软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(9):4310−4335 [doi: 10.13328/j.cnki.jos.006657]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

RSA 及其变体算法的格分析方法研究进展*

周永彬[1,2,3], 姜子铭[1,2], 王天宇[1,2], 袁思蒙[1,2], 许 军[1,2], 王鲲鹏[1,2], 刘月君[3]

[1](中国科学院 信息工程研究所, 北京 100093)

[2](中国科学院大学 网络空间安全学院, 北京 100049)

[3](南京理工大学 网络空间安全学院, 江苏 南京 210094)

通信作者: 刘月君, E-mail: liuyuejun@njust.edu.cn

摘 要: 格分析是一种利用格困难问题的求解算法分析公钥密码安全性的分析方法, 是研究 RSA 类密码算法安全性的有力数学工具之一. 格分析的关键在于构造格基, 虽然目前已有通用简洁的格基构造策略, 然而, 这种通用方法无法充分、灵活地利用 RSA 及其变体的代数结构. 近年来, RSA 类算法的格分析工作大多在通用策略的基础上引入特殊格基构造技巧. 首先介绍了格分析方法以及通用格基构造策略, 并总结提炼了几种常用格基构造技巧; 其次, 回顾了标准 RSA 算法格分析的主要成果, 即模数分解攻击、小解密指数攻击以及部分私钥泄漏攻击; 然后, 总结了几种主流 RSA 变体算法的特殊代数结构, 及其适用的特殊格基构造技巧; 最后, 对现有 RSA 及其变体算法的格分析工作进行了分类总结, 并展望了格分析方法的研究与发展方向.

关键词: RSA; Coppersmith 方法; 格分析; RSA 变体; LLL 算法

中图法分类号: TP309

中文引用格式: 周永彬, 姜子铭, 王天宇, 袁思蒙, 许军, 王鲲鹏, 刘月君. RSA及其变体算法的格分析方法研究进展. 软件学报, 2023, 34(9): 4310–4335. http://www.jos.org.cn/1000-9825/6657.htm

英文引用格式: Zhou YB, Jiang ZM, Wang TY, Yuan SM, Xu J, Wang KP, Liu YJ. Progress of Lattice-based Cryptanalysis of RSA and Its Variant Algorithms. Ruan Jian Xue Bao/Journal of Software, 2023, 34(9): 4310–4335 (in Chinese). http://www.jos.org.cn/1000-9825/6657.htm

Progress of Lattice-based Cryptanalysis of RSA and Its Variant Algorithms

ZHOU Yong-Bin[1,2,3], JIANG Zi-Ming[1,2], WANG Tian-Yu[1,2], YUAN Si-Meng[1,2], XU Jun[1,2], WANG Kun-Peng[1,2], LIU Yue-Jun[3]

[1](Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

[2](School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China)

[3](School of Cyber Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract: Lattice-based cryptanalysis, an analysis method using the algorithms solving hard Lattice problems to analyze the security of public-key cryptosystems, has become one of the powerful mathematical tools for studying the security of the Rivest-Shamir-Adleman (RSA)-type cryptographic algorithms. The key point of this method is the construction of the Lattice basis. There exists a general strategy for Lattice basis construction. However, this general strategy fails to fully and flexibly utilize the algebraic structure of the RSA algorithm and its variants. In recent years, Lattice-based cryptanalysis of RSA-type algorithms mostly focuses on introducing special techniques of Lattice base construction on the basis of the general strategy. This study starts by outlining Lattice-based cryptanalysis and the general strategy for Lattice basis construction and summarizing several commonly used techniques of Lattice basis construction. Subsequently, the main achievements in Lattice-based cryptanalysis of the standard RSA algorithm are reviewed, and they involve factoring with known bits, small private exponent attacks, and partial key exposure attacks. Then, the special algebraic structures of several mainstream variants of the

* 基金项目: 国家自然科学基金 (U1936209, 61632020, 62002353, 61872442); 北京市自然科学基金 (4192067); 信工所攀登计划 (E0Z0251112)
收稿时间: 2021-12-01; 修改时间: 2022-01-15; 采用时间: 2022-02-17; jos 在线出版时间: 2022-05-24
CNKI 网络首发时间: 2022-12-29

RSA algorithm and the techniques of Lattice basis construction applicable to these variants are summarized. Finally, the available work on Lattice-based cryptanalysis of the RSA algorithm and its variants is classified and summed up, and the prospects of the research and development of lattice-based cryptanalysis are presented.

Key words: Rivest-Shamir-Adleman (RSA); Coppersmith's method; Lattice-based cryptanalysis; RSA variants; LLL algorithm

基于格理论的密码分析方法是分析公钥密码安全性的重要数学工具. 格理论最早可追溯到开普勒于 1611 年提出的球堆积与覆盖问题, 随着数学界对该问题的研究, 逐渐形成了格理论体系. 格理论在密码学领域的发展大致可以分为两条路线: 首先是密码设计, 即利用格上困难问题构造公钥密码原语; 其次是密码分析, 即利用格上困难问题的求解算法, 分析格上或经典 (非格上) 公钥密码体制的安全性. 最短非零向量问题 (shortest vector problem, SVP) 是格理论中最著名的计算困难问题之一, SVP 的具体描述见问题 1, l_2 范数下的 SVP 已被证明是 NP 困难问题[1]. 虽然精确的 SVP 是计算困难问题, 但目前可以在多项式时间求解近似 SVP, 近似 SVP 的具体描述见问题 2. 1982 年, Lenstra 等人[2]提出了第一个求解近似 SVP 的多项式时间算法, 即 LLL 格基约化算法. 随后的若干工作对 LLL 格基约化算法进行了推广和改进, 目前, 最实用的格基约化算法是 Schnorr 等人提出的 BKZ 算法[3].

问题 1. SVP. 给定格 $\mathcal{L}$, 找到一个非零向量 $\mathbf{v}\in\mathcal{L}$, 满足对任意非零向量 $\mathbf{u}\in\mathcal{L}$, 都有 $\|\mathbf{v}\|\leqslant\|\mathbf{u}\|$.

问题 2. SVP-γ. 给定格 $\mathcal{L}$, 找到一个非零向量 $\mathbf{v}\in\mathcal{L}$, 满足对任意非零向量 $\mathbf{u}\in\mathcal{L}$, 都有 $\|\mathbf{v}\|\leqslant\gamma\|\mathbf{u}\|$, 其中 γ 称为近似因子.

格分析方法的基本思想是, 先从公钥密码体制的公私钥以及其他参数之间的代数关系出发, 将破解公钥密码体制转化为某个格上困难问题, 进而利用 LLL 格基约化等算法求解格上困难问题. 格分析方法在密码学领域应用广泛, 在 RSA 及其变体算法的密码分析方面已经取得了一些很好的分析结果, 是 RSA 密码分析的一种非常重要的基础工具. 此外, 格分析也可以应用于分析 DSA 和 ECDSA 等其他经典公钥密码算法的安全性, 以及求解隐藏数问题、近似公因子问题等.

RSA 密码算法是第一个实用的公钥密码算法. RSA 算法由麻省理工学院的 Rivest 等人[4]于 1978 年提出, 可用于构造公钥加密, 数字签名和伪随机数生成器等经典密码原语. RSA 是迄今为止最著名的公钥密码算法之一, 其安全性分析一直是密码学界的研究热点. RSA 密码算法的理论安全性依赖于 RSA 问题的困难性, RSA 问题的具体描述见问题 3. 40 多年以来, 虽然 RSA 算法的理论安全性和实际安全性都经历了各种考验, 但在非量子计算模型, 且没有获得额外信息的情况下, 目前暂无破解 RSA 密码系统的多项式时间算法, 故 RSA 的密码分析一直是密码学领域的研究难点之一. 虽然直接求解 RSA 问题是困难的, 但在某些特殊情况下, 例如, 加密指数或解密指数较小、私钥部分比特泄漏, 利用格分析方法可以在多项式时间内破解 RSA 密码系统.

问题 3. RSA 问题. 令 $N=pq$ 是两个奇素数 p, q 的乘积, e 是一个与 $\varphi(N)=(p-1)(q-1)$ 互素的正整数. 给定 N, e, 以及任意 $y\in\mathbb{Z}_N^*$, 计算 $x\in\mathbb{Z}_N^*$, 满足 $x^e\equiv y \mod N$.

RSA 密码系统的格分析开创性工作是由 Coppersmith 提出的. 1996 年, Coppersmith 基于 LLL 格基约化算法, 提出了求解单变元模方程小根[5]和双变元整数方程小根[6]的多项式时间算法, 于 1997 年将这两个工作总结完善[7]并应用于求解加密指数较小、素因子部分比特泄漏等 RSA 问题的特殊实例. Coppersmith 方法是借助格上短向量求解算法计算方程小根的一类方法的统称, 该方法的核心思想是, 目标模方程的系数向量按照某种合适的顺序排列后可映射为一个格基矩阵, 通过格上的短向量求解算法, 例如 LLL 约化算法, 得到格上的短向量, 如果格基约化算法输出的向量足够短, 那么该短向量对应的模方程的小根实际上就是整数域上多项式方程的小根, 此时通过结式消元法或 Gröbner 基等方法即可在多项式时间内求解.

随后的若干工作对 Coppersmith 原始方法进行了推广、改进与应用. 鉴于 Coppersmith 原始方法[5−7]相对复杂, 1997 年, Howgrave-Graham[8]针对单变元模方程, 提出了更简洁的格基构造方法, 该方法可以扩展到多变元模方程的情形; 通过对偶格的方法可以证明 Howgrave-Graham 方法与 Coppersmith 原始方法本质上是等价的, 但是在计算效率方面有略微的优势; 注意, Howgrave-Graham 的方法基于一个启发式假设——LLL 算法输出的约化基是代数独立的, 需要实验验证该假设是否成立. 2004 年, Coron[9]提出了一个求解双变元整数方程小根的简单算法, 其核心思想与 Howgrave-Graham 计算模方程小根的方法类似, Coron 的方法也可以扩展到多变元整数方程的情形, 但

同样基于上述启发式假设. 2006 年, Jochemsz 等人[10]提出了通用模方程和整数方程小根的求解方法, 给出了利用目标方程构造满秩格的一般策略, 包括“基础策略”和“扩展策略”, 该方法同样基于上述启发式假设. 目前, Coppersmith 方法一般指经过 Howgrave-Graham[8], Coron[9]和 Jochemsz 等人[10]改进后的一类分析方法的统称, 用于求解任意变元模方程或整数方程的小根, 但对于多变元的情形, 该方法需基于启发式假设——格基约化算法输出的向量是代数无关的.

虽然 Jochemsz 等人[10]给出了通用且简洁的构造满秩格的一般策略, 但对于某些具有特殊代数关系的多项式方程, 使用通用策略可能无法充分利用目标多项式的代数结构, 故无法达到最优的攻击效果. 因此, Coppersmith 方法的基本思想发展成熟后, 后续研究工作重点关注特殊格基构造技巧, 即如何充分利用变元、单项式或多个方程之间的特殊代数关系, 选择合适的单项式、多项式来构造格基.

本文主要论述 RSA 及其变体算法的格分析方法研究进展, 主要工作分为 3 部分.

(1) 从现有格分析工作中提炼出几种常用的特殊格基构造技巧, 即变元代换技巧[11]、均衡化技巧[12]、指数优化技巧[13]、拆分线性化技巧[14]、两步格方法[15]等, 阐述它们的基本原理、适用范围及攻击效果.

(2) 回顾标准 RSA 算法格分析的重要研究成果, 主要包括模数分解攻击、小解密指数攻击以及部分私钥泄漏攻击, 以标准 RSA 的部分私钥泄漏攻击为例讨论格分析方法中泄漏信息的利用方式.

(3) 针对几种主流的 RSA 变体算法, 即中国剩余定理 (Chinese remainder theorem, CRT) 指数 RSA、素数幂 RSA、多素数 RSA 以及共素数 RSA 算法, 总结现有格分析方法常用的特殊代数结构, 及其适用的特殊格基构造技巧.

本文第 1 节主要介绍格分析方法, 即 Coppersmith 方法的基本原理及步骤; 第 2 节就几种常用的格基构造技巧展开论述; 第 3 节讨论了格分析方法在 RSA 算法密码分析中的几个重要成果; 第 4 节针对格分析方法在 RSA 变体算法密码分析中的主要成果做了回顾; 最后在第 5 节中给出结论与展望.

1 Coppersmith 方法

Coppersmith 方法用于求 k 变元模方程或 $k+1$ 变元整数方程的小根, 其中, 正整数 $k \geqslant 1$. 本节简述经过 Howgrave-Graham[8], Coron[9]和 Jochemsz 等人[10]改进后的 Coppersmith 方法的基本原理及步骤.

1.1 预备知识

格可视为 m 维欧式空间 $\mathbb{R}^m$ 中一类具有周期性结构的离散点的集合, 假设正整数 $n \leqslant m$, 令 $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ 是 $\mathbb{R}^m$ 中的 n 个线性无关向量, 则称 $\mathcal{L}=\left\{v \in \mathbb{R}^m:\ v=\sum_{i=1}^{n} x_i \mathbf{b}_i, x_i \in \mathbb{Z}, i=1, \ldots, n\right\}$ 为 $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ 生成的格, 其中, 正整数 m 与 n 分别称为格 $\mathcal{L}$ 的维数与秩, 记 $\dim(\mathcal{L})=m$, $\operatorname{rank}(\mathcal{L})=n$, 满足 $m=n$ 的格称为满秩格; 向量组 $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ 称为格 $\mathcal{L}$ 的一组生成基, 同一个格可以采用不同的格基表示.

将格基向量视为行向量, 格 $\mathcal{L}$ 可以被一个格基矩阵表示 $\mathbf{B}(\mathcal{L})=\left[\mathbf{b}_1{}^{\mathrm{T}}, \mathbf{b}_2{}^{\mathrm{T}}, \ldots, \mathbf{b}_n{}^{\mathrm{T}}\right]^{\mathrm{T}} \in \mathbb{R}^{m \times n}$, 格 $\mathcal{L}$ 的行列式定义为 $\det(\mathcal{L})=\sqrt{\det\left(\mathbf{B}(\mathcal{L})^{\mathrm{T}} \mathbf{B}(\mathcal{L})\right)}$, 对于满秩格, 有 $\det(\mathcal{L})=|\det(\mathbf{B}(\mathcal{L}))|$. 如无特殊说明, 本文中的格默认是满秩格, 范数默认取 l_2 范数.

1.2 模方程小根的求解

问题 4. k 变元模方程小根的求解问题. 假设 W 是一个因子分解未知的大整数, b 是 W 的一个因子且 $b \geqslant W^{\beta}$, 其中 $0<\beta \leqslant 1$. 记 $f(x_1, \ldots, x_k)$ 为 k 变元多项式, 其中正整数 $k \geqslant 1$. 要求找到方程:

$$f(x_1, \ldots, x_k) \equiv 0 \mod b \tag{1}$$

的所有整数解 $\left(x_1^{(0)}, \ldots, x_k^{(0)}\right)$, 其中解的上界为 $\left|x_1^{(0)}\right| \leqslant X_1, \ldots, \left|x_k^{(0)}\right| \leqslant X_k$. 该问题的目标是最大化可求解的小根的上界 $X_1, \ldots, X_k$, 同时保证求解算法的时间复杂度关于其输入规模 $(\log W, k, \delta)$ 仍是多项式的, 其中, 正整数 δ 为多项式 $f(x_1, \ldots, x_k)$ 最高次项的次数. 注意, 模数 b 不必是素数.

Coppersmith 方法的核心思想是将求解模方程的小根问题转化为求解整数方程组的小根问题, 即利用目标多项式 $f(x_1, \ldots, x_k)$, 构造出模方程 (1) 同解的整数方程组:

$$\begin{cases} h_1(x_1,\ldots,x_k)=0 \\ \quad\vdots \\ h_k(x_1,\ldots,x_k)=0 \end{cases} \tag{2}$$

从而通过高效的结式消元法或 Gröbner 基方法来求解上述整数方程组. 具体地, 利用 Coppersmith 方法求解 k 变元模方程的小根大致可以分为以下 4 个步骤.

(1) 构造多项式集合 C: 对于固定正整数 m (由后续步骤确定 m 的最优取值), 利用目标多项式 $f(x_1,\ldots,x_k)$ 构造一个多项式的集合 $C=\left\{g_i(x_1,\ldots,x_k): g_i\left(x_1^{(0)},\ldots,x_k^{(0)}\right)\equiv 0 \mod b^m;\ i=1,\ldots,n\right\}$, 其中 $n\geqslant k$. 对于集合 C 中任意多项式 g_i, 若 $\left(x_1^{(0)},\ldots,x_k^{(0)}\right)$ 是 $f(x_1,\ldots,x_k)\equiv 0 \mod b$ 的解, 那么 $g_i\left(x_1^{(0)},\ldots,x_k^{(0)}\right)\equiv 0 \mod b^m$ 成立, 即:

$$f\left(x_1^{(0)},\ldots,x_k^{(0)}\right)\equiv 0 \mod b \Rightarrow g_i\left(x_1^{(0)},\ldots,x_k^{(0)}\right)\equiv 0 \mod b^m, i=1,\ldots,n.$$

多项式 $g_1,g_2,\ldots,g_n$ 的构造及其排列顺序决定了格基的构造, 进而决定了可求解的小根的上界, 故本步骤是 Coppersmith 方法的关键. 多项式 $g_1,\ldots,g_n$ 的具体构造及排序方式将在第 2 节格基构造方法中展开讨论.

