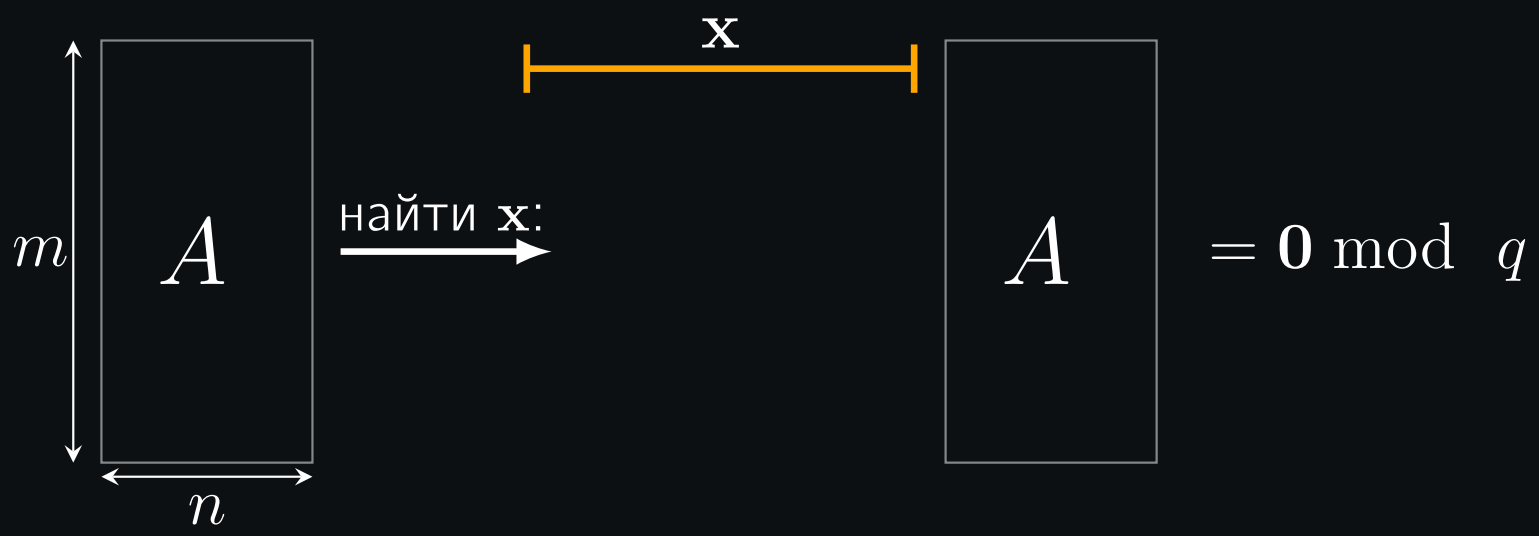
Современная криптография на решётках

Елена Киршанова

Курс “Криптография на решётках”

Трудные задачи на решётках: SIS



т.ч. $0 < \|\mathbf{x}\| \leq B$

Трудные задачи на решётках: SIS

т.ч. $0 < \|\mathbf{x}\| \leq B$

- A задаёт решётку ранга m

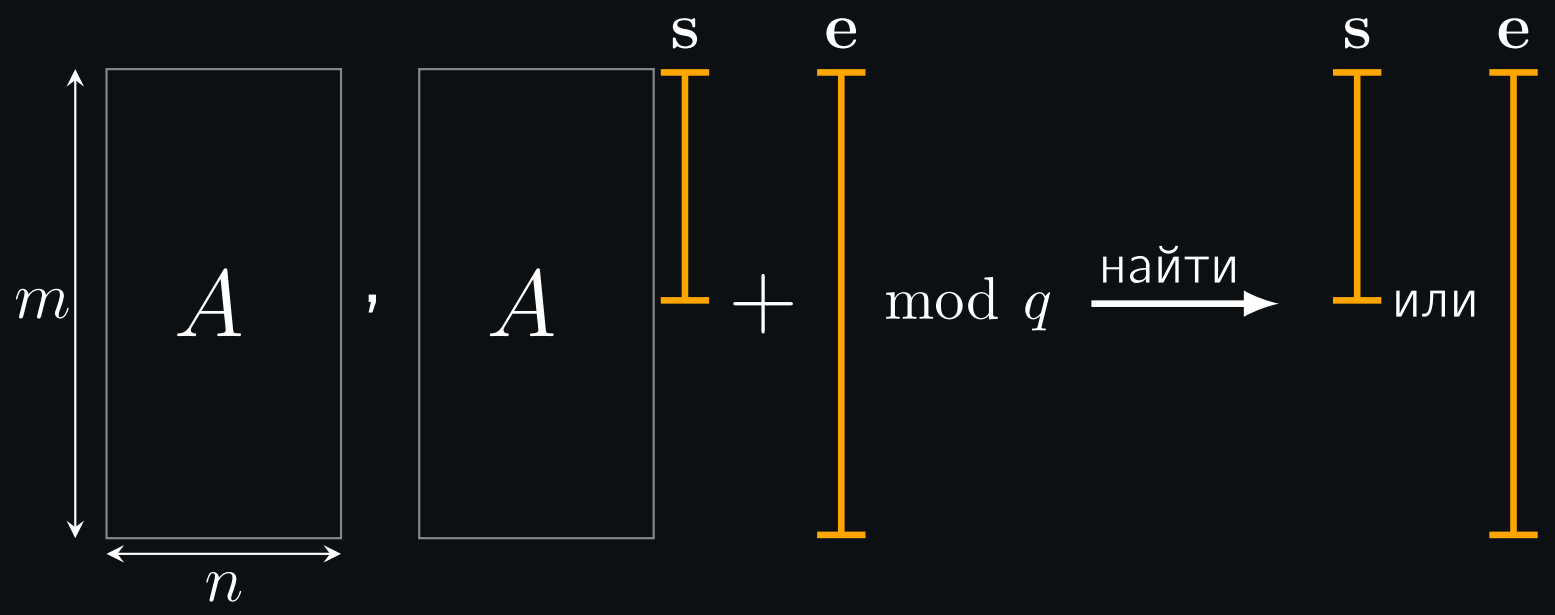
$$\mathcal{L}_q^{\perp}(A) = \{\mathbf{x} \in \mathbb{Z}^m \ : \ \mathbf{x}^{\mathsf{t}} A = 0 \bmod q\}$$

