Лекция №13.

Задача SIS её сложность

I Определение

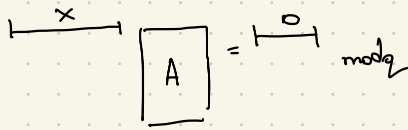
Ajtai'96: " SIS есть SVP на решётках конструкции-A"

Опр. ($SIS_{q,m,\beta}$). Пусть $n>0$; $m\geq n$; $q\geq 2$, $\beta>0$ (m, q, β зависят от n)

Short Integer Solution

В задаче $SIS_{q(n),m(n),\beta(n)}$ для матрицы $A\leftarrow U(\mathbb{Z}_q^{m\times n})$, требуется найти $x\in\mathbb{Z}^m$, т.ч.

1. $x^T A \equiv 0 \mod q$
2. $0 < \|x\| \leq \beta$



Обычно, имеем в виду пар-ры: $q = poly(n)$, $m = O(n\lg n)$

Замечание Задача SIS – это SVP_γ для след. семейства случ. решёток

$$A^\perp = \{b\in\mathbb{Z}^m : b^T\cdot A = 0 \mod q\} \text{ для } A\leftarrow U(\mathbb{Z}_q^{m\times n}).$$

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

$\Rightarrow$ граница Минковского $\lambda_1(A^\perp) = \Theta\left(\min\limits_{m'\leq m} \sqrt{m'}\, q^{\frac{n}{m'}}\right) = \Theta(\sqrt{n\lg n})$ для "типичных" пар-ов.

$\Rightarrow$ $SIS = SVP_{\gamma=\frac{\beta}{\sqrt{n\lg n}}}$ на решётке $A^\perp$.

Алг-м 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 $\Rightarrow$ криптографическая хэш-функция

$h: D \to R$ – эффективная ф-ия, т.ч. $|D| \gg R$ и для h сложно (обычно $D = \{0,1\}^*$) найти коллизию.

На сложности SIS можно построить семейство криптограф. хэш-функций

$$h_A : \{0,1\}^m \to \mathbb{Z}_q^n \qquad (n \lg q < m)$$

$$x \mapsto x^T A \bmod q$$

$\exists (x, x')$ – коллизия для h_A, т.е. $x^T \cdot A = x'^T A \bmod q$

$$\underbrace{(x^T - x'^T)}_{\in A^\perp} A = 0 \bmod q$$

$$0 < \|x - x'\| \le \sqrt{m}.$$

III Сложность SIS

Цель: редукция от $\underset{\text{в "худшем"}}{SIVP_\gamma}$ к $\underset{\text{в "среднем"}}{SIS_{q,m,\beta}}$.

(Shortest independent vectors problem)

Опр. $SIVP_\gamma$ – по заданному базису B решётки L найти $s_1 .. s_n \in L$ – лин. независимые, т.ч. $\max_i \|s_i\| \le \gamma \cdot \lambda_n(L)$.

Теорема [Ajtai'96, GPV'08]. $\forall$ полиномиальный алг-м, решающий $SIS_{q,m,\beta}$ с непренебрежимо малой вероятностью ($> \frac{1}{poly(n)}$), может быть использован для решения задачи $SIVP_{\gamma(n)}$ в решётке размерности n с в-ю $1 - 2^{-\Omega(n)}$ для $\gamma \ge q \ge 2n\beta\sqrt{m}$.

$\triangleleft$ Промежуточная задача:

$IncIVP(B, S, \mathcal{H})$: найти $v \in L(B) \setminus \mathcal{H}$, т.ч. $\|v\| < \max_{s_i \in S} \|s_i\| / 2$

(incremental indep. vector problem)

B – базис, S – мн-во лин. независ. векторов, $\mathcal{H}$ – гиперплоскость

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

Редукция от IncIVP к SIS.

Вход: $B, S \subset L, \mathcal{H}$; O^{SIS} – оракул для SIS
Выход: v – решение IncIVP

1. Из B и S построить базис C решётки L, т.ч. $\max\limits_i r_{ii} \le \max\limits_i \|S_i\|$ для $C=QR$ (LLL алгоритм)

2. Для $i = 1..m$:

   Выбрать $y_i \leftarrow D_{L,\sigma,0}$, где $\sigma = \sqrt{n}\cdot\max\|S_i\|$ (используем Klein)

3. Вызвать O^{SIS} на $A = (\underbrace{B^{-1}\cdot Y})^T \bmod q$, $Y = [y_1 \dots y_m]$

   i-ая строка матрицы A — вектор координат для y_i относ. базиса B, взятый mod q.

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

4. Вернуть $v = Y \cdot x / q = \frac{1}{q} \sum_i x_i \cdot \vec{y}_i$.

Замечания: ① $x \in \mathbb{Z}^m$ – обнуляет координаты y_i относ. базиса B mod q $\Rightarrow$ $Y \cdot x$ – короткий вектор решётки L с координатами относ. базиса B, кратными q.

② Редукция работает за время $poly(n)$

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

Утверждение 1. Распределение матрицы A на шаге 3. обладает стат. разностью с $U(\mathbb{Z}_q^{m\times n})$ в $2^{-\Omega(n)}$.

