. *Lecture Notes in Computer Science*, 2018: 351-367.
- [3] Dachman-Soled D, Ducas L, Gong H J, et al. LWE with side information: attacks and concrete security estimation[C]. *CRYPTO 2020*: 329-358.
- [4] Albrecht M R. on dual lattice attacks against small-secret lwe and parameter choices in helib and seal[C]. *Eurocrypt 2017*: 103-129.
- [5] Bi L, Lu X H, Luo J J, et al. Hybrid Dual Attack on LWE with Arbitrary Secrets[J]. *Cybersecurity*, 2022, 5(1): 15.
- [6] Cheon J H, Hhan M, Hong S, et al. A Hybrid of Dual and Meet-in-the-Middle Attack on Sparse and Ternary Secret LWE[J]. *IEEE Access*, 2019, 7: 89497-89506.
- [7] Espitau T, Joux A, Kharchenko N. On a Dual/Hybrid Approach to Small Secret LWE[C]. *Progress in Cryptology – INDOCRYPT 2020*, 2020: 440-462.
- [8] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for Hard Lattices and New Cryptographic Constructions[C]. *The fortieth annual ACM symposium on Theory of computing*, 2008: 197-206.
- [9] Alkim E, Ducas L, Pöppelmann T, et al. Post-Quantum Key Exchange: A New Hope[C]. *The 25th USENIX Conference on Security Symposium*, 2016: 327-343.
- [10] Lyubashevsky V, Micciancio D. Asymptotically Efficient Lattice-Based Digital Signatures[J]. *Journal of Cryptology*, 2018, 31(3): 774-797.
- [11] Gentry C, Halevi S, Smart N P. Fully Homomorphic Encryption with Polylog Overhead[C]. *Advances in Cryptology – EUROCRYPT 2012*, 2012: 465-482.
- [12] Albrecht M R, Player R, Scott S. On the Concrete Hardness of Learning with Errors[J]. *Journal of Mathematical Cryptology*, 2015, 9(3): 169-203.
- [13] Albrecht M R, Göpfert F, Virdia F, et al. Revisiting the expected cost of solving uSVP and applications to LWE[C]. *ASIACRYPT 2017*: 297-322.
- [14] Lindner R, Peiert C. Better key sizes (and attacks) for LWE-based encryption[C]. *CT-RSA 2011*: 319-339.
- [15] Albrecht M R, Faugère J-C, Fitzpatrick R, et al. Lazy Modulus Switching for the BKW Algorithm[C]. *PKC 2014*: 429-445.
- [16] Arora S, Ge R. New Algorithms for Learning in Presence of Errors[M]. Automata, Languages and Programming. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 403-415.
- [17] Submission requirements and evaluation criteria for the post-quantum cryptography standardization process[EB]. <https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/call-for-proposals-final-dec-2016.pdf>.
- [18] Micciancio D, Regev O. Lattice-Based Cryptography[M]. Post-Quantum Cryptography. Berlin, Heidelberg: Springer, 2009: 147-191.
- [19] Gama N, Nguyen P Q. Finding short lattice vector within mordell's inequality[C]. *STOC*, 2008: 207-216.
- [20] Chen Y. Réduction de réseau et sécurité concrete du chiffrement complètement homomorphe[D]. Paris: Université Paris 13, 2013.
- [21] Bos J, Ducas L, Kiltz E, et al. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM[C]. *2018 IEEE European Symposium on Security and Privacy*, 2018: 353-367.



毕蕾 于 2022 年在中国科学院大学网络空间安全专业获得博士学位。现任中国科学院信息工程研究所助理研究员。研究领域为格密码。研究兴趣包括：格密码分析。Email: bilei@iie.ac.cn



路献辉 于 2009 年在西南交通大学信息安全专业获得博士学位。现任中国科学院信息工程研究所研究员。研究领域为密码学。研究兴趣包括：抗量子密码、全同态密码等。Email: luxianhui@iie.ac.cn



罗俊杰 于 2019 年在中国科学院大学运筹学与控制论专业获得博士学位。现任北京交通大学讲师。研究领域为算法与计算复杂性。研究兴趣包括：计算经济学、格密码分析等。Email: jluo1@bjtu.edu.cn



王鲲鹏 于 2000 年在清华大学数学专业获得博士学位。现任中国科学院信息工程研究所研究员。研究领域为椭圆曲线密码学、格密码。研究兴趣包括：后量子密码学、全同态密码等。Email: wangkunpeng@iie.ac.cn