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

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

- Криптографические хэш-функции, цифровые подписи

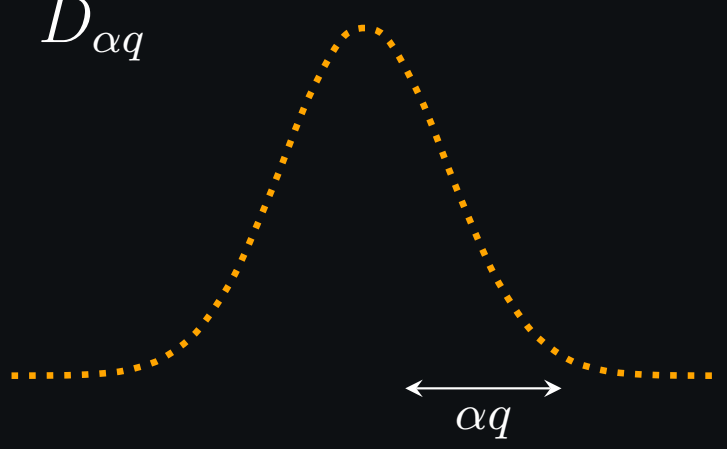
Трудные задачи на решётках: LWE



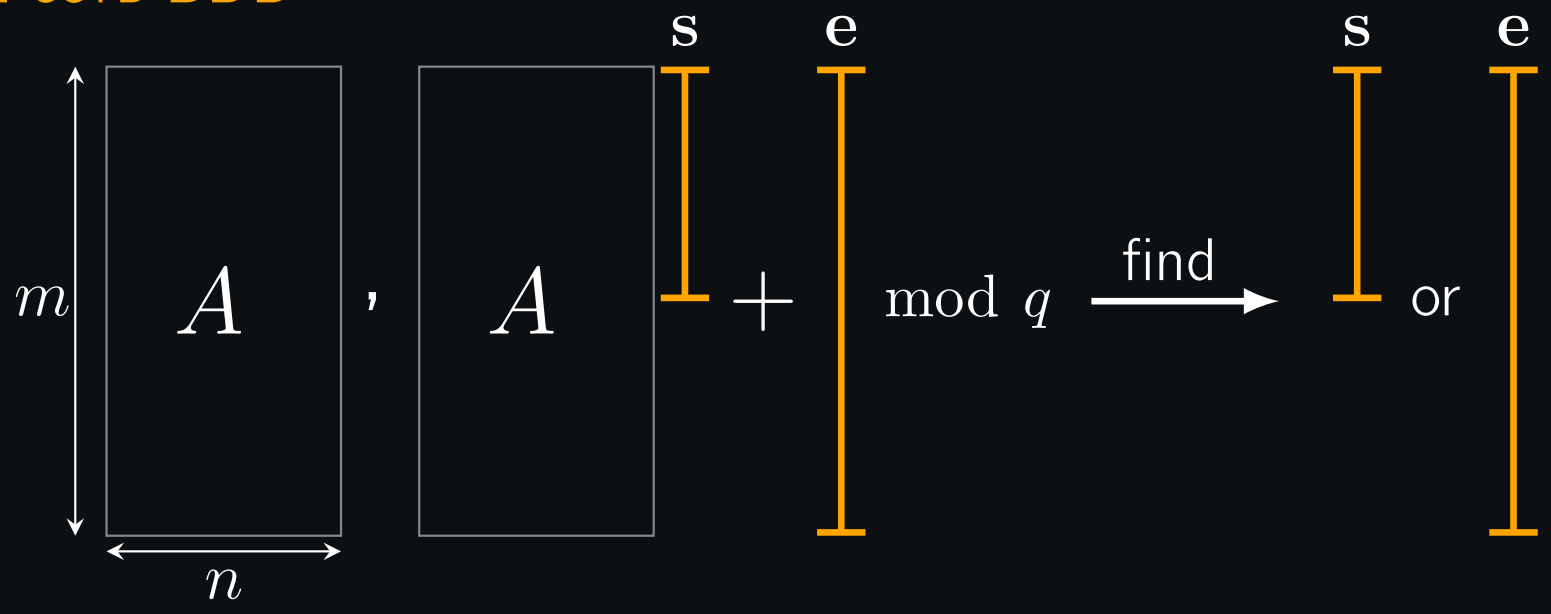
$$A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$$

