Криптография на решётках: трудные задачи и конструкции

Елена Киршанова

Семинар "Математические методы криптографического анализа"
Москва, Россия

Представлюсь

- Диссертация на тему
  “Complexity of the Learning with Errors Problem and Memory-Efficient Lattice Sieving”,
  под руководством А. Мая.
  Рурский Университет г. Бохума, Германия 2012–2016
- Пост-док под руководством Д.Штеле.
  ENS Lyon, Франция 2016–2019
- Научный сотрудник лаборатории Мат. методы защиты информации,
  БФУ им. Канта, Калининград 2019–

Область интересов: криптография на решетках, криптанализ, алгоритмы для трудных задач на решетках и кодах, квантовые ускорения для таких алгоритмов.

`https://crypto-kantiana.com/elena.kirshanova/`

План

- Сложные задачи на Евклидовых решётках
- Задачи в среднем: задача LWE
- Задачи в среднем: задача SIS
- Построение подписи на решётках
- Открытые вопросы

Часть I

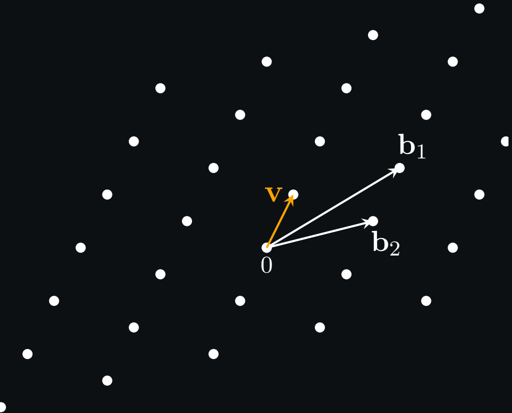
Евклидовы решётки

Определения

Решётка – это множество $\mathcal{L} = \{\sum_{i \le n} x_i \mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ для лин. независимых $\mathbf{b}_i \in \mathbb{R}^n$

$\{\mathbf{b}_i\}_i$– базис $\mathcal{L}$, $|\{\mathbf{b}_i\}|$ – ранг $\mathcal{L}$.

Определения



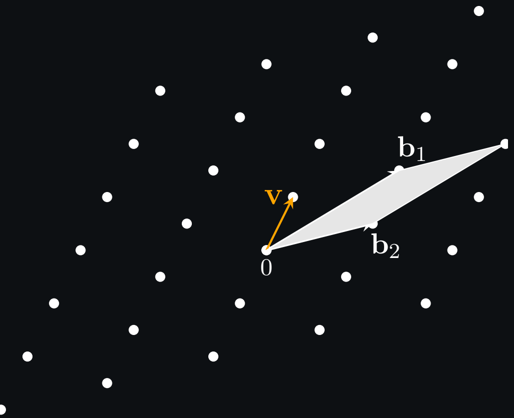
Минимум

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{v}\in\mathcal{L}\setminus\mathbf{0}} \|\mathbf{v}\|$$

Решётка – это множество $\mathcal{L} = \{\sum_{i\leq n} x_i\mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ для лин. независимых $\mathbf{b}_i \in \mathbb{R}^n$

$\{\mathbf{b}_i\}_i$– базис $\mathcal{L}$, $|\{\mathbf{b}_i\}|$ – ранг $\mathcal{L}$.

Определения



Минимум

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{v}\in\mathcal{L}\setminus\mathbf{0}} \|\mathbf{v}\|$$

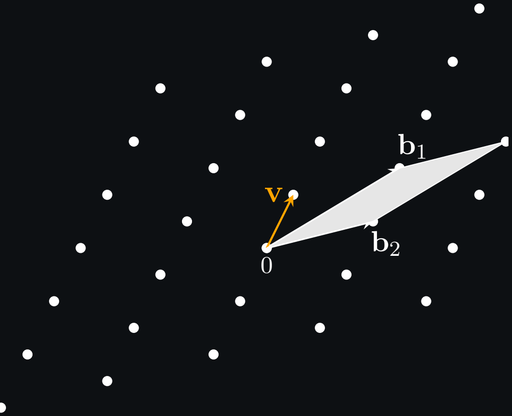
Определитель

$$\det(\mathcal{L}) = |\det(\mathbf{b}_i)_i|$$

Решётка – это множество $\mathcal{L} = \{\sum_{i\le n} x_i\mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ для лин. независимых $\mathbf{b}_i \in \mathbb{R}^n$

$\{\mathbf{b}_i\}_i$– базис $\mathcal{L}$, $|\{\mathbf{b}_i\}|$ – ранг $\mathcal{L}$.

