

# Attack RSA with Lattice

RSA 是被广泛应用的公钥密码体制, 因此对于 RSA 的安全性分析是十分有必要的。基于格基规约的 Coppersmith 方法是分析 RSA 的用力工具。本文第一部分将介绍有关 RSA、格、LLL 格基规约算法、Howgrave-Graham 定理 [1] 等基础知识以及 Coppersmith 求模方程小根的基本思想; 第二部分将介绍 Herrmann, May 对于 Boneh, Durfee 小指数攻击的改进 [2]。

## 1 基础知识

### 1.1 RSA 体制

RSA 是基于大整数分解困难问题而设计的公钥密码体制。在该体制中, 选取两个大素数  $p, q$ , 计算  $N = pq, \varphi(N) = (p-1)(q-1)$ , 选择  $e$  满足  $\gcd(e, \varphi(N)) = 1$  并计算  $d \equiv 1 \pmod{\varphi(N)}$ 。在该体制中,  $p, q, \varphi(N), d$  作为私钥保存,  $N, e$  作为公开信息。其中  $e$  用来加密消息, 称为公钥;  $d$  用来解密消息, 称为私钥。

若 A 的公钥为  $e$ , 私钥为  $d$ , 模数为  $N$ , B 想给 A 发送消息  $m$  则计算

$$c = m^e \pmod{N}$$

A 得到  $c$  后计算

$$m = c^d = m^{ed} \pmod{N}$$

即可恢复消息。

### 1.2 格与 LLL 格基规约算法

**定义 格:** 格是  $n$  维向量空间的离散加法子群。

即对于一组线性无关的基向量  $\mathbf{B} = \{b_1, b_2, \dots, b_m\}$ , 由其构成的集合

$$L = \left\{ x \in \mathbb{R}^n \mid x = \sum_{i=1}^m a_i b_i, a_i \in \mathbb{Z} \right\}$$

称为格; 向量  $\mathbf{B} = \{b_1, b_2, \dots, b_m\}$  称为格基, 若  $m = n$  则称其为满秩格, 以下讨论的均是满秩格的情况。同一个格可以由不同的格基生成, 如果生成格的基向量长度较小且每组向量之间大致正交, 则认为这是一组好的格基。格的行列式为  $\det(L) = \det(\mathbf{B})$ , 不同格基生成的格的行列式相同。

最短向量问题 (Shortest Vector Problem, SVP) 是格中的经典问题。以下是该问题的定义:

**定义 最短向量问题:** 给一组格  $L$  的格基  $\mathbf{B}$ , 找到一个非零向量  $\mathbf{v}$  使得向量长度  $\|\mathbf{v}\| = \lambda_1(L)$ , 其中  $\lambda_1(L)$  表示格中最短向量的长度。

解决 SVP 问题的一个经典算法是 LLL 算法，该算法与施密特正交化 (Schmidt orthogonalization) 的过程相似。

**定义 施密特正交化:** 给  $n$  个线性无关的向量  $b_1, b_2, \dots, b_n \in \mathbb{R}^n$ , 经过施密特正交化后的向量为  $\tilde{b}_1, \tilde{b}_2, \dots, \tilde{b}_n$ , 其中  $\tilde{b}_i = b_i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{b}_j$ ,  $\mu_{i,j} = \frac{\langle b_i, \tilde{b}_j \rangle}{\langle \tilde{b}_j, \tilde{b}_j \rangle}$

经过施密特正交化后的向量之间相互正交。例如，当在线性空间  $\mathbb{R}^2$  中，取两个线性无关的向量  $b_1, b_2$ ，设两向量间夹角为  $\theta$ ， $b_2$  在  $b_1$  上的投影为  $c$ ，则

$$\begin{aligned} \tilde{b}_1 &= b_1 & \|c\| &= \|b_2\| \cos \theta & \cos \theta &= \frac{\langle b_2, \tilde{b}_1 \rangle}{\|\tilde{b}_1\| \|b_2\|} \\ c &= \tilde{b}_1 \cdot \|c\| = \frac{\langle \tilde{b}_1, b_2 \rangle}{\langle \tilde{b}_1, \tilde{b}_1 \rangle} \cdot \tilde{b}_1 \\ \tilde{b}_2 &= b_2 - c = b_2 - \frac{\langle \tilde{b}_1, b_2 \rangle}{\langle \tilde{b}_1, \tilde{b}_1 \rangle} \cdot \tilde{b}_1 = b_2 - \mu \tilde{b}_1 \end{aligned}$$

