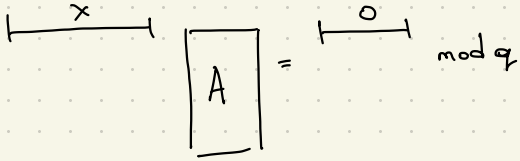
Лекция №12
Задача SIS и её сложность.

I Определение

Ajtai '96: "SIS есть SVP на решётках конструкции-A".

Опр-ие $SIS_{q,m,\beta}$: Пусть $n>0$, $m \geq n$, $q \geq 2$, $\beta > 0$ (m, q, β зависят от n). В задаче Short Integer Solution $SIS_{q(n),m(n),\beta(n)}$ для матрицы $A \leftarrow U(\mathbb{Z}_q^{m \times n})$ требуется найти $X \in \mathbb{Z}^m$, т.ч.

1. $X^T \cdot A = 0 \bmod q$
2. $0 < \|X\| \leq \beta$



обычно имеем в виду: $q = poly(n)$, $m = O(n \log n)$

Замечание: задача SIS – это $\overset{approx}{\forall} SVP_\gamma$ для следующего семейства случайных решёток:

$$\Lambda^\perp = \{ b \in \mathbb{Z}^m : b^t \cdot A = 0 \bmod q \}$$

для $A \leftarrow U(\mathbb{Z}_q^{m \times n})$

- $\dim \Lambda^\perp = m$ $\quad (q\mathbb{Z}^m \subset \Lambda^\perp)$
- $\det \Lambda^\perp = q^n$ с вероятностью $> 1 - 2^{-\Omega(n)}$ для простого q

$\Rightarrow$ Граница Минковского: $\lambda_1(\Lambda^\perp) = \Theta\left(\min_{m' \leq m} \sqrt{m'}\, q^{\frac{n}{m'}}\right) = \Theta(\sqrt{n \lg n})$ ↑ для "типичных пар-ов".

$\Rightarrow$ SIS – это $approx\,SVP_\gamma = \frac{\beta}{\sqrt{n \lg n}}$ на решётке $\Lambda^\perp$.

Алгоритм BKZ решает SVP_γ за время $2^{\Theta\left(n \cdot \frac{\lg q}{\lg^2 \beta} \cdot \lg\left(\frac{n \lg q}{\lg^2 \beta}\right)\right)}$.

II SIS => криптографическая хэш-функция

$h: D \to R$ — эффективно вычисляемая ф-ция, т.ч. $|D| \gg R$ и для h сложно найти коллизию (т.е. $x \neq x'$, т.ч. $h(x) = h(x')$)
(обычно $D = \{0,1\}^*$)

На сложности SIS можно построить семейство криптографических хэш-фий:

$$h_A : \{0,1\}^m \to \mathbb{Z}_q^n \quad (2^m > q^n \Rightarrow m > n \lg q)$$
$$x \longmapsto x^T \cdot A \bmod q$$

$\exists$ (x, x') — коллизия для h_A, т.е. $xA = x'A \bmod q$ $(x \neq x')$

$$\Downarrow \in \{0, \pm 1\}^m$$
$$\underbrace{(x - x')}_{\in \Lambda^\perp} A = 0 \bmod q$$
$$0 < \|x - x'\| \leq \sqrt{m}$$

III Сложность SIS

в "худшем" в "среднем"

Цель: редукция от трудной задачи на решётках (SIVP) к SIS

ОПР $SIVP_\gamma$ — по заданному базису B решётки L найти $s_1 .. s_n \in L$ — (Shortest Independent Vector Problem)
линейно-независимые, такие что $\max_i \|s_i\| \leq \gamma \cdot \lambda_n(L)$

ТЕОРЕМА [Ajtai'96, GPV'08] (< Gentry-Peikert-Vaikuntanathan). $\forall$ полиномиальный алг-м, решающий $SIS_{q,m,\beta}$ с непренебрежимо малой вероятностью $\left(\geq \frac{1}{poly(n)}\right)$, может быть использован для решения задачи $SIVP_{\gamma(n)}$ в решётке ранга n с вероятностью $> 1 - 2^{-\Omega(n)}$ для $\gamma \geq q \geq 2n\beta\sqrt{m}$.

4 Промежуточная задача

базис | мнво лин независ. векторов | гиперплоскость

Inc IVP $(B, S, \mathcal{H})$ (Incremental Independent Vector Problem): найти $v \in L(B) \setminus \mathcal{H}$, т.ч.

$\|v\| < \max_{s_i \in S} \left(\frac{\|s_i\|}{2}\right)$, где

$\max_i \|s_i\| > \gamma \cdot \lambda_n(L)$.

Редукция от Inc IVP к SIS

Вход: B, $S \subset L$, $\mathcal{H}$, O^{SIS} – оракул, решающий SIS

Выход: v – решение Inc IVP

$C = \mathbb{Q}\mathbb{R}$

1. Из B и S построить базис C решётки L, т.ч. $\max_i \|c_i\| \le \max_i \|s_i\|$ (LLL алгоритм)

2. Для $i = 1 \dots m$

   Выбрать $y_i \leftarrow D_{L,\sigma,0}$, где $\sigma = \sqrt{n} \cdot \max_i \|s_i\|$

   (используем алг-м Клейна, см. лекцию №11)

3. Вызвать O^{SIS} на $A = \underbrace{(B^{-1} \cdot Y)^T} \bmod q$

   i-ая строка матрицы A – вектор-коэффиц. для y_i относительно базиса B, взятый $\bmod q$

   Пусть O^{SIS} вернёт $x \in \mathbb{Z}^m$: $x^T \cdot A = 0 \bmod q$

4. Вернуть $v = Y \cdot x \cdot \frac{1}{q} = \frac{1}{q} \sum x_i \cdot \vec{y_i}$.