Определения



Минимум

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{v}\in\mathcal{L}\setminus\mathbf{0}} \|\mathbf{v}\|$$

Определитель

$$\det(\mathcal{L}) = |\det(\mathbf{b}_i)_i|$$

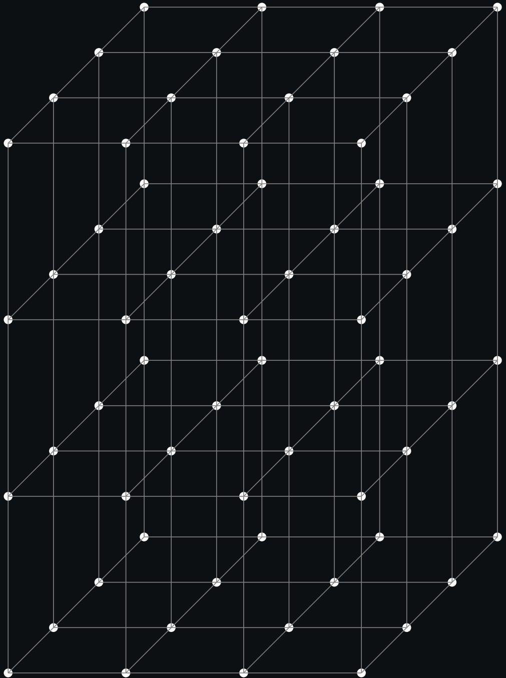
Граница Минковского

$$\lambda_1(\mathcal{L}) \leq \sqrt{n}\cdot\det(\mathcal{L})^{\frac{1}{n}}$$

Решётка – это множество $\mathcal{L} = \{\sum_{i\leq n} x_i\mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ для лин. независимых $\mathbf{b}_i \in \mathbb{R}^n$

$\{\mathbf{b}_i\}_i$– базис $\mathcal{L}$, $|\{\mathbf{b}_i\}|$ – ранг $\mathcal{L}$.

Решетка $\mathbb{Z}^n$



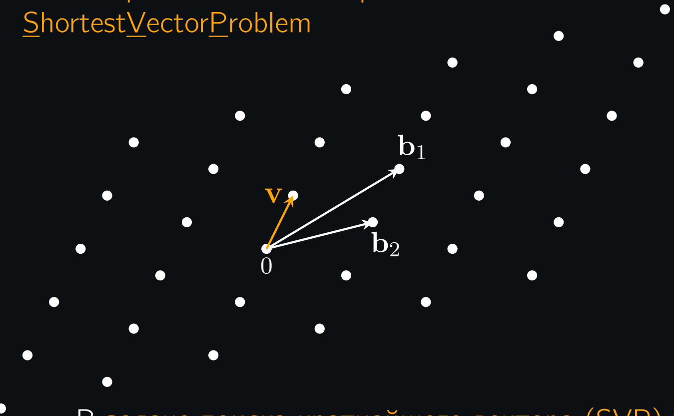
Решетка ранга n

$\det(\mathcal{L}) = 1$

$\lambda_1(\mathcal{L}) = 1$

$\mathbf{b}_i = \mathbf{e}_i.$

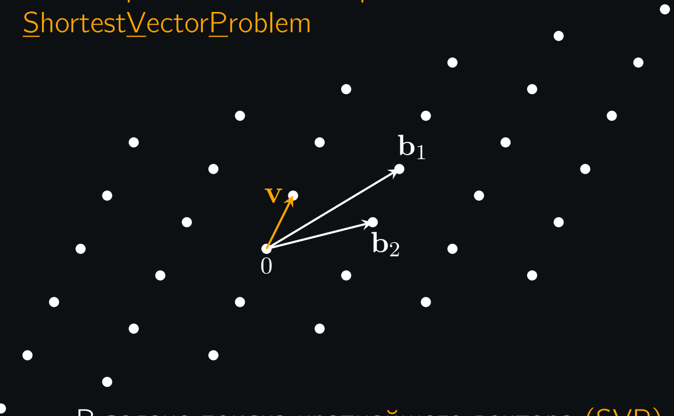
Поиск кратчайшего вектора
ShortestVectorProblem