当  $b_2$  减去在  $\tilde{b}_1$  上的投影后得到的  $\tilde{b}_2$  与  $\tilde{b}_1$  正交，如下图所示。

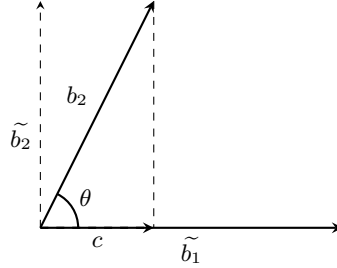


图 1:  $\mathbb{R}^2$  中的施密特正交化

LLL 格基规约算法借鉴了施密特正交化的过程，具体算法描述如下：

---

#### 算法 1 LLL 算法

---

输入: 格基  $b_1, b_2, \dots, b_n, \delta \in (\frac{1}{4}, 1)$

输出:  $\delta$ -LLL 规约后的格基

start: compute  $\tilde{b}_1, \tilde{b}_2, \dots, \tilde{b}_n$

for  $i = 2$  to  $n$  do

  for  $j = i - 1$  to  $1$  do

$$b_i = b_i - c_{i,j} b_j, c_{i,j} = \lceil \frac{\langle b_i, \tilde{b}_j \rangle}{\langle \tilde{b}_j, \tilde{b}_j \rangle} \rceil$$

if  $\exists i$  s.t.  $\delta \|\tilde{b}_i\|^2 > \|\mu_{i+1,i} \cdot \tilde{b}_i + \tilde{b}_{i+1}\|^2$  then

$b_i \leftrightarrow b_{i+1}$

  goto start

---

其中  $\lceil \cdot \rceil$  表取最近的整数。

在该算法中,  $c_{i,j}$  为整数, 则每次计算得到的  $b_i$  也必然在格中, 经过 LLL 格基规约后的格基两两间大致正交并满足以下两个性质:

$$\begin{aligned} 1. & \forall 1 \leq i \leq n, j < i, |\mu_{i,j}| \leq \frac{1}{2} \\ 2. & \forall 1 \leq i \leq n, \delta \|\tilde{b}_i\|^2 \leq \|\mu_{i+1,i}\tilde{b}_i + \tilde{b}_{i+1}\|^2 \end{aligned}$$

对第二条性质做如下变换:

$$\begin{aligned} \mu_{i+1,i}^2 \|\tilde{b}_i\|^2 + \|\tilde{b}_{i+1}\|^2 &\geq \|\mu_{i+1,i}\tilde{b}_i + \tilde{b}_{i+1}\|^2 \geq \delta \|\tilde{b}_i\|^2 \\ \|\tilde{b}_{i+1}\|^2 &\geq (\delta - \mu_{i+1,i}^2) \|\tilde{b}_i\|^2 \geq (\delta - \frac{1}{4}) \|\tilde{b}_i\|^2 \end{aligned}$$

**定理 1 柯西-施沃茨不等式 (Cauchy-Schwartz inequality):**

对于两个向量  $\mathbf{x} = (x_1, x_2, \dots, x_n), \mathbf{y} = (y_1, y_2, \dots, y_n)$ , 有  $\langle \mathbf{x}, \mathbf{y} \rangle^2 \leq |\mathbf{x}|^2 \cdot |\mathbf{y}|^2$ ,

$$\text{即 } (\sum_{i=1}^n x_i y_i)^2 \leq (\sum_{i=1}^n x_i^2) \cdot (\sum_{i=1}^n y_i^2).$$

