

# Современная криптография на решётках

Елена Киршанова

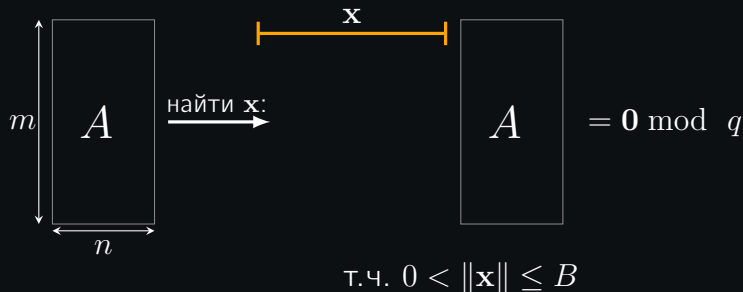
Курс “Криптография на решётках”

## Трудные задачи на решётках: SIS



т.ч.  $0 < \|\mathbf{x}\| \leq B$

## Трудные задачи на решётках: SIS



- $A$  задаёт решётку ранга  $m$

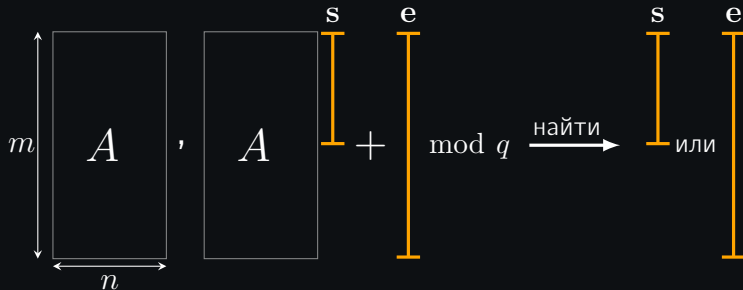
$$\mathcal{L}_q^\perp(A) = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x}^\top A = \mathbf{0} \pmod{q}\}$$

- SIS –  $\gamma$ -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

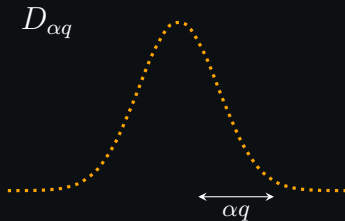
# Трудные задачи на решётках: LWE



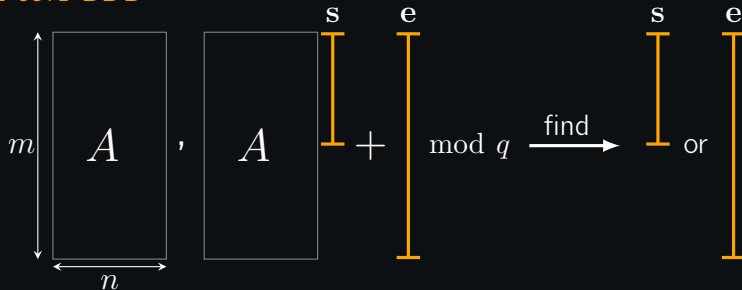
$$A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$$

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

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



## LWE есть BDD



- $A$  задает решетку конструкции  $A$

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

- $\dim(\mathcal{L}_q(A)) = m$  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

## Polynomial-LWE, SSTX'09

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  $s$ .

## Polynomial-LWE, SSTX'09

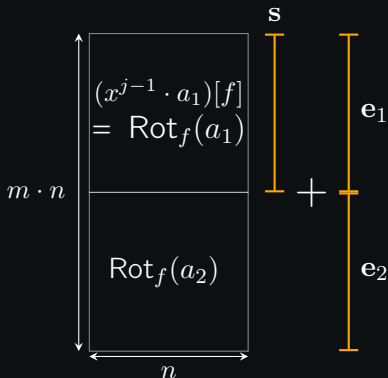
Пусть  $f \in \mathbb{Z}[x]$  - унитарный неприводимый степени  $n$ ,  
 $q \geq 2, \alpha > 0$

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

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  $s$ .





## Polynomial-LWE, SSTX'09

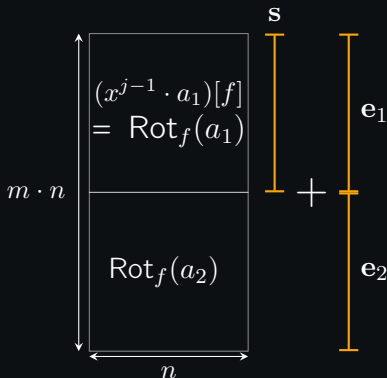
Пусть  $f \in \mathbb{Z}[x]$  - унитарный неприводимый степени  $n$ ,  
 $q \geq 2, \alpha > 0$

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

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

Вандермонда для  $\omega_i$ '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  $n = 2^k$ ,  $q \geq 2, \alpha > 0$

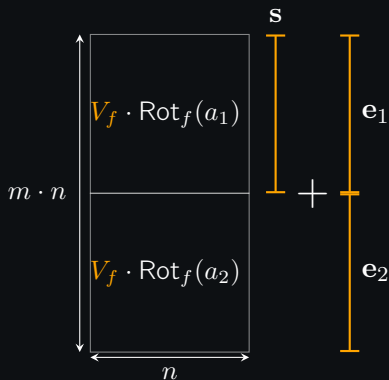
Пусть  $\omega_1, \dots, \omega_n \in \mathbb{C}$  - корни  $f$ ,  $V_f$  - матрица