(2) 构造格 $\mathcal{L}$: 利用集合 C 中的多项式构造一个 n 维格 $\mathcal{L}$, 格基为 $\{\mathbf{b}_1,\ldots,\mathbf{b}_n\}$. 具体地, 对于 $i=1,\ldots,n$, 向量 $\mathbf{b}_i$ 的各分向量对应多项式 $g_i(x_1X_1,\ldots,x_kX_k)$ 各单项式的系数. 将格基向量视为行向量, 格基矩阵:

$$\mathbf{B}(\mathcal{L})=\begin{bmatrix}\mathbf{b}_1\\ \vdots \\ \mathbf{b}_n\end{bmatrix} \Leftrightarrow \begin{bmatrix} g_1(x_1X_1,\ldots,x_kX_k)\\ \vdots \\ g_n(x_1X_1,\ldots,x_kX_k)\end{bmatrix}.$$

(3) 寻找格 $\mathcal{L}$ 上的 k 个短向量: 应用 LLL 等格基约化算法得到格 $\mathcal{L}$ 上的 k 个短向量 $\mathbf{v}_1,\ldots,\mathbf{v}_k$, 对 $j=1,\ldots,k$, 由 $\mathbf{v}_j$ 的分向量得到多项式 $h_j(x_1X_1,\ldots,x_kX_k)$ 对应的单项式系数, 再除去对应的解的上界, 即可得到多项式 $h_j(x_1,\ldots,x_k)$, 从而构造出方程组 (2). 格 $\mathcal{L}$ 中向量对应的多项式即为集合 C 中多项式的整数线性组合, 故对 $i=1,\ldots,n$, 若 $\left(x_1^{(0)},\ldots,x_k^{(0)}\right)$ 是 $g_i(x_1,\ldots,x_k)\equiv 0 \mod b^m$ 的解, 那么 $h_j\left(x_1^{(0)},\ldots,x_k^{(0)}\right)\equiv 0 \mod b^m$ 成立, 即:

$$g_i\left(x_1^{(0)},\ldots,x_k^{(0)}\right)\equiv 0 \mod b^m, i=1,\ldots,n \Rightarrow h_j\left(x_1^{(0)},\ldots,x_k^{(0)}\right)\equiv 0 \mod b^m, j=1,\ldots,k.$$

注意, 求解 k 个未知量至少需要 k 个整数方程, 故需输出至少 k 个短向量, 格 $\mathcal{L}$ 维度至少为 k.

(4) 求解 k 变元整数方程组: 若模方程 (1) 的根足够小, 使得对于 $j=1,\ldots,k$, 都有 $\left\|h_j\left(x_1^{(0)},\ldots,x_k^{(0)}\right)\right\|<b^m$, 那么 $h_j\left(x_1^{(0)},\ldots,x_k^{(0)}\right)=0$ 在整数域上也成立, 即:

$$h_j\left(x_1^{(0)},\ldots,x_k^{(0)}\right)\equiv 0 \mod b^m \Rightarrow h_j\left(x_1^{(0)},\ldots,x_k^{(0)}\right)=0, j=1,\ldots,k.$$

采用 Gröbner 基计算方法或结式消元法即可在多项式时间计算出整数方程组 (2) 的所有解, 将这些解代入 $f\left(x_1^{(0)},\ldots,x_k^{(0)}\right)\equiv 0 \mod b$ 验证, 即可得到 $f(x_1,\ldots,x_k)\equiv 0 \mod b$ 的所有小根 $\left(x_1^{(0)},\ldots,x_k^{(0)}\right)$.

值得注意的是, 由于目标模方程包含 k 个变元, 因此需要用 LLL 等格基约化算法得到至少 k 个代数独立的多项式, 这样才能确保通过代数方法可以得到整数方程组 (2) 的解. Coppersmith 方法通常假设第 3 步中输出的向量是代数独立的, 见假设 1. 正是因为这条假设的存在, Coppersmith 方法在大多数情形下是启发式方法, 需要实验验证该方法的可靠性. Blömer 等人[16]指出, 在某些情形下, 该假设是不需要的; Coppersmith 方法后续工作[16,17]的实验证实, 只有少数情况下 LLL 算法输出的多项式是代数相关的. 因此, 格分析工作通常认为该假设是成立的.

假设 1. Coppersmith 方法中, 利用 LLL 等格基约化算法得到的 k 个约化基向量对应的 k 个多项式是代数独立的, 即多项式 $h_j(x_1,\ldots,x_k)$, $j=1,\ldots,k$ 是代数独立的, 可以通过 Gröbner 基计算方法或结式消元法有效计算出整数方程组 (2) 的解.

引理 1. LLL[2]. 令 $\mathcal{L}$ 是一个 n 维格, 那么在多项式时间内, LLL 算法输出的约化基向量 $\mathbf{v}_i, i=1,\ldots,l$, 对于 $l\leqslant n$, 满足 $\|\mathbf{v}_l\|\leqslant 2^{\frac{n(n-1)}{4(n+1-l)}}\det(\mathcal{L})^{\frac{1}{(n+1-l)}}$.

引理 2. Howgrave-Graham[8]. 令 $h(x_1,\ldots,x_l)\in\mathbb{Z}[x_1,\ldots,x_l]$ 为一个包含 ω 个单项式的整数多项式, M 是一个正整数, 若 $h(x_1,\ldots,x_l)$ 满足:

(1) $h\left(x_1',\ldots,x_l'\right)\equiv 0 \mod M$, $\left|x_1'\right|<X_1,\ldots,\left|x_l'\right|<X_l$.

(2) $\|h(x_1X_1,\ldots,x_lX_l)\| < M/\sqrt{\omega}$.

则 $h\left(x'_1,\ldots,x'_l\right)=0$ 在整数域上也成立.

对于给定的 n 维格 $\mathcal{L}$, LLL 格基约化算法可以在多项式时间输出 $l\leqslant n$ 个短向量[2], 引理 1 给出了 LLL 算法输出的 k 个短向量范数的上界. 为使短向量对应的 k 个方程都可以在整数域上求解, 多项式 $h_1,\ldots,h_k$ 需满足 $\left\|h_j(x_1X_1,\ldots,x_lX_k)\right\| < b^m/\sqrt{\omega}$, $j=1,\ldots,k$, 见引理 2. 由于 $\mathbf{v}_j$ 的分向量与多项式 $h_j(x_1X_1,\ldots,x_lX_k)$ 的单项式系数一一对应, 所以 $\left\|\mathbf{v}_j\right\|=\left\|h_j(x_1X_1,\ldots,x_lX_k)\right\|$. 因此, Coppersmith 方法成功的条件为:

$$2^{\frac{n(n-1)}{4(n+1-k)}}\det(\mathcal{L})^{\frac{1}{(n+1-k)}}\leqslant b^m/\sqrt{\omega}.$$

通常省略渐近复杂度较小的项, 将 Coppersmith 方法成功的条件简化为:

$$\det(\mathcal{L})^{\frac{1}{\dim(\mathcal{L})}}\leqslant b^m \tag{3}$$

为提升可求解的小根的上界, 需构造出性质更好的格基. 条件 (3) 成立时即可恢复出模方程的小根, 其中 $\det(\mathcal{L})^{\frac{1}{\dim(\mathcal{L})}}$ 通常是小根上界方幂的乘积. 因此, 对于固定的正整数 m, 如果构造出 $\det(\mathcal{L})^{\frac{1}{\dim(\mathcal{L})}}$ 更小的格基, 那么就可以提升可求解的小根的上界. 为使行列式的计算相对简单, 现有 RSA 格分析工作大多构造三角格基矩阵, 其行列式即为所有对角线元素的乘积. 基于此, May[18]将三角格基矩阵中对角线元素小于 b^m 的向量定义为有益向量, 并指出对于三角格基, 有益向量的加入有助于提升可求解的小根的上界. Takayasu 等人[12]在此基础上提出了有益多项式的概念, 将 May[18]的思想推广至一般 (非三角) 格基, 见定义 1, Takayasu 等人[12]提出可以通过收集尽可能多的有益多项式, 以及尽可能少的非有益多项式来构造格基矩阵, 从而提升可求解的小根的上界.

定义 1. 有益多项式[12]. 令 $\mathbf{B}$ 表示利用 Coppersmith 方法求解模方程 $f(x_1,\ldots,x_l)\equiv 0 \mod b$ 小根时构造的格基矩阵, 假设 $\mathbf{B}$ 是由多项式 $g_i(x_1X_1,\ldots,x_lX_l)$ 对应的向量构成的, 其中 $g_i(x_1,\ldots,x_l)\equiv 0 \mod b^m$, $i=1,\ldots,t$. 令矩阵 $\mathbf{B}'$ 包含 $\mathbf{B}$ 中的所有向量, 且 $\mathbf{B}'$ 仅比 $\mathbf{B}$ 多一个向量 $\mathbf{v}'$, 向量 $\mathbf{v}'$ 的各分量对应多项式 $\hat{g}(x_1X_1,\ldots,x_lX_l)$ 中各单项式的系数, 当:

$$\det(\mathbf{B}')/\det(\mathbf{B}) < b^m$$

时, 称 $\hat{g}(x_1,\ldots,x_l)$ 为有益多项式; 否则, 称 $\hat{g}(x_1,\ldots,x_l)$ 为非有益多项式.

1.3 多变元整数方程小根的求解

问题 5. k+1 变元整数方程小根的求解问题. 假设 $f(x_1,\ldots,x_s)$ 是包含 $k+1=s$ 个变元的多项式, 其中正整数 $k\geqslant 1$. 要求找到方程 $f(x_1,\ldots,x_s)=0$ 的所有小根 $\left(x_1^{(0)},\ldots,x_s^{(0)}\right)$, 小根上界为 $\left|x_1^{(0)}\right|\leqslant X_1,\ldots,\left|x_s^{(0)}\right|\leqslant X_s$. 该问题的目标是最大化可求解的小根的上界 $X_1,\ldots,X_s$, 同时满足求解算法的时间复杂度关于其输入规模 (s,δ) 仍是多项式的, 其中 δ 为多项式 $f(x_1,\ldots,x_s)$ 最高次项的次数.

Coppersmith 方法求解整数方程的基本思想是, 通过选取合适的模数 M, 将原始问题转化为模方程 $f(x_1,\ldots,x_s)\equiv 0 \mod M$ 的求解问题. 模数 M 的构造可参考 Jochemsz-May 通用策略[10], 具体地, 令 d_j 表示变元 x_j 在 $f(x_1,\ldots,x_s)$ 中出现的最高次数, 令 $F=\|f(x_1X_1,\ldots,x_sX_s)\|_\infty$. 对于固定正整数 m, 构造模数:

$$M=F\prod_{j=1}^{s}X_j^{d_j(m-1)},$$

于是 $f(x_1,\ldots,x_s)$ 在整数域上的小根即为 $f(x_1,\ldots,x_s)$ 模 M 的小根, 即:

$$f\left(x_1^{(0)},\ldots,x_s^{(0)}\right)=0 \Rightarrow f\left(x_1^{(0)},\ldots,x_s^{(0)}\right)\equiv 0 \mod M,$$

其中, 模方程 $f\left(x_1^{(0)},\ldots,x_s^{(0)}\right)\equiv 0 \mod M$ 的求解可以采用第 1.2 节中的方法. 本文重点关注模方程的求解, 整数方程求解的具体细节参见 Jochemsz-May 通用策略[10].

2 格基构造方法

格分析方法的关键在于格基构造, 虽然 Jochemsz 等人[10]给出了通用简洁的满秩格构造策略, 但对于某些具有特殊代数关系的多项式方程, 这种通用策略无法充分、灵活地利用目标多项式的特殊代数结构, 故无法达到最优攻击效果. 现有多种 RSA 变体算法, 且 RSA 变体算法的私钥、公钥之间可能存在的不同代数关系, 近年来 RSA

类算法的格分析工作大多在 Jochemsz-May 通用格基构造策略的基础上, 针对具体算法的特殊代数结构, 采用特殊格基构造技巧以提升攻击效果, 常用格基构造技巧包括: 变元代换、均衡化、指数优化、拆分线性化、两步格方法等, 对于某些 RSA 问题的特殊实例, 使用这些格基构造技巧的攻击效果优于 Jochemsz-May 通用策略. 为方便行列式的计算, 现有 RSA 类算法的格分析工作大多构造三角格基矩阵, 本节以模方程的求解为例, 简述 Jochemsz-May 通用格基构造方法以及常用格基构造技巧构造三角格基矩阵的基本原理.

2.1 通用格基构造方法

Jochemsz-May 通用格基构造方法[10]包括基础策略 (basic strategy) 和扩展策略 (extended strategy). 以问题 4 为例, 假设 $f(x_1,\ldots,x_k)=\sum_{i=0}^{l}a_i x_1^{s_i^{(1)}}\ldots x_k^{s_i^{(k)}}$ 是包含 l 个单项式的 k 变元多项式, 第 l 个单项式 $a_l x_1^{s_l^{(1)}}\ldots x_k^{s_l^{(k)}}$ 为首项, 记为 $\lambda=a_l x_1^{s_l^{(1)}}\ldots x_k^{s_l^{(k)}}$. 假设首项系数 $a_l=1$, 若 $a_l\neq 1$, 则可通过乘 a_l 的逆 $a'=a_l^{-1} \bmod W$ 得到首一多项式 $f'(x_1,\ldots,x_k)=a'\cdot f(x_1,\ldots,x_k)$; 若不存在 $a_l^{-1} \bmod W$, 则可以找到 W 的分解.

(1) Jochemsz-May 基础策略. 对于固定的正整数 m, 以及 $u\in\{0,\ldots,m+1\}$, 定义单项式的集合 M_u:

$$M_u:=\left\{x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}:\ x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}\ 是\ f^m 的单项式,\ 且\frac{x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}}{\lambda^u}是 f^{m-u}\ 的单项式\right\}.$$

第 1.2 节定义的多项式集合 C 中的多项式通常称为 shift 多项式, Jochemsz-May 策略中定义 shift 多项式为:

$$g_{t,i_1,\ldots,i_k}(x_1,\ldots,x_k)=\frac{x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}}{\lambda^t}f(x_1,\ldots,x_k)^t W^{m-t},$$

其中, $t=0,1,\ldots,m$ 且 $x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}\in M_t\backslash M_{t+1}$. 显然, 对于上述 shift 多项式, 有 $g_{i_1,\ldots,i_k}\left(x_1^{(0)},\ldots,x_k^{(0)}\right)\equiv 0 \bmod b^m$. 根据下标 $t,i_1,\ldots,i_k$ 的值将 shift 多项式按合适的顺序排列, 即可通过 $g_{t,i_1,\ldots,i_k}(x_1X_1,\ldots,x_kX_k)$ 的系数得到一个三角格基矩阵, 具体地, 若 $t<t'$, 则多项式 $g_{t,*}$ 排在 $g_{t',*}$ 之前; 否则根据 $i_1,\ldots,i_k$ 的字典序排列 shift 多项式. 此时, 多项式 $g_{t,i_1,\ldots,i_k}(x_1X_1,\ldots,x_kX_k)$ 对应的对角线元素为 $X_1^{i_1}X_2^{i_2}\ldots X_k^{i_k}W^{m-t}$, 格基矩阵的行列式为:

$$\det(\mathcal{L})=\prod_{t=0}^{m}\prod_{x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}\in M_t\backslash M_{t+1}}X_1^{i_1}X_2^{i_2}\ldots X_k^{i_k}W^{m-t}.$$

(2) Jochemsz-May 扩展策略. 对于某些多项式, 在 Jochemsz-May 基础策略的基础上额外采用某个变元的 shift 多项式, 可以优化格基构造. 例如, 额外采用 x_1-shift 多项式, 单项式的集合 M_u 扩展为:

$$M_u:=\bigcup_{0\leqslant j\leqslant r}\left\{x_1^{i_1+j}x_2^{i_2}\ldots x_k^{i_k}:\ x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}是\ f^m 的单项式,\ 且\frac{x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}}{\lambda^u}是 f^{m-u}\ 的单项式\right\}.$$

后续格基构造与 Jochemsz-May 基础策略一致. 注意, 可以额外采用某几个变元, 或某些变元组合后的 shift 多项式, 实用中需确定变元的最优组合方式以达到最优的结果.

2.2 变元代换技巧

2000 年, Durfee 等人[11]在分析素因子 p, q 比特长度不平衡的 RSA 变体算法时提出变元代换技巧, 该技巧的核心思想是充分利用变元之间的代数关系, 通过变元代换构造更好的格基. 变元代换技巧适用于已知目标多项式部分变元之间代数关系的情形, 广泛应用于 RSA 类算法的格分析. 例如, 对于已知代数关系 $N=pq$ 的 RSA 算法, 当所求小根中有 p 或 q 时, 可通过引入新变元 (其小根为 q 或 p) 以优化格分析[19]; 对于 CRT-RSA 算法, Takayasu 等人[20,21]在代数关系 $N=pq$ 的基础上, 利用 CRT-RSA 算法特殊的代数关系 $x_q=x_p+1$ 改进了 CRT-RSA 算法的小指数攻击.

本节以 CRT-RSA 算法的小指数攻击为例, 简要介绍格基构造中的变元代换技巧. CRT-RSA 公钥为 (N,e), 私钥为 $\left(d,p,q,d_p,d_q\right)$, 其中 $N=pq$, $ed\equiv 1 \bmod \varphi(N)$, $d_p=d \bmod (p-1)$, $d_q=d \bmod (q-1)$, 假设 $e=N^{\alpha}$, $p=N^{\beta}$, $d_p=N^{\delta_p}$, $d_q=N^{\delta_q}$, 考虑素因子不平衡的 CRT-RSA, 不失一般性, 本节假设 $p<q$, 即 $\beta<0.5$. 由 $ed_q\equiv 1 \bmod (q-1)$ 可得等式:

$$ed_q = 1 + k(q-1) \tag{4}$$

于是, 破解 CRT-RSA 算法可以转换为等式 (4) 中(d_q,k,q)的求解问题. 将等式 (4) 模e, 可以得到模方程:

$$f_q(x_q,y_q) = 1 + x_q(y_q - 1) \pmod{e} \tag{5}$$

模方程 (5) 的解$(x_q^{(0)},y_q^{(0)}) = (k,q)$, 解的上界为$|x_q^{(0)}| < X_q = N^{\alpha+\beta+\delta_q-1}, |y_q^{(0)}| < Y_q = N^{1-\beta}$. 将等式 (4) 两侧同时乘$p$, 可得等式$ed_q p = N + (k-1)(N-p)$, 该等式对应模$e$的模方程为:

$$f_p(x_p,y_p) = N + x_p(N - y_p) \pmod{e} \tag{6}$$

模方程 (6) 的解$(x_p^{(0)},y_p^{(0)}) = (k-1,p)$, 解的上界为$|x_p^{(0)}| < X_p = N^{\alpha+\beta+\delta_q-1}, |y_p^{(0)}| < Y_p = N^{\beta}$.