В задаче поиска кратчайшего вектора (SVP) требуется найти $\mathbf{v}_{\text{shortest}} \in \mathcal{L}$:

$$\|\mathbf{v}_{\text{shortest}}\| = \lambda_1(\mathcal{L})$$

Поиск кратчайшего вектора
ShortestVectorProblem



В задаче поиска кратчайшего вектора (SVP) требуется найти $\mathbf{v}_{\text{shortest}} \in \mathcal{L}$:

$$||\mathbf{v}_{\text{shortest}}|| = \lambda_1(\mathcal{L})$$

Упрощение: поиск аппроксимации (γ-SVP) к $\mathbf{v}_{\text{shortest}}$:

$$||\mathbf{v}_{\text{short}}|| \leq \gamma \cdot \lambda_1(\mathcal{L})$$

Поиск ближайшего вектора CVP / BDD

В задаче поиска ближайшего вектора (CVP) для $\mathbf{t} \notin \mathcal{L}$ требуется найти $\mathbf{v} \in \mathcal{L}$:

$$\|\mathbf{v} - \mathbf{t}\| \text{ минимально для всех } \mathbf{v} \in \mathcal{L}$$

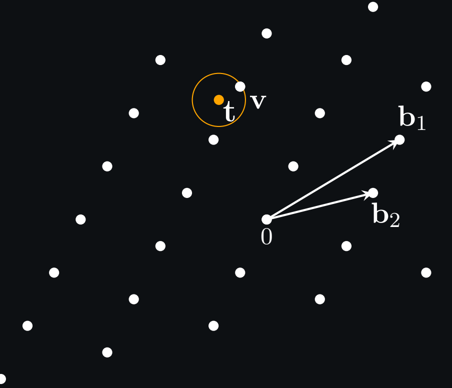
Поиск ближайшего вектора CVP / BDD

В задаче поиска ближайшего вектора (CVP) для $\mathbf{t} \notin \mathcal{L}$ требуется найти $\mathbf{v} \in \mathcal{L}$:

$$\|\mathbf{v} - \mathbf{t}\| \text{ минимально для всех } \mathbf{v} \in \mathcal{L}$$

Часто: $\mathrm{dist}(t, \mathcal{L}) \leq \frac{1}{\gamma}\lambda_1(\mathcal{L})$. Получаем задачу Декодирования с Ограниченным расстоянием, γ-BDD

Поиск ближайшего вектора CVP / BDD



Для решения BDD в $\mathcal{L}$,
вызываем оракул для approx-SVP
“связанной” решетке р-ти+ 1.

В задаче поиска ближайшего вектора (CVP) для $\mathbf{t} \notin \mathcal{L}$ требуется найти $\mathbf{v} \in \mathcal{L}$:

$$\|\mathbf{v} - \mathbf{t}\| \text{ минимально для всех } \mathbf{v} \in \mathcal{L}$$

Часто: $\mathrm{dist}(t, \mathcal{L}) \leq \frac{1}{\gamma}\lambda_1(\mathcal{L})$. Получаем задачу Декодирования с Ограниченным расстоянием, γ-BDD

От задачи BDD к approxSVP: вложение Каннана

Для задачи BDD $(\mathcal{L}, \mathbf{t})$, где $\mathcal{L}$ имеет базиз B, рассмотрим для константы c

