Лекция №13
"Потайной ход" (trapdoor) для задачи SIS

I "Потайной ход" (trapdoor) для задачи SIS (Micciancio-Peikert'12)

<u>Задача</u>: выбрать $A \leftarrow U(\mathbb{Z}_q^{m\times n})$ вместе с коротким базисом $A^\perp$, где
$$A^\perp = \{x \in \mathbb{Z}^m : x^t \cdot A = 0 \mod q\}.$$

Начнём с A особого вида. Будем называть следующую матрицу гаджетом:

$$g \in \begin{bmatrix} 1 \\ 2 \\ \vdots \\ 2^{k-1} \end{bmatrix} \in \mathbb{Z}^k$$

<u>Лемма 1</u> Если q – степень двойки, положим $k = \log_2 q$ и

$$S_k = \underbrace{\begin{bmatrix} 2 & -1 & & 0 \\ & 2 & -1 & \\ 0 & & \ddots & -1 \\ & & & 2 \end{bmatrix}}_{k} \quad \begin{bmatrix} 1 \\ 2 \\ \vdots \\ 2^{k-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Иначе, положим $k = \lceil \log_2 q \rceil$ и $q = \sum\limits_{i=0}^{k-1} 2^i \cdot q_i$, $q_i \in \{0,1\}$,

$$S_k = \begin{bmatrix} 2 & -1 & & 0 \\ & \ddots & \ddots & \\ 0 & & 2 & -1 \\ q_0 & q_1 & \dots & q_{k-1} \end{bmatrix}.$$

Тогда S_k – базис $g^\perp$ и $\forall i$ $\|\underset{i\text{-ый столбец } S_k}{s_i}\| \le \sqrt{6}$.

◁ 1. $S_k \cdot g = 0 \mod q$

2. Покажем, что $\det S_k = \det g^\perp$ (т.к. $\operatorname{rank} S_k = k = \operatorname{rank} g^\perp$, равенство определителей даст р-во решёток).

2.1. $\det S_k = 2^k = q$ (в первом случае)

$$\det S_k = -q_0 \cdot \underbrace{\det \begin{bmatrix} -1 & & 0 \\ 2 & \ddots & -1 \\ 0 & 2 & -1 \end{bmatrix}}_{-1} + 2 \underbrace{\det \begin{bmatrix} 2 & -1 & & \\ & 2 & -1 & \\ q_1 & \cdots & & q_{k-1} \end{bmatrix}}_{\underbrace{2\left(q_1 + 2\det \begin{bmatrix} 2 & -1 & \\ & 2 & -1 \\ q_2 & \cdots & q_k \end{bmatrix}\right)}_{2q_1 + 4q_2 + \ldots + 2^{k-1} \cdot q_{k-1}}} = q$$

$$q_0$$

2.2. Покажем, $\det g^{\perp} = q$ (т.к. $g^{\perp} \subset \mathbb{Z}^k$, $S_k\mathbb{Z}^k \subset \mathbb{Z}^k$ и если $\det g^{\perp} = q = \det S_k$, то S_k - базис $g^{\perp}$).

$\measuredangle\ \varphi : \mathbb{Z}^k \to \mathbb{Z}_q$

$x \mapsto x^t \cdot g \bmod q$ - сюрьекция $\Rightarrow \mathbb{Z}_q \simeq \mathbb{Z}^k / \ker \varphi = \mathbb{Z}^k / g^{\perp}$

$$\Rightarrow q = \# \mathbb{Z}_q = \# (\mathbb{Z}^k / g^{\perp}) = \frac{\det g^{\perp}}{\underbrace{\det \mathbb{Z}^k}_{= 1}} = \det g^{\perp}. \quad \blacktriangleright$$

Положим, $$G = \begin{bmatrix} 1 & 0 & & 0 \\ g & \vdots & & 0 \\ 1 & 0 & & \vdots \\ 0 & 1 & & \vdots \\ 0 & g & & \\ \vdots & 1 & \cdots & 0 \\ & & & 1 \\ 0 & & & g \\ 0 & & & 1 \end{bmatrix} = g \otimes I_e \in \mathbb{Z}^{e \cdot k \times e}$$

$$S = S_k \otimes I_e = \begin{bmatrix} S_k & & 0 \\ & S_k & \\ 0 & & S_k \end{bmatrix} \text{ - базис } G^{\perp}$$

Опр-ие (G-потайной ход) Пусть $A \in \mathbb{Z}_q^{m \times n}$, $G \in \mathbb{Z}_q^{w \times n}$. Тогда матрица $R \in \mathbb{Z}_q^{w \times (m-w)}$ называется G-потайным ходом (G-trapdoor) для A, если

$$\begin{array}{c} \overbrace{\qquad\qquad}^{m-w} \\ w \left[\ R \mid I_w \ \right] \\ \underbrace{\qquad\qquad}_{m} \end{array} \cdot \ m \overset{\leftarrow n \rightarrow}{\left[\ A\ \right]} = w \overset{n}{\left[\ G\ \right]}.$$

Далее нас будет интересовать "малые" R (R с небольшими эл-тами).

Лемма 2 $\exists S \in \mathbb{Z}^{w \times n}$ – базис $G^{\perp}$ как определено выше.