考虑到$X_p = X_q, Y_p < Y_q$, May[22]构造了$f_p(x_p,y_p)$的x_p-shift 和y_p-shift 多项式:

$$\begin{cases} g_{[i,u]}^{x_p} = x_p^i f_p^u(x_p,y_p) e^{m-u};\ u = 0,\ldots,m;\ i = 0,\ldots,m-u \\ g_{[j,u]}^{y_p} = y_p^j f_p^u(x_p,y_p) e^{m-u};\ u = 0,\ldots,m;\ j = 1,\ldots,t \end{cases}.$$

上述 shift 多项式在模e^m下与模方程 (6) 同解. 以$m = 1, t = 2$为例, May 格攻击中的格基为:

$$\begin{array}{c} e \\ ex_p \\ f_p \\ ey_p \\ y_p f_p \\ ey_p^2 \\ y_p^2 f_p \end{array} \begin{bmatrix} e & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & eX_p & 0 & 0 & 0 & 0 & 0 \\ N & NX_p & -X_pY_p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & eY_p & 0 & 0 & 0 \\ 0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & eY_p^2 & 0 \\ 0 & 0 & 0 & 0 & NX_pY_p^2 & NY_p^2 & -X_pY_p^3 \end{bmatrix}.$$

注意, May 格基矩阵中ey_p^2是非有益多项式, 但为使格基构成三角矩阵, 非有益多项式ey_p^2是必需的.

Bleichenbacher 等人[19]利用代数关系$y_p y_q = N$, 在 May 格攻击的基础上引入新的变量y_q, 通过构造y_q-shift 多项式以优化格基矩阵的构造, 进而提升攻击效果, 本节将该工作简称为 BM 格攻击. 具体地, 对$m = 1, t = 2$, BM 格攻击将 May 格攻击的 shift 多项式ey_p^2, $y_p^2 f_p$替换为ey_q, $N^{-1}y_q f_p$, 从而得到三角格基矩阵:

$$\begin{array}{c} e \\ ex_p \\ f_p \\ ey_p \\ y_p f_p \\ ey_q \\ N^{-1}y_q f_p \end{array} \begin{bmatrix} e & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & eX_p & 0 & 0 & 0 & 0 & 0 \\ N & NX_p & -X_pY_p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & eY_p & 0 & 0 & 0 \\ 0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & eY_q & 0 \\ 0 & -X_p & 0 & 0 & 0 & Y_q & X_pY_q \end{bmatrix},$$

对于上述 May 格攻击以及 BM 格攻击, 当$\beta > \frac{2}{7}$时, 使用变元代换技巧后的 BM 格攻击效果更好.

Takayasu 等人[20,21]利用代数关系$x_q = x_p + 1$进一步优化了格基构造, 本文将该工作简称为 TLP 格攻击. BM 格攻击中, 加入$N^{-1}y_q f_p$后新增两个元素Y_q, X_pY_q, 因此为使格基构成三角矩阵, 必须引入非有益多项式ey_q. TLP 格攻击利用代数关系$x_q = x_p + 1$, 引入新的变元x_q, 可得:

$$N^{-1}y_q f_p = -x_p + y_q + x_p y_q = -x_p + y_q + (x_q - 1)y_q = -x_p + x_q y_q.$$

此时加入$N^{-1}y_q f_p$后仅新增一个元素$X_q Y_q$, 因此去掉非有益多项式ey_q后格基矩阵仍是三角矩阵:

$$\begin{array}{c} e \\ ex_p \\ f_p \\ ey_p \\ y_p f_p \\ N^{-1}y_q f_p \end{array} \begin{bmatrix} e & 0 & 0 & 0 & 0 & 0 \\ 0 & eX_p & 0 & 0 & 0 & 0 \\ N & NX_p & -X_pY_p & 0 & 0 & 0 \\ 0 & 0 & 0 & eY_p & 0 & 0 \\ 0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & 0 \\ 0 & -X_p & 0 & 0 & 0 & X_qY_q \end{bmatrix},$$

TLP 格攻击去掉了 BM 格攻击中的非有益多项式 ey_q, 同时 $X_pY_q = X_qY_q$, 因此使用变元代换技巧的 TLP 格攻击效果更好.

2.3 均衡化技巧

对于多变元方程, 不同变元小根的上界大小可能不均衡, 均衡化技巧旨在将格基的构造与小根的上界联系起来. 该技巧的核心思想是, 在格构造阶段引入新变量以限制 shift 多项式的上限, 将 shift 多项式的选取与小根的上界联系起来, 通过灵活选取 shift 多项式优化格基构造, 进而提升攻击效果. 均衡化技巧适用于多变元 (模) 方程, 特别是小根上界的大小不平衡的情形. 新变量的最优值取决于小根的上界, 现有工作中确定新变量最优值的方法大致可分为两类: 有益多项式法和极值法.

Takayasu 等人[12]提出可以利用有益多项式, 即通过收集更多的有益多项式和更少的非有益多项式优化格基构造, 提升可求解的小根的上界. 本节以 Takayasu 等人提出的 RSA 部分解密指数泄漏攻击[23]为例, 简述如何通过有益多项式的概念确定 shift 多项式的选取. RSA 算法公钥为 (N,e), 私钥为 (d,p,q), 其中 $N=pq$, $ed \equiv 1 \mod \varphi(N)$. 假设 $p \approx q \approx N^{0.5}$, $d = N^{\beta}$. 考虑解密指数 d 的高位比特泄漏场景, $d = d_0M + d_1$, 其中已知 d_0 以及 $M = 2^{\lfloor \delta \log N \rfloor}$. 由 $ed \equiv 1 \mod \varphi(N)$ 可得密钥生成等式 $ed = 1 + l(N-(p+q-1))$, 由于 d 的高位比特已知, 故可通过 d_0 估计未知量 l 的高位 $l_0 = \lfloor (ed_0M-1)/N \rfloor$, 将 $l = l_0 + l_1$ 带入密钥生成等式可得:

$$e(d_0M + d_1) = 1 + (l_0 + l_1)(N-(p+q-1)).$$

将上式模 e, 可以得到目标模方程:

$$f_{MSBs}(x,y) = 1 + (l_0 + x)(N + y) \pmod{e},$$

模方程的解 $(x_0,y_0) = (l_1, -p-q+1)$, 解的上界为 $|x_0| < X = N^{\gamma=\max\{\delta,\beta-0.5\}}, |y_0| < Y = N^{0.5}$. 对于正整数 m 以及模数 e^m, 构造 x-shift 多项式和 y-shift 多项式:

$$\begin{cases} g^{MSBs1}_{[i,u]}(x,y) = x^{u-i} f_{MSBs}(x,y)^i e^{m-i}; & u=0,\ldots,m; \quad i=0,\ldots,u \\ g^{MSBs2}_{[j,u]}(x,y) = y^{j} f_{MSBs}(x,y)^u e^{m-u}; & u=0,\ldots,m; \quad j=1,\ldots,\lfloor 2km+\tau u \rfloor \end{cases},$$

其中, 变量 k,τ 待取最优值. 由有益多项式的定义, 当 $k = \beta - \gamma, \tau = 1 + 2\gamma - 4\beta$ 时, y-shift 多项式是有益多项式, 即对于 y-shift 多项式, 有 $\det(\mathbf{B}')/\det(\mathbf{B}) < e^m$ 成立. 以此借助有益多项式的概念确定 shift 多项式的选取.

极值法广泛应用于 RSA 类算法的格分析. 例如, TLP 格攻击[20,21]采用的均衡化技巧, 在构造格基时引入新的变量 τ_p, τ_q 以确定 shift 多项式的选取. 具体地, 考虑加密指数 e 较大的场景, 对于正整数 m 以及模数 e^m, TLP 格攻击中构造的 x-shift, y-shift, f_p-shift 多项式分别为:

$$\begin{cases} g^{x_p}_{[i,j]}(x_p,y_p) = x_p^j f_p^i(x_p,y_p) e^{m-i}; & i=0,\ldots,m; \quad j=0,\ldots,m-i \\ g^{y_p}_{[i,j]}(x_p,y_p) = y_p^j f_p^i(x_p,y_p) e^{m-i}; & i=0,\ldots,m; \quad j=1,\ldots,\lceil \tau_p m \rceil \\ g^{f_q}_{[i,j]}(x_p,x_q,y_p,y_q) = f_q^j(x_q,y_q) f_p^{i-j}(x_p,y_p) e^{m-i}; & i=1,\ldots,m; \quad j=1,\ldots,\lceil \tau_q i \rceil \end{cases},$$

其中, CRT-RSA 算法参数与第 2.2 节一致, 变量 τ_p, τ_q 待取最优值. 计算出上述 shift 多项式对应的格的行列式后, 将新变量 τ_p, τ_q 以及小根的上界代入条件 (3), 可以得到关于变量 τ_p, τ_q 和小根上界的不等式, 即对于 $e = N^{\alpha}$, $d_q < N^{\delta}$, $p = N^{\beta}$, $\beta < 0.5$ 且 $\alpha > \beta/(1-\beta)$, 格攻击成功的条件为:

$$\frac{2+3\tau_p+2\tau_q}{6}(\alpha+\beta+\delta-1) + \frac{1+3\tau_p{}^2+3\tau_q}{6}\beta + \frac{\tau_q{}^2}{6}(1-\beta) + \left(\frac{2+3\tau_p+\tau_q}{6} - \frac{1+2\tau_p+\tau_q}{2}\right)\alpha < 0.$$

为使不等式左侧达到极小值, 需取 $\tau_p = \dfrac{1-2\beta-\delta}{2\beta}$, $\tau_q = \dfrac{1-\beta-\delta}{1-\beta}$. 以此通过极值法确定 shift 多项式的选取.

2.4 指数优化技巧

Lu 等人[13]在求解线性模方程时提出指数优化技巧, 其核心思想是利用已知的模数特殊指数结构, 例如模数 $N = p^r q$, 在格构造阶段引入新变量, 将多项式的选择与 r 联系起来, 以进一步优化格基构造. 指数优化技巧适用于模数有特殊指数性质的模方程求解, 常用于素数幂 RSA、共素数 RSA 算法的格分析.

本节以 LZPL 格攻击[13]中单变元模方程 $f(x)=x+a \pmod{p^v}$ 的求解为例, 简述指数优化技巧. 其中, 已知正整数 N,u,v 以及特殊指数结构 $N\equiv 0 \bmod p^u$, 素因子 p 是未知的, 小根的上界 $|x_0|<X=N^\gamma$. LZPL 格攻击引入新变量 τ 以确定 shift 多项式的上限. 具体地, 对于正整数 m, 定义 shift 多项式为:

$$g_k(x)=f^k(x)N^{\max\{\lceil v(t-k)/u\rceil,0\}};\ \ k=0,\ldots,m;\ \ t=\tau m,\ 0\leqslant\tau<1.$$

显然 $g_k(x_0)\equiv 0 \bmod p^{vt}$, 其中, 变量 τ 的值取决于 u,v,β. 具体地, 计算出上述 shift 多项式对应格的行列式后, 将 τ 以及小根上界代入条件 (3), 可得关于 τ 和小根上界的不等式, 忽略较小的项后, 上界 γ 需满足:

$$\gamma<2\beta v\tau-\frac{v\tau(\tau m+1)}{u(m+1)}.$$

为提升可求解的小根的上界, 需使不等式右侧达到极大值, 以此确定取值 $\tau=\beta u+\dfrac{1}{2m}(2\beta u-1)\approx\beta u$.

2.5 拆分线性化技巧

2009 年, Herrmann 等人[14]在分析基于模幂的伪随机数生成器时提出了拆分线性化技术. 拆分线性化的核心思想是, 在格基构造阶段引入新变元, 将 shift 多项式的集合中, 某些多变元非线性方程转化为相对直观简单的线性方程, 简化格的构造; 在此基础上, 通过进一步挖掘方程中隐含的代数关系, 优化格分析结果. 2010 年, Herrmann 等人将拆分线性化技术应用于 RSA 的小解密指数攻击[24], 达到了与目前最优的 RSA 小解密指数攻击——Boneh-Durfee 格攻击[25]相同的攻击效果, 虽然拆分线性化技术未能提升小解密指数攻击的边界, 但 Herrmann-May 的格基构造及行列式的计算比 Boneh-Durfee 格攻击简单. 拆分线性化技术适用于多变元 (模) 方程的求解, 该技巧广泛应用于 RSA 及其变体算法的格分析.

本节以 RSA 小指数攻击, 即 Herrmann-May 格攻击为例[24], 简述拆分线性化的基本思想. 记 RSA 公钥为 (N,e), 私钥为 (d,p,q), 其中 $N=pq$, $ed\equiv 1 \bmod \varphi(N)$. 由等式 $ed=l(p-1)(q-1)+1$ 可导出模方程:

$$f(x,y)=x(N+y)+1 \pmod{e}.$$

模方程的解 $(x_0,y_0)=(l,1-p-q)$, 假设 $e\approx N$, $d=N^\beta$, $p\approx q$, 小根的上界 $|x_0|<X=N^\beta$, $|y_0|<Y=N^{0.5}$. 对于正整数 m 以及模数 e^m, Boneh-Durfee 格攻击构造了下述 shift 多项式:

$$\begin{cases} g^x_{[u,i]}(x,y)=x^{u-i}f^i(x,y)e^{m-i}; & u=0,\ldots,m;\quad i=0,\ldots,u\\ g^y_{[u,j]}(x,y)=y^jf^u(x,y)e^{m-u}; & u=0,\ldots,m;\quad j=1,\ldots,t\end{cases}.$$

根据均衡化技巧取 $t=(1-2\beta)u$. 显然, 上述 shift 多项式满足 $g^x_{[u,i]}(x_0,y_0)\equiv g^y_{[u,j]}(x,y)(x_0,y_0)\equiv 0 \bmod e^m$. 将 $g^x_{[u,i]}(xX,yY)$ 和 $g^y_{[u,j]}(xX,yY)$ 的系数作为格基向量, 构成的格基矩阵为三角矩阵, 例如, 对于 $m=2$, $t=2$, Boneh-Durfee 格基矩阵为:

$$\begin{array}{c} \\ e^2\\ xe^2\\ \\ \vdots\\ \\ \\ \\ \\ y^2e^2\\ \\ \vdots\\ \\ \end{array}\begin{bmatrix} e^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & Xe^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ e & NXe & XYe & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & X^2e^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & Xe & 0 & NX^2e & X^2Ye & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 1 & 2NX & 2XY & N^2X^2 & 2NX^2Y & X^2Y^2 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & Ye^2 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & Y^2e^2 & 0 & 0 & 0 & 0\\ 0 & 0 & NXYe & 0 & 0 & 0 & Ye & 0 & XY^2e & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & Y^2e & NXY^2e & XY^3e & 0 & 0\\ 0 & 0 & 2NXY & 0 & N^2X^2Y & 2NX^2Y^2 & Y & 0 & 2XY^2 & 0 & X^2Y^3 & 0\\ 0 & 0 & 0 & 0 & 0 & N^2X^2Y^2 & 0 & Y^2 & 2NXY^2 & 2XY^3 & 2NX^2Y^3 & X^2Y^4 \end{bmatrix}.$$

虽然 y^2e^2 是非有益多项式, 但去掉 y^2e^2 后的格基矩阵不再是满秩矩阵, 当矩阵维数较大时, 非满秩矩阵行列式的计算较为复杂. Boneh-Durfee 格攻击去掉部分非有益多项式后, 利用非满秩的子格输出短向量, 使用几何渐进矩阵估计非满秩格基矩阵的行列式, 这种方法十分复杂.

Herrmann-May 格攻击通过引入新变元 $z=xy+1$, 将 $f(x,y)=x(N+y)+1 \pmod e$ 转换为线性模方程:

$$\hat{f}(x,y,z)=z+Nx=0 \pmod e.$$

解 $(x_0,y_0,z_0)=(k,1-p-q,1-k(p+q-1))$, 小根的上界 $|x_0|<X=N^{\beta}$, $|y_0|<Y=N^{0.5}$, $|z_0|<Z=XY$. 对于正整数 m 以及模数 e^m, Herrmann-May 格攻击构造了下述 shift 多项式:

$$\begin{cases} \hat{g}^x_{[u,i]}(x,y,z)=x^{u-i}\hat{f}^i(x,y)e^{m-i}; & u=0,\ldots,m; \quad i=0,\ldots,u \\ \hat{g}^y_{[u,j]}(x,y,z)=y^j\hat{f}^u(x,y)e^{m-u}; & u=0,\ldots,m; \quad j=1,\ldots,t \end{cases},$$

其中, 根据均衡化技巧, 变量 t 取 $(1-2\delta)u$ 时最优. 显然 $\hat{g}^x_{[u,i]}(x_0,y_0,z_0)\equiv\hat{g}^y_{[u,j]}(x_0,y_0,z_0)\equiv 0 \pmod{e^m}$. 将 $\hat{g}^x_{[u,i]}(xX,yY,zZ)$ 和 $\hat{g}^y_{[u,j]}(xX,yY,zZ)$ 的系数作为格基向量, 对于 $m=2$, $t=1+u$, Herrmann-May 格基矩阵为:

$$\begin{bmatrix} e^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Xe^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & NXe & Ze & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & X^2e^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & NX^2e & XZe & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & N^2X^2 & 2NXZ & Z^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & Ye^2 & 0 & 0 & 0 & 0 \\ -Ne & 0 & NZe & 0 & 0 & 0 & 0 & YZe & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -NYe & NYZe & Y^2Ze & 0 & 0 \\ 0 & -N^2X & -2NZ & 0 & N^2XZ & 2NZ^2 & 0 & 0 & 0 & YZ^2 & 0 \\ N^2 & 0 & -2N^2Z & 0 & 0 & N^2Z^2 & 0 & -2NYZ & 0 & -2NYZ^2 & Y^2Z^2 \end{bmatrix}.$$

Herrmann-May 格攻击构造的格不包含非有益多项式 y^2e^2, 同时, 格基矩阵仍是下三角矩阵. 事实上, 多项式 $\hat{g}^y_{[u,j]}(x,y,z)$ 中某些单项式同时包含变元 x 和 y, 例如 $y\hat{f}^2=x^2y+xyz+yz^2$, 利用代数关系 $xy=z-1$ 替换其中的 xy 后, 格基即为三角矩阵.

2.6 两步格方法

Peng 等人[15]在讨论 RSA 模数隐式分解问题的工作中提出两步格方法. 其核心思想是将困难问题的求解分为两步, 首先构造一个维数较低的格, 将目标变元或向量嵌入低维格中, 采用格基约化算法将目标变元分裂为多个更小变元的线性组合; 然后利用分裂后小变元间的代数关系, 导出一个新的模方程, 再进行格分析得到最终结果. 两步格方法主要应用于对偶 RSA[26]的格分析、求解 RSA 模数隐式分解问题等.