$$B' = \begin{bmatrix} B & \mathbf{t} \\ \mathbf{0} & \mathsf{c} \end{bmatrix}$$

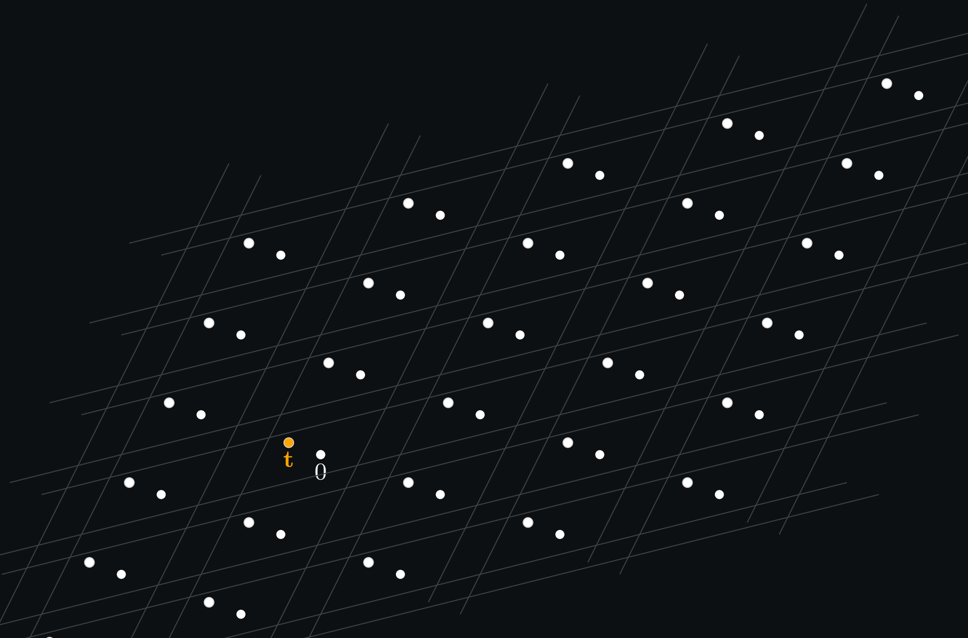
- столбцы B' лин. независимы
- Для "грамотно" выбранной c и $\mathbf{t}$ – достаточно близкого к $\mathcal{L}$

$$\begin{bmatrix} B & \mathbf{t} \\ \mathbf{0} & \mathsf{c} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{x} \\ -1 \end{bmatrix} = \begin{bmatrix} B\mathbf{x} - \mathbf{t} \\ -\mathsf{c} \end{bmatrix}$$

– короткий вектора в $\mathcal{L}(B')$ (намного короче, чем любой $\mathbf{v} \in \mathcal{L}(B')$ не параллельный ему).

От задачи BDD к approxSVP: вложение Каннана

От задачи BDD к approxSVP: вложение Каннана



Асимптотическая сложность approxSVP

$$\|\mathbf{v}_{\text{short}}\| \leq \gamma \cdot \|\mathbf{v}_{\text{shortest}}\|$$

Асимптотическая сложность approxSVP

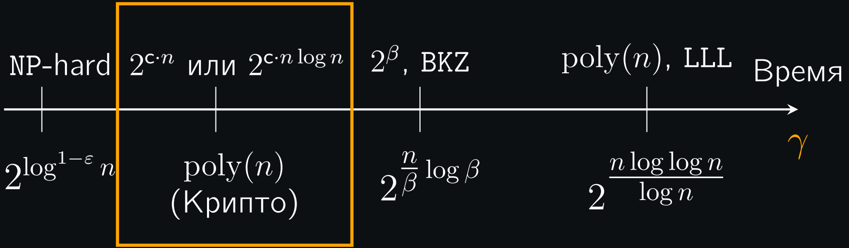
$$\|\mathbf{v}_{\text{short}}\| \leq \gamma \cdot \|\mathbf{v}_{\text{shortest}}\|$$

Время	NP-hard	$2^{\mathsf{c}\cdot n}$ или $2^{\mathsf{c}\cdot n\log n}$	2^{β}, BKZ	$\mathrm{poly}(n)$, LLL
γ	$2^{\log^{1-\varepsilon} n}$	$\mathrm{poly}(n)$ (Крипто)	$2^{\frac{n}{\beta}\log\beta}$	$2^{\frac{n\log\log n}{\log n}}$

BKZ – Block Korkine-Zolotarev, LLL – Lenstra, Lenstra, Lovász

Асимптотическая сложность approxSVP

$$||\mathbf{v}_{\text{short}}|| \leq \gamma \cdot ||\mathbf{v}_{\text{shortest}}||$$



- Просеивание:

$$\text{Время(SVP)} = 2^{cn+o(n)} \qquad \text{Память} = 2^{cn+o(n)}$$

- Перечисление:

$$\text{Время(SVP)} = 2^{cn\log n + o(n\log n)} \qquad \text{Память} = \mathrm{poly}(n)$$

На сегодняшний день не существует эффективного алгоритма (ни классического, ни квантового) для задачи SVP!