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

$$\mathbf{e} \leftarrow D_{\alpha q}^{m}$$



LWE есть BDD



- A задает решетку конструкции A

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

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

$\Longrightarrow$ ‘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, $q \geq 2, \alpha > 0$

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

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 $(a_1, \ldots, a_m)$ и $(a_1 \cdot s + e_1, \ldots a_m \cdot s + e_m)$, найти s.

Polynomial-LWE, SSTX'09

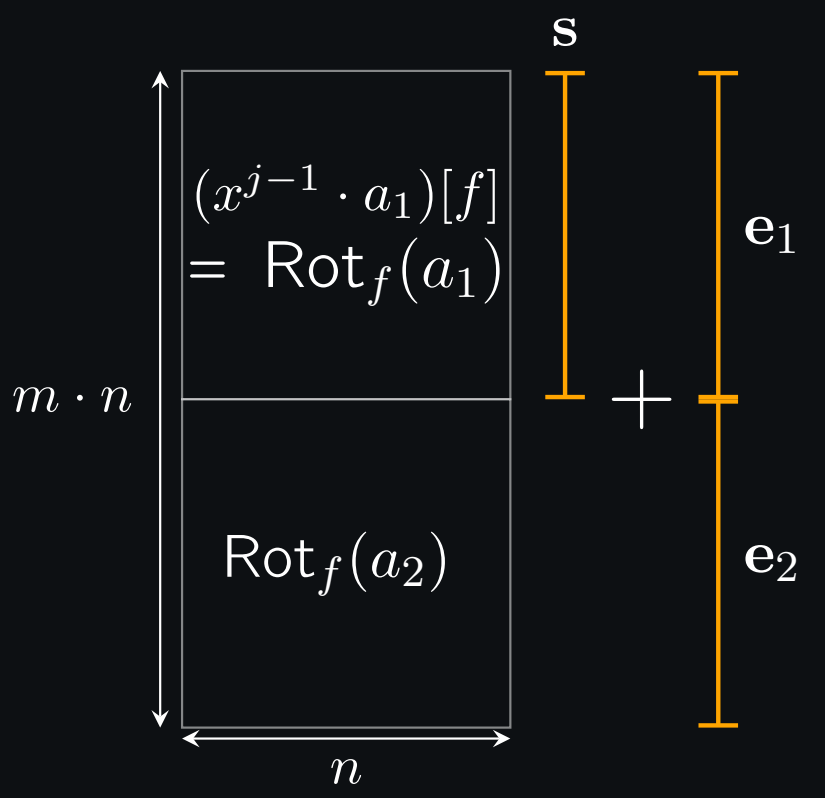
Пусть $f \in \mathbb{Z}[x]$ - унитарный неприводимый степени n, $q \geq 2, \alpha > 0$

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

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 $(a_1, \ldots, a_m)$ и $(a_1 \cdot s + e_1, \ldots a_m \cdot s + e_m)$, найти s.