本节以对偶 RSA 方案的格分析为例[27], 简述两步格方法的基本原理. 假设对偶 RSA 方案 $N_1=p_1q_1$, $N_2=p_2q_2$, 用户 1 和用户 2 的密钥分别为 $(pk_1=(N_1,e),sk_1=(p_1,q_1,d))$ 和 $(pk_2=(N_2,e),sk_2=(p_2,q_2,d))$, 两个用户拥有相同的加密指数 e 和解密指数 d, 且 $\log N_1\approx\log N_2$. 于是, 有:

$$\begin{cases} ed=k_1(N_1-p_1-q_1+1)+1 \\ ed=k_2(N_2-p_2-q_2+1)+1 \end{cases}.$$

首先, 选择一个比特长度约为 $\frac{1}{2}\log N_1$ 的正整数 A, 构造一个二维格 $\mathcal{L}_1=\begin{bmatrix} A & e \\ 0 & N_1 \end{bmatrix}$, 并计算出格 $\mathcal{L}_1$ 上的两个短向量 λ_1 和 λ_2, 其中 $\lambda_1=[l_{11},l_{12}]$, $\lambda_2=[l_{21},l_{22}]$. 对于格 $\mathcal{L}_1$ 上的一个特殊向量 $\mathbf{v}$:

$$\begin{aligned} \mathbf{v}&=d[A,e]-k_1[0,N_1]=[Ad,ed-k_1N_1] \\ &=a_1\lambda_1+a_2\lambda_2=[a_1l_{11}+a_2l_{21},a_1l_{12}+a_2l_{22}]. \end{aligned}$$

因此, $d=a_1\frac{l_{11}}{A}+a_2\frac{l_{21}}{A}$, 其中 a_1 和 a_2 是未知的. 令 $l'_{11}=\frac{l_{11}}{A}$, $l'_{21}=\frac{l_{21}}{A}$, 将 d 代入用户 2 的密钥生成等式, 有 $ed=k_2(N_2-p_2-q_2+1)+1=e(a_1l'_{11}+a_2l'_{21})$, 该等式模 el'_{21} 可以得到目标模方程:

$$f(x,y,z)=x(N_2+y)-el'_{11}z+1\equiv 0 \pmod{el'_{21}}.$$

模方程的解为 $(x_0,y_0,z_0)=(k_2,-p_2-q_2+1,a_1)$. 通过两步格方法, 将求解较大未知量 d 转换为了求解较小未知量 a_1, 进而可以通过 Coppersmith 方法求解.

3 标准 RSA 的格分析

对于标准 RSA 密码体制, 记公钥为 (N,e), 私钥为 (d,p,q), 其中 p,q 是两个随机选取的大素数, 二者的比特长度通常是相等的; $N=pq$ 为 RSA 模数; e 是随机选取的满足 $\gcd(e,\varphi(N))=1$ 的正整数, 其中欧拉函数 $\varphi(N)=(p-1)(q-1)$; d 是满足 $ed\equiv 1 \mod \varphi(N)$ 的正整数, 可以由扩展欧几里得算法高效计算. RSA 问题的困难性依赖于大整数分解问题的困难性, 除 Shor[28]提出的量子算法外, 目前非量子计算模型下暂时没有可以在多项式时间内分解大整数的算法. 对于 p,q 比特长度近似相等的情形, 目前已知最优的大整数分解算法是数域筛法, 其渐近时间复杂度为亚指数级别.

虽然 RSA 问题理论上是困难的, 但 RSA 问题的某些特殊实例可以在多项式时间内求解. 例如, 实用中为提升 RSA 加密或解密效率, 一个最简单直接的方法是选取较小的加密指数 e 或解密指数 d, 但使用较小的加密或解密指数会导致密码系统面临被攻破的风险, 见第 3.2 节小指数攻击.

另一方面, 虽然理论上私钥是完全保密的, 但密码系统在实际运行过程中会受到某些物理攻击, 这些攻击有时可恢复私钥的部分比特信息, 如果能通过这部分泄漏的私钥信息恢复出整个私钥, 那么这种攻击会对 RSA 密码体制产生严重威胁. 目前的泄漏模型大致可以分为 5 类:

(1) 最高有效位 (most significant bits, MSBs) 泄漏.

(2) 最低有效位 (least significant bits, LSBs) 泄漏.

(3) 最高有效位 MSBs 和最低有效位 LSBs 同时泄漏.

(4) 中间有效位 (middle bits, MBs) 泄漏.

(5) 非连续有效位泄漏.

特别地, 记 n 为未知比特块的个数, 那么前 3 类可视为 $n=1$ 时的非连续有效位泄漏, 第 4 类 MBs 泄漏可视为 $n=2$ 时的非连续有效位泄漏. 私钥的泄漏来源于针对 RSA 密码系统的侧信道攻击, 包括故障攻击[29]、计时攻击[30]以及能量攻击[31]等, 或者来源于社会工程学, 包括密码系统的使用不当导致私钥或随机数的泄漏等. 通过上述非数学手段获得私钥部分比特后, 需要借助格分析等数学方法恢复整个私钥. 注意, 信息泄漏场景下的格分析方法通常假设已拿到了私钥的部分比特, 不关注泄漏比特的具体获得方式. 利用模数素因子 p 或 q 的泄漏比特的格分析方法见第 3.1 节, 模数分解攻击; 利用解密指数 d 的泄漏比特的格分析方法见第 3.3 节, 部分私钥泄漏攻击.

3.1 模数分解攻击

已知模数素因子 p 或 q 部分比特的前提下, 分解 RSA 模数 N 的攻击方式即模数分解攻击, 也被称为已知比特分解问题. 由于实用中 RSA 素因子 p 和 q 的比特长度通常是相等的, 不失一般性, 本节假设泄漏 p 的部分比特. 模数分解攻击最早是由 Rivest 等人[32]于 1985 年提出, 利用整数规划方法在已知 p 的 $\frac{2}{3}$ 连续比特时成功分解了模数 N.

Coppersmith[6]利用格分析方法给出了更好的结果. 假设 $\widetilde{p}$ 表示已知比特对应的十进制数, 对于 MSBs 泄漏攻击, 构造模方程 $f_M(x)=\widetilde{p}+x \pmod p$; 对于 LSBs 泄漏攻击, 构造模方程 $f_L(x)=x\cdot 2^t+\widetilde{p} \pmod p$, 其中整数 t 表示 $\widetilde{p}$ 的比特长度, 注意, $2^{-t} \mod N$ 是可高效计算的, 因此 $f_L(x)$ 可高效地转化为首一多项式 $f'_L(x)=x+\widetilde{p}\cdot 2^{-t} \pmod p$. 通过格分析方法计算上述首一单变元模方程的小根, 即可恢复私钥 p. 目前, 已知 p 的 50% 连续比特即可在多项式时间内成功分解模数 N.

Herrmann 等人[33]首次考虑了素因子非连续有效位泄漏场景下的模数分解攻击, 假设存在 n 个未知比特块, 令 $\widetilde{p}_n,\widetilde{p}_{n-1},\ldots,\widetilde{p}_0$ 分别表示已知比特块对应的十进制数, 通过格分析方法计算 n 变元线性模方程 $f(x_1,\ldots,x_n)=\widetilde{p}_n+x_n2^{t_n}+\widetilde{p}_{n-1}+\ldots+x_12^{t_1}+\widetilde{p}_0 \pmod p$ 的小根, 即可恢复私钥 p. 目前, 已知 p 的 $\ln 2\approx 70\%$ 随机比特即可在多项式时间内分解模数 N, 但该算法的时间复杂度与未知比特块数 n 是指数相关的.

3.2 小指数攻击

密码系统的安全性不仅依赖于底层困难问题的计算复杂度, 还与密码系统的实际参数密切相关. 实用中为提升 RSA 加密或解密效率, 一个最简单直接的方法是选取较小的加密指数 e 或解密指数 d, 但是当 e 或 d 较小时会受

到小加密或解密指数攻击. 与小加密指数攻击相比, 小解密指数攻击的成功条件相对简单, 只要求解密指数 $d < N^{0.292}$ 即可攻破 RSA 密码系统. 此外, 前者通常恢复的是一条或者几条明文, 而后者可以完全攻破 RSA 密码系统. 本节主要介绍现有 RSA 小加密指数攻击和小解密指数攻击, 如无特殊说明, 本文中的小指数攻击指小解密指数攻击.

(1) 小加密指数攻击. Coppersmith[7]提出了 RSA 小加密指数攻击. 具体地, 假设已知密文 $c = m^e \mod N$ 以及明文高位 m_0, 要求计算明文低位 $m_1 \approx N^\delta$, 满足 $(m_0 + m_1)^e \equiv c \mod N$, 即求解 $f(x) = (m_0 + x)^e - c \pmod N$, 该方程的解 $x_0 = m_1$, 解的上界为 $|x_0| < X = N^\delta$. 当 $|m_1| < N^{\frac{1}{e}}$ 时, 简单应用格分析方法即可恢复明文的全部比特. 例如, 对于 $e = 3$ 的 RSA 加密算法, 当已知明文高位 $\frac{2}{3}$ 连续比特时, 即可在多项式时间内恢复明文.

(2) 小解密指数攻击. 最早的小解密指数攻击是 Wiener 连分式攻击[34], 1990 年, Wiener 提出如果解密指数 $d < \frac{1}{3}N^{0.25}$, 那么敌手就能够在多项式时间内分解模数 N, 从而恢复完整的私钥并攻破 RSA 密码系统, 整个攻击依赖连分式有理逼近的性质. 随后, 2000 年, Boneh 等人[25]采用格分析方法提升了小指数攻击的结果, 将 Wiener 攻击的边界从 $d < \frac{1}{3}N^{0.25}$ 提升至 $d < N^{0.292}$, Boneh-Durfee 格攻击是目前最优的小解密指数攻击. 2010 年, Herrman 等人[24]将拆分线性化技术应用于 RSA 小指数攻击, 优化了 Boneh-Durfee 格攻击的格结构, 虽然没有提升小指数攻击的边界, 但给出了更简洁的格基构造方法. 后续工作对小指数攻击进行了深入的研究[35], 但目前 $d \leqslant N^{0.292}$ 仍是小指数攻击最好的结果.

Boneh-Durfee 格攻击是 Coppersmith 方法早期的启发式应用, 它很大程度上扩展了 Coppersmith 原始方法在 RSA 小解密指数攻击的求解范围, 也是第一个考虑使用子格来优化格基构造的工作. Boneh-Durfee 格攻击及后续工作是围绕着如何用格分析方法计算双变元模方程小根展开的. 具体地, 根据 RSA 密钥生成等式 $ed \equiv 1 \mod \varphi(N)$, 可得等式 $ed = 1 + k\varphi(N) = 1 + k(N - (p + q - 1))$, 模 e 后可以得到双变元模方程:

$$f_e(x, y) = Nx + xy + 1 \pmod e.$$

模方程的解为 $(x_0, y_0) = (k, -(p + q - 1))$. 假设 $e = N^\alpha$, $d = N^\delta$, 于是待求的小根满足如下条件:

$$\begin{cases} |x_0| = k = (ed - 1)/\varphi(N) < 2ed/N = 2N^{\alpha+\delta-1} = X \\ |y_0| = p + q - 1 < 3N^{0.5} = Y \end{cases}.$$

对于正整数 m, 构造 x-shift 多项式和 y-shift 多项式, 使得小根 (x_0, y_0) 是它们在模 e^m 下的根:

$$\begin{cases} g_{i,k}(x, y) = x^i f_e^k(x, y) e^{m-k} \\ h_{j,k}(x, y) = y^j f_e^k(x, y) e^{m-k} \end{cases},$$

其中, 参数 i, j, k 的范围需慎重选取. 后续应用格分析方法即可恢复小根 $(k, -p - q + 1)$. 将 Boneh-Durfee 格攻击构造的格记为 $\mathcal{L}$, 根据格分析方法的基本原理, 当格 $\mathcal{L}$ 满足条件 (3), 即第 1.2 节的公式 (3) 时, 才可以恢复小根 $(k, -p - q + 1)$, 从而攻破 RSA 密码系统. 因此 Boneh-Durfee 攻击及其后续工作的重心在于研究如何选择参数 i, j, k, 使得 $\det(\mathcal{L})^{\frac{1}{\dim(\mathcal{L})}}$ 尽可能小. Boneh-Durfee 攻击首先选取了如下参数以确保格基矩阵是一个满秩三角矩阵:

$$\begin{cases} \{g_{i,k}(x, y):\ 0 \leqslant k \leqslant m,\ 0 \leqslant i \leqslant m - k\} \\ \{h_{j,k}(x, y):\ 0 \leqslant k \leqslant m,\ 1 \leqslant j \leqslant t\} \end{cases},$$

其中, 新引入的变量 t 用于控制 y-shift 多项式个数, 旨在通过均衡化技巧灵活选取 shift 多项式, 进而提升攻击效果. 事实上, 如果不引入 y-shift 多项式, Boneh-Durfee 格攻击仅在 $d < N^{0.25}$ 时才能成功, 而引入 y-shift 多项式后, 可求解的小指数上界扩展为 $d < N^{0.2847}$, 这一边界被称为 Boneh-Durfee 格攻击的弱边界.

为确保格基矩阵是满秩三角矩阵, Boneh-Durfee 的格构造中收集了一些非有益多项式. 为进一步提升攻击效果, 一个简单直接的方法是直接去掉这些非有益多项式, 利用 $\mathcal{L}$ 的子格进行求解. 在 Boneh-Durfee 格基矩阵的基础上, 直接去掉非有益多项式会得到一个非满秩格基矩阵. 格的维度较大时, 计算非满秩格基矩阵的行列式十分复杂, 为解决这一问题, Boneh 等人[25]引入一类被称为“几何渐进矩阵”的特殊矩阵, 以此估计非满秩矩阵的行列式. Boneh 等人[25]通过去掉非有益多项式, 将可求解的小指数的上界扩展为 $d < N^{0.292}$, 这一边界被称为 Boneh-Durfee

格攻击的强边界, 至今没有其他攻击能够超过这一界限.

Herrman 等人[14]提出拆分线性化技术并将其应用于 RSA 的小解密指数攻击, 同样得到了 $d < N^{0.292}$ 这一界限, 同时不再需要使用几何渐进矩阵这种复杂的分析方式. 拆分线性化的核心思想是, 将目标方程 $f_e(x,y) = Nx + xy + 1 \pmod{e}$ 中的 $xy+1$ 看成新变元 u, 从而将原方程线性化为 $\hat{f}_e(x,u) = u + Nx \pmod{e}$. 后续构造格基时, 利用代数关系 $xy+1=u$ 简化格基的构造, 拆分线性化的具体细节见第 2.5 节. 拆分线性化技术在去掉非有益多项式的同时, 保证了格基矩阵仍是满秩三角矩阵, 虽然未能提升格分析的攻击效果, 但简化了行列式的计算.

事实上, RSA 小解密指数攻击可以抽象为一个“小逆问题”, 即寻找一个绝对值较小的整数 $-k$, 使得它在模 e 下的逆 $N-(p+q-1)$ 接近于 N. Boneh 等人[25]提出, 只要 $d < N^{0.5}$ 小逆问题就有唯一解. 不少学者认为, $d < N^{0.292}$ 这一界限是格分析方法所能攻击的极限. 因此, 目前学术界的一个公开问题是, 是否存在更好的攻击方法, 使得可求解的小指数的上界超过 $N^{0.292}$.

3.3 部分私钥泄漏攻击

本节介绍基于格分析方法的标准 RSA 部分私钥泄漏攻击. 本文中的部分私钥泄漏攻击指部分解密指数泄漏攻击, 假设敌手已获得解密指数 d 的部分比特, 不关注泄漏的获取方式. 解密指数的泄漏位置、泄漏量, 以及解密指数的大小, 对 RSA 算法的安全性有着不同的影响. 基于格的部分私钥泄漏攻击可视为小解密指数攻击的推广, 同样是在 Coppersmith 方法的框架下, 在 Jochemsz-May 通用格基构造方法的基础上, 根据具体泄漏场景使用特殊格基构造技巧, 如均衡化技巧、拆分线性化技巧.

● MSBs 泄漏攻击. 假设 $e = N^{\alpha}$, $d = N^{\beta}$, 敌手通过某些方式获取了解密指数的 MSBs, 记为 $\hat{d}$, $|d-\hat{d}| < N^{\delta}$, 其中 $0 \leqslant \delta \leqslant \beta$. 记 $d_0 = d - \hat{d}$ 为 d 未知的低位, RSA 密钥生成等式可写作 $e\left(\hat{d}+d_0\right) - l(N-(p+q-1)) - 1 = 0$, 其中 d_0, l, $(p+q-1)$ 是未知的. 于是 RSA 问题就转化为求解三变元整数方程:

$$f_M(x,y,z) = ex + y(z-N) + e\hat{d} - 1.$$

该方程的解 $(x_0,y_0,z_0) = (d_0, l, p+q-1)$, 待求的小根满足如下条件:

$$\begin{cases} |x_0| = |d_0| = \left|\hat{d}-d\right| < N^{\delta} = X \\ |y_0| = |l| = (ed-1)/\varphi(N) < ed/\varphi(N) < N^{\alpha+\beta-1} = Y \\ |z_0| = |p+q-1| < N^{0.5} = Z \end{cases}.$$

注意, 若仿照第 3.2 节小解密指数攻击, 直接导出模 e 的目标模方程 $f(x,y,z) = y(z-N) - 1 \pmod{e}$, 会丢失泄漏信息. 因此, 需通过 Coppersmith 方法求解三变元整数方程 $f_M(x,y,z) = 0$, 进而恢复私钥 d.

