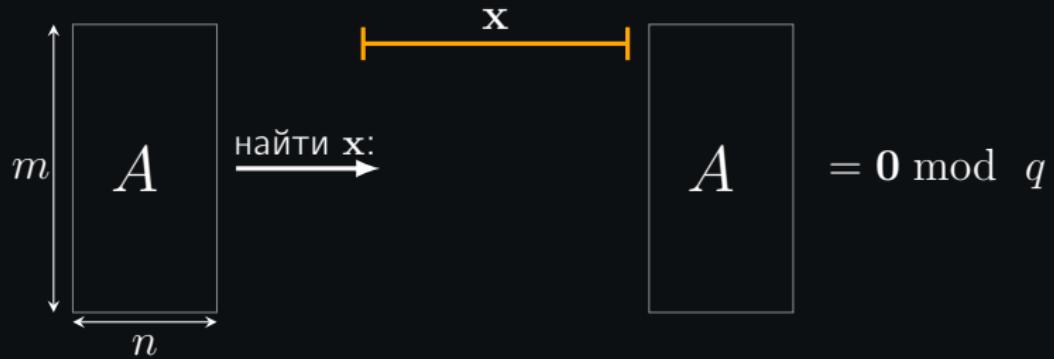


Современная криптография на решётках

Елена Киршанова

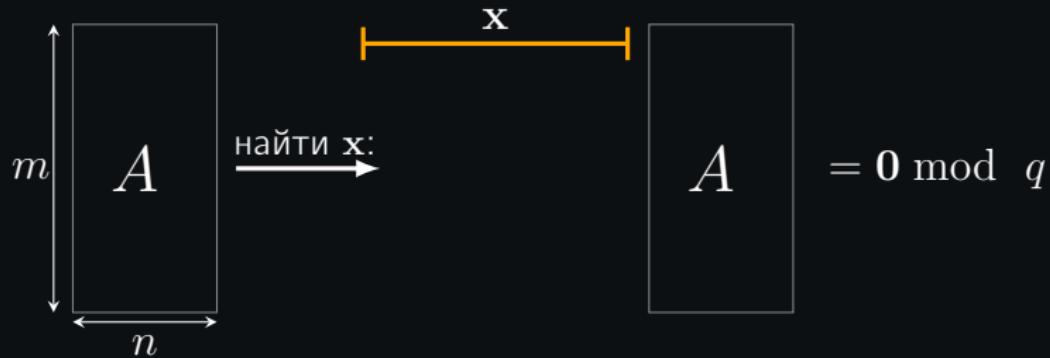
Курс “Криптография на решётках”

Трудные задачи на решётках: SIS



$$\text{т.ч. } 0 < \|x\| \leq B$$

Трудные задачи на решётках: SIS



$$\text{т.ч. } 0 < \|x\| \leq B$$

- A задаёт решётку ранга m

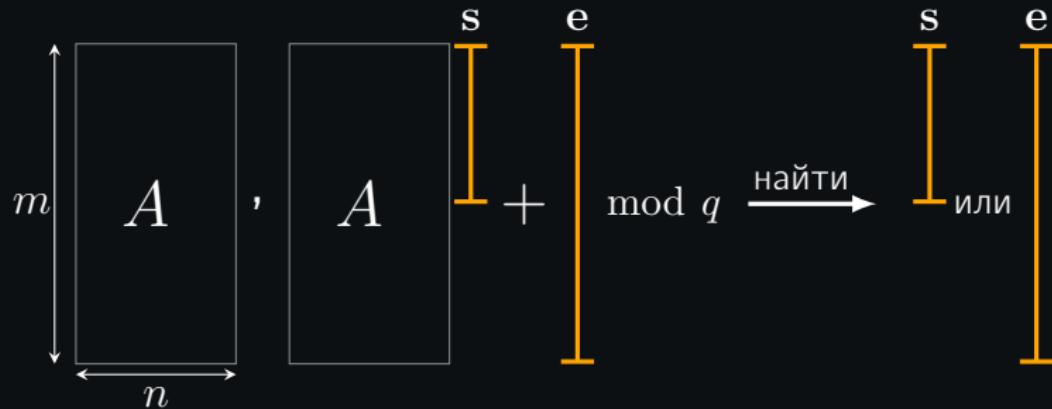
$$\mathcal{L}_q^\perp(A) = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x}^t A = 0 \bmod q\}$$