BKZ – Block Korkine-Zolotarev, LLL – Lenstra, Lenstra, Lovász

Часть II

Задача обучения с ошибками (The Learning with Errors problem, LWE)

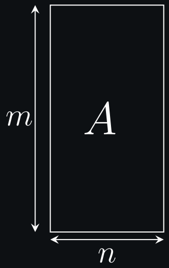
Построение решеток

Зафиксируем модуль q. $\mathbb{Z}_q$ – кольцо вычетов по модулю q.

- Выберем случайным образом $A \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{m\times n}$, $m > n$
- A задает решетку

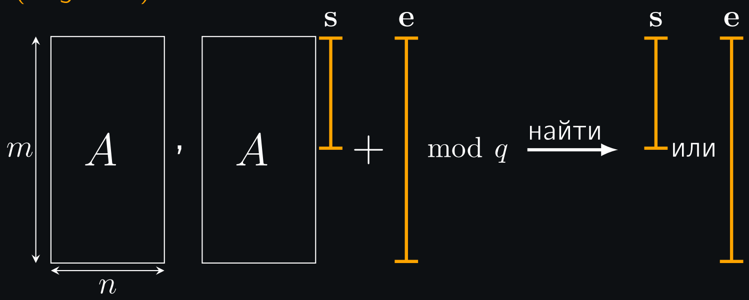
$$\mathcal{L}_q(A) = A\mathbb{Z}_q^n + q\mathbb{Z}^m$$

- С большой вероятностью $\mathcal{L}_q(A)$ ранга m и $\det(\mathcal{L}_q(A)) = q^{m-n}$



Такая конструкция носит название Конструкция А.

LWE (Regev'05)



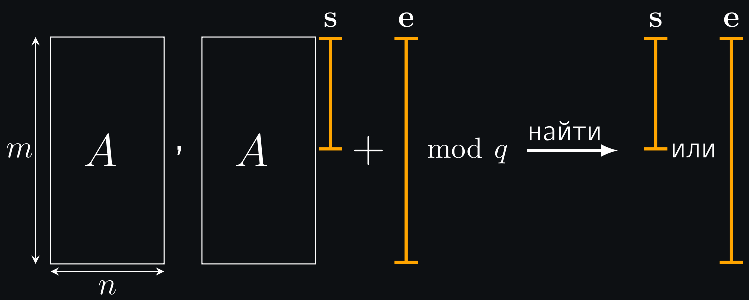
$$A \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$$

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

$$\mathbf{e} \leftarrow \mathbb{Z}^{m}, \|\mathbf{e}\| < B$$

Часто: $n = \Theta($ур-нь безопасности$)$, $q = n^{\Theta(1)}$, $m = \Theta(n \log q)$, $B = \Omega(\sqrt{n})$ $(\sigma = \Omega(\sqrt{n}))$

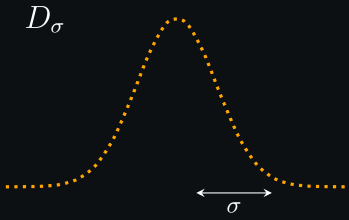
LWE (Regev'05)



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

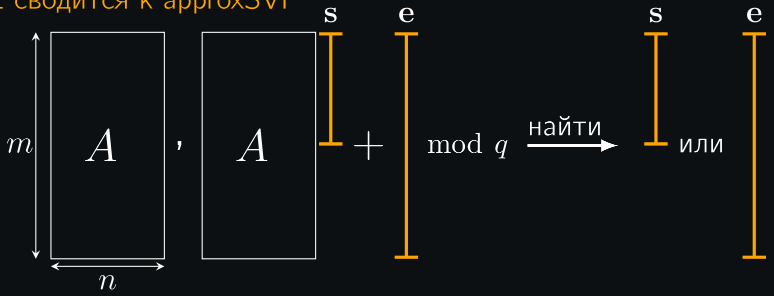
$$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^{n}$$

$$\mathbf{e} \leftarrow D_\sigma$$



Часто: $n = \Theta($ур-нь безопасности$)$, $q = n^{\Theta(1)}$, $m = \Theta(n \log q)$, $B = \Omega(\sqrt{n})$ $(\sigma = \Omega(\sqrt{n}))$