为进一步利用泄漏信息, 可以借助解密指数 d 泄漏的 MSBs 降低变元 y 的上界. 具体地, 由于 d 和 l 满足等式 $ed = 1 + l(N-(p+q-1))$, 且已知 d 的高位比特 $\hat{d}$, 故可通过 $\hat{d}$ 估计未知量 l 的高位 $\hat{l} = \left\lfloor \left(e\hat{d}-1\right) \Big/ N \right\rfloor$, 记 $l = \hat{l} + l_0$ 并带入 RSA 密钥生成等式可得 $e\left(\hat{d}+d_0\right) = 1 + \left(\hat{l}+l_0\right)(N-(p+q+1))$, 由此得到三变元整数方程:

$$\hat{f}_M(x,y',z) = ex + \left(y' + \hat{l}\right)(z-N) + e\hat{d} - 1.$$

该方程的解 $\left(x_0, y_0', z_0\right) = (d_0, l_0, p+q-1)$, 与变元 y 相比, y' 小根的上界降低为:

$$\left|y_0'\right| = |l_0| = \left|l - \hat{l}\right| = \left| \frac{e\left(\hat{d}+d_0\right)-1}{\varphi(N)} - \left\lfloor \frac{e\hat{d}-1}{N} \right\rfloor \right| < \max\left\{N^{\alpha+\delta-1}, N^{\alpha+\beta-1.5}\right\} = Y'.$$

将泄漏信息嵌入小根上界 Y' 的另一个优势是, 可以在保留泄漏信息的同时导出目标模方程. 具体地, 三变元整数方程 $\hat{f}_M(x,y',z)$ 模 e 后可转化为双变元模方程:

$$\hat{f}_M(y',z) = \left(y' + \hat{l}\right)(z-N) - 1 \pmod{e},$$

嵌入了泄漏信息的同时减少了变元个数, 使格分析方法更简洁直观.

在早期 RSA 的 MSBs 泄漏攻击中, 格分析方法主要围绕三变元整数方程的求解展开, 同时对加密指数 $e = N^{\alpha}$ 的大小有一定的限制. Boneh 等人[36]甚至可以在 $\alpha < 0.5$ 时基本确定 l 的范围, 在额外泄漏长度为 $1-\alpha$ 的解密指数

MSBs 后, 可在多项式时间内恢复解密指数 d. 2005 年, Ernst 等人[37]首次考虑了公钥尺寸 $e \approx N$ 的攻击场景. 后续工作围绕双变元模方程 $\widehat{f_M}(y',z) \equiv 0 \mod e$ 的求解展开[23,38]. 2014 年, Takayasu 等人[23]借助变元代换、拆分线性化等格基构造技巧, 将未知量 $\left|d-\hat{d}\right| < N^{\delta}$ 的界限进一步提升至:

$$\begin{cases} \delta < \dfrac{1}{2}\left(1+\beta-\sqrt{-1+6\beta-3\beta^2}\right), & \beta \leqslant 0.5 \\ 6\gamma\sigma-3\sigma^2+2\sigma^3 < (\sigma-2(\beta-\gamma))^3 \Big/ (2+2\gamma-4\beta), & 0.5 < \beta \leqslant 0.5625 \end{cases},$$

其中, $\gamma = \max\left\{\delta, \beta-\dfrac{1}{2}\right\}, \sigma = 1-(2\beta-1)\Big/\left(1-2\sqrt{1+\gamma-2\beta}\right)$. Takayasu-Kunihiro 格攻击[23]是目前已知的 MSBs 泄漏场景下, RSA 部分私钥泄漏攻击的最优结果.

● LSBs 泄漏攻击. 假设 $e = N^{\alpha}$, $d = N^{\beta}$, 敌手获取了解密指数的 LSBs, 记为 $\tilde{d} = d \mod M$, M 为 2 的方幂. 于是解密指数 $d = d_0 M + \tilde{d}$, 其中 d_0 是未知量, 且 $|d_0| < N^{\delta}$. 此时可建立与 MSBs 泄漏情形类似的等式 $e\left(Md_0+\tilde{d}\right) = 1 + l(N-(p+q-1))$, 于是 RSA 问题就转化为求解三变元整数方程:

$$f_L(x,y,z) = eMx - Ny + yz + e\tilde{d} - 1.$$

该方程的解 $(x_0,y_0,z_0) = (d_0, l, p+q-1)$. 与 MSBs 泄漏场景的不同之处在于, 此时不能利用 d 的泄漏比特估计 l 的高位, 故小根的上界为 $|x_0| < X,\ |y_0| < Y,\ |z_0| < Z$. 与 MSBs 泄漏场景类似, 若仿照第 3.2 节小解密指数攻击导出目标模方程 $f(x,y,z) = y(z-N) - 1 \pmod e$, 同样会丢失泄漏信息. 因此, 需通过 Coppersmith 方法求解三变元整数方程 $f_L(x,y,z) = 0$, 进而恢复私钥 d.

考虑到 $\tilde{d}$ 的比特长度是已知的, 即已知 M, 故可以构造模数为 eM 的目标模方程:

$$f_L(y,z) = y(z-N) + e\tilde{d} - 1 \pmod{eM},$$

嵌入了泄漏信息的同时减少了变元的个数, 使格分析方法更简洁直观.

与泄漏 MSBs 情形类似, 早期 RSA 的 LSBs 泄漏攻击主要围绕三变元整数方程的求解展开, 同时对加密指数 $e = N^{\alpha}$ 的大小有一定的限制. Boneh 等人[36]考虑了加密指数 e 较小的情形, 在 e 为常数大小时, 只要泄漏 25% 的解密指数即可攻破 RSA; 在 $\alpha < 1$ 且非常数大小时, 未知量 $\delta \leqslant \dfrac{5}{6} - \dfrac{1}{3}\sqrt{6\alpha-1}$ 即可攻击成功. Ernst 等人[37]首次提出了公钥尺寸 $e \approx N$ 的部分私钥 LSBs 泄漏攻击. 后续工作围绕模方程 $f_L(y,z) \equiv 0 \mod eM$ 的求解展开[23,39,40]. 2014 年, Takayasu 等人[23]利用拆分线性化将未知量界限进一步提升至:

$$\delta < \frac{1}{2}\left(1+\beta-\sqrt{-1+6\beta-3\beta^2}\right),\ \beta \leqslant \frac{1}{12}\left(9-\sqrt{21}\right).$$

Takayasu-Kunihiro 格攻击[23]是目前已知的 LSBs 泄漏场景下, RSA 部分私钥泄漏攻击的最优结果.

● 同时泄漏 MSBs 和 LSBs 攻击. 除泄漏 MSBs 和泄漏 LSBs 两种攻击场景外, Ernst 等人[37]还考虑了同时泄漏 MSBs 和 LSBs 时的格攻击. 假设 $e = N^{\alpha}$, $d = N^{\beta}$, 且敌手通过某些方式获取了解密指数的高位 $\hat{d}$ 和低位 $\tilde{d}$, 于是有 $d = \hat{d}M_2 + d_0 M_1 + \tilde{d}$, 其中 d_0 是未知量, 且 $|d_0| < N^{\delta}$; 正整数 M_1, M_2 均为 2 的方幂, 可由泄漏比特的长度计算. 此时由密钥生成等式可导出整数方程 $f(x,y,z) = eMx - Ny + yz + R = 0$, 其中 $R = e\tilde{d} + eM_1M_2\hat{d} - 1$ 为已知常数, 于是 RSA 问题就转化为求解三变元整数方程小根问题. 利用与泄漏 MSBs 中类似的技巧对 l 的高位估值, 可得到更优的攻击结果.

STK 格攻击[41]将 Takayasu-Kunihiro 格攻击[23]推广至同时泄漏 MSBs 和 LSBs 的攻击场景, 具体的, 与分别泄漏 MSBs 及 LSBs 场景中模方程的导出类似, 同时泄漏 MSBs 和 LSBs 比特场景下的 RSA 问题可以转化为求解下述模方程组:

$$\begin{cases} \hat{f}_M(y',z) = \left(y'+\hat{l}\right)(z-N) - 1 \pmod e \\ f_L(y,z) = y(z-N) + e\tilde{d} - 1 \pmod{eM} \end{cases}.$$

模方程的解及解的上界与上文中一致. STK 格攻击的核心思想是, 使用 Takayasu-Kunihiro 格攻击在 LSBs 泄漏场景下的格基构造方法, 在此基础上采用其在 MSBs 泄漏场景下的拆分规则. LSBs 泄漏量为 0 的 STK 格攻击退化为了 Takayasu-Kunihiro 的 MSBs 泄漏攻击, 类似的, MSBs 泄漏量为 0 的 STK 格攻击退化为了 Takayasu-Kunihiro 的 LSBs 泄漏攻击, 同时泄漏 MSBs 和 LSBs 的部分私钥泄漏攻击可视为泄漏 MSBs、泄漏 LSBs 攻击的推广.

MSBs 泄漏、LSBs 泄漏、以及 MSBs 和 LSBs 同时泄漏均可视为解密指数未知比特块个数 $n=1$ 的泄漏场景. 目前, $n=1$ 的泄漏场景下, 基于格的 RSA 部分私钥泄漏攻击成功所需的泄漏量均与解密指数 d 的大小有关, 解密指数 d 越大, 格攻击所需的解密指数泄漏比例越高, 泄漏量的下界可参考表 1.

表 1　RSA 部分私钥泄漏攻击的泄漏量下界

攻击类型	$\log_N d$	高位		低位		格攻击
		泄漏量$\log_N d_{\text{MSBs}}$	泄漏百分比 (%)	泄漏量$\log_N d_{\text{LSBs}}$	泄漏百分比 (%)	
小指数攻击	0.292	0	0	0	0	Boneh-Durfee[25]
MSBs泄漏攻击	0.3	0.01401	4.67	0	0	Takayasu-Kunihiro[23]
	0.4	0.17958	44.90	0	0	
	0.5	0.30902	61.80	0	0	
	0.5625	0.37500	66.67	0	0	
LSBs泄漏攻击	0.3	0	0	0.01401	4.67	
	0.32	0	0	0.05141	16.06	
	0.34	0	0	0.08629	25.38	
	0.36812	0	0	0.13188	35.83	
同时泄漏MSBs和LSBs攻击	0.3	0.00701	23.37	0.007	23.33	STK格攻击[41]
	0.4	0.14130	35.33	0.04	10	
	0.5	0.22915	45.83	0.1	20	

● MBs 泄漏攻击和非连续有效位泄漏攻击. 对于解密指数未知比特块个数 $n>1$ 的攻击场景, 现有格分析工作通常将 n 个未知块视为 n 个变元, 通过密钥生成等式导出多变元方程, 进而采用格分析方法恢复解密指数.

Sarkar[42]首次考虑了解密指数未知比特块的个数 $n>1$ 的攻击场景, 假设解密指数 d 存在 n 个未知比特块, 记 $d=\widetilde{d}_n+D_n2^{t_n}+\widetilde{d}_{n-1}+D_{n-1}2^{t_{n-1}}+\ldots+\widetilde{d}_1+D_12^{t_1}+\widetilde{d}_0$, 其中, $\widetilde{d}_n,\widetilde{d}_{n-1},\ldots,\widetilde{d}_0$ 分别表示已知比特块对应的十进制数, $t_1,\ldots,t_n$ 是已知正整数, RSA 密钥生成等式可写作 $e\left(\widetilde{d}_n+D_n2^{t_n}+\ldots+D_12^{t_1}+\widetilde{d}_0\right)-l(N-(p+q-1))-1=0$, 于是可将 RSA 问题转化为 $n+2$ 变元整数方程 $f(x_1,\ldots,x_{n+2})=e\left(\widetilde{d}_n+x_n2^{t_n}+\ldots+x_12^{t_1}+\widetilde{d}_0\right)-x_{n+1}(N+x_{n+2})-1=0$ 的求解问题, 应用 Jochemsz-May 通用策略和均衡化等技巧即可恢复解密指数. 假设 $e\approx N$, $d=N^{\beta}$ 且 $\beta<0.75$, 根据 Sarkar[42]的结果, 已知 $\left(\beta+\frac{1}{2}\sqrt{1+4\beta}-1\right)\log N$ 随机比特即可在多项式时间内恢复 d, 但该算法的时间复杂度与未知比特块数 n 是指数相关的.

随后, Wang 等人[43]改进了 MBs 泄漏场景下, 即 $n=2$ 时 Sarkar[42]的结果, 记 $d=d_22^{t_2}+\widetilde{d}_12^{t_1}+d_0$, 其中 $\widetilde{d}_1$ 是泄漏比特, t_1,t_2 是已知正整数, 由密钥生成等式 $e\left(d_22^{t_2}+\widetilde{d}_12^{t_1}+d_0\right)-l(N-(p+q-1))-1=0$ 可导出模方程 $f(x,y,z)=ex-y(N-z)+e\widetilde{d}_12^{t_1}\pmod{e2^{t_2}}$, 以此将泄漏信息嵌入格结构.

理论上, 泄漏比特为 0 的部分私钥泄漏攻击等价于小指数攻击, 故部分私钥泄漏攻击可视为小指数攻击的推广. 因此, RSA 的部分私钥泄漏攻击致力于覆盖最优的小指数攻击界限, 即 Boneh-Durfee 格攻击的强边界 $d<N^{0.292}$. 早期部分私钥泄漏攻击[36−39]只能达到 Boneh-Durfee 格攻击的弱边界 $d<N^{0.284}$, 随着 Coppersmith 方法的完善与格基构造方法的发展, 借助拆分线性化等特殊格基构造技巧, 后续 RSA 部分私钥泄漏攻击[23,40,41]已达到 Boneh-Durfee 格攻击的强边界 $d<N^{0.292}$.

总的来说, RSA 的部分私钥泄漏攻击大多沿用了 Jochemsz-May 通用格基构造策略, 在此基础上使用变元代换、均衡化、拆分线性化等技巧优化格基构造. 部分私钥泄漏攻击的难点在于如何更充分地利用泄漏比特, 以模方程为例, 现有工作大多利用 MSBs 降低某变元小根的上界、利用 LSBs 提升模方程的模数. 是否存在更好的泄漏信息利用方式, 仍是学术界的一个公开问题.

4　RSA 变体的格分析

模幂运算是 RSA 类密码体制中不可避免的高耗时操作, 为加快加密或解密速度, 一个简单直接的方法是采用

较小的加密或解密指数, 但当加密或解密指数较小时会受到小加密或解密指数攻击. 为抵抗小指数攻击的同时提升 RSA 算法的效率, 密码学领域针对不同的应用场景设计了不同的 RSA 密码算法, 这些算法可视为标准 RSA 算法的变体. 目前, 常用的 RSA 变体包括: 中国剩余定理 (Chinese remainder theorem, CRT) 指数 RSA 变体、素数幂 (prime power, PP) RSA 变体、多素数 (multi-prime, MP) RSA 变体、共素数 (common prime, CP) RSA 变体. RSA 变体格攻击的核心思想大多是由标准 RSA 的格攻击推广而来, 主要方法继承了 Jochemsz-May 通用策略求解多变元模方程或整数方程的思想, 但若想达到更优的攻击效果, 往往要针对 RSA 变体的特殊代数结构, 采用特殊的格基构造技巧.

4.1 CRT 指数 RSA

为在抵抗 Wiener 小指数攻击的同时加速解密或签名操作, 1982 年, Quisquater 等人[44]提出在 RSA 解密或签名阶段, 可以通过中国剩余定理, 利用模数的素因子 p 和 q 分解密码系统的私钥 d, 记:

$$d_p = d \mod (p-1),\ d_q = d \mod (q-1) \tag{7}$$

若 d_p 和 d_q 的值较小, 那么利用中国剩余定理即可提升解密或签名效率. 这样的密码系统通常称为 CRT 指数 RSA 密码系统 (简称 CRT-RSA). 实际 RSA 密码系统的标准实现方法通常采用 CRT-RSA.

CRT-RSA 算法的公钥为 (N,e), 私钥为 $\left(d,d_p,d_q,p,q\right)$. 虽然 CRT-RSA 密码系统避免了针对标准 RSA 假设中私钥 d 的小指数攻击, 但是在 d_p 或 d_q 相对于模数 N 太小时, CRT-RSA 密码系统同样面临小 CRT 指数攻击的威胁. 与标准 RSA 密码体制相比, CRT-RSA 涉及的变元更多, 变元间的代数关系更复杂, 由 CRT-RSA 的密钥生成等式 (7) 以及等式 $ed \equiv 1 \mod \varphi(N)$ 可以推导出涉及 6 个变元的 5 个模方程:

$$\begin{cases} ed_q = 1 + k_q(q-1) \\ ed_p = 1 + k_p(p-1) \\ ed_q\ p = N + \left(k_q - 1\right)(N-p) \\ ed_p q = N + \left(k_p - 1\right)(N-q) \\ ed_q \cdot ed_p = \left(1 + k_q(q-1)\right)\left(1 + k_p(p-1)\right) \end{cases} \Rightarrow \begin{array}{l} f_{q,1}\left(x_{q,1}, y_q\right) = 1 + x_{q,1}\left(y_q - 1\right) \equiv 0 \mod e \\ f_{p,2}\left(x_{p,2}, y_p\right) = 1 + x_{p,2}\left(y_p - 1\right) \equiv 0 \mod e \\ f_{p,1}\left(x_{p,1}, y_p\right) = N + x_{p,1}\left(N - y_p\right) \equiv 0 \mod e \\ f_{q,2}\left(x_{q,2}, y_q\right) = N + x_{q,2}\left(N - y_q\right) \equiv 0 \mod e \\ h\left(x_{p,1}, x_{q,1}, x_{p,2}, x_{q,2}\right) = N x_{q,1} x_{p,2} - x_{p,1} x_{q,2} \equiv 0 \mod e \end{array} .$$

方程的解 $\left(x_{p,1}^{(0)}, x_{q,1}^{(0)}, x_{p,2}^{(0)}, x_{q,2}^{(0)}, y_p^{(0)}, y_q^{(0)}\right) = \left(k_q - 1,\ k_q, k_p, k_p - 1,\ p,\ q\right)$. CRT-RSA 格分析的困难点在于如何充分利用变元之间、模方程之间的代数关系.

● CRT-RSA 的小指数攻击. 最早由 May[22]提出基于 Coppersmith 模方程求解方法的 CRT-RSA 小指数攻击, 该工作讨论了素因子 p,q 比特长度不平衡的场景, 针对 $p \gg q$ 分别给出了 $q < N^{0.382}$ 和 $q < N^{0.375}$ 下的两种攻击.

1) 由等式 $ed_p = 1 + k_p(p-1)$ 导出模方程 $f(x,y) = ex - y \pmod p$.

2) 由等式 $ed_q\ p = N + \left(k_q - 1\right)(N-p)$ 导出模方程 $f_{p,1}\left(x_{p,1}, y_p\right) = N + x_{p,1}\left(N - y_p\right) \pmod e$.

May 攻击局限性较强, 需要在 $q < N^{0.382}$ 且 d_p 很小时才能达到较好的攻击效果. 随后 Bleichenbacher 等人[19]利用变元代换技巧改进了上述 May 格攻击[22]中的方法 2), 引入新变元 y_q, 利用代数关系 $y_p y_q = N$ 优化格基构造, 对于素因子 p,q 不平衡的 CRT-RSA, 将小指数攻击对 q 的限制条件提升至 $q < N^{0.468}$.