Polynomial-LWE, SSTX'09

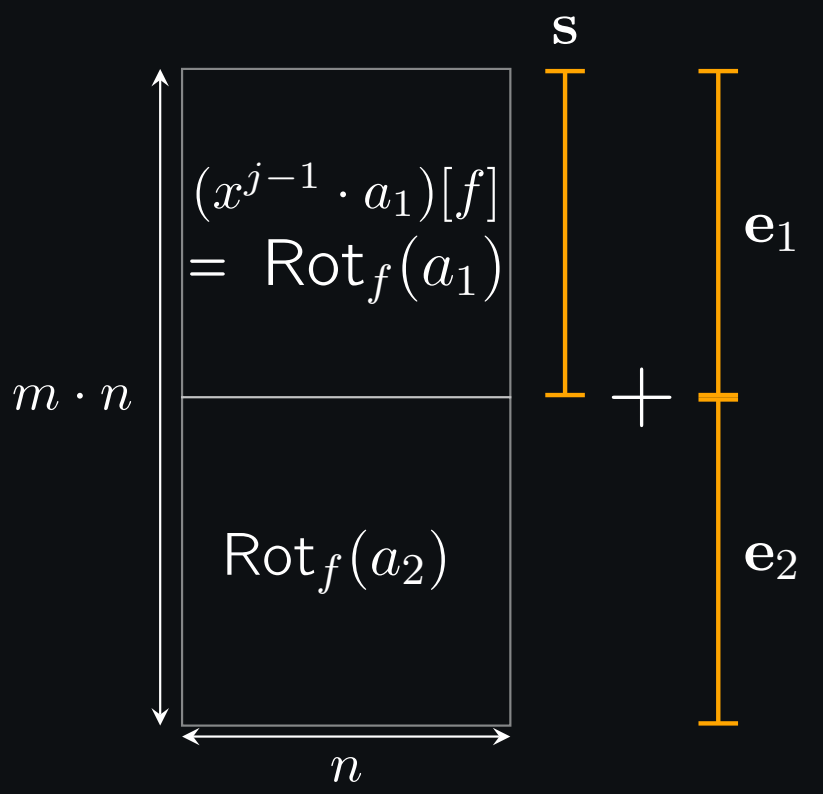
Пусть $f \in \mathbb{Z}[x]$ - унитарный неприводимый степени n, $q \geq 2, \alpha > 0$

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

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 $(a_1, \ldots, a_m)$ и $(a_1 \cdot s + e_1, \ldots a_m \cdot s + e_m)$, найти s.



Одна пара $(a_i, a_i s + e_i)$ дает LWE выборку из n эл-тов

Многочлены могут быть умножены за время $\widetilde{\mathcal{O}}(n)$

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 $\omega_1, \ldots, \omega_n \in \mathbb{C}$ - корни f, V_f - матрица Вандермодна для ω_i's

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

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

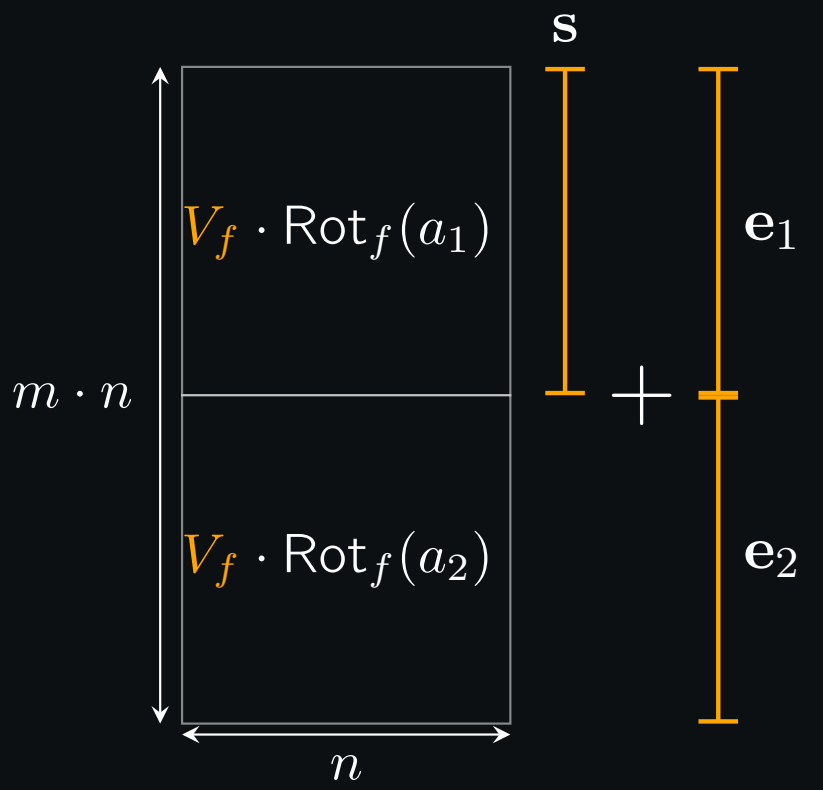
Пусть $f = x^n + 1$ - круговой степени $n = 2^k$, $q \geq 2, \alpha > 0$

Пусть $\omega_1, \ldots, \omega_n \in \mathbb{C}$ - корни f, V_f - матрица Вандермодна для ω_i's

