Задача SIS (Short Integer Solution)

Monday 12 April 2021 10:42

Задача нахождения короткого целого решения

I Определение

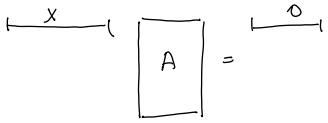
Ajtai '96: "SIS есть SVP на решётках конструкции-А"

Опр 1 ($SIS_{q,m,\beta}$). Пусть $n>0$; $m \geq n$, $q \geq 2$, $\beta > 0$ (m, q, β зависят от n).

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. $x^T \cdot A = 0 \mod q$
2. $0 < \|x\| \leq \beta$



- SIS – задача "в среднем" (A выбирается случ. равномерно из $\mathbb{Z}_q^{m \times n}$)
- SVP – задача "в худшем" (A может быть произвольной).

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

Замечание. Задача SIS – это SVP_γ для следующего семейства случ. решёток:

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

$\dim \Lambda^\perp = m$

$\det \Lambda^\perp = q^n$ с вероятностью $\geq 1 - 2^{-\omega(n)}$ для простого q. } $\Rightarrow$ граница Минковского:

$$\lambda_1(\Lambda^\perp) = \Theta\left(\min_{m' \leq m} \sqrt{m'} \cdot q^{\frac{n}{m'}}\right) = \Theta(\sqrt{n \lg n}) \text{ для "типичных" пар-ов.}$$

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

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

II SIS $\Rightarrow$ криптографическая хэш-фция

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

На сложности SIS можно построить семейство (криптогр.) хэш-фций

$$h_A: \{0,1\}^m \to \mathbb{Z}_q^n, \quad x \mapsto xA \mod q \qquad (n \lg q < m).$$

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

$$(x^T - x'^T) \cdot A = 0 \mod q$$

$$0 < \|x^T - x'^T\| \leq \sqrt{m}.$$

III Сложность SIS

Покажем, что задача $SIVP_\gamma$ (задача "в худшем") сводится к $SIS_{q,m,\beta}$ (задача "в среднем").

Опр 2 $SIVP_\gamma$: по базису B решётки L, найти ли
(shortest independen