- SIS – γ -SVP для $\gamma = \frac{q^{n/m}}{B}$.

$$T(\text{SIS}) = \exp \left(c \frac{\lg q}{\lg^2 B} \lg \left(\frac{n \lg q}{\lg^2 B} \right) \cdot n \right)$$

- Криптографические хэш-функции, цифровые подписи

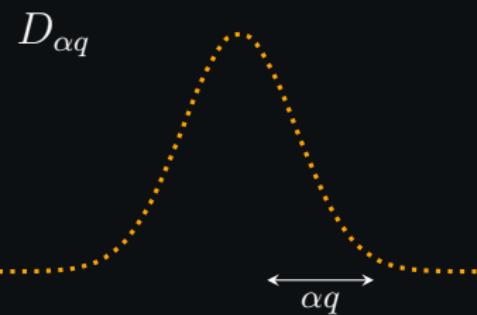
Трудные задачи на решётках: LWE



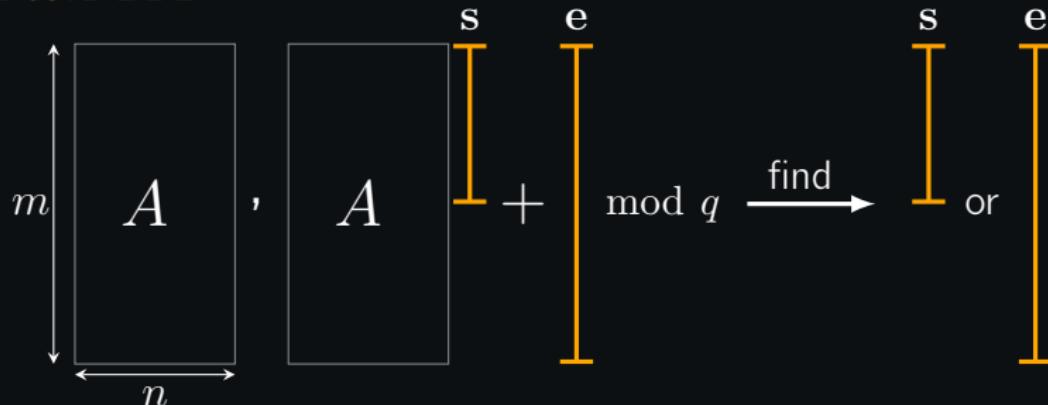
$$A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$$

$$s \xleftarrow{\$} \mathbb{Z}_q^n$$

$$e \xleftarrow{\$} D_{\alpha q}^m$$



LWE есть BDD



- A задает решетку конструкции А

$$\mathcal{L}_q(A) = A\mathbb{Z}_q^n + q\mathbb{Z}^m$$

- $\dim(\mathcal{L}_q(A)) = m$ и $\det(\mathcal{L}_q(A)) = q^{m-n}$.
- $As + e \bmod q$ – вектор, на расстоянии $\Theta(\sqrt{m}\alpha q)$ от $\mathcal{L}_q(A)$
- $(A, As + e)$ – BDD задача для $\mathcal{L}_q(A)$ с $\gamma = \frac{q^{1-n/m}}{\alpha q}$
- PKE, IBE, ABE, NIKZ, гомоморфное шифрование

Алгебраические предположения трудности

- Для хранения LWE выборки необходимо $\Omega(n^2 \log q)$ бит
- Умножение матрицы на вектор требует $O(n^2)$ операций в \mathbb{Z}_q

⇒ ‘стандартное’ LWE довольно медленно

Решение:

1. Алгебраические версии SIS/LWE
2. NTRU

Пусть $f \in \mathbb{Z}[x]$ - унитарный неприводимый степени n ,
 $q \geq 2, \alpha > 0$

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a_0, \dots, a_{n-1}) \in \mathbb{Z}^n$$

Задача поиска Poly-LWE _{f} :

- Выбрать $s \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Выбрать a_i 's $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Выбрать коэф-ты e_i из $D_{\alpha q}$

По данным (a_1, \dots, a_m) и
 $(a_1 \cdot s + e_1, \dots, a_m \cdot s + e_m)$,
найти s .