Вандермонда для  $\omega_i$ '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  $n = 2^k$ ,  $q \geq 2, \alpha > 0$

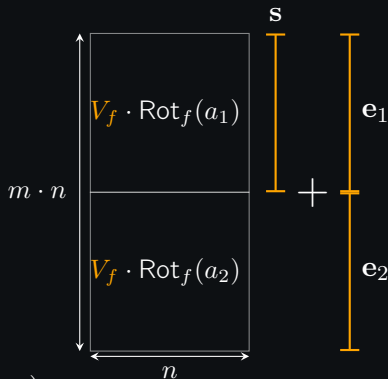
Пусть  $\omega_1, \dots, \omega_n \in \mathbb{C}$  - корни  $f$ ,  $V_f$  - матрица

Вандермонда для  $\omega_i$ '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  $D_{\alpha q}$



- 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]

## NTRU, HPS'98

Пусть  $q \geq 2$ ,  $\Phi$  - 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  $R_\Phi$  с коэфф-ами из  $\{-1, 0, 1\}$
- Выбрать  $g$  с коэфф-ами 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, HPS'98

Пусть  $q \geq 2$ ,  $\Phi$  - 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  $R_\Phi$  с коэфф-ами из  $\{-1, 0, 1\}$
- Выбрать  $g$  с коэфф-ами 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:

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

- $h$  задает решетку  
размерность  $2n$

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

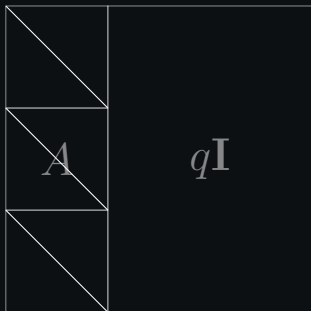
- $(\vec{g}, \vec{f})$  - короткий в  $\mathcal{L}$

## Сложность Poly/Ring LWE и NTRU

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

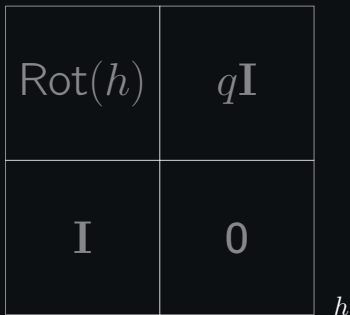
$$R_\Phi = \mathbb{Z}_q[x]/(\Phi)$$

Ring-/Poly-LWE



$A$  задает модуль ранга  $m$  над  $R_\Phi$

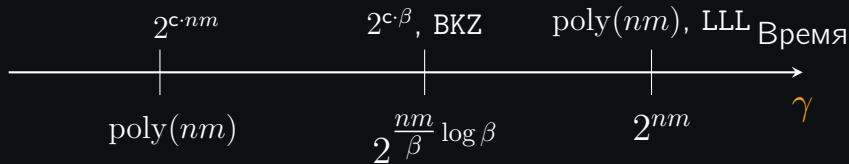
NTRU



задает модуль ранга 2 над  $R_\Phi$

## Сложность Poly/Ring LWE и NTRU относительно атак на решетках

Для  $t > 1$ , SVP в модуле ранга  $t$  над  $R_\Phi$  не проще 'стандартной' SVP на произвольной решетке размерность  $nm$  (poly( $n$ ) ускорения существуют):





## Сложность Poly/Ring LWE и NTRU

Уточнения:

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

## Сложность Poly/Ring LWE и NTRU

Уточнения:

- SVP в любом модуле **ранга-1** кругового поля  $R_{\Phi}$ , может достичь  $\gamma = 2^{\tilde{O}(\sqrt{n})}$  за время  $2^{\tilde{O}(\sqrt{n})}$   
Biasse-Espitau-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  $\beta$ -BKZ with

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

для достаточно больших  $q$  и  $\alpha q$ . 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 стандартизации<sup>1</sup> пост-кватовых примитивов: цифровой подписи и KEM (Key Encapsulation Mechanism).
- В ноябре 2017 было получено 87 кандидатов от академии и индустрии
- В стандарт вошли 3 схемы на решетках + одна подпись на хэш-функциях <https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>

| KEM           | Подписи  |
|---------------|--|
| Kyber (M-LWE) | Dilithium (M-LWE + M-SIS)<br>Falcon (M-SIS)<br>SPHINCS+ (hash-based) |

Подробнее см. <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf>

<https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf>

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

## Открытые вопросы

1. Улучшенные алгоритмы SVP для алгебраических решёток: алгебраический LLL (для алг. нормы), SVP, BKZ
2. Комбинаторные алгоритмы для SIS (Торсукова)
3. Практический анализ NTRU
4. Эффективные конструкции на решетках: слепая подпись
5. Построение решеток из кодов: анализ качества решеток (кратчайшего вектора относительно определителя), построенных из различных кодов
6. Анализ качества решеток как кодов (актуально для квантовых кодов, исправляющих ошибки)
7. Криптоанализ задачи Lattice Isomorphism Problem (LIP): по двух решеткам  $\mathcal{L}, \mathcal{L}' \subset \mathbb{R}^n$ , найти ортонормальную матрицу  $O$ , т.ч.  $\mathcal{L}' = O\mathcal{L}$ .