**证明:**

$$\begin{aligned} \langle \mathbf{x}, \mathbf{y} \rangle &= |\mathbf{x}| \cdot |\mathbf{y}| \cos \theta \\ \langle \mathbf{x}, \mathbf{y} \rangle^2 &= |\mathbf{x}|^2 |\mathbf{y}|^2 \cos^2 \theta \leq |\mathbf{x}|^2 |\mathbf{y}|^2 \end{aligned}$$

结合上述不等式, 可得如下推论:

**推论 1:** 设  $\mathbf{B} = \{b_1, b_2, \dots, b_n\}$  为一组格基,  $\tilde{\mathbf{B}} = \{\tilde{b}_1, \tilde{b}_2, \dots, \tilde{b}_n\}$  为经过 LLL 规约后的格基, 则  $\lambda_1(L(\mathbf{B})) \geq \min_{i \in \{1, 2, \dots, n\}} \|\tilde{b}_i\|$ 。

**证明:**

假设  $\mathbf{x} \in \mathbb{Z}^n$  为非零向量, 要证明上述结论成立则需要证明格中的点  $\mathbf{x}\mathbf{B}$  的下界为  $\min_{i \in \{1, 2, \dots, n\}} \|\tilde{b}_i\|$ 。取  $\tilde{b}_j$  为  $\tilde{\mathbf{B}}$  中的任意一个向量, 则有:

$$\begin{aligned} |\langle \mathbf{x}\mathbf{B}, \tilde{b}_j \rangle| &= |\langle \sum_{i=1}^n x_i b_i, \tilde{b}_j \rangle| \\ &= |\langle x_j \sum_{i=1}^n b_i, \tilde{b}_j \rangle| \\ &\geq |x_j| |\langle b_j, \tilde{b}_j \rangle| \\ &\geq |x_j| \cdot \|\tilde{b}_j\|^2 \end{aligned}$$

通过柯西-施沃茨不等式可得:

$$|\langle \mathbf{x}\mathbf{B}, \tilde{b}_j \rangle| \leq \|\mathbf{x}\mathbf{B}\| \cdot \|\tilde{b}_j\|$$

因此有:

$$\begin{aligned} |x_j| \cdot \|\tilde{b}_j\|^2 &\leq \|\mathbf{x}\mathbf{B}\| \cdot \|\tilde{b}_j\| \\ |x_j| \cdot \|\tilde{b}_j\| &\leq \|\mathbf{x}\mathbf{B}\| \\ \|\tilde{b}_j\| &\leq \|\mathbf{x}\mathbf{B}\| \end{aligned}$$

而  $\mathbf{x}\mathbf{B}$  可以表示格中的任意一个非零向量, 因此有  $\lambda_1(L(\mathbf{B})) \geq \min_{i \in \{1, 2, \dots, n\}} \|\tilde{b}_i\|$ 。

结合 LLL 规约后格基的第二条性质以及推论 1, 有如下推论:

**推论 2:** 若  $b_1, b_2, \dots, b_n$  为经 LLL 规约后的向量, 则  $\|b_1\| \leq (\frac{2}{\sqrt{4\delta-1}})^{n-1} \cdot \lambda_1(L)$

**证明:**

根据性质 2 有:

$$\|b_n\|^2 \geq (\delta - \frac{1}{4})\|b_{n-1}\|^2 \geq (\delta - \frac{1}{4})^2\|b_{n-2}\|^2 \geq \dots \geq (\delta - \frac{1}{4})^{n-1}\|b_1\|^2$$

即:

$$\|b_1\| \leq (\delta - \frac{1}{4})^{-\frac{n-1}{2}} \|b_n\| \leq (\delta - \frac{1}{4})^{-\frac{n-1}{2}} \|b_i\|$$

根据推论 1, 对于任意一组格基  $b_1, b_2, \dots, b_n$  都有  $\min_i \|\tilde{b}_i\| \leq \lambda_1(L)$ , 结合上式有:

$$\|b_1\| \leq (\delta - \frac{1}{4})^{-\frac{n-1}{2}} \min_i \|b_i\| \leq (\delta - \frac{1}{4})^{-\frac{n-1}{2}} \cdot \lambda_1(L) = (\frac{2}{\sqrt{4\delta-1}})^{n-1} \cdot \lambda_1(L)$$

