Шифрование на LWE

Monday 10 May 2021 11:59

I. HNF-форма LWE

HNF-форма LWE: секрет s выбран не произвольно из $\mathbb{Z}_q^n$, а аналогично распр-ию ошибки из $D_{\mathbb{Z}^n, \alpha q}$.

HNF-LWE и "обычная" форма LWE экв-ны по сложности, т.к. $\exists$ отображение м/у 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 матрицу $A^* = \begin{bmatrix} - a_1 - \\ - a_2 - \\ \vdots \\ - a_n - \end{bmatrix}$.

Для каждой последующей пары (a, b) отобразить

$$(a,b) \to (a', b') = \left(A^{*-T} \cdot a,\ -b + \langle A^{*-T} a,\ \underset{A^* \cdot s + e}{\underbrace{b^*}} \rangle \right)$$

- Если $(a,b) \leftarrow U(\mathbb{Z}_q^n, \mathbb{Z}_q)$, то и $(a', b') \leftarrow U(\mathbb{Z}_q^n, \mathbb{Z}_q)$
- Если (a,b) из LWE, то $a' \leftarrow U(\mathbb{Z}_q^n)$, а $b' = -\langle a, s\rangle - e + a \cdot A^{*-1} \cdot (A^* s + e^*) = -\cancel{a^T s} - e + a \cdot \underbrace{A^{*-1} A^*}_{Id} \cdot s + a A^{*-1} \cdot e^*$

$= \langle a', e^* \rangle - e$

e^* — новый секрет

II. PKE

KeyGen

$pk = A \leftarrow U(\mathbb{Z}_q^{n \times n})$, $b = A s + e \mod q$, где $e, s \leftarrow D_{\mathbb{Z}^n, \alpha q}$

$sk = s$

Enc(pk, $\mu \in \{0,1\}$)

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

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

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

$c = (c_1, c_2)$

Dec(sk, $c = (c_1, c_2)$)

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

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

$$= \underbrace{(t^T \cdot e + f' - t^T f)}_{\le \sqrt{\sum (\alpha q \sqrt{n})^2 \|e\|^2} + \alpha q \sqrt{n} - \sqrt{\sum (\alpha q \sqrt{n})^2 \|f\|^2}} + \mu \cdot \lfloor q/2 \rfloor$$

$$= 3 (\alpha q \sqrt{n})^2$$

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

— // — к $0 \Rightarrow \mu = 0$.

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

Безопасность: (IND-CPA) = злоумышленник, зная pk, не может отличить $Enc(pk, 0)$ от $Enc(pk, 1)$. (т.е. $(pk, Enc(pk,0)) \approx (pk, Enc(pk,1))$)

Имеем,

$$(\underbrace{A,\ As + e}_{pk},\ t^T A + f^T,\ \overset{= Enc(0)}{t^T (As + e) + f' })$$

$\approx$ вычислительно, под предположением трудности decision-LWE

$$(A,\ b \leftarrow U(\mathbb{Z}_q^n),\ \underbrace{t^T A + f,\ t^T b + f'}_{})$$

$t^T \cdot \begin{bmatrix} -A- \\ -b- \end{bmatrix} + (f,\ f')$

$\approx$ — // —

$(A, b, \underset{\uparrow U(\mathbb{Z}_q^n)}{c}, d) \leftarrow U(\mathbb{Z}_q)$.

Аналогично для $Enc(pk, 1)$.