Лекция №16.

Задача обучения с ошибками (Learning with Errors, LWE).

I. Определение задачи LWE.

O. Regev "On lattices, learning with errors, random linear codes, and cryptography", 2005.

- Распределение LWE $D_{n,q,\alpha}(s)$: для пар-ов $n \geq 1$, $q \geq 2$, $\alpha \in (0,1)$ и секрета $s \in \mathbb{Z}_q^n$:

  1) Выбрать $a \xleftarrow{\$} \mathbb{Z}_q^n$

  2) Выбрать $e \leftarrow D_{\mathbb{Z},\alpha q}$ - Гауссово р-ие со среднекв. отклонением αq

  Выход: $(a,\ b = \langle a, s\rangle + e \bmod q)$
  $\in \mathbb{Z}_q^n \times \mathbb{Z}_q$

- Задача поиска $LWE_{n,q,\alpha}$ (search-LWE): ∃ s-фиксировано. Имея выборку из распр-ия LWE $D_{n,q,\alpha}(s)$ произвольного р-ра, найти s.

Дано:
$$\underset{m}{\updownarrow}\overset{\leftarrow n \rightarrow}{\begin{bmatrix} - a_1 - \\ - a_2 - \\ A \\ \vdots \end{bmatrix}}, \qquad \begin{bmatrix} \\ A \\ \\ \end{bmatrix} \overset{s}{\begin{bmatrix} \\ \\ \end{bmatrix}} + \overset{e}{\begin{bmatrix} \\ \\ \\ \end{bmatrix}} = \overset{b}{\begin{bmatrix} \\ \\ \\ \end{bmatrix}} \bmod q$$

Найти: s (или e).

- Задача принятия решения $LWE_{n,q,\alpha}$ (decision-LWE): Имея выборку либо из $D_{n,q,\alpha}(s)$ для фикс. s, либо выборку $U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$ произвольного р-ра, понять, какая выборка дана.

Формально: построить ppt A, т.ч. $\Pr_{s \leftarrow U(\mathbb{Z}_q^n)}\left[\, \left|\Pr[A^{D(s)} \to 1] - \Pr[A^{U} \to 1]\right| \geq \frac{1}{poly(n)}\right] \geq \frac{1}{poly(n)}$.

Сложность задачи LWE относ. пар-ов:

1. $\alpha = 0 \Rightarrow \alpha \cdot q = 0 \Rightarrow$ LWE тривиально (решение лин. ур-ий, т.к. $e = 0$)
2. $\alpha = 1 \Rightarrow$ LWE сложно ($\langle a, s\rangle + e \sim U(\mathbb{Z}_q^n) \Rightarrow$ OTP).

   Обычно, $\alpha \sim \frac{1}{poly(n)}$
3. Чем больше n (при фикс. q, α), тем сложнее LWE.
4. Типичные пар-ры для криптосистемы ур-ня безопасности λ:

$$\underset{\approx 300 \div 1000}{n = O(\lambda)}, \quad q = n^2, \quad \alpha = 1/poly(n), \quad m = \Theta(n)$$

II Задача поиска LWE $\approx$ Задача принятия решения

(для $\alpha = O\left(\frac{1}{\sqrt{n}}\right)$, $q = poly(n)$, q-простое).

- Направление "decision-to-search" (от принятия решения к поиску) тривиально: подать на вход алг-му SearchLWE выборку, если он вернёт s', выдать "LWE" за ответ.

- Направление "search-to-decision"

  $\exists s^*$ - секрет. Найдём $s_1^* \in \mathbb{Z}_q$.

  Пусть $s_1' \in \mathbb{Z}_q$ - предположение о значении s_1^*.

  Проверим его с помощью алг-ма decision-LWE.

$$(a_i, b_i) = (a_i, \langle a_i, s^*\rangle + e_i \bmod q) \to \left(a_i + \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}, \langle a_i, s^*\rangle + e_i + s_1'\right)$$

$$s_1' = \langle (1, 0, .., 0), s^*\rangle$$

$$\langle a_i, s^*\rangle + s_1' = \langle a_1 + \begin{pmatrix}1\\ \vdots\end{pmatrix}, s^*\rangle + e_i$$

- корректная выборка из $D(s^*)$, если $s_1' = s_1^*$
- случ. равномерная из $U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$, если $s_1' \neq s_1^*$.

$\Rightarrow$

$\Rightarrow$ Запускаем decision-LWE на модифицированной выборке.
Редукция работает за время $O(q \cdot n)$ вызовов Decision-LWE для восстановления s^*.