对于格的最短向量长度, Minkowski 第一定理给出了一个粗略的范围:

**定理 2 Minkowski 第一定理 (Minkowski's First Theorem):** 假设  $L$  为一个  $n$  维满秩格, 则有:

$$\lambda_1(L) \leq \sqrt{n} |\det(L)|^{\frac{1}{n}}$$

结合推论 2 与定理 2 可以得到经过 LLL 规约后得到的第一个向量与格行列式之间的关系:

$$\|b_1\| \leq (\frac{2}{\sqrt{4\delta-1}})^{n-1} \sqrt{n} \cdot |\det(L)|^{\frac{1}{n}}$$

### 1.3 Howgrave-Graham 定理与 Coppersmith 方法

对于多项式  $f(x_1, x_2, \dots, x_n) = \sum a_{t_1, t_2, \dots, t_n} x_1^{t_1} x_2^{t_2} \dots x_n^{t_n}$ , 其二范数

$$\|f(x_1, x_2, \dots, x_n)\| = \sqrt{\sum |a_{t_1, t_2, \dots, t_n}|^2}.$$

**定理 3 Howgrave-Graham 定理:**

如果多项式  $f(x_1, x_2, \dots, x_n) \in \mathbb{Z}[x_1, x_2, \dots, x_n]$  中含有至多  $m$  个单项式, 并且其零点  $(x_1^{(0)}, x_2^{(0)}, \dots, x_n^{(0)}) \in \mathbb{Z}^n$  满足以下两个条件:

$$(1) f(x_1^{(0)}, x_2^{(0)}, \dots, x_n^{(0)}) \equiv 0 \pmod{N}, |x_1^{(0)}| < X_1, |x_2^{(0)}| < X_2, \dots, |x_n^{(0)}| < X_n;$$

$$(2) \|f(X_1 x_1, X_2 x_2, \dots, X_n x_n)\| < \frac{N}{\sqrt{m}}$$

那么多项式  $f(x_1^{(0)}, x_2^{(0)}, \dots, x_n^{(0)}) \equiv 0 \pmod{N}$  在整数上成立。

**证明:**

根据条件 1 有:

$$\begin{aligned} |f(x_1, x_2, \dots, x_n)| &= \sum_1^m |a_{t_1, t_2, \dots, t_n} x_1^{t_1} x_2^{t_2} \dots x_n^{t_n}| \\ &< \sum_1^m |a_{t_1, t_2, \dots, t_n} \cdot X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}| \end{aligned}$$

根据二范数的定义有:

$$||f(X_1x_1, X_2x_2, \dots, X_nx_n)|| = \sqrt{\sum_1^m |a_{t_1, t_2, \dots, t_n} \cdot X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}|^2}$$

结合柯西-施沃茨不等式  $(\sum_{i=1}^n x_i y_i)^2 \leq (\sum_{i=1}^n x_i)^2 \cdot (\sum_{i=1}^n y_i)^2$ ,

取  $x_i$  为  $a_{t_1, t_2, \dots, t_n} \cdot X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}$ ,  $y_i$  为 1, 则有:

$$\begin{aligned} (\sum_1^m |a_{t_1, t_2, \dots, t_n} \cdot X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}| \cdot 1)^2 &\leq \sum_1^m |a_{t_1, t_2, \dots, t_n} \cdot X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}|^2 \cdot \sum_1^m 1^2 \\ \sum_1^m |a_{t_1, t_2, \dots, t_n} \cdot X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}| &\leq \sqrt{m} \cdot \sqrt{\sum_1^m |a_{t_1, t_2, \dots, t_n} \cdot X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}|^2} \\ &= \sqrt{m} \cdot ||f(X_1x_1, X_2x_2, \dots, X_nx_n)|| \end{aligned}$$

联合以上不等式与条件 2 得:

$$\begin{aligned} |f(x_1, x_2, \dots, x_n)| &< \sqrt{m} \cdot ||f(X_1x_1, X_2x_2, \dots, X_nx_n)|| \\ &< \sqrt{m} \cdot \frac{N}{\sqrt{m}} \\ &= N \end{aligned}$$