Пусть $f \in \mathbb{Z}[x]$ - унитарный неприводимый степени n ,
 $q \geq 2, \alpha > 0$

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a_0, \dots, a_{n-1}) \in \mathbb{Z}^n$$

Задача поиска Poly-LWE _{f} :

- Выбрать $s \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Выбрать a_i 's $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Выбрать коэф-ты e_i из $D_{\alpha q}$

По данным (a_1, \dots, a_m) и
 $(a_1 \cdot s + e_1, \dots, a_m \cdot s + e_m)$,
найти s .

$$\begin{matrix} & \mathbf{s} \\ \uparrow & \\ \begin{matrix} (x^{j-1} \cdot a_1)[f] \\ = \text{Rot}_f(a_1) \end{matrix} \\ \hline \\ \begin{matrix} \text{Rot}_f(a_2) \end{matrix} \\ \downarrow & \\ \mathbf{e}_1 & + & \mathbf{e}_2 \end{matrix}$$

Пусть $f \in \mathbb{Z}[x]$ - унитарный неприводимый степени n ,
 $q \geq 2, \alpha > 0$

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a_0, \dots, a_{n-1}) \in \mathbb{Z}^n$$

Задача поиска Poly-LWE _{f} :

- Выбрать $s \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Выбрать a_i 's $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Выбрать коэф-ты e_i из $D_{\alpha q}$

По данным (a_1, \dots, a_m) и
 $(a_1 \cdot s + e_1, \dots, a_m \cdot s + e_m)$,
найти s .

Одна пара $(a_i, a_i s + e_i)$ дает LWE выборку из n эл-тов
Многочлены могут быть умножены за время $\tilde{O}(n)$

Ring-LWE для $f = x^{2^k} + 1$, LPR'10

Пусть $f = x^n + 1$ - круговой степени $n = 2^k$, $q \geq 2$, $\alpha > 0$

Пусть $\omega_1, \dots, \omega_n \in \mathbb{C}$ - корни f , V_f - матрица

Вандермодна для ω_i 's

$$\sigma : \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a(\omega_0), \dots, a(\omega_{n-1})) \in \mathbb{C}^n$$

Задача поиска Ring-LWE_f :

- Выбрать $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Выбрать a_i 's $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Выбрать $\sigma(\mathbf{e}_i)$'s из $D_{\alpha q}$

Ring-LWE для $f = x^{2^k} + 1$, LPR'10

Пусть $f = x^n + 1$ - круговой степени $n = 2^k$, $q \geq 2$, $\alpha > 0$

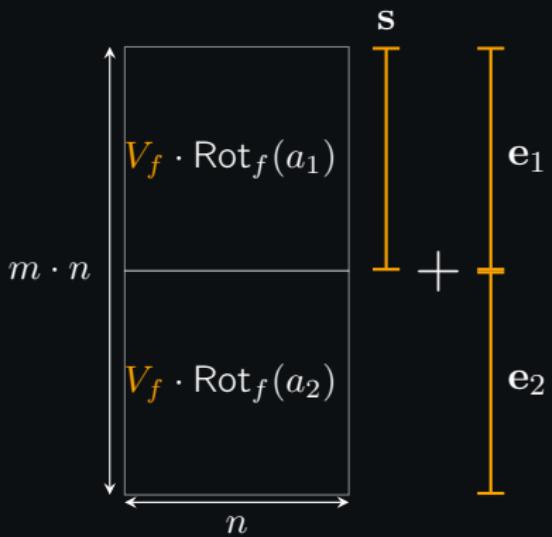
Пусть $\omega_1, \dots, \omega_n \in \mathbb{C}$ - корни f , V_f - матрица