R – G-потайной ход для $A \in \mathbb{Z}_q^{m \times n}$ и

W – эта матрица, т.ч. $W \cdot G = \left[\begin{array}{c|c} -I & 0 \end{array}\right] \begin{bmatrix} A \\ \end{bmatrix}$

(W можно отыскать с помощью решения системы лин. ур-ий из G, A)

Тогда $S_A = \left[\begin{array}{c|c} I & W \\ \hline 0 & S \end{array}\right] \cdot \left[\begin{array}{c|c} I & 0 \\ \hline R & I \end{array}\right]$ – базис для $A^{\perp}$.

II Как получить G-потайной ход для A?

Лемма 3 (Leftover Hash Lemma)

Пусть $A \leftarrow U(\mathbb{Z}_q^{m \times n})$, $u \leftarrow U(\mathbb{Z}_q^n)$, $r \leftarrow D_{\mathbb{Z}^m, \sigma}$. При этом

$m \geqslant n \cdot \log q$, $\sigma > \sqrt{m}$, q-простое. Тогда

$$\Delta\left[\,(A, r^t \cdot A),\ (A, u)\,\right] \leq 2^{-\Omega(n)}.$$

$\triangleleft$ 1. $\forall\ \varphi_A : \mathbb{Z}^m \to \mathbb{Z}_q^n$ – сюрьекция (если строки A образуют $\mathbb{Z}_q^n$, это происходит с вероятностью ~ 1 для простого q).

$x \to x^t \cdot A \bmod q$

$\Rightarrow \mathbb{Z}^m / \operatorname{Ker} \varphi_A = \mathbb{Z}^m / A^{\perp} \simeq \mathbb{Z}_q^n \Rightarrow$

$\Rightarrow D_{\mathbb{Z}^m, \sigma} \cdot A$ – случайное равномерное в $\mathbb{Z}_q^n$ $\Longleftrightarrow$ $D_{\mathbb{Z}^m, \sigma} \bmod A^{\perp}$ – случ. равномерно в $\mathbb{Z}^m / A^{\perp}$.

$$\Pr_{b \leftarrow \mathbb{Z}^m}\left[\, b \text{ – класс смежности в } A^{\perp} \,\right] = \frac{\rho_\sigma(b + A^{\perp})}{\rho_\sigma(\mathbb{Z}^m)} \underset{\uparrow}{\approx} \frac{\rho_\sigma(A^{\perp})}{\rho_\sigma(\mathbb{Z}^m)}$$

верно в точности до множителя $[1 \pm 2^{-\Omega(n)}]$, независимо от b, если $\sigma \geqslant \eta_{2^{-n}}(A^{\perp})$

2. Покажем, что $\eta_{2^{-n}}(A^{\perp}) \le \Omega(\sqrt{m})$.

$$\eta_{2^{-n}}(A^{\perp}) \le \frac{\sqrt{m}}{\lambda_1(\widehat{A^{\perp}})}, \qquad \widehat{A^{\perp}} = \frac{1}{q} L_q(A) = \frac{1}{q}\left(A\mathbb{Z}_q^{n} + q\mathbb{Z}^{m}\right).$$

экв. норм ($\|x\|_2 \ge \|x\|_\infty$)

$$\lambda_1(\widehat{A^{\perp}}) = \frac{1}{q}\lambda_1(L_q(A)) \ge \frac{1}{q}\lambda_1^{\infty}(L_q(A)) \ge \frac{1}{q}\cdot\frac{1}{4}\left(q^{1-\frac{n}{m}}\right)$$

Минковский - Хлавка (Лекция №2)

$\ge \Omega(1)$ с вероятностью $\ge 1-2^{-m}$

$m \ge n\cdot\log q$

$$\Rightarrow \eta_{2^{-n}}(A^{\perp}) \le \frac{\sqrt{m}}{\Omega(1)} < \Omega(\sqrt{m}).$$

Построение R — G-trapdoor для A

Для того, чтобы сгенерировать G-trapdoor для A.

$$\begin{bmatrix} \overbrace{R}^{m'} & I_{m-m'} \end{bmatrix} \cdot \begin{array}{c} \overbrace{\begin{bmatrix} A_{top} \\ A_{bot} \end{bmatrix}}^{n} \end{array} \begin{array}{l} \updownarrow \bar{m} \\ \updownarrow m-\bar{m} \end{array} = \begin{bmatrix} G \end{bmatrix} \mod q$$

1. Выбираем $A_{top} \leftarrow U(\mathbb{Z}_q^{\bar{m}\times n})$, где $\bar{m}$ удовлетворяет условию для m из Леммы 3 ($\bar{m} > n\cdot \lg q$)

2. Выбираем строки R из $D_{\mathbb{Z}_q^{\bar{m}},\sigma}$, где σ удовлетворяет условию Леммы 3 ($\sigma > \sqrt{\bar{m}}$)

3. $A_{bot} = G - \underbrace{R\cdot A_{top}}$

по Лемме 3, $R\cdot A_{top}$ распределена как случайная равномерная матрица $\Rightarrow A = \dfrac{A_{top}}{A_{bot}} \underset{2^{-\Omega(n)}}{\sim} U(\mathbb{Z}_q^{m\times n})$.