LWE сводится к approxSVP



- A задает решётку A-Конструкции

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

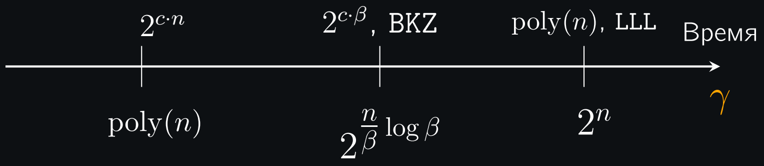
- $As \in \mathcal{L}_q(A)$
- $As + e$ – вектор, на расстоянии $\|e\|$ от $\mathcal{L}_q(A)$
- $(A, As + e)$ – пример BDD задачи для $\mathcal{L}_q(A)$ с

$$\gamma = \frac{\lambda_1(\mathcal{L}_q(A))}{\mathrm{dist}(As + e, \mathcal{L}_q(A))} = \frac{q^{1-n/m}}{|e_i|}$$

Сложность LWE

LWE $(A, As + e)$ – BDD в $\mathcal{L}_q(A)$ с параметром

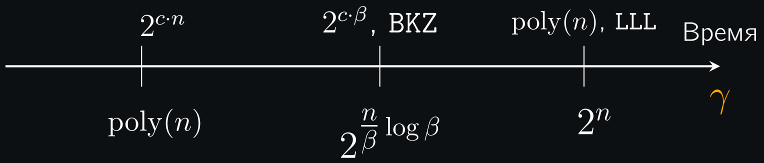
$$\gamma = \frac{\lambda_1(\mathcal{L}_q(A))}{\mathrm{dist}(As + e, \mathcal{L}_q(A))} = \frac{q^{1-n/m}}{|e_i|}$$



Сложность LWE

LWE $(A, As + e)$ – BDD в $\mathcal{L}_q(A)$ с параметром

$$\gamma = \frac{\lambda_1(\mathcal{L}_q(A))}{\mathrm{dist}(As + e, \mathcal{L}_q(A))} = \frac{q^{1-n/m}}{|e_i|}$$



В асимптотике для константы c:

$$T(\mathsf{LWE}) = \exp\left(\mathsf{c} \cdot \frac{\lg q}{\lg^2(q/|e_i|)} \lg\left(\frac{n \lg q}{\lg^2(q/|e_i|)}\right) \cdot n\right)$$

Эта формула получена решением уравнения для β

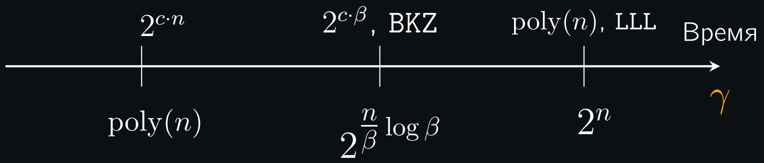
$$2^{\frac{m}{\beta}\log\beta} = \frac{q^{1-n/m}}{|e_i|},$$

и выбором $m = \Omega(n)$, минимизирующем решение.

Сложность LWE

LWE $(A, As+e)$ – BDD в $\mathcal{L}_q(A)$ с параметром

$$\gamma = \frac{\lambda_1(\mathcal{L}_q(A))}{\mathrm{dist}(As+e, \mathcal{L}_q(A))} = \frac{q^{1-n/m}}{|e_i|}$$



В асимптотике для константы c:

$$T(\mathrm{LWE}) = \exp\left(\mathrm{c} \cdot \frac{\lg q}{\lg^2(q/|e_i|)} \lg\left(\frac{n \lg q}{\lg^2(q/|e_i|)}\right) \cdot n\right)$$

Эта формула получена решением уравнения для β

$$2^{\frac{m}{\beta}\log\beta} = \frac{q^{1-n/m}}{|e_i|},$$

и выбором $m = \Omega(n)$, минимизирующем решение.

Улучшения константы c и конкретные значения $T(\mathrm{LWE})$ – открытые вопросы криптоанализа.