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

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

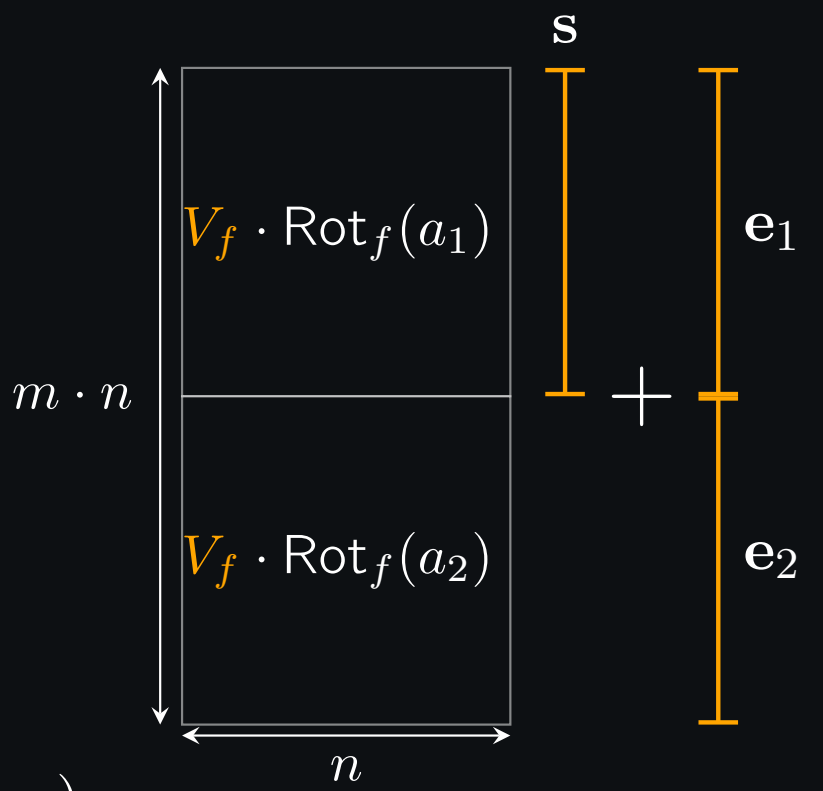
Пусть $f = x^n + 1$ - круговой степени $n = 2^k$, $q \geq 2, \alpha > 0$

Пусть $\omega_1, \ldots, \omega_n \in \mathbb{C}$ - корни f, V_f - матрица Вандермодна для ω_i's

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

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 $q \geq 2$, 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 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 $q \geq 2$, 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 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:

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

- h задает решетку размерность $2n$

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

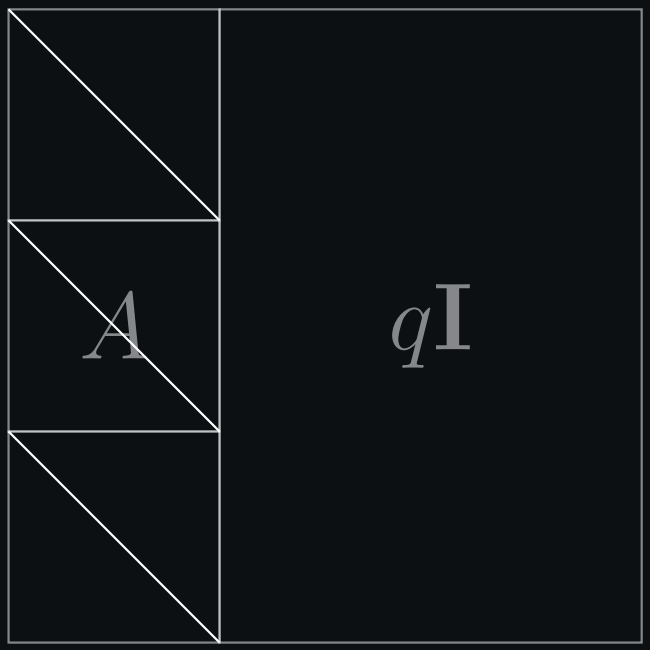
- $(\vec{g}, \vec{f})$ - короткий в $\mathcal{L}$

