Лекция №14
Подпись на решётках

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

Задача: выбрать $A \leftarrow \mathcal{U}(\mathbb{Z}_q^{m\times n})$ вместе с коротким базисом $A^\perp$.

$$A^\perp = \{ x \in \mathbb{Z}^m : \; x^T A = 0 \bmod q \}$$

Начнём с A особого вида, называющегося гаджетом:

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

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

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

Иначе, положим $k = \lceil \log_2 q \rceil$ и $q = \sum_i 2^i q_i \quad q_i \in \{0,1\}$,

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

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

$\triangleleft$ 1. $S_k \cdot g = 0 \bmod q$

2. $\det S_k = 2^k = q$ (в первом случае) $(q_1 + 2(q_2 + \dots)$

$$\det S_k = -q_0 \cdot \det \overbrace{\begin{bmatrix} -1 & & \\ 2 & -1 & \\ & \ddots & -1 \end{bmatrix}}^{-1} + 2 \cdot \det \begin{bmatrix} 2 & -1 & \\ & & \\ q_1 & \dots & q \end{bmatrix} = q.$$

3. Покажем, что и $\det g^{\perp} = q$ (отсюда, т.к. $g^{\perp} \subset \mathbb{Z}^k$, $S_k \cdot \mathbb{Z}^k \subset \mathbb{Z}^k$ и $\det g^{\perp} = \det S_k$, то S_k – базис $g^{\perp}$).

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

$x \mapsto x^T \cdot g \bmod q$ – сюрьекция $\Rightarrow \mathbb{Z}_q \cong \mathbb{Z}^k / \ker \varphi = \mathbb{Z}^k / g^{\perp}$

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

Опр-ие Положим,

$$G = \begin{bmatrix} 1 & 0 & 0 \\ g & & \\ 1 & & 0 \\ 0 & 1 & \\ \vdots & g & \\ 0 & 1 & \\ & 0 & 1 \\ & & g \\ & & 1 \end{bmatrix} = g \otimes I_\ell \in \mathbb{Z}^{\ell \cdot k \times \ell}.$$

$$S = S_k \otimes I_\ell = \begin{bmatrix} S_k & & \\ & S_k & \\ & & S_k \end{bmatrix} \text{ – базис } G^{\perp}$$

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

$$w\overset{m-w}{\left[\begin{array}{c|c} R & I_w \end{array}\right]} \cdot m\left[\,A\,\right] = w\overset{n}{\left[\,G\,\right]}$$

Нас будет интересовать "малое" R.

Лемма 2 $\exists\, S \in \mathbb{Z}^{w \times n}$ – это базис $G^{\perp}$ как опр-но выше

R – G-trapdoor для $A \in \mathbb{Z}_q^{m \times n}$, n

W – это матрица, т.ч. $W \cdot G = \boxed{-I \mid 0} \cdot A$

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

Тогда

$$S_A = \left[\begin{array}{c|c} I & W \\ \hline 0 & S \end{array}\right] \cdot \left[\begin{array}{c|c} I & 0 \\ \hline R & I \end{array}\right] -$$

это базис $A^{\perp}$.

◁ док-во на практике ▷.

II Как получить G-потайной ход для A?

Лемма 3 (Leftover hash lemma)

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

$m \geq n \lg q$, $\sigma > \sqrt{m}$, q - простое.

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

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

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

$\Rightarrow \mathbb{Z}^m / \ker \varphi_A = \mathbb{Z}^m / A^{\perp} \cong \mathbb{Z}_q^n \Rightarrow$

$\Rightarrow D_{\mathbb{Z}^m, \sigma} \cdot A$ - случайное равном. $\Leftrightarrow D_{\mathbb{Z}^m, \sigma} \bmod A^{\perp}$ - случ. равн. в $\mathbb{Z}^m / A^{\perp}$.

$$\Pr_{b \leftarrow \mathbb{Z}^m}[b\text{ - класс смежности в } A^\perp] = \frac{\rho_\sigma(b+A^\perp)}{\rho_\sigma(\mathbb{Z}^m)} \approx \frac{\rho_\sigma(A^\perp)}{\rho_\sigma(\mathbb{Z}^m)}$$

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

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

$$\eta_{2^{-n}}(A^\perp) < \frac{\sqrt{m}}{\lambda_1(\widehat{A^\perp})} \qquad \widehat{A^\perp} = \frac{1}{q} L_q(A) = \frac{1}{q}(A \cdot \mathbb{Z}_q^n + q\mathbb{Z}^m)$$

$$\lambda_1(\widehat{A^\perp}) = \frac{1}{q}\lambda_1(L_q(A)) \geq \frac{1}{q}\lambda_1^\infty(L_q(A)) \geq$$

$$\underset{\text{Минковский-Хлавака из лекции №2}}{\geq} \frac{1}{q}\cdot\frac{1}{4}\left(q^{1-\frac{n}{m}}\right) \underset{\text{т.к. } m \geq n\lg q}{\geq} \Omega(1) \text{ с вероятностью } \geq 1-2^{-m}.$$

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

Вывод Для того, чтобы сгенерировать G-trapdoor для A:

$$\begin{array}{c} \bar{m} \\ \left[\begin{array}{c|c} R & I \end{array}\right] \end{array} \cdot \bar{m} \begin{bmatrix} A_{top} \\ A_{bot} \end{bmatrix} = G \mod q$$

1) Выбираем $A_{top} \leftarrow U(\mathbb{Z}_q^{\bar{m} \times n})$, $\bar{m}$ удовлетворяет усл-иям для m из Леммы 3.

2) Выбираем $\overset{\text{строки } R}{v} \leftarrow D_{\mathbb{Z}_q, \sigma}$ (σ удовлет. условию Леммы 3)

3) $A_{bot} = G - \underbrace{R \cdot A_{top}}_{\text{по Лемме 3, распределено как случ. равномерное}}$

III Подпись GPV (Gentry-Peikert-Vaikuntanathan)

Подпись = [KeyGen, Sign, Verify] - эфф. алг-мы

- $KeyGen(1^\lambda) \to (sk, vk)$
- $Sign(sk, m) \to \sigma$
- $Verify(vk, m, \sigma) \to \{0,1\}$

Корректность $\forall m$: $Verify(vk, m, Sign(sk, m)) = 1$

с вероятностью $\geq 1 - 2^{-\Omega(n)}$ (вероятность берётся над случ битами $Sign()$, $KeyGen()$).