

权重 $a_1, \dots, a_n \in \{1, \dots, X\}$, $X \geq 2^{n^2(\frac{1}{2} + \varepsilon)}$, $\varepsilon > 0$

密文 $s = \langle a, x \rangle$, $x \in \{0, 1\}^n$, 解出 x 的概率为 $1 - 2^{-n^2(\varepsilon - o(1))}$

证: 设 $s \geq (\sum_{i=0}^n a_i)/2$ (若不满足则 $s \leftarrow \sum_i a_i - s$)

(Proof 1) 理想的构造为存在一个格 L , x 是 L 上的最短向量.

且不与 x 平行的向量都比 x 长很多。(大 $2^{\frac{n}{2}}$ 倍以上)

由于 LLL 算法给出的是 $SVP_{2^{\frac{n}{2}}}$ 的解, 所以

这样的解一定是 $k(\frac{x}{b})$ 的形式。设 multiplier = $b = \lceil \sqrt{n \cdot 2^n} \rceil$

$$B = \begin{pmatrix} I_{n \times n} & 0_{n \times 1} \\ -bA & bs \end{pmatrix} \text{ 构造格基 } \in \mathbb{Z}^{(n+1) \times (n+1)}$$

之前别的方案的格基 be like $\begin{pmatrix} I_{n \times n} & 0_{n \times 1} \\ A & -s \end{pmatrix}$,

此处是多乘了 b .

乘 b 的效果: 放大不满足 $\langle a, z \rangle = s$ 的向量的范围, 使得非解向量的范式远大于 LLL 生成向量的范式。

由于格基矩阵最后一行都是 B 的倍数.

考虑

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ -ba_1 & -ba_2 & \cdots & -ba_n & bS \end{pmatrix} \begin{pmatrix} z_1 \\ \vdots \\ z_n \\ \vdots \\ z_{n+1} \end{pmatrix}$$

解 x 需要满足 $b < a, x > -bs \cdot z_{n+1} = 0$ (展开最后一个分量)

如果某向量 $\begin{pmatrix} z \\ z_{n+1} \end{pmatrix}$ 不满足上述导式，即：

$$-ba_1 \cdot z_1 - ba_2 \cdot z_2 - \dots - ba_n \cdot z_n + bs z_{n+1} = q \neq 0$$

可提出一个 b 的公因数，那么 z 的最后一分量的坐标

q 被 b 整除，therefore，这样的向量长度一定大于等于 b
而 $b = \lceil \sqrt{n} \cdot 2^{\frac{n}{2}} \rceil > 2^{\frac{n}{2}} \|x\| \geq 2^{\frac{n}{2}} \lambda_1 (\underline{L})$ 矛盾！

Thus LLL 输出的 $SVP_{\frac{n}{2}}(\underline{L})$ 的结果一定是 $R(\begin{pmatrix} z \\ 0 \end{pmatrix})$ 的形式

其最大的长度不超过 $2^{\frac{n}{2}} \sqrt{n}$ 。接下来证明这样的 $\begin{pmatrix} z \\ 0 \end{pmatrix}$

极大概率就是 $\binom{x}{0}$ (Proof 2)

假设有 $\begin{pmatrix} z \\ 0 \end{pmatrix} \in \mathbb{Z}^{n+1}$, $\|z\| \leq 2^{\frac{n}{2}} \sqrt{n}$, 而且 $z \neq kx$

证明这样的 $\begin{pmatrix} z \\ 0 \end{pmatrix} \in \underline{L}$ 的概率。即 $B \cdot \begin{pmatrix} z \\ z_{n+1} \end{pmatrix} = \begin{pmatrix} z \\ 0 \end{pmatrix}$,

那就有最后一分量 的乘法结果 = 前文假设 $S z \frac{1}{2} \sum_{i=1}^n a_i$

$$-ba_1 \cdot z_1 - ba_2 \cdot z_2 - \dots - ba_n \cdot z_n + bs z_{n+1} = 0$$

$$\Leftrightarrow a_1 z_1 + a_2 z_2 + \dots + a_n z_n = S z_{n+1}$$

$$\Leftrightarrow \langle a, z \rangle = S z_{n+1} \Leftrightarrow S |z_{n+1}| = |\langle a, z \rangle| \leq \|z\| \sum_{i=1}^n a_i \leq 2S \|z\|$$

$$\text{Thus } S |z_{n+1}| \leq 2S \|z\| \Rightarrow |z_{n+1}| \leq 2 \|z\|$$

确定一对 (z, z_{n+1}) 时，有

$$\langle a, z \rangle = S z_{n+1} = z_{n+1} \langle a, x \rangle$$

$$a_1 z_1 + a_2 z_2 + \dots + a_n z_n = z_{n+1} (a_1 x_1 + \dots + a_n x_n)$$

$$\Leftrightarrow a_1(z - z_{n+1}x_1) + \dots + a_n(z_n - z_{n+1}x_n) = 0$$

令 $y = z - z_{n+1}x$, 有 $\langle a, y \rangle = 0$

由于 $z \neq kx$, 故 $y \neq 0$. (肯定有分量不为 0)

设有 $y_i \neq 0$, 则 $a_i = -\left(\sum_{i=1}^n a_i y_i\right) / y_i$.

这里计算的是上限概率. 若有若干 $\neq 0$ 的 y_i , 则用独立事件计算概率.

若这样的 $(\vec{y}) \in \mathbb{F}$, 则上述等式均成立, 有 $\langle a, y \rangle \geq 0$.

计算 $\Pr_{a_i}[\langle a, y \rangle \geq 0] = \Pr[a_i = -\left(\sum_{i=1}^n a_i y_i\right) / y_i] \leq 1/X$
(因为 a_i 是从 $\{1, \dots, X\}$ 中随机得的.)

△ 总概率 = (-组 (z, z_{n+1}) 出现的概率) \times 可能存在的 (z, z_{n+1}) 组数

$$\begin{cases} \|z\| \leq 2^{\frac{n}{2}} \sqrt{n} \leq b, \text{ 最大的分量绝对值 } \leq b \Rightarrow z_{n+1} \text{ 取 } (2b+1)^n \text{ 种} \\ |z_{n+1}| \leq 2 \|z\| \leq 2b \Rightarrow z_{n+1} \text{ 取 } (4b+1) \text{ 种} \end{cases}$$

$$\Pr_{a_i} \text{ 共取 } (2b+1)^n \cdot (4b+1) \text{ 种} \leq (5b)^{n+1} \leq 2^{n^2(\frac{1}{2} + o(1))}$$

$$X = 2^{n^2(\frac{1}{2} + \varepsilon)} (\varepsilon > 0)$$

$$\begin{aligned} \text{对于固定的 } (z, z_{n+1}) \text{ 有 } 1/X \text{ 的概率, 共有 } (2b+1)^n (4b+1) \text{ 种} \\ \text{可能, 故总概率 } \leq 1/X \cdot (2b+1)^n (4b+1) \leq 2^{-n^2(\frac{1}{2} + \varepsilon) + n^2(\frac{1}{2} + o(1))} \\ = 2^{-n^2(\varepsilon - o(1))} \end{aligned}$$

故 $z = kx$ 的概率为 $1 - 2^{-n^2(\varepsilon - o(1))}$