Сложность Poly/Ring LWE и NTRU

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

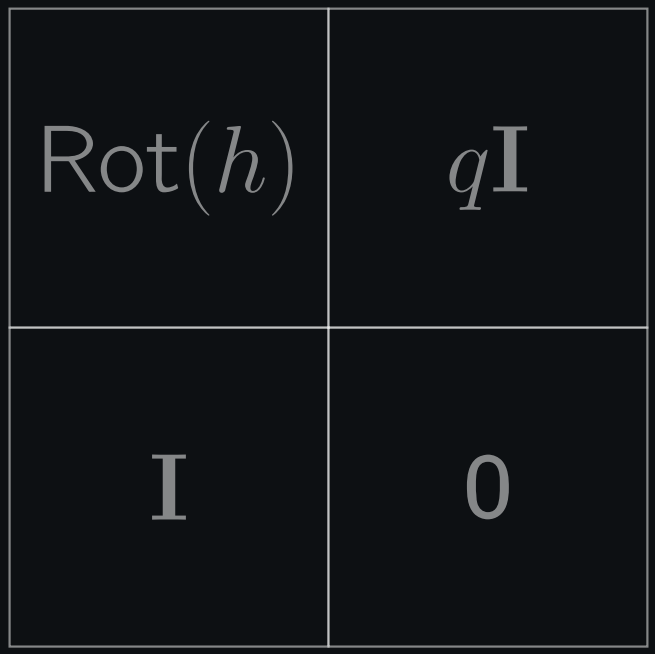
$$R_\Phi = \mathbb{Z}_q[x]/(\Phi)$$

Ring-/Poly-LWE



A задает модуль ранга m над R_Φ

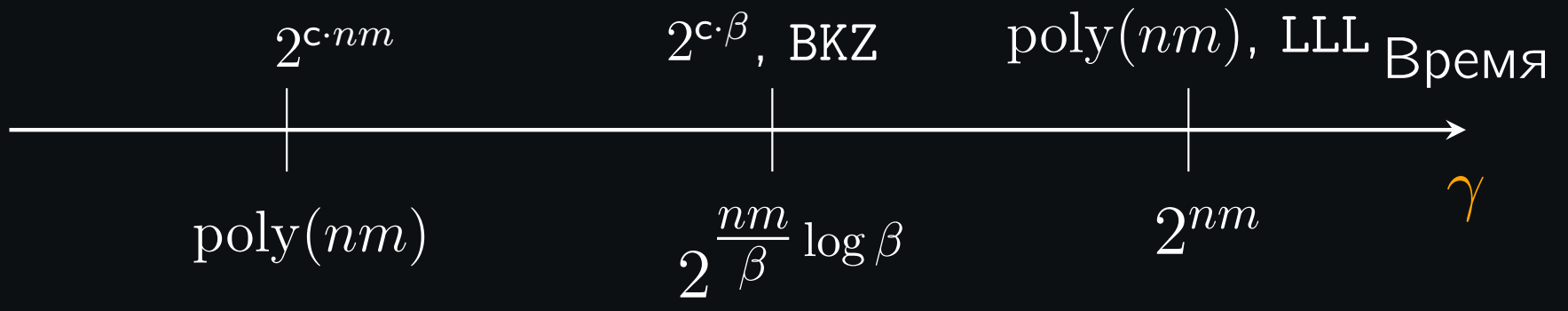
NTRU



задает модуль ранга 2 над R_Φ

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 ($\mathrm{poly}(n)$ ускорения существуют):



Сложность Poly/Ring LWE и NTRU

Уточнения:

- SVP в любом модуле ранга-1 кругового поля R_Φ, может достичь $\gamma = 2^{\widetilde{\mathcal{O}}(\sqrt{n})}$ за время $2^{\widetilde{\mathcal{O}}(\sqrt{n})}$
  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_Φ, может достичь $\gamma = 2^{\widetilde{\mathcal{O}}(\sqrt{n})}$ за время $2^{\widetilde{\mathcal{O}}(\sqrt{n})}$
  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 β-BKZ with

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

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

Процесс стандартизации NIST

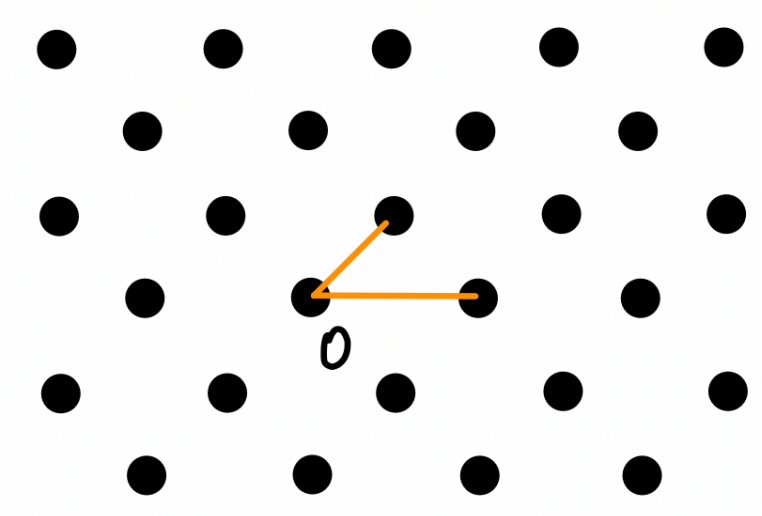
- В декабре 2016 года NIST (National Institute of Standards and Technology) запустил процесс стандартизации[1] пост-кватовых примитивов: цифровой подписи и KEM (Key Encapsulation Mechanism).
- В ноябре 2017 было получено 87 кандидатов от академии и индустрии
- В стандарт вошли 3 схемы на решетках + одна 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)
	Falcon (M-SIS)
	SPHINCS+ (hash-based)