因此:

$$-N < f(x_1, x_2, \dots, x_n) < N$$

所以如果能够满足上述两个条件, 那么模方程  $f(x_1, x_2, \dots, x_n) \equiv 0 \pmod{N}$  的解即可在整数意义下求得。即  $f(x_1, x_2, \dots, x_n) = 0$  的解也为上述模方程的解。

Coppersmith 方法的基本思想是通过已有的模方程  $f(x_1, x_2, \dots, x_n) \equiv 0 \pmod{N}$  来构造一组具有相同解的模方程, 并且各模方程的系数可以构成一组格基, 在该格基中每一个格点对应的多项式都与已有模方程根相同, 因此如果对上述格基规约后得到的第一个向量能够满足 Howgrave-Graham 定理的要求, 将很容易的在整数意义下求出模方程的根来达到攻击 RSA 的目的。

## 2 RSA 小指数攻击

在此先规定各符合含义, 便于后续说明。假设模数  $N$  的比特长度为  $n$ ,  $e, d$  的比特长度分别为  $\alpha n, \delta n$ ,  $e, d$  满足等式  $ed = x\varphi(N) + 1$ 。以下讨论均假设  $\alpha \approx 1$ 。

最早的小指数攻击由 Wiener 提出, 他指出当  $\beta < \frac{1}{4}$  时, 可由连分数攻击恢复私钥  $d$ ; 之后 Boneh, Durfee 使用格方法将小指数攻击的理论范围提高至  $\delta < \frac{2-\sqrt{2}}{2} \approx 0.292$ ; 后由 Herrmann, May 使用拆分线性化的技巧对 Boneh, Durfee 的方法进行了简化, 虽然并没有提高理论 upper 界, 但是使格基构造与证明过程更加简洁。以下将重点介绍 Herrmann, May 的方法。

根据定义有  $\varphi(N) = (p-1)(q-1)$ , 对 RSA 密钥等式可以重新写为:

$$\begin{aligned} ed &= 1 + x\varphi(N) \\ &= 1 + x(N + 1 + (-p - q)) \end{aligned}$$

设  $A = N + 1, y = -p - q$ , 则有  $ed = 1 + x(A + y)$ 。因此需要找模多项式

$$f(x, y) = 1 + x(A + y) = xA + xy + 1 \pmod{e}$$

的小根。其中  $xy$  为二次项, Herrmann 与 May 通过引入参数  $u = 1 + xy \pmod{e}$  使上述多项式变为线性多项式  $\bar{f}(u, x) = u + Ax \pmod{e}$ , 且有  $xy = u - 1$ 。

根据多项式  $\bar{f}$  构造多项式

$$\bar{g}_{i,k}(u, x) = x^i \bar{f}^k e^{m-k} \quad k = 0, \dots, m \quad \text{and} \quad i = 0, \dots, m - k$$

称为  $x$  移位多项式 ( $x\text{-shifts}$ )。则对于任意的  $i, k$  都有  $\bar{g}(u, x) \pmod{e^m} = 0$ , 其中  $m$  为一个可调的正整数。

若仅使用  $x$  移位多项式来构造格基, 可以得到 Wiener 关于  $\delta < 0.25$  的结论。引入  $y$  移位多项式 ( $y\text{-shifts}$ )

$$\bar{h}_{j,k}(u, x) = y^j \bar{f}^k e^{m-k} \quad j = 1, \dots, t \quad \text{and} \quad k = \left\lfloor \frac{m}{t} \right\rfloor j, \dots, m$$

其中  $t$  为正整数, 且  $m \geq t$ 。同样对于任意的  $j, k$  都有  $\bar{h}(u, x) \pmod{e^m} = 0$ 。为方便后续分析设  $t = \tau m$ 。