同时, Bleichenbacher 等人[19]也提出了基于 Coppersmith 整数方程求解方法的小指数攻击, 由等式 $ed_q = 1 + k_q(q-1)$ 和 $ed_p = 1 + k_p(p-1)$, 可得等式 $ed_q - 1 + k_q = k_q q$ 和 $ed_p - 1 + k_p = k_p p$, 将二者相乘可得等式 $e^2 d_p d_q + ed_p\left(k_q - 1\right) + ed_q\left(k_p - 1\right) + \left(k_p - 1\right)\left(k_q - 1\right) = N k_p k_q$, 由此导出四变元整数方程:

$$f(x_1,x_2,x_3,x_4) = e^2 x_1 x_2 + e x_1 (x_4 - 1) + e x_2 (x_3 - 1) + (x_3 - 1)(x_4 - 1) - N x_3 x_4.$$

将 $f(x_1,x_2,x_3,x_4)$ 线性化后给出了四变元线性方程的求解方法, 对于素因子 p,q 平衡的情形, CRT-RSA 小指数攻击边界为 $d_p, d_q < \min\left\{\frac{1}{4}(N/e)^{\frac{2}{5}},\ \frac{1}{3}N^{\frac{1}{4}}\right\}$, 但要求 e 较小. 随后, Jochemsz 等人[45]应用 Jochemsz-May 通用策略求解四变元整数方程 $f(x_1,x_2,x_3,x_4)$, 解除了对 e 的限制条件, 将攻击边界提升至 $d_p, d_q < N^{0.073}$.

2017 年, TLP 格攻击[20,21]借助变元代换技巧改进了 Bleichenbacher 等人[19]基于模方程的攻击, 具体地, TLP 格

攻击中采用了下述 3 个模方程构造 shift 多项式:

$$\begin{cases} f_{p,2}\left(x_{p,2},y_p\right)=1+x_{p,2}\left(y_p-1\right)\ (\mathrm{mod}\ e) \\ f_{p,1}\left(x_{p,1},y_p\right)=N+x_{p,1}\left(N-y_p\right)\ (\mathrm{mod}\ e) \\ h\left(x_{p,1},x_{q,1},x_{p,2},x_{q,2}\right)=Nx_{q,1}x_{p,2}-x_{p,1}x_{q,2}\ (\mathrm{mod}\ e) \end{cases}.$$

在已有工作的基础上引入了模方程 $f_{p,2}\left(x_{p,2},y_p\right)$ 和 $h\left(x_{p,1},x_{q,1},x_{p,2},x_{q,2}\right)$, 以及第 2 个代数关系 $x_{p,2}=x_{q,2}+1$, 更充分地利用 CRT-RSA 的代数结构, 具体细节见第 2.2 节; 对于不平衡 CRT-RSA, TLP 格攻击将小指数攻击边界提升至 $p<N^{0.5}$, 解决了关于小 CRT 指数 RSA 安全性的一个重要开放性问题; 对于平衡 CRT-RSA, 将小指数攻击边界提升至 $d_p,d_q<N^{0.122}$. 随后, Peng 等人[46]在 TLP 格攻击的基础上采用了均衡化技巧, 统一了上述工作的攻击场景, 在 d_p 非常小或 p 显著小于 $N^{0.5}$ 时可以得到比 TLP 格攻击更好的结果.

● CRT-RSA 的部分私钥泄漏攻击. 与标准 RSA 的部分私钥泄漏攻击类似, 解密指数 d_p, d_q 的泄漏位置、泄漏量以及解密指数的大小, 对 CRT-RSA 密码体制的安全性有着不同的影响. 根据泄漏模型, 现有格分析工作大致可分为两大类: ① d_p 或 d_q 泄漏; ② d_p 和 d_q 同时泄漏.

情形 1: d_p 或 d_q 泄漏. 假设 p,q 等长, 且 d_p, d_q 等长, 不失一般性, 假设 d_p 的部分比特泄漏, 现有格分析工作大多由密钥生成等式 $ed_p=1+k_p(p-1)$ 导出目标方程.

2003 年, Blömer 等人[39]提出首个 CRT-RSA 的部分私钥泄漏攻击, 利用等式 $ed_p=1+k_p(p-1)$, 在 MSBs 和 LSBs 泄漏场景下分别构造了 kp 的近似值, 其中 k 不被 q 整除, 应用近似公因子问题求解方法[47]即可分解模数, 但这一攻击局限性较强, MSBs 泄漏攻击要求 $e<N^{0.25}$, LSBs 泄漏攻击要求 $e=poly(\log N)$.

Lu 等人[48]提出了基于 Coppersmith 模方程求解方法的攻击, 从等式 $ed_p=1+k_p(p-1)$ 出发, 分别在 MSBs 和 LSBs 泄漏场景下导出模数为 p 的双变元线性模方程, 应用双变元线性模方程求解方法[49]恢复私钥, 这一攻击仅在 $e<N^{0.25}$ 时才能成功; 对于 LSBs 泄漏场景, 记 $d_{L0}=d \bmod M$ 为已知的低位, Lu 等人由等式 $ed_p=1+k_p(p-1)$ 导出模方程 $f_{LSB'}(x,y)=x(y-1)-ed_{L0}+1\ (\mathrm{mod}\ eM)$, 在通用求解方法的基础上, 利用变元代换 (代数关系 $N=pq$)、均衡化等技巧优化格基构造, 但该方法仅在 $e<N^{0.375}$ 时才能攻击成功.

Takayasu 等人[50]提出了基于 Coppersmith 整数方程求解方法的攻击, 同样从 $ed_p=1+k_p(p-1)$ 出发, 在 MSBs 和 LSBs 泄漏场景下分别导出三变元整数方程, 并使用 Jochemsz-May 通用策略进行求解, 为利用代数关系 $N=pq$ 优化格基, 引入了第 4 个变元以采用变元代换技巧, 该工作降低了 $d_p\approx N^{0.5}$ 时已有工作对泄漏量的要求, 同时将 MSBs 泄漏攻击边界提升至 $e<N^{0.375}$.

随后, Takayasu 等人[51]进一步优化了 LSBs 泄漏攻击, 对于 $f(x,y)=x(y-1)-ed_{L0}+1\ (\mathrm{mod}\ eM)$ 的求解, Takayasu 等人在已有工作的基础上去掉了一些非有益多项式, 同时加入新的有益多项式, 降低了已有工作中对泄漏量的要求, 但仍要求 $e<N^{0.375}$.

Sarkar 等人[52]首次研究了解密指数未知分块 $n>1$ 的攻击场景, 从等式 $ed_p=1+k_p(p-1)$ 出发, 构造了模数为 p 的 $n+1$ 变元线性模方程, 应用多变元线性模方程求解方法[49]恢复解密指数.

情形 2: d_p 和 d_q 同时泄漏. 现有工作大多为 CRT-RSA 小指数攻击的推广.

Sarkar 等人[53]提出了基于 Coppersmith 整数方程求解方法的攻击, 将 Jochemsz 等人[45]小指数攻击推广到 MSBs 泄漏场景, 根据等式 $ed_q=1+k_q(q-1)$ 和 $ed_p=1+k_p(p-1)$, 分别借助 d_q 和 d_p 的 MSBs 估计 k_q 和 k_p 的高位, 以此将泄漏信息嵌入格结构. 随后, Takayasu 等人[50]使用 Jochemsz-May 通用方法中的扩展策略改进了 Sarkar 等人[53]的 MSBs 泄漏攻击结果, 同时给出了类似的 LSBs 泄漏攻击.

MNS 格攻击[54]提出了基于 Coppersmith 模方程求解方法的攻击, 将 TLP 小指数攻击[20,21]的方法推广到 LSBs 泄漏场景, 假设 $d_p=d_{p1}M+d_{p0}, d_q=d_{q1}M+d_{q0}$, 其中 d_{p0},d_{q0} 是已知比特, M 是泄漏比特长度对应的十进制数, MNS 格攻击将 TLP 小指数攻击中目标方程的模数由 e 提升至 eM, 以此将泄漏信息嵌入格结构.

目前, $n=1$泄漏场景下, 基于格的 CRT-RSA 部分私钥泄漏攻击所需泄漏量均与解密指数d_p, d_q的大小有关, 解密指数越大, 格攻击所需的解密指数泄漏比例越高, 此外, 现有 CRT-RSA 部分私钥泄漏攻击大多对加密指数e的大小有一定的要求. 现有 CRT-RSA 部分私钥泄漏攻击所需泄漏量的下界可参考表 2.

表 2 CRT-RSA 部分私钥泄漏攻击的泄漏量下界

部分私钥泄漏攻击	$\log_N d_p$, $\log_N d_q$	$\log_N e$	高位		低位		格攻击
			泄漏量	泄漏百分比 (%)	泄漏量	泄漏百分比 (%)	
泄漏d_p或d_q	0.3	0.22	0.11124	37.08	0	0	Takayasu-Kunihiro[50]
	0.3	0.37	0.20732	69.11	0	0	
	0.5	0.22	0.43237	86.47	0	0	
	0.5	0.37	0.49800	99.60	0	0	
	0.3	0.22	0	0	0.11124	37.08	
	0.3	0.37	0	0	0.20732	69.11	
	0.5	0.22	0	0	0.43141	86.28	Takayasu-Kunihiro[51]
	0.5	0.37	0	0	0.49799	99.60	
同时泄漏d_p和d_q	0.3	0.4	0.08000	26.67	0	0	Takayasu-Kunihiro[50]
	0.3	0.9	0.26405	88.02	0	0	
	0.5	0.4	0.36000	72.00	0	0	
	0.5	0.9	0.49616	99.23	0	0	
	0.3	0.9	0	0	0.26405	88.02	
	0.5	0.9	0	0	0.49616	99.23	
	0.1	任意值	0	0	0.02	20.00	MNS格攻击[54]
	0.3	任意值	0	0	0.26	86.67	
	0.5	任意值	0	0	0.5	100.00	

根据目前的研究结果, CRT-RSA 的小指数攻击研究已进入瓶颈期, TLP 格攻击是否为现有格分析框架下最优的 CRT-RSA 小指数攻击是目前的一个公开问题.

CRT-RSA 的部分私钥泄漏攻击可视为小指数攻击的推广, 将最优小指数攻击的思想推广至信息泄漏攻击场景, 可能会改进现有 CRT-RSA 部分私钥泄漏攻击的结果. 目前攻击效果最好的 CRT-RSA 小指数攻击是 TLP 格攻击和 PT 格攻击, 它们涉及的目标模方程及变元较多, 变元、模方程之间的代数关系较复杂, 在此基础上进一步嵌入泄漏信息可能会引入新的单项式或变元, 此时, 直接应用拆分线性化、均衡化等格基构造技巧十分困难. 如何将 TLP 攻击的思想应用于 MSBs 泄漏、同时泄漏 MSBs 和 LSBs 等攻击场景还有待进一步研究. 此外, 现有 CRT-RSA 的部分私钥泄漏攻击大多针对$n=1$的泄漏场景, 泄漏模型有待完善.

4.2 素数幂 RSA

素数幂 (prime power, PP) RSA 是由 Takagi 于 1998 年提出的一类高效加密系统[55], 现广泛应用于电子货币交易系统. 与标准 RSA 密码系统的主要区别在于, 这 PP-RSA 变体的模数形式为$N=p^rq$. 根据密钥生成方式不同, PP-RSA 存在两种变体.

1) $ed\equiv 1 \mod \lambda(N)$, 其中$\lambda(N)=\mathrm{lcm}(p-1,q-1)$, 解密过程需借助 Hensel 提升引理和中国剩余定理.

2) $ed\equiv 1 \mod \varphi(N)$, 其中$\varphi(N)=p^{r-1}(p-1)(q-1)$.

2000 年, Lim 等人[56]将 PP-RSA 的模数推广至$N=p^rq^l$形式. 由于 PP-RSA 的模数$N=p^rq^l$存在特殊指数结构, 故可采用指数优化技巧提升格分析的攻击效果.

● 模数分解攻击. 基于格的模数$N=p^rq^l$分解攻击大多是围绕单变元r次模方程的求解展开的, 现有工作通常假设模数的素因子p,q等长, 即$p\approx q\approx N^{\frac{1}{r+l}}$.

1999 年, Boneh 等人[57]给出了首个 MSBs 泄漏场景下$N=p^rq$的模数分解攻击, 假设P是已知的 MSBs, Boneh 等人通过求解模方程$f(x)=(P+x)^r \pmod{p^r}$, 证明了已知p的$\frac{1}{r+1}$比特即可分解N. 2013 年, Lu 等人[58]

结合 HM 模数分解攻击[33]中的线性模方程求解方法, 将 Boneh 等人[57]的结果推广至 n 个不连续的分块, 证明了 n 较大时, 已知 p 的 $\ln(r+1)/r$ 随机比特就可以分解模数 N, 该工作在 $r=1$ 时等价于 HM 模数分解攻击[33], $n=1$ 时等价于 Boneh 等人的攻击[57]. 2015 年, Lu 等人[13]利用方程 $f(x)=(P+x)^r \pmod{p^r}$ 模数的特殊指数结构, 采用指数优化技巧改进了的求解方法, 达到了与 Boneh 等人[57]相同的攻击结果, 但攻击中构造的格的维度更低, 提升了实际攻击的效率.

2017 年, Lu 等人[59]将 n 块泄漏场景模数分解攻击[58]推广至模数形式为 $N=p^rq^l$ 的情形, 证明了已知 p 的 $\min\{l/(r+l), 2(r-l)/(r+l)\}$ 比特即可分解 N. 此外, 对于 $N=p^rq^l$ 的模数分解攻击, Coron 等人[60,61]通过代数方法, 将 $N=p^rq^l$ 转化为 $N^\alpha=P^uQ$ 的形式, 进而将 Boneh 等人[57]的攻击结果推广至模数 $N=p^rq^l$, 但二者只是已有格攻击的应用, 并未对格分析方法本身进行优化改进.

● 小解密指数攻击. 对于 PP-RSA, 使用较小的解密指数, 同样会导致密码系统面临小解密指数攻击的威胁.

变体 1. $ed\equiv 1 \pmod{\varphi(N)}$. 现有攻击大多由密钥生成等式 $ed=1+kp^{r-1}(p-1)(q-1)$ 导出目标方程. 2004 年, May[62]利用格分析方法分别给出了 $d<N^{r(r+1)^{-2}}$ 和 $d<N^{(r-1)^2(r+1)^{-2}}$ 时的两种小指数攻击: 由密钥生成等式以及正整数 $E=e^{-1} \pmod{N}=(1+cN)/e$, 可得等式:

1) $d-E=\left(Ekp^{r-2}(p-1)(q-1)-cp^{r-1}qd\right)p=Kp$, 若 $|Kp-E|=|d|<N^{r(r+1)^{-2}}$, 那么应用 Boneh 等人[57]的攻击方法即可分解 N.

2) $d-E=(Ek(p-1)(q-1)-cpqd)p^{r-1}$, 可导出模方程 $f(x)=x-E \pmod{p^{r-1}}$, 应用单变元模方程求解方法即可恢复小根 d.

2014 年, Sarkar[63]提出了基于 Coppersmith 模方程求解方法的 PP-RSA 小解密指数攻击, 由密钥生成等式导出模方程 $f(x,y,z)=1+x\left(N-y^r-y^{r-1}z+y^{r-1}\right) \pmod{e}$, 借助变元代换 (代数关系 $N=p^rq$) 和均衡化技巧改进了 May[62]在 $r\leqslant 5$ 的结果. Sarkar[64]于 2016 年进一步改进了 $r=3,4$ 时的小指数攻击结果.

2015 年, LZPL 格攻击[13]提出了指数优化技巧并将 May[62]的边界提升至 $d<N^{r(r-1)(r+1)^{-2}}$, 具体地, 由密钥生成等式导出模方程 $f(x)=ex-1 \pmod{p^{r-1}}$, 利用模方程模数的特殊指数结构优化格基构造. 随后, Lu 等人[59]将小指数攻击推广至模数形式为 $l>1$ 的 PP-RSA, 对应的攻击边界为 $d<N^{1-(3r+l)(r+l)^{-2}}$, $l=1$ 时的结果与 LZPL 格攻击[13]一致. 注意, $r\leqslant 4$ 时 Sarkar[63,64]攻击效果更好, $r\geqslant 5$ 时 LZPL 格攻击效果更好.

2016 年, Takayasu 等人[65]从密钥生成等式出发, 采用变元代换 (代数关系 $N=p^rq$)、均衡化等技巧给出了两种小解密指数攻击.

1) 求解整数方程 $f(x,y,z_1,z_2)=1+ex+yz_1{}^{r-1}(z_1-1)(z_2-1)$.

2) 求解模方程 $f(y,z_1,z_2)=1+yz_1{}^{r-1}(z_1-1)(z_2-1) \pmod{e}$.

上述 Takayasu 等人[65]提出的两个工作中, 工作 2) 的攻击效果优于工作 1). 该工作在加密指数 e 较小时能达到较好的攻击效果, 与 LZPL 格攻击[13]的结果对比见表 3, 其中 $\alpha=\log_N e$.

表 3 LZPL[13]与 Takayasu-Kunihiro[65]的 PP-RSA 小指数攻击结果对比 (l=1)

r	$\log_N d$						格攻击
	$\alpha=0.5$	$\alpha=0.6$	$\alpha=0.7$	$\alpha=0.8$	$\alpha=0.9$	$\alpha=1$	
5	0.5555	0.5555	0.5555	0.5555	0.5555	0.5555	LZPL格攻击[13]
	0.6741	0.6442	0.6167	0.5911	0.5670	0.5422	Takayasu-Kunihiro[65]-(1)
	0.6837	0.6528	0.6244	0.5979	0.5730	0.5495	Takayasu-Kunihiro[65]-(2)
6	0.6122	0.6122	0.6122	0.6122	0.6122	0.6122	LZPL格攻击[13]
	0.6946	0.6668	0.6412	0.6174	0.5950	0.5738	Takayasu-Kunihiro[65]-(1)
	0.7046	0.6759	0.6494	0.6248	0.6017	0.5798	Takayasu-Kunihiro[65]-(2)

变体 2. $ed\equiv 1 \pmod{\lambda(N)}$. 现有小指数攻击大多由密钥生成等式 $ed=1+k(p-1)(q-1)$ 导出目标方程.