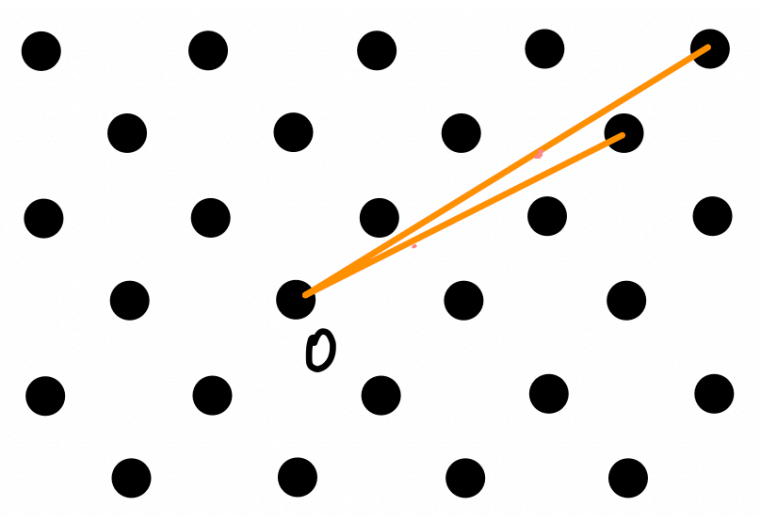
Подробно см. `https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf`