III HNF-форма LWE:

Секрет s выбран не произвольно из $\mathbb{Z}_q^n$, а аналог. распределению ошибки из $D_{\mathbb{Z}^n, \alpha \cdot q}$

HNF-форма LWE и "обычная" форма LWE эквивалентны по сложности, т.к. $\exists$ отображение м/д ними. А именно:

1) Возьмём выборку $(a_i^*, b_i^*)_{1 \le i \le n}$, т.ч. a_i^* - лин. независимы в $\mathbb{Z}_q^n$.

Составим
$$A^* = \begin{bmatrix} - & a_1^* & - \\ & \vdots & \\ - & a_n^* & - \end{bmatrix}$$
– обратима $\quad b^* = (b_1^*, \ldots, b_n^*)$

Для каждой последующей пары (a, b) отобразить
$$(a, b) \to (a', b'), \text{ где } \Big(A^{*-T} \cdot a, \; -b + \langle A^{*-T} a, \underset{\overset{\parallel}{A^* \cdot s + e^*}}{b^*} \rangle \Big)$$

- Если $(a, b) \leftarrow U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$, то $(a', b') \sim U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$
- Если (a, b) из LWE, то $a' = A^{*-T} \cdot a \sim U(\mathbb{Z}_q^*)$, и

$$-b + \langle A^{*-T} \cdot a, b^* \rangle = -\langle a, s \rangle - e + (A^{*-T} \cdot a)^T \cdot (A^* \cdot s + e^*) =$$

$$= \underbrace{\cancel{-a^T \cdot s}} - e + \underbrace{\cancel{a^T \cdot \underbrace{A^{*-1} \cdot A^*}_{Id} \cdot s}} + a^T \cdot (A^*)^{-1} \cdot e^* =$$

$$= a^T \cdot (A^*)^{-1} \cdot e^* - e = (A^{*-T} \cdot a) \cdot \underset{\substack{\uparrow \\ \text{новый секрет}}}{e^*} - e.$$

IV PKE

• KeyGen

$$pk = \boxed{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{m\times n}),\quad \overset{b}{[\,]} = \boxed{A}\overset{s}{[\,]} + \overset{e}{[\,]} \bmod q,$$

$$s \leftarrow D_{\mathbb{Z}_q^n, \alpha q},\quad e \leftarrow D_{\mathbb{Z}_q^m, \alpha q}$$

$$sk = s$$

• Enc$(pk, \mu \in \{0,1\})$

1) $t \leftarrow D_{\mathbb{Z}_q^m, \alpha q}\quad f \leftarrow D_{\mathbb{Z}_q^n, \alpha q},\quad f' \leftarrow D_{\mathbb{Z}, \alpha q}$

2) $c_1 = t^T \cdot \boxed{A} + f^T \bmod q \in \mathbb{Z}_q^n$

$$c_2 = t^T \cdot b + f' + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q$$

$$c = (c_1, c_2)$$

• Dec$(sk, c = (c_1, c_2))$

$$c_2 - c_1^T \cdot s = t^T \cdot b + f' + \mu \left\lfloor \frac{q}{2} \right\rfloor -$$

$$- t^T \cdot A \cdot s - f^T \cdot s =$$

$$= t^T \cdot \cancel{A} \cdot s + t^T \cdot e + f' + \mu \left\lfloor \frac{q}{2} \right\rfloor - t^T \cdot \cancel{A} \cdot s - f^T \cdot s$$

$$= \underbrace{(t^T \cdot e + f' - f^T \cdot s)}_{} + \mu \left\lfloor \frac{q}{2} \right\rfloor$$

$$\leq \sqrt{\sum_{i=1}^{m} (\underset{\downarrow\sqrt{m}}{\alpha q})^2 \cdot \|e\|^2} + \alpha q\sqrt{n} + \sqrt{\sum_{i=1}^{n} (\alpha q\sqrt{n}) \cdot \|f\|^2}$$

$$\leq 3\left(\alpha q \cdot (\sqrt{m} + \sqrt{n})\right)^2$$

Если $|c_2 - c_1^T s|$ близко к $q/2 \Rightarrow \mu_1 = 1$

$|c_2 - c_1^T s|$ близко к $0 \Rightarrow \mu_2 = 0$

Схема корректна, если $3(\alpha q(\sqrt{m}+\sqrt{n})^2 \le \frac{q}{4}$.