2008 年, Itoh 等人[66]提出了基于 Coppersmith 模方程求解方法的攻击, 由密钥生成等式导出模方程 $f(x,y,z)=$

$1+x(y-1)(z-1) \pmod{e}$, 借助变元代换技巧 (代数关系 $N=p^rq$) 和几何渐进矩阵, 证明了 $d \leqslant N^{\frac{2-\sqrt{2}}{r+1}}$ 时可以恢复 d. Lu 等人[59]将 Itoh 等人[66]的结果推广至模数形式为 $N=p^rq^l$ 的素数幂 RSA 变体, 对应的边界为 $d \leqslant N^{\frac{7-2\sqrt{7}}{3(r+l)}}$, $l=1$ 时的结果与 Itoh 等人[66]一致.

2016 年, Takayasu 等人[65]从密钥生成等式出发, 采用变元代换技巧 (代数关系 $N=p^rq$)、均衡化技巧以及拆分线性化技术, 对于 $e=N^{\alpha}$, 分别给出了 $\alpha \leqslant 1/(r+1)$ 和 $1/(r+1) \leqslant \alpha$ 时的两种小解密指数攻击.

1) 求解整数方程 $f(x,y,z_1,z_2)=1+ex+y(z_1+1)(z_2+1)$, 对应的边界为 $d \leqslant N^{(7-2\sqrt{1+3(r+1)\alpha})/(3(r+1))}$.

2) 求解模方程 $f(y,z_1,z_2)=1+y(z_1-1)(z_2-1) \pmod{e}$, 对应的边界为 $d \leqslant N^{(2-\sqrt{(r+1)\alpha})/(r+1)}$.

该工作在加密指数 e 较小时能达到较好的攻击效果, 在 $\alpha=2/(r+1)$ 时的攻击结果与 Itoh 等人[66]的结果一致, 但行列式的计算更简单.

现有 PP-RSA 的小指数攻击大多采用变元代换 (代数关系 $N=p^rq$)、指数优化、均衡化等技巧. 理论上, $r=1$ 的 PP-RSA 即为标准 RSA, 故 PP-RSA 的小指数攻击可视为标准 RSA 小指数攻击的推广. 因此, PP-RSA 的小指数攻击致力于覆盖最优标准 RSA 小指数攻击边界, 即 Boneh-Durfee 格攻击的强边界 $d<N^{0.292}$. 上述对 $ed \equiv 1 \bmod \varphi(N)$ 变体的小指数攻击, 现有工作未覆盖最优的标准 RSA 小指数攻击, 仍有一定改进空间; 对于 $ed \equiv 1 \bmod \lambda(N)$ 变体的小指数攻击, 现有攻击结果已覆盖 Boneh-Durfee 格攻击的强边界. 加密指数取最大值, 即 $e \approx \varphi(N)$ 或 $e \approx \lambda(N)$ 时, 上述素数幂 RSA 小指数攻击结果对比见表 4.

表 4 PP-RSA 小指数攻击结果对比

小指数攻击	l	$\log_N d$									格攻击
		$r=2$	$r=3$	$r=4$	$r=5$	$r=6$	$r=7$	$r=8$	$r=9$	$r=10$	
$ed \equiv 1 \bmod \varphi(N)$ 变体	1	0.222	0.250	0.360	0.444	0.510	0.562	0.605	0.640	0.669	May[62]
	1	0.222	0.375	0.480	0.555	0.612	0.656	0.691	0.720	0.744	Lu等人[13]
	1	0.395	0.461	0.508	0.545	0.574	0.598	0.619	0.637	0.653	Sarkar[63,64]
	1	0.396	0.463	0.512	0.550	0.580	0.605	0.626	0.644	0.660	Takayasu-Kunihiro[65]
	2	0.500	0.560	0.611	0.653	0.688	0.716	0.740	0.760	0.778	Lu等人[59]
	3	0.640	0.667	0.694	0.719	0.741	0.760	0.777	0.792	0.805	
$ed \equiv 1 \bmod \lambda(N)$ 变体	1	0.195	0.146	0.117	0.098	0.084	0.073	0.065	0.059	0.053	Itoh等人[66], Takayasu-Kunihiro[65]
	2	0.142	0.114	0.095	0.081	0.071	0.063	0.057	0.052	0.048	Lu等人[59]
	3	0.114	0.095	0.081	0.071	0.063	0.057	0.052	0.048	0.044	

● 部分私钥泄漏攻击. 现有 PP-RSA 的部分私钥泄漏攻击大多是 PP-RSA 小指数攻击的推广. 对于泄漏 MSBs 的情况, 假设已知 $\tilde{d}$, 记 $d=\tilde{d}+d_1$; 对于泄漏 LSBs 的情况, 假设已知 d_0 和 M, 记 $d=d_0 \bmod M$.

变体 1. $ed \equiv 1 \bmod \varphi(N)$. May 首次将小指数攻击分别推广至 MSBs、LSBs 泄漏场景[62], 随后, Lu 等人[13]应用指数优化技巧将攻击边界分别提升至 $|d-\tilde{d}| \leqslant N^{r(r-1)(r+1)^{-2}}$ 和 $M>N^{(3r+1)(r+1)^{-2}}$. Sarkar 将小指数攻击推广至 MSBs 泄漏场景[64], 与标准 RSA 的 MABs 泄漏攻击类似, 通过降低变元小根的上界嵌入泄漏信息. Takayasu 等人[65]从密钥生成等式 $ed=1+kp^{r-1}(p-1)(q-1)$ 出发, 利用变元代换 (代数关系 $N=p^rq$)、均衡化等技巧给出两种部分私钥泄漏攻击.

1) MSBs 和 LSBs 泄漏攻击, 求解整数方程 $f(x,y,z_1,z_2)=1-e\tilde{d}+eMx+y{z_1}^{r-1}(z_1-1)(z_2-1)$, 其中 $\tilde{d}$ 为已知比特, 泄漏 MSBs 时 $M=1$, 泄漏 LSBs 时 $M=2^{\lceil \log_2 \tilde{d} \rceil}$.

2) LSBs 泄漏攻击, 求解模方程 $f(y,z_1,z_2)=1-ed_0+y{z_1}^{r-1}(z_1-1)(z_2-1) \pmod{eM}$.

该工作改进了解密指数 d 较小时的部分私钥泄漏攻击, 是目前已知的最优部分私钥泄漏攻击.

变体 2. $ed \equiv 1 \bmod \lambda(N)$. Huang 等人[67]从密钥生成等式 $ed=1+k(p-1)(q-1)$ 出发, 提出了:

1) MSBs 泄漏攻击, 将 $d=\tilde{d}+d_1$ 代入, 可导出模方程 $f(w,x,y,z)=1+x(y-1)(z-1)+ew \pmod{e\tilde{d}}$.

2) LSBs 泄漏攻击, 将 $d=d_0 \bmod M$ 代入, 可导出模方程 $f(x,y,z)=1+x(y-1)(z-1)-ed_0 \pmod{eM}$.

3) MBs 泄漏攻击, 假设已知 $\bar{d}$ 和 2 的方幂 M_1, M_2, 将 $d = d_2 M_2 + \bar{d} M_1 + d_1$ 代入密钥生成等式, 导出模方程 $f(w,x,y,z) = 1 + x(y-1)(z-1) - ew - e\bar{d}M_1 \pmod{eM_2}$.

上述模方程的求解参考了 Itoh 等人提出的 PP-RSA 小指数攻击方法[66]. Takayasu 等人[65]改进了 Huang 等人[67]的攻击结果, 从密钥生成等式 $ed = 1 + k(p-1)(q-1)$ 出发, 采用变元代换 (代数关系 $N = p^r q$)、拆分线性化和均衡化等技巧给出了两种部分私钥泄漏攻击.

1) MSBs 和 LSBs 泄漏攻击, 求解整数方程 $f(x,y,z_1,z_2) = 1 - e\tilde{d} + eMx + y(z_1+1)(z_2+1)$, 其中 $\tilde{d}$ 为已知比特, 泄漏 MSBs 时 $M = 1$, 泄漏 LSBs 时 $M = 2^{\lceil \log_2 \tilde{d} \rceil}$.

2) LSBs 泄漏攻击, 求解模方程组:

$$\begin{cases} f(y,z_1,z_2) = 1 - ed_0 + y(z_1+1)(z_2+1) \pmod{eM} \\ f(y,z_1,z_2) = 1 + y(z_1+1)(z_2+1) \pmod{e} \end{cases}.$$

该工作改进了 Huang 等人[67]的工作, 是目前已知的最优部分私钥泄漏攻击.

总的来说, 现有 PP-RSA 的格分析工作大致可分为两条路线: (1) 对于 PP-RSA 的模数分解攻击, 以及对于 $ed \equiv 1 \mod \varphi(N)$变体的小指数攻击和部分私钥泄漏攻击, 由于模数 $N = p^r q^l$ 以及密钥生成等式的模数 $\varphi(N) = p^{r-1}(p-1)(q-1)$ 都存在特殊的指数结构, 故研究重点在于如何利用指数优化技巧提升格攻击效果; (2) 对于 $ed \equiv 1 \mod \lambda(N)$ 变体的格分析, 现有工作的主要思路是在 Jochemsz-May 通用格基构造策略的基础上, 利用均衡化、拆分线性化、变元代换 (代数关系 $N = p^r q$) 等技巧优化格基构造.

在 PP-RSA 的小指数攻击研究方面, 对于 $ed \equiv 1 \mod \varphi(N)$ 变体, 现有格分析未覆盖最优的标准 RSA 小指数攻击, 如何进一步挖掘 PP-RSA 的特殊代数结构以优化格攻击效果仍待研究. 此外, 现有 PP-RSA 的部分私钥泄漏攻击大多针对 $n = 1$ 的泄漏场景, 泄漏模型有待完善.

4.3 多素数 RSA

多素数 (multi-prime, MP) RSA 变体的模数形式为 $N = p_1 p_2 \ldots p_r$, 最早是由 Collins 等人[68]于 1997 年申请为专利, 最初使用的模数形式为 $N = p_1 p_2 p_3$. 标准 RSA 可以看作 MP-RSA 变体模数只含两个素因子的特殊情况. 相比于标准 RSA, MP-RSA 变体模数的素因子比特长度较小, 随机选取素数的效率较高, 因此加快了密钥生成的效率. 与此同时, 解密阶段也可以借助中国剩余定理提高解密效率. 此外, 随着 r 的增大, 早期的小指数攻击以及部分私钥泄漏攻击的效果越差; 但随着 r 的增大, 利用椭圆曲线方法[69]分解 MP-RSA 的模数越容易, 因此 r 的取值不能无限大, 通常取 $r = 3,4,5$. MP-RSA 存在一种特殊的格分析方法—小素数差攻击.

小素数差攻击是已知比特分解问题的特殊情形. 实际上, 当模数的素因子之间差异较小时, 可以知道所有素因子的 MSBs. 不失一般性, 假设 $p_1 < \ldots < p_r$, 且 $\frac{1}{2}N^{\frac{1}{r}} < p_1 < N^{\frac{1}{r}} < p_r < 2N^{\frac{1}{r}}$, 第 2 个条件暗示了素因子是平衡的, 即素因子比特长度基本相等. 素数差定义为 $\Delta := \max_{i \neq j} |p_i - p_j| = p_r - p_1 = N^{\gamma}$, 其中 $0 < \gamma < \frac{1}{r}$. 素数差的概念是由 Weger[70]提出的, 该工作证明了小的素数差可以提升小指数攻击的效果. Bahig 等人[71]证明了对于已知素数差 $\Delta = N^{\gamma}$ 和公钥 $(N, e \approx N)$, 若 γ 和 d 满足 $2d^2 + 1 < \frac{1}{6r}N^{\frac{2}{r}-\gamma}$ 则 MP-RSA 算法是不安全的.

4.4 共素数 RSA

共素数 (common prime, CP) RSA 是指 RSA 模数 N 的两个素因子 p 和 q, 满足 $p-1$ 和 $q-1$ 有一个较大的公因子. CP-RSA 最早是由 Wiener[34]提出的, 用于抵御连分式攻击, 之后由 Hinek[72]将其命名为 CP-RSA 算法. 不失一般性, 假设 $p = 2ga + 1$, $q = 2gb + 1$, 其中 $g \approx N^{\gamma}$, $gcd(a,b) = 1$. 加密指数 e 和解密指数 d 满足 $ed \equiv 1 \mod 2gab$, 其中 $e \approx N^{1-\gamma}$, $d \approx N^{\beta}$. CP-RSA 的格分析工作大多关注小指数攻击.

Wiener[34]证明了若私钥 $d < N^{1/4-\gamma/2}$, 那么就可以利用连分式攻击在多项式时间内分解 N. Hinek[72]提出了 2 种基于格的攻击方法, 证明了若私 $\beta < \gamma^2$ 或 $\beta < \frac{2}{5}\gamma$ 就可以在多项式时间内分解 N. Jochemsz 等人[10]改进了 Hinek[72]中多项式方程变元的选取, 利用 $p-1$ 和 $q-1$ 有公因子这一特殊关系, 构造出四变元方程, 其中一个变元包含解密

指数d, 将 CP-RSA 小指数攻击边界提升至$\beta < \frac{1}{4}(4+4\gamma-\sqrt{13+20\gamma+4\gamma^2})$. Sarkar 等人[73]提出了两种基于格的攻击方法, 分别适用于$\gamma \leqslant 0.051$和$0.051 < \gamma \leqslant 0.2087$的情况, $\gamma > 0.2087$时 Jochemsz 等人[10]仍是最优的攻击结果. Lu 等人[13]应用指数优化技巧, 改进了 Jochemsz 等人[10]在$\gamma \geqslant 0.3872$时的攻击结果, γ越大该工作的改进越明显, 特别是γ接近 0.5 时, 将小指数攻击的边界从 Jochemsz 等人[10]的$\beta < 0.2752$提升至了$\beta < 0.5$.

5 结论与展望

格分析方法是分析 RSA 类密码算法安全性的一种重要工具, 现有标准 RSA 的格分析工作大致可以分为 3 类: 模数分解攻击、小解密指数攻击和部分私钥 (解密指数) 泄漏攻击. 其中, 小解密指数攻击和部分私钥泄漏攻击较复杂.

对于 RSA 的小解密指数攻击, 格分析方法的核心是格基构造, 主要思想是将特殊条件下, 即解密指数较小的 RSA 问题转化为多变元模方程或整数方程小根的求解问题, 再将后者转化为格上的短向量求解问题, 最后利用格基约化算法进行求解. 在上述过程中, 如何将多变元模方程或整数方程的求解问题转化为格上的短向量求解问题, 即如何构造格基是最关键的步骤. 现有工作大多在 Jochemsz-May 通用格基构造策略的基础上, 借助均衡化技巧、拆分线性化技术等优化格基构造, 目前最优的攻击结果是 Boneh-Durfee 格攻击的强边界$d < N^{0.292}$. 总的来说, 小解密指数攻击大多依赖于参数选取的特殊性, 并没有直接威胁实用密码体制本身的安全性, 可以通过选取足够大的解密指数避免该攻击.

对于 RSA 的部分私钥泄漏攻击, 根据私钥泄漏位置, 泄漏信息的利用方式可以分为 4 大类: (1) MSBs 泄漏场景, 在构造模方程时, 利用已知的 MSBs 降低某变元小根的上界, 以此通过降低格的行列式将泄漏信息嵌入格中; (2) LSBs 泄漏场景, 在构造模方程时, 利用已知的 LSBs 提升模方程的模数, 以此将泄漏信息嵌入格中; (3) MSBs 和 LSBs 同时泄漏场景, 通过联立 MSBs 和 LSBs 泄漏场景下的模方程, 与此同时将 MSBs 和 LSBs 泄漏信息嵌入格中; (4) 未知比特块的个数$n > 1$的泄漏场景, 现有格分析工作通常将n个未知比特块视为n个变元, 通过密钥生成等式导出多变元方程, 以此利用泄漏信息. 整体上看, 部分解密指数泄漏攻击分析的对象本质上是实际密码系统依赖的计算困难问题的特定实例. 这种情况下格分析要求密码系统的参数较为特殊, 例如要求解密指数较小, 同时对泄漏量有一定的要求, 目前仅适用于分析特定的 RSA 密码系统, 还有进一步的发展空间.

对于 RSA 变体算法, 现有格分析方法大多是在标准 RSA 格分析工作的基础上, 结合 RSA 变体参数之间特殊的代数关系, 借助特殊格基构造技巧以优化格攻击. 对于 CRT-RSA 变体, 格分析工作中采用的格基优化技巧主要包括变元代换、均衡化、拆分线性化等, 格分析的困难点在于如何充分利用变元之间、模方程之间的代数关系; 对于 PP-RSA 以及 CP-RSA, 由于模数可能存在特殊的指数结构, 故利用指数优化技巧能有效提升格攻击效果. 除模数分解攻击、小解密指数攻击和部分私钥 (解密指数) 泄漏攻击外, 某些 RSA 变体存在特殊格攻击, 例如 MP-RSA 变体的小素数差攻击. 总体而言, 上述 RSA 变体的格分析要求所分析的密码系统的参数较为特殊, 且目前的泄漏模型尚不完善, 仍有一定的发展空间.

综上所述, 虽然 RSA 及其变体算法的格分析工作已取得了很好的结果, 但这些格攻击大多依赖于密码系统参数选取的特殊性, 或对私钥的泄漏量有一定的要求, 并没有对实用 RSA 密码体制产生根本上的威胁, 通过选择合理的参数可以避免格攻击. 具体地, 素因子p,q的比特长度应是平衡的, 但同时要保证有足够大的素数差; 应选取足够大的解密指数$d > N^{0.292}$, 以及足够大的 CRT 解密指数$d_p, d_q > N^{0.122}$; 应尽量避免取较小的加密指数.

致谢 本文是国家自然科学基金通用联合重点项目 (U1936209) 承研团队内部讨论班的直接工作结果, 这一工作由项目承研团队全体成员共同讨论完成. 多位在该工作完成过程中作出直接技术贡献并提出宝贵建议的专家学者并未参与本文署名, 包括但不仅限于中国信息安全测评中心石竑松研究员、陈佳哲副研究员、魏伟博士、曹伟琼博士等, 中国科学院信息工程研究所国家重点实验室的于伟副研究员、田松博士以及孙硕、李帅刚、李秀秀、高婧等多位博士研究生, 谨向他们致谢.