Herrmann 与 May 证明了当这样选择  $x$  移位多项式与  $y$  移位多项式时, 每一项多项式都只会比之前已有单项式多出一个单项式, 且仅包含  $X, Y, U, e$ , 即得到关于  $\bar{g}_{i,k}(Uu, Xx)$  与  $\bar{h}_{j,k}(Uu, Xx)$  的单项式系数矩阵一定为下三角方阵, 形成的格基矩阵的行列式即为对角线元素的积。例如下图描绘了一个  $m = 2, t = 1$  时所形成的格基矩阵:

$$\begin{matrix} & 1 & x & u & x^2 & ux & u^2 & u^2 y \\ e^2 & \left( \begin{array}{ccccccc} e^2 & & & & & & \\ & e^2 X & & & & & \\ & eAX & eU & & & & \\ & & & e^2 X^2 & & & \\ & & & eAX^2 & eUX & & \\ & & & A^2 X^2 & 2AX & U^2 & \\ & -A^2 X & -2AU & & A^2 UX & 2AU^2 & U^2 Y \end{array} \right) \end{matrix}$$

图 2:  $m = 2, t = 1$  时所形成的格基矩阵

以下分析按照上述方法得到的格基矩阵的行列式, 并设  $s_x$  代表  $X$  在矩阵对角线中出现的次数。根据  $x$  移位多项式有:

$$\begin{aligned}
s_x &= \sum_{k=0}^m \sum_{i=0}^{m-k} i \\
&= \sum_{k=0}^m \frac{(m-k)(m-k+1)}{2} = \sum_{k=0}^m \frac{m^2 + k^2 - 2mk - m - k}{2} \\
&= \frac{1}{2} \cdot \frac{m(m+1)(2m+1)}{6} + o(m^3) \\
&= \frac{1}{6}m^3 + o(m^3)
\end{aligned}$$

对于第一个求和符号, 是对  $i$  的求和, 即为等差数列的求和展开; 对第二个求和符号, 是对  $k^2$  的求和, 为整数平方求和。当  $m \rightarrow \infty$  时,  $s_x$  的大小主要取决于  $\frac{1}{6}m^3$ 。

根据  $y$  移位多项式有:

$$\begin{aligned}
s_y &= \sum_{j=1}^{\tau m} \sum_{k=\frac{1}{\tau}j}^m j \\
&= \sum_{j=1}^{\tau m} (m - \frac{1}{\tau}j + 1)j = \sum_{j=1}^{\tau m} (mj - \frac{1}{\tau}j^2 + j) \\
&= \frac{(m + \tau m^2)(\tau m - 1)}{2} - \frac{1}{\tau} \cdot \frac{\tau m(\tau m + 1)(2\tau m + 1)}{6} + o(m^3) \\
&= \frac{\tau^2 m^3}{2} - \frac{2\tau^2 m^3}{6} + o(m^3) \\
&= \frac{\tau^2 m^3}{6} + o(m^3)
\end{aligned}$$

对于第一个求和符号, 是对  $k$  求和, 但是求和变量是  $j$ , 因此拆开为求和次数与  $j$  的乘积。

同理可以求出:

$$\begin{aligned}
s_u &= \sum_{k=0}^m \sum_{i=0}^{m-k} k + \sum_{j=1}^{\tau m} \sum_{k=\frac{1}{\tau}j}^m k = (\frac{1}{6} + \frac{\tau}{3})m^3 + o(m^3) \\
s_e &= \sum_{k=0}^m \sum_{i=0}^{m-k} (m-k) + \sum_{j=1}^{\tau m} \sum_{k=\frac{1}{\tau}j}^m (m-k) = (\frac{1}{3} + \frac{\tau}{6})m^3 + o(m^3)
\end{aligned}$$

以及格基的维数:

$$\dim(L) = \sum_{k=0}^m \sum_{i=0}^{m-k} 1 + \sum_{j=1}^{\tau m} \sum_{k=\frac{1}{\tau}j}^m 1 = (\frac{1}{2} + \frac{\tau}{2})m^2 + o(m^2)$$

结合 1.2 中 LLL 规约后得到第一个向量与格行列式之间的关系:

$$\|b_1\| \leq \left(\frac{2}{\sqrt{4\delta-1}}\right)^{n-1} \sqrt{n} \cdot |\det(L)|^{\frac{1}{n}}$$