Вандермодна для ω_i 's

$$\sigma : \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a(\omega_0), \dots, a(\omega_{n-1})) \in \mathbb{C}^n$$

Задача поиска Ring-LWE _{f} :

- Выбрать $s \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Выбрать a_i 's $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Выбрать $\sigma(e_i)$'s из $D_{\alpha q}$



Ring-LWE для $f = x^{2^k} + 1$, LPR'10

Пусть $f = x^n + 1$ - круговой степени $n = 2^k$, $q \geq 2$, $\alpha > 0$

Пусть $\omega_1, \dots, \omega_n \in \mathbb{C}$ - корни f , V_f - матрица

Вандермодна для ω_i 's

$$\sigma : \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a(\omega_0), \dots, a(\omega_{n-1})) \in \mathbb{C}^n$$

Задача поиска Ring-LWE _{f} :

- Выбрать $s \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Выбрать a_i 's $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Выбрать $\sigma(e_i)$'s из $D_{\alpha q}$

$$s = \begin{matrix} V_f \cdot \text{Rot}_f(a_1) \\ \vdots \\ V_f \cdot \text{Rot}_f(a_2) \end{matrix} + \begin{matrix} e_1 \\ \vdots \\ e_2 \end{matrix}$$

- Умножение за время $O(n \log q)$
- Poly-LWE и Ring-LWE связаны для f т.ч. V_f имеет малую операторную норму, [RSW'18]

Пусть $q \geq 2$, Φ - многочлен степени n ,

$$R_\Phi = \mathbb{Z}_q[x]/(\Phi)$$

Примеры $\Phi = x^n - 1$ или $\Phi = x^n + 1$ или $\Phi = x^p - x - 1$

Задача поиска NTRU:

- Выбрать обратимый f в R_Φ с коэффициентами из $\{-1, 0, 1\}$
- Выбрать g с коэффициентами из $\{-1, 0, 1\}$
- Вычислить $h = g/f \in R_\Phi$

По h , сложно отыскать
'малые' (f, g) т.ч.
 $h = g/f \in R_\Phi$.

Пусть $q \geq 2$, Φ - многочлен степени n ,

$$R_\Phi = \mathbb{Z}_q[x]/(\Phi)$$

Примеры $\Phi = x^n - 1$ или $\Phi = x^n + 1$ или $\Phi = x^p - x - 1$

Задача поиска NTRU:

- Выбрать обратимый f в R_Φ с коэффициентами из $\{-1, 0, 1\}$
- Выбрать g с коэффициентами из $\{-1, 0, 1\}$
- Вычислить $h = g/f \in R_\Phi$

По h , сложно отыскать 'малые' (f, g) т.ч.
 $h = g/f \in R_\Phi$.

NTRU решётка:

$$\begin{bmatrix} \text{Rot}(h) & q\mathbf{I} \\ \mathbf{I} & 0 \end{bmatrix} \cdot \begin{bmatrix} \vec{f} \\ \vec{k} \end{bmatrix} = \begin{bmatrix} \vec{g} \\ \vec{f} \end{bmatrix}$$

- h задает решётку размерность $2n$

$$\mathcal{L} = \left\{ \begin{bmatrix} \text{Rot}(h) & q\mathbf{I} \\ \mathbf{I} & 0 \end{bmatrix} \cdot R_\Phi^2 \right\}$$

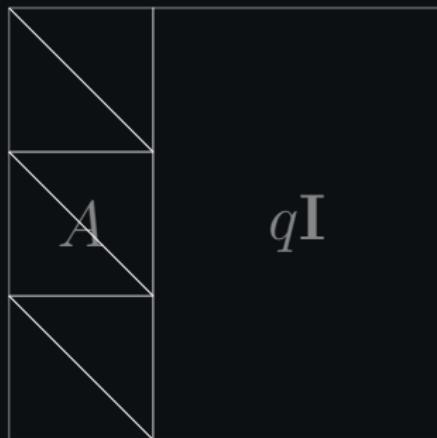
- (\vec{g}, \vec{f}) - короткий в \mathcal{L}