References:

[1] Ajtai M. The shortest vector problem in L_2 is NP-hard for randomized reductions. In: Proc. of the 30th Annual ACM Symp. on the Theory of Computing. Dallas: ACM, 1998. 10–19. [doi: 10.1145/276698.276705]

[2] Lenstra AK, Lenstra Jr HW, Lovász L. Factoring polynomials with rational coefficients. Mathematische Annalen, 1982, 261(4): 515–534. [doi: 10.1007/BF01457454]

[3] Schnorr CP, Euchner M. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. Mathematical Programming, 1994, 66(1–3): 181–199. [doi: 10.1007/BF01581144]

[4] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21(2): 120–126. [doi: 10.1145/359340.359342]

[5] Coppersmith D. Finding a small root of a univariate modular equation. In: Proc. of the 1996 Int'l Conf. on Advances in Cryptology. Saragossa: Springer, 1996. 155–165. [doi: 10.1007/3-540-68339-9_14]

[6] Coppersmith D. Finding a small root of a bivariate integer equation; factoring with high bits known. In: Proc. of the 1996 Int'l Conf. on Advances in Cryptology. Saragossa: Springer, 1996. 178–189. [doi: 10.1007/3-540-68339-9_16]

[7] Coppersmith D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 1997, 10(4): 233–260. [doi: 10.1007/s001459900030]

[8] Howgrave-Graham N. Finding small roots of univariate modular equations revisited. In: Proc. of the 6th IMA Conf. on Cryptography and Coding. Cirencester: Springer, 1997. 131–142. [doi: 10.1007/BFb0024458]

[9] Coron JS. Finding small roots of bivariate integer polynomial equations revisited. In: Proc. of the 2004 Int'l Conf. on Advances in Cryptology. Interlaken: Springer, 2004. 492–505. [doi: 10.1007/978-3-540-24676-3_29]

[10] Jochemsz E, May A. A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In: Proc. of the 12th Int'l Conf. on Advances in Cryptology. Shanghai: Springer, 2006. 267–282. [doi: 10.1007/11935230_18]

[11] Durfee G, Nguyen PQ. Cryptanalysis of the RSA schemes with short secret exponent from Asiacrypt'99. In: Proc. of the 6th Int'l Conf. on Advances in Cryptology. Kyoto: Springer, 2000. 14–29. [doi: 10.1007/3-540-44448-3_2]

[12] Takayasu A, Kunihiro N. Better lattice constructions for solving multivariate linear equations modulo unknown divisors. IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, 2014, E97-A(6): 1259–1272. [doi: 10.1587/transfun.E97.A.1259]

[13] Lu Y, Zhang R, Peng LQ, Lin DD. Solving linear equations modulo unknown divisors: Revisited. In: Proc. of the 21st Int'l Conf. on Advances in Cryptology. Auckland: Springer, 2015. 189–213. [doi: 10.1007/978-3-662-48797-6_9]

[14] Herrmann M, May A. Attacking power generators using unravelled linearization: When do we output too much? In: Proc. of the 15th Int'l Conf. on Advances in Cryptology. Tokyo: Springer, 2009. 487–504. [doi: 10.1007/978-3-642-10366-7_29]

[15] Peng LQ, Hu L, Lu Y, Huang ZJ, Xu J. Implicit factorization of RSA moduli revisited (Short Paper). In: Proc. of the 10th Int'l Workshop on Advances in Information and Computer Security. Nara: Springer, 2015. 67–76. [doi: 10.1007/978-3-319-22425-1_5]

[16] Blömer J, May A. Low secret exponent RSA revisited. In: Proc. of the Int'l Conf. on Cryptography and Lattices. Providence: Springer, 2001. 4–19. [doi: 10.1007/3-540-44670-2_2]

[17] Hinek MJ. Small private exponent partial key-exposure attacks on multiprime RSA. 2005. https://cacr.uwaterloo.ca/techreports/2005/cacr2005-16.pdf

[18] May A. Using LLL-reduction for solving RSA and factorization problems. In: Nguyen PQ, Vallée B, eds. The LLL Algorithm: Survey and Applications. Berlin: Springer, 2010. 315–348. [doi: 10.1007/978-3-642-02295-1_10]

[19] Bleichenbacher D, May A. New attacks on RSA with small secret CRT-exponents. In: Proc. of the 9th Int'l Conf. on Public Key Cryptography. New York: Springer, 2006. 1–13. [doi: 10.1007/11745853_1]

[20] Takayasu A, Lu Y, Peng LQ. Small CRT-exponent RSA revisited. In: Proc. of the 36th Annual Int'l Conf. on Advances in Cryptology. Paris: Springer, 2017. 130–159. [doi: 10.1007/978-3-319-56614-6_5]

[21] Takayasu A, Lu Y, Peng LQ. Small CRT-exponent RSA revisited. Journal of Cryptology, 2019, 32(4): 1337–1382. [doi: 10.1007/s00145-018-9282-3]

[22] May A. Cryptanalysis of unbalanced RSA with small CRT-exponent. In: Proc. of the 22nd Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2002. 242–256. [doi: 10.1007/3-540-45708-9_16]

[23] Takayasu A, Kunihiro N. Partial key exposure attacks on RSA: Achieving the Boneh-Durfee bound. In: Proc. of the 21st Int'l Conf. on Selected Areas in Cryptography. Montreal: Springer, 2014. 345–362. [doi: 10.1007/978-3-319-13051-4_21]

[24] Herrmann M, May A. Maximizing small root bounds by linearization and applications to small secret exponent RSA. In: Proc. of the 13th Int'l Conf. on Public Key Cryptography. Paris: Springer, 2010. 53–69. [doi: 10.1007/978-3-642-13013-7_4]

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

1339–1349. [doi: 10.1109/18.850673]

[26] Sun HM, Wu ME, Ting WC, Hinek MJ. Dual RSA and its security analysis. IEEE Trans. on Information Theory, 2007, 53(8): 2922–2933. [doi: 10.1109/TIT.2007.901248]

[27] Lu Y, Peng LQ, Kunihiro N. Recent progress on Coppersmith's lattice-based method: A survey. In: Takagi T, Wakayama M, Tanaka K, Kunihiro N, Kimoto K, Duong DH, eds. Mathematical Modelling for Next-generation Cryptography. Singapore: Springer, 2018. 297–312. [doi: 10.1007/978-981-10-5065-7_16]

[28] Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1997, 26(5): 1484–1509. [doi: 10.1137/S0097539795293172]

[29] Coron JS, Joux A, Kizhvatov I, Naccache D, Paillier P. Fault attacks on RSA signatures with partially unknown messages. In: Proc. of the 11th Int'l Conf. on Cryptographic Hardware and Embedded Systems. Lausanne: Springer, 2009. 444–456. [doi: 10.1007/978-3-642-04138-9_31]

[30] Kocher PC. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Proc. of the 16th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 1996. 104–113. [doi: 10.1007/3-540-68697-5_9]

[31] Novak R. SPA-based adaptive chosen-ciphertext attack on RSA implementation. In: Proc. of the 5th Int'l Workshop on Public Key Cryptography. Paris: Springer, 2002. 252–262. [doi: 10.1007/3-540-45664-3_18]

[32] Rivest RL, Shamir A. Efficient factoring based on partial information. In: Proc. of the Workshop on Advances in Cryptology. Linz: Springer, 1985. 31–34. [doi: 10.1007/3-540-39805-8_3]

[33] Herrmann M, May A. Solving linear equations modulo divisors: On factoring given any bits. In: Proc. of the 14th Int'l Conf. on Advances in Cryptology. Melbourne: Springer, 2008. 406–424. [doi: 10.1007/978-3-540-89255-7_25]

[34] Wiener MJ. Cryptanalysis of short RSA secret exponents. IEEE Trans. on Information Theory, 1990, 36(3): 553–558. [doi: 10.1109/18.54902]

[35] Kunihiro N, Shinohara N, Izu T. A unified framework for small secret exponent attack on RSA. In: Proc. of the 18th Int'l Workshop on Selected Areas in Cryptography. Toronto: Springer, 2011. 260–277. [doi: 10.1007/978-3-642-28496-0_16]

[36] Boneh D, Durfee G, Frankel Y. An attack on RSA given a small fraction of the private key bits. In: Proc. of the Int'l Conf. on Advances in Cryptology. Beijing: Springer, 1998. 25–34. [doi: 10.1007/3-540-49649-1_3]

[37] Ernst M, Jochemsz E, May A, De Weger B. Partial key exposure attacks on RSA up to full size exponents. In: Proc. of the 24th Annual Int'l Conf. on Advances in Cryptology. Aarhus: Springer, 2005. 371–386. [doi: 10.1007/11426639_22]

[38] Sarkar S, Gupta SS, Maitra S. Partial key exposure attack on RSA—Improvements for limited lattice dimensions. In: Proc. of the 11th Int'l Conf. on Progress in Cryptology. Hyderabad: Springer, 2010. 2–16. [doi: 10.1007/978-3-642-17401-8_2]

[39] Blömer J, May A. New partial key exposure attacks on RSA. In: Proc. of the 23rd Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2003. 27–43. [doi: 10.1007/978-3-540-45146-4_2]

[40] Aono Y. A new lattice construction for partial key exposure attack for RSA. In: Proc. of the 12th Int'l Conf. on Public Key Cryptography. Irvine: Springer, 2009. 34–53. [doi: 10.1007/978-3-642-00468-1_3]

[41] Suzuki K, Takayasu A, Kunihiro N. Extended partial key exposure attacks on RSA: Improvement up to full size decryption exponents. Theoretical Computer Science, 2020, 841: 62–83. [doi: 10.1016/j.tcs.2020.07.004]

[42] Sarkar S. Partial key exposure: Generalized framework to attack RSA. In: Proc. of the 12th Int'l Conf. on Progress in Cryptology. Chennai: Springer, 2011. 76–92. [doi: 10.1007/978-3-642-25578-6_7]

[43] Wang SX, Qu LJ, Li C, Fu SJ. A new attack on RSA with known middle bits of the private key. IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98-A(12): 2677–2685. [doi: 10.1587/transfun.E98.A.2677]

[44] Quisquater JJ, Couvreur C. Fast decipherment algorithm for RSA public-key cryptosystem. Electronics Letters, 1982, 18(21): 905–907. [doi: 10.1049/el:19820617]

[45] Jochemsz E, May A. A polynomial time attack on RSA with private CRT-exponents smaller than $N^{0.073}$. In: Proc. of the 27th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2007. 395–411. [doi: 10.1007/978-3-540-74143-5_22]

[46] Peng LQ, Takayasu A. Generalized cryptanalysis of small CRT-exponent RSA. Theoretical Computer Science, 2019, 795: 432–458. [doi: 10.1016/j.tcs.2019.07.031]

[47] Howgrave-Graham N. Approximate integer common divisors. In: Proc. of the 2001 Int'l Conf. on Cryptography and Lattices. Providence: Springer, 2001. 51–66. [doi: 10.1007/3-540-44670-2_6]

[48] Lu Y, Zhang R, Lin DD. New partial key exposure attacks on CRT-RSA with large public exponents. In: Proc. of the 12th Int'l Conf. on Applied Cryptography and Network Security. Lausanne: Springer, 2014. 151–162. [doi: 10.1007/978-3-319-07536-5_10]

[49] Takayasu A, Kunihiro N. Better lattice constructions for solving multivariate linear equations modulo unknown divisors. In: Proc. of the

18th Australasian Conf. on Information Security and Privacy. Brisbane: Springer, 2013. 118–135. [doi: 10.1007/978-3-642-39059-3_9]

[50] Takayasu A, Kunihiro N. Partial key exposure attacks on CRT-RSA: Better cryptanalysis to full size encryption exponents. In: Proc. of the 13th Int'l Conf. on Applied Cryptography and Network Security. New York: Springer, 2015. 518–537. [doi: 10.1007/978-3-319-28166-7_25]

[51] Takayasu A, Kunihiro N. Partial key exposure attacks on CRT-RSA: General improvement for the exposed least significant bits. In: Proc. of the 19th Int'l Conf. on Information Security. Honolulu: Springer, 2016. 35–47. [doi: 10.1007/978-3-319-45871-7_3]

[52] Sarkar S, Venkateswarlu A. Partial key exposure attack on CRT-RSA. In: Proc. of the 15th Int'l Conf. on Progress in Cryptology. New Delhi: Springer, 2014. 255–264. [doi: 10.1007/978-3-319-13039-2_15]

[53] Sarkar S, Maitra S. Partial key exposure attack on CRT-RSA. In: Proc. of the 7th Int'l Conf. on Applied Cryptography and Network Security. Paris-Rocquencourt: Springer, 2009. 473–484. [doi: 10.1007/978-3-642-01957-9_29]

[54] May A, Nowakowski J, Sarkar S. Partial key exposure attack on short secret exponent CRT-RSA. In: Proc. of the 27th Int'l Conf. on Advances in Cryptology. Singapore: Springer, 2021. 99–129. [doi: 10.1007/978-3-030-92062-3_4]

[55] Takagi T. Fast RSA-type cryptosystem modulo $p^k q$. In: Proc. of the 18th Annual Int'l Cryptology Conf. Santa Barbara: Springer, 1998. 318–326. [doi: 10.1007/BFb0055738]

[56] Lim S, Kim S, Yie I, Lee H. A generalized Takagi-cryptosystem with a modulus of the form $p^r q^s$. In: Proc. of the 1st Int'l Conf. on Progress in Cryptology. Calcutta: Springer, 2000. 283–294. [doi: 10.1007/3-540-44495-5_25]

[57] Boneh D, Durfee G, Howgrave-Graham N. Factoring $N = p^r q$ for large r. In: Proc. of the 19th Annual Int'l Cryptology Conf. Santa Barbara: Springer, 1999. 326–337. [doi: 10.1007/3-540-48405-1_21]

[58] Lu Y, Zhang R, Lin DD. Factoring multi-power RSA modulus $N = p^r q$ with partial known bits. In: Proc. of the 18th Australasian Conf. on Information Security and Privacy. Brisbane: Springer, 2013. 57–71. [doi: 10.1007/978-3-642-39059-3_5]

[59] Lu Y, Peng LQ, Sarkar S. Cryptanalysis of an RSA variant with moduli $N=p^r q^l$. Journal of Mathematical Cryptology, 2017, 11(2): 117–130. [doi: 10.1515/jmc-2016-0025]

[60] Coron JS, Faugère JC, Renault G, Zeitoun R. Factoring $N=p^r q^s$ for Large r and s. In: Proc. of the RSA Conf. on Topics in Cryptology. Berlin: Springer, 2016. 448–464. [doi: 10.1007/978-3-319-29485-8_26]

[61] Coron JS, Zeitoun R. Improved factorization of $N=p^r q^s$. In: Proc. of the 2018 Cryptographer's Track at RSA Conf. San Francisco: Springer, 2018. 65–79. [doi: 10.1007/978-3-319-76953-0_4]

[62] May A. Secret exponent attacks on RSA-type schemes with moduli $N=p^r q$. In: Proc. of the 7th Int'l Workshop on Public Key Cryptography. Singapore: Springer, 2004. 218–230. [doi: 10.1007/978-3-540-24632-9_16]

[63] Sarkar S. Small secret exponent attack on RSA variant with modulus $N=p^r q$. Designs, Codes and Cryptography, 2014, 73(2): 383–392. [doi: 10.1007/s10623-014-9928-6]

[64] Sarkar S. Revisiting prime power RSA. Discrete Applied Mathematics, 2016, 203: 127–133. [doi: 10.1016/j.dam.2015.10.003]

[65] Takayasu A, Kunihiro N. How to generalize RSA cryptanalyses. In: Proc. of the 19th Int'l Conf. on Public-key Cryptography. Taipei: Springer, 2016. 67–97. [doi: 10.1007/978-3-662-49387-8_4]

[66] Itoh K, Kunihiro N, Kurosawa K. Small secret key attack on a variant of RSA (due to Takagi). In: Proc. of the Cryptographers' Track at the RSA Conf. San Francisco: Springer, 2008. 387–406. [doi: 10.1007/978-3-540-79263-5_25]

[67] Huang ZJ, Hu L, Xu J, Peng LQ, Xie YH. Partial key exposure attacks on Takagi's variant of RSA. In: Proc. of the 12th Int'l Conf. on Applied Cryptography and Network Security. Lausanne: Springer, 2014. 134–150. [doi: 10.1007/978-3-319-07536-5_9]

[68] Collins T, Hopkins D, Langford S, Sabin M. Public key cryptographic apparatus and method: US, 5848159. 1998-12-08.

[69] Lenstra Jr HW. Factoring integers with elliptic curves. Annals of Mathematics, 1987, 126(3): 649–673. [doi: 10.2307/1971363]

[70] De Weger B. Cryptanalysis of RSA with small prime difference. Applicable Algebra in Engineering, Communication and Computing, 2002, 13(1): 17–28. [doi: 10.1007/s002000100088]

[71] Bahig HM, Bhery A, Nassr DI. Cryptanalysis of multi-prime RSA with small prime difference. In: Proc. of the 14th Int'l Conf. on Information and Communications Security. Hong Kong: Springer, 2012. 33–44. [doi: 10.1007/978-3-642-34129-8_4]

[72] Hinek MJ. Another look at small RSA exponents. In: Proc. of the Cryptographers' Track at the RSA Conf. San Jose: Springer, 2006. 82–98. [doi: 10.1007/11605805_6]

[73] Sarkar S, Maitra S. Cryptanalytic results on 'dual CRT' and 'common prime' RSA. Designs, Codes and Cryptography, 2013, 66(1–3): 157–174. [doi: 10.1007/s10623-012-9675-5]

周永彬(1973－), 男, 博士, 教授, 博士生导师, CCF 高级会员, 主要研究领域为网络与信息安全理论及技术.

许军(1982－), 男, 博士, 副研究员, 主要研究领域为公钥密码分析, 计算数论.

姜子铭(1995－), 女, 博士生, 主要研究领域为格加密, 格分析.

王鲲鹏(1971－), 男, 博士, 研究员, 博士生导师, 主要研究领域为密码理论与技术, 密码协议理论与技术.

王天宇(1992－), 男, 博士生, 主要研究领域为格分析, 格密码.

刘月君(1994－), 女, 博士, 主要研究领域为格密码, 公钥密码分析.

袁思蒙(1994－), 女, 硕士生, 主要研究领域为 RSA 及其变体算法的格分析.