和 Howgrave-Graham 定理, 考虑当  $m \rightarrow \infty$ , 即忽略对不等式影响较小的项, 当:

$$\begin{aligned} \det(L)^{\frac{1}{\dim(L)}} &< e^m \\ \det(L) &< e^{m \dim(L)} \end{aligned}$$

时, 即可以在整数意义下求解出模方程的解, 即求出 RSA 的私钥  $d$ 。( $e^m$  为构造模方程的模数)

考虑 RSA 体制中选取的参数  $p, q$  是平衡的, 即  $|y| \leq Y = N^{\frac{1}{2}}$ , 且有:

$$\begin{aligned} ed &= 1 + x\varphi(N) \\ x &\approx \frac{ed}{\varphi(N)} \approx d \end{aligned}$$

即  $|x| \leq X = N^\delta$ , 则  $|u| \leq U = N^{\delta+\frac{1}{2}}$ 。因此:

$$\begin{aligned} \det(L) &= X^{s_x} Y^{s_y} U^{s_u} e^{s_e} \\ &= N^{\delta s_x + \frac{1}{2} s_y + (\delta + \frac{1}{2}) s_u + s_e} \\ &\approx N^{\frac{1}{6} m^3 \delta + \frac{1}{2} \cdot \frac{\tau^2}{6} m^3 + (\delta + \frac{1}{2}) (\frac{1}{6} + \frac{\tau}{3}) m^3 + (\frac{1}{3} + \frac{\tau}{6}) m^3} \\ e^{m \dim(L)} &\approx N^{(\frac{1}{2} + \frac{\tau}{2}) m^3} \end{aligned}$$

代入  $\det(L) < e^{m \dim(L)}$  得:

$$\begin{aligned} N^{\frac{1}{6} m^3 \delta + \frac{1}{2} \cdot \frac{\tau^2}{6} m^3 + (\delta + \frac{1}{2}) (\frac{1}{6} + \frac{\tau}{3}) m^3 + (\frac{1}{3} + \frac{\tau}{6}) m^3} &< N^{(\frac{1}{2} + \frac{\tau}{2}) m^3} \\ \tau^2 + (4\delta - 2)\tau + 4\delta - 1 &< 0 \end{aligned}$$

即该问题转化为: 当  $\tau$  为参数  $\delta$  为自变量时, 求是否存在  $\delta$  满足上述不等式。

当不等式左侧最大值小于 0 时,

$$\tau = -\frac{4\delta - 2}{2} = 1 - 2\delta$$

代入原不等式有:

$$\begin{aligned} (1 - 2\delta)^2 + (4\delta - 2)(1 - 2\delta) + 4\delta - 1 &< 0 \\ 2\delta^2 - 4\delta + 1 &> 0 \end{aligned}$$

解得:

$$\delta < \frac{2 - \sqrt{2}}{2} \quad \text{or} \quad \delta > \frac{2 + \sqrt{2}}{2}$$

由  $\delta < 1$  即取  $\delta < \frac{2 - \sqrt{2}}{2} \approx 0.292$ 。

即当  $d < N^{0.292}$  时可由格攻击恢复 RSA 的私钥  $d$ 。



### 3 结语

本文对 RSA 格攻击的所需要的基础知识及 RSA 小指数攻击进行了介绍。在 RSA 小指数攻击中，忽略了大量细节因此求得的界仅为理论上界，在实际攻击中并不能达到。对于二元或多元方程，是需要找到相应个数的线性无关多项式在通过结式或者 Gröbner 基 (Gröbner basis) 来求解，而大多分析仅针对经过 LLL 规约得到的第一个向量，这也将导致格攻击不能达到理论上界。

杨峥嵘

### 参考文献

- [1] N. Howgrave-Graham. Finding small roots of univariate modular equations revisited. In M.J. Darnell, editor, *Cryptography and Coding 1997*, volume 1355 of *LNCS*, pages 131–142. Springer, Heidelberg, 1997.
- [2] Herrmann Mathias and Alexander May. Maximizing small root bounds by linearization and applications to small secret exponent rsa. In *Public Key Cryptography–PKC 2010: 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings 13*. Springer Berlin Heidelberg, 2010.