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

$$\varphi: \begin{array}{l} L \to \mathbb{Z}_q^n \\ y \mapsto B^{-1}\cdot y \bmod q \end{array} \quad \text{– сюръективный гомоморфизм.}$$

$\Rightarrow \exists$ биекция м/д $\mathbb{Z}_q^n$ и $L/\mathrm{Ker}\,\varphi = L/qL$

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

Для $\sigma \geq \eta_{2^{-n}}(qL)$ справедливо $\Delta(D_{L,\sigma} \bmod qL,\ U(L/qL)) \leq 2^{-\Omega(n)}$:

$\{$ для $b \in L/qL$: $Pr(b \leftarrow D_{L/qL,\sigma}) = \underset{y \in b+qL}{Pr}[y \in b+qL] =$

$$= \sum_{y \in b+qL} \frac{\rho_\sigma(y)}{\rho_\sigma(L)} = \frac{\rho_\sigma(b+qL)}{\rho_\sigma(L)} \leftarrow \text{не зависит } b \text{ при } \sigma \geq \eta_{2^{-n}}(qL) \ \}$$

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

Утверждения 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) $Pr[v \notin H] = \Omega(1)$.

$\triangleleft$ 1) $v = Y \cdot x \cdot \frac{1}{q} = \frac{1}{q} \cdot B \cdot \underbrace{B^{-1} Y \cdot x}_{x^T \cdot \underbrace{(B^{-1}Y)^T}_{x^T \cdot A \equiv 0 \bmod q}} = B \cdot \frac{1}{q} \cdot \underline{\underline{c}} \cdot q\mathbb{Z}^m = B \cdot \mathbb{Z}^m \in L(B)$

2) $\|v\| = \frac{1}{q}\|Y \cdot x\| \leq \frac{1}{q} \cdot \underbrace{\|x\|_1}_{\sum |x_i|} \cdot \underbrace{\max_i \|y_i\|}_{\leq \sqrt{n} \cdot \sigma \text{ (Гауссов хвост)}} \leq \frac{1}{q}\sqrt{m}\beta \cdot \sqrt{n} \cdot \sigma \leq \frac{1}{q}\sqrt{mn}\beta \cdot \max_i \|s_i\|$

$\|x\|_1 \leq \sqrt{m} \cdot \|x\|_2$

3) **Утверждение 2.1.** L – решётка, H – гиперплоскость, $\frac{\sigma}{\sqrt{2}} \geq \eta_{2^{-n}}(L)$, то $\underset{y \leftarrow D_{L,\sigma}}{Pr}[y \notin H] = \Omega(1)$

$\triangleleft$ $\exists$ H – гиперплоскость, ортогональная $(1, 0 \ldots, 0)$

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

$$\Pr[y \in \mathcal{H}] = \Pr[y_1 = 0] \underset{\text{н-во Маркова}}{\le} \mathbb{E}[\rho_\sigma(\mathbf{y}_1)] =$$

$$= \sum_{b \in L} \rho_\sigma(\mathbf{y}_1) \frac{\rho_\sigma(\vec{\mathbf{y}})}{\rho_\sigma(L)} \qquad \rho_\sigma(\vec{\mathbf{y}}) \longrightarrow \rho_\sigma(\mathbf{y}_1)\cdot\rho_\sigma(\mathbf{y}_2)\cdots\rho_\sigma(\mathbf{y}_n) \quad \Rightarrow$$

$$\rho_\sigma(L) \to e^{-\frac{\pi \|b\|^2}{\sigma}}$$

$$\underbrace{\rho_\sigma(\mathbf{y}_1)\cdot\rho_\sigma(\mathbf{y}_1)}_{e^{-\frac{\pi b_1^2}{(\sigma^2/2)}}}\ \rho_\sigma(\mathbf{y}_2)\cdots\rho_\sigma(\mathbf{y}_n)$$

$$= \sum_{\mathbf{y} \in L} \rho_{\sigma/\sqrt{2}}(\mathbf{y}_1)\cdot \frac{\rho_\sigma(\mathbf{y}_2)\cdots\rho_\sigma(\mathbf{y}_n)}{\rho_\sigma(L)} \overset{PSF}{=} \frac{1}{\rho_\sigma(L)}\cdot\det(\hat{L})\cdot\frac{\sigma^n}{\sqrt{2}}\sum_{\hat{\mathbf{y}} \in \hat{L}}\Big(\rho_{\frac{\sqrt{2}}{\sigma}}(\hat{\mathbf{y}}_1)\cdots\rho_{\frac{1}{\sigma}}(\hat{\mathbf{y}}_n)\Big) \le$$

$$\le \frac{\det(\hat{L})\,\sigma^n}{\rho_\sigma(L)\cdot\sqrt{2}} \underbrace{\sum_{\hat{\mathbf{y}} \in \hat{L}} \rho_{\frac{\sqrt{2}}{\sigma}}(\hat{\mathbf{y}})}_{\le 1 + 2^{-n}} \le \frac{\det(\hat{L})\,\sigma^n}{\rho_\sigma(L)\cdot\sqrt{2}}\,(1+2^{-n})$$

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

т.к. $\frac{\sigma}{\sqrt{2}} \ge \eta_{2^{-n}}(L)$

$$\le \left(1 + 2^{-\Omega(n)}\right)\cdot\frac{1}{\sqrt{2}}$$

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

$\blacksquare$