[1] `https://csrc.nist.gov/Projects/post-quantum-cryptography`

Шифрование на решетках

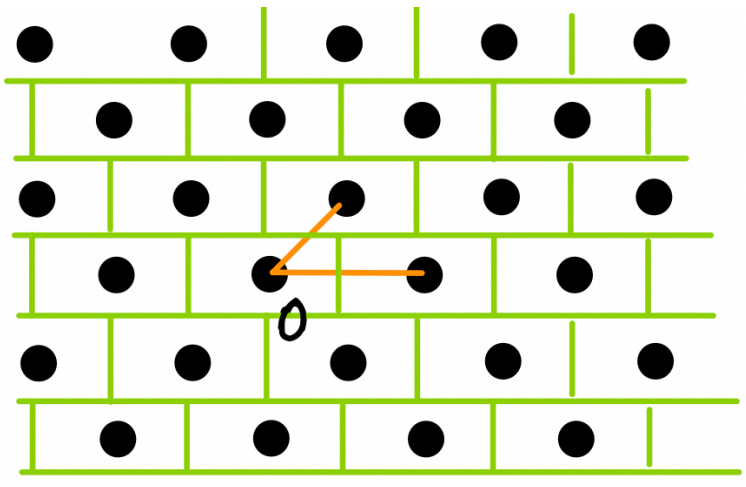


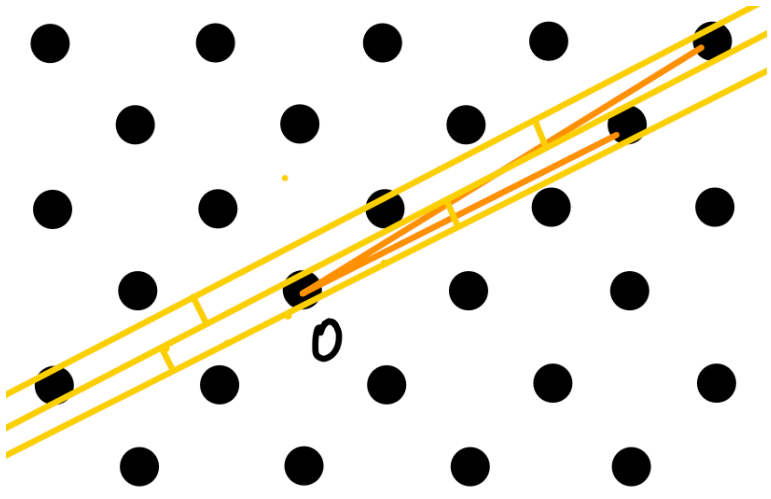
Хороший базис



Плохой базис

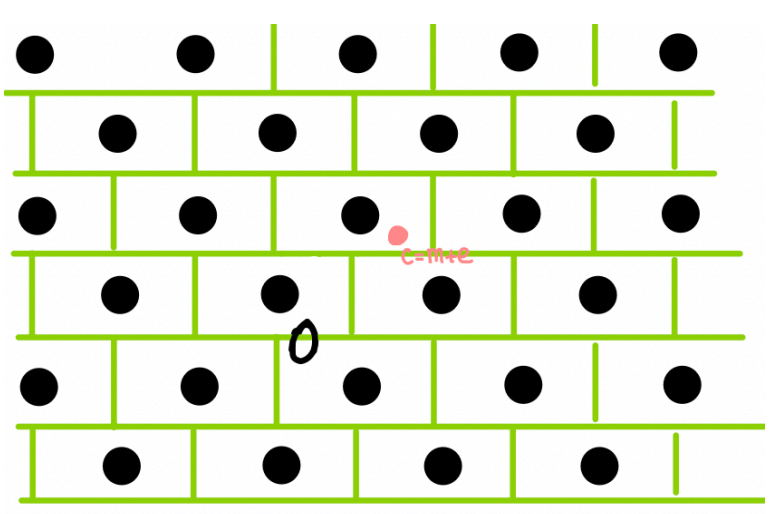
Шифрование на решетках II

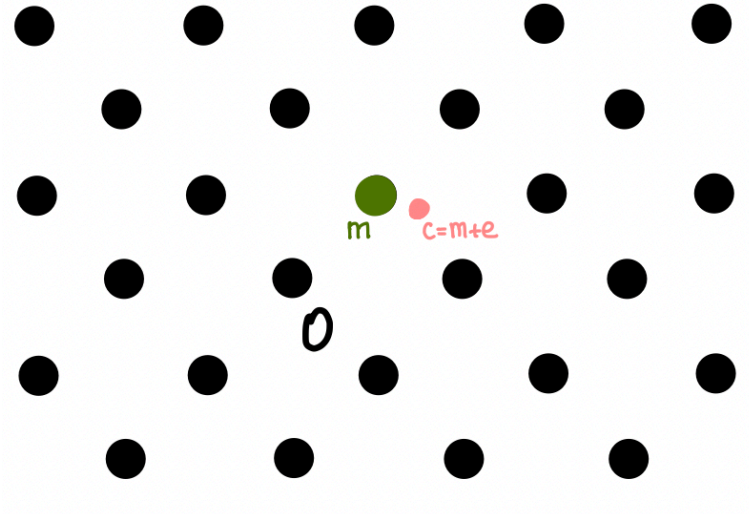




Грам-Шмидт базисы

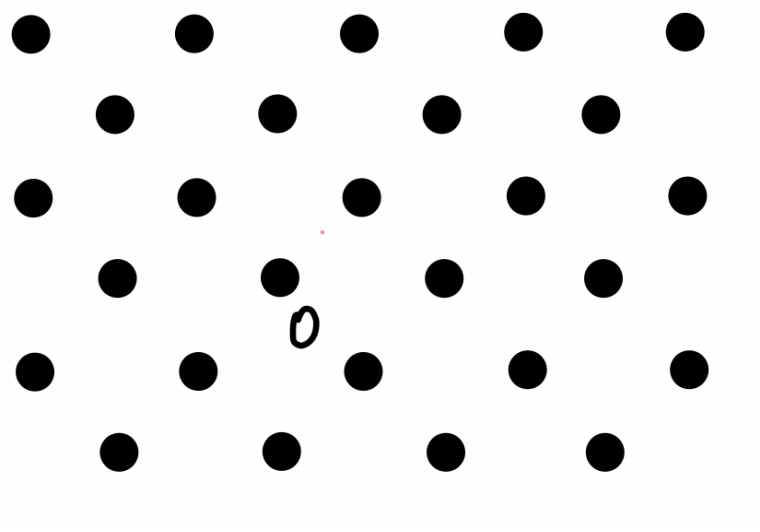
Шифрование на решетках III



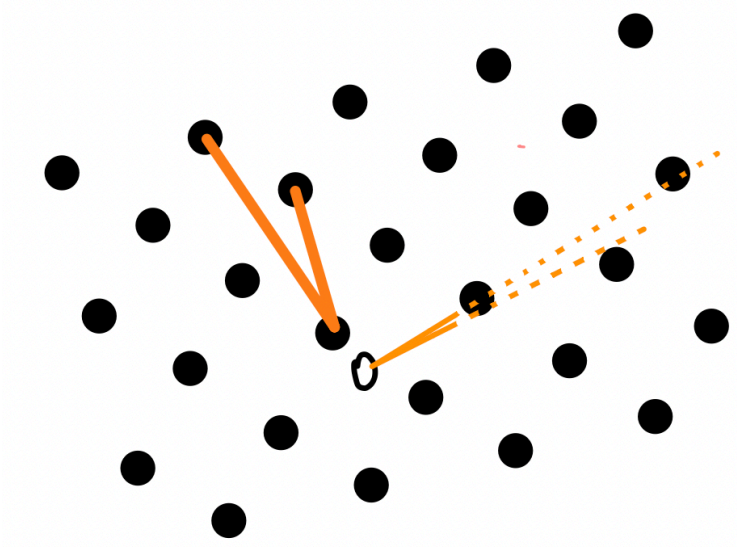


Шифрование сообщения m

Что если использовать разные решетки?



$\mathcal{L}$



$O \cdot \mathcal{L}, O \in \mathcal{O}_n(\mathbb{R})$

Задача Изоморфизма Решеток (Lattice Isomorphism Problem)

По заданным базисам $B, B' \in \mathbb{R}^{n \times n}$, найти $O \in \mathcal{O}_n(\mathbb{R})$ и $U \in \mathtt{GL}_n(\mathbb{R})$, чтобы выполнялось:

$$B' = O \cdot B \cdot U.$$

- $\mathtt{Min}(\mathcal{L}(B')) = O \cdot \mathtt{Min}(\mathcal{L}(B))$
- На практике решается нахождение коротких векторов в $\mathcal{L}(B)$ и $\mathcal{L}(B')$ и нахождение изометрии между ними
- LIP лежит в основе подписи HAWK

Открытые вопросы

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