Сложность Poly/Ring LWE и NTRU

Пусть $q \geq 2$, Φ - многочлен степени n ,

$$R_\Phi = \mathbb{Z}_q[x]/(\Phi)$$

Ring-/Poly-LWE



A задает модуль ранга m над R_Φ

NTRU

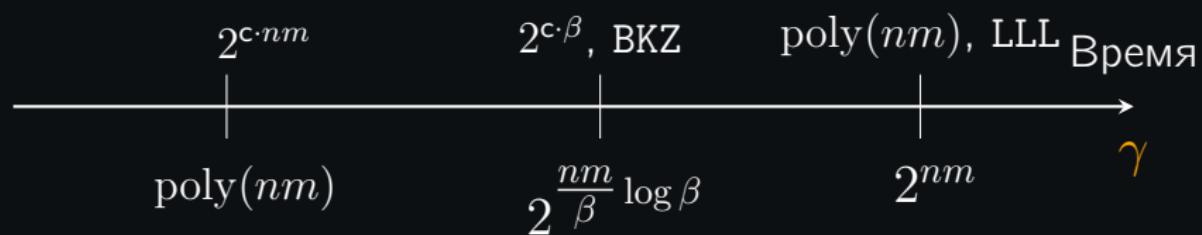
$\text{Rot}(h)$	$q\mathbf{I}$
\mathbf{I}	0

задает модуль ранга 2 над R_Φ

h

Сложность Poly/Ring LWE и NTRU относительно атак на решетках

Для $m > 1$, SVP в модуле ранга m над R_Φ не проще ‘стандартной’ SVP на произвольной решетке размерность nm ($\text{poly}(n)$ ускорения существуют):



Hardness of Poly/Ring LWE and NTRU under lattice attacks

Уточнения:

- SVP в любом модуле ранга-1 кругового поля R_Φ , может достичь $\gamma = 2^{\tilde{O}(\sqrt{n})}$ за время $2^{\tilde{O}(\sqrt{n})}$
Biasse-Espitalu-Fouque-Gélin-Kirchner'17 /
Cramer-Ducas-Peikert-Regev'16/
Cramer-Ducas-Wesolowski'17

Hardness of Poly/Ring LWE and NTRU under lattice attacks

Уточнения:

- SVP в любом модуле ранга-1 кругового поля R_Φ , может достичь $\gamma = 2^{\tilde{O}(\sqrt{n})}$ за время $2^{\tilde{O}(\sqrt{n})}$
Biasse-Espitalu-Fouque-Gélin-Kirchner'17 /
Cramer-Ducas-Peikert-Regev'16 /
Cramer-Ducas-Wesolowski'17
- В задаче NTRU n -коротких векторов (ротации (f, g)).
Этот факт позволяет для $(f, g) \leftarrow D_{\alpha q}^{2n}$ решить задачу NTRU с помощью β -BKZ with

$$\beta = \tilde{O}\left(\frac{n \lg(\alpha q)}{\lg^2 q}\right)$$

для достаточно больших q и αq . Сложность $\text{poly}(n)$ для $q = 2^{\tilde{O}(\sqrt{n})}$.

Процесс стандартизации NIST

- В декабре 2016 года NIST (National Institute of Standards and Technology) запустил процесс стандартизации¹ пост-квантовых примитивов: цифровой подписи и KEM (Key Encapsulation Mechanism). Свежее видео
<https://www.youtube.com/watch?v=DcwupScEa0Q>
- В ноябре 2017 было получено 87 кандидатов от академии и индустрии
- В ходе 3х раундов на сегодняшний день осталось 7 основных кандидатов и 8 альтернативных

KEM	Подписи
Classic McEliece (code-based)	Dilithium (M-LWE + M-SIS)
NTRU	Falcon (M-SIS)
Kyber (M-LWE)	Rainbow (multivariate)
Saber (M-LWR)	

¹<https://csrc.nist.gov/Projects/post-quantum-cryptography>

Открытые вопросы

1. Улучшенные алгоритмы SVP для “идеальных” решёток
2. Алгоритмы SVP для других норм, например, ℓ_∞ .
3. Практическая реализация алгоритмов декодирования

?