Замечание

① $x \in \mathbb{Z}^m$ – обнуляет коэффициенты y_i относ. базиса $B \bmod q$

$\Rightarrow Y \cdot x$ – короткий вектор решётки L с коэффициентами относ. базиса B, кратными q.

② Редукция работает за время $\text{poly}(n)$

③ Вероятность успеха редукции можно увеличить до $1 - 2^{-\Omega(n)}$, повторяя шаги 2–4 $\text{poly}(n)$ раз.

Утверждение №1 Распределение матрицы A на шаге 3 алг-ма редукции обладает стат. разностью от $U(\mathbb{Z}_q^{m \times n})$ в $2^{-\Omega(n)}$.

◁ Докажем для строки $a_1 = (B^{-1} \cdot y_1)^T \bmod q$. Для $a_2 \dots a_m$ док-во аналог., т.к. y_i выбираются независимо.

$$\varphi : L \to \mathbb{Z}_q^n$$
$$y \mapsto B^{-1} y \bmod q$$

– сюръективный гомоморфизм

$\Rightarrow \exists$ биекция м/у $\mathbb{Z}_q^n$ и $L / \ker \varphi = L / qL$

$\Rightarrow B^{-1} y$ распределён равномерно в $\mathbb{Z}_q^n \Leftrightarrow y \bmod qL$ распределён равномерно в L/qL

Для $\sigma \geq \eta_{2^{-n}}(qL)$ справедливо $\Delta(D_{L,\sigma} \bmod qL, U(L/qL)) < 2^{-\Omega(n)}$, т.к. рассмотрим $b \in L/qL$, $\Pr[b \leftarrow D_{L/qL,\sigma}] = \sum_{y \in b+qL} \frac{\rho_\sigma(y)}{\rho_\sigma(L)} =$

$= \frac{\rho_\sigma(b+qL)}{\rho_\sigma(L)}$ ← не зависит от b при $\sigma \geq \eta_{2^{-n}}(qL)$.

$\Rightarrow$ оракул O^{SIS} получает на вход A с "корректным" распределением. ▶

Утверждение №2 При условии корректной работы O^{SIS}:

1) $v \in L$
2) $\|v\| \leq \frac{1}{q} \beta \cdot n\sqrt{m} \cdot \max_i \|s_i\|$
3) $\Pr[v \notin \mathcal{H}] = \Omega(1)$

◁ 1) и 2) – см. упражнения.

3) Покажем, что для решётки L, и $\mathcal{H}$ – гиперплоскости, и $\frac{\sigma}{\sqrt{2}} \geq \eta_{2^{-n}}(L)$ справедливо $\Pr_{Y \leftarrow D_{L,\sigma}}[y \notin \mathcal{H}] = \Omega(1)$

$\exists \mathcal{H}$ – гиперплоскость, ортогональная $(1, 0, \dots, 0)$, и

$y \leftarrow D_{L,\sigma}$, $y = (y_1 \dots y_n)$

$$\Pr[y \in \mathcal{R}] = \Pr[y_1 = 0] \le \mathbb{E}[\rho_\sigma(y_1)] =$$

(по неравенству Маркова)

$$= \sum_{y \in L} \rho_\sigma(y_1) \frac{\rho_\sigma(y)}{\rho_\sigma(L)} \to \rho_\sigma(y_1) \cdot \rho_\sigma(y_2) \cdot \ldots \cdot \rho_\sigma(y_n) \Rightarrow$$

$\rho_\sigma(y_1) = e^{-\frac{\pi y_1^2}{\sigma^2}}$, $\rho_\sigma(y) = e^{-\frac{\pi y^2}{\sigma^2}}$

$$e^{-\frac{\pi y_1^2}{\sigma^2}} \to e^{-\frac{\pi y_1^2}{(\sigma^2/2)}} = \rho_{\frac{\sigma}{\sqrt{2}}}(y_1)$$

$$\Rightarrow \sum_{y \in L} \rho_{\frac{\sigma}{\sqrt{2}}}(y_1) \cdot \frac{\rho_\sigma(y_2) \ldots \rho_\sigma(y_n)}{\rho_\sigma(L)} \overset{\text{PSF}}{=} \frac{1}{\rho_\sigma(L)} \cdot \det(L) \cdot \frac{\sigma^n}{\sqrt{2}} \sum_{\hat{y} \in \hat{L}}{}' \rho_{\frac{\sqrt{2}}{\sigma}}(y_1) \ldots$$

$$\ldots \underbrace{\rho_{\frac{1}{\sigma}}(y_n)}_{\le \rho_{\frac{\sqrt{2}}{\sigma}}(y_n)} \le \frac{\det(L)\,\sigma^n}{\rho_\sigma(L) \cdot \sqrt{2}} \underbrace{\sum_{\hat{y} \in \hat{L}} \rho_{\frac{\sqrt{2}}{\sigma}}(\hat{y})}_{\le 1 + 2^{-n},\ \text{т.к. } \frac{\sigma}{\sqrt{2}} \ge \eta_{2^{-n}}(L)} \le \frac{(1+2^{-n})}{\sqrt{2}} (1+2^{-n}).$$

$\frac{\det(L)\,\sigma^n}{\rho_\sigma(L) \cdot \sqrt{2}} \in [1-2^{-n}, 1+2^{-n}]$

$$\Pr[y \notin \mathcal{R}] \ge 1 - \frac{(1+2^{-n})(1+2^{-n})}{\sqrt{2}} \ge 1 - \frac{1+2^{-\Omega(n)}}{\sqrt{2}} = \Omega(1). \blacksquare$$