Часть III

Нахождение короткого целого решения (Short Integer Solution, SIS)

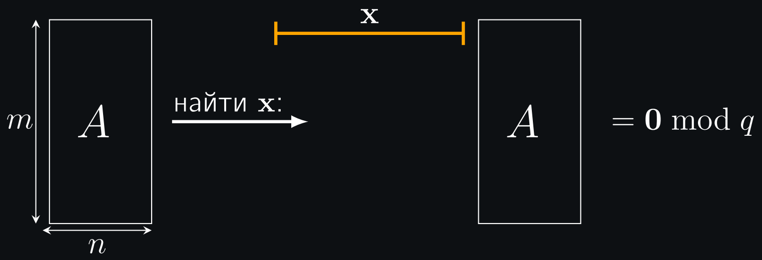
Задача нахождения короткого целого решения (SIS), Ajtai'96

$A \in \mathbb{Z}^{m \times n}$: m, n

найти $\mathbf{x}$: $\mathbf{x} A = \mathbf{0} \bmod q$

и $0 < \|\mathbf{x}\| \leq B$

Задача нахождения короткого целого решения (SIS), Ajtai'96



и $0 < \|\mathbf{x}\| \le B$

- A задаёт ортогональную решетку ранга m

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

- SIS – это γ-SVP в $\mathcal{L}_q^{\perp}(A)$ с $\gamma = \frac{\sqrt{m} q^{\frac{n}{m}}}{B}$. Аналогично LWE,

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

LWE vs. SIS

LWE

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

approxSVP в $\mathcal{L}_q(A)$

$f(\mathbf{x}, \mathbf{e}) = A\mathbf{x} + \mathbf{e}$
– инъекция

KEM, IBE, ABE, FHE

SIS

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

approxSVP в $\mathcal{L}_q^{\perp}(A)$

$f(\mathbf{x}) = \mathbf{x}A$
– сюръекция

Хэш-функции, подписи

$\mathcal{L}_q(A)$ – дуальная к $q\mathcal{L}_q^{\perp}(A)$

LWE $\iff$ SIS

Часть IV

Подписи на решётках

Две парадигмы построения подписи на решётках

I. Парадигма Hash-and-Sign

Пример: Falcon = NTRUSign + [GPV08]

Преимущество: короткие подписи

Недостаток: сложна в реализации, время генерации ключей

II. Эвристика Фиат-Шамира [FS]

Пример: Lyubashevsky, Bai-Gabraith, Dilithium, Tesla

Преимущество: простая реализация

Недостаток: более длинные подписи

Конструкция Lyubashevsky (упрощено)

Параметры: $n, m, \ell \in \mathbb{Z}$, $q \in \mathbb{Z}$ – модуль

Элементы малой $\|\cdot\|_\infty$ – Оранжевые

$\mathcal{H} : \{0,1\}^\star \to \mathbb{Z}^{\ell \times \ell}$ – хэш-функция, $\|\mathcal{H}()\|_\infty$–мала

Конструкция Lyubashevsky (упрощено)

Параметры: $n, m, \ell \in \mathbb{Z}$, $q \in \mathbb{Z}$ – модуль

Элементы малой $\|\cdot\|_\infty$ – Оранжевые

$\mathcal{H} : \{0,1\}^\star \to \mathbb{Z}^{\ell\times\ell}$ – хэш-функция, $\|\mathcal{H}()\|_\infty$–мала

I. KeyGen :

1. $\mathbf{A} \leftarrow \mathbb{Z}_q^{m\times n}$
2. $\mathsf{X} \leftarrow \mathbb{Z}^{\ell\times m}$,
3. $\mathsf{T} = \mathsf{X} \cdot \mathbf{A} \bmod q$
4. $\mathsf{sk} = \mathsf{X}$, $\mathsf{vk} = (\mathbf{A}, \mathsf{T})$

Конструкция Lyubashevsky (упрощено)

Параметры: $n, m, \ell \in \mathbb{Z}$, $q \in \mathbb{Z}$ – модуль

Элементы малой $\|\cdot\|_\infty$ – Оранжевые

$\mathcal{H} : \{0,1\}^\star \to \mathbb{Z}^{\ell\times\ell}$ – хэш-функция, $\|\mathcal{H}()\|_\infty$–мала

I. KeyGen :

1. $\mathbf{A} \leftarrow \mathbb{Z}_q^{m\times n}$
2. $\mathsf{X} \leftarrow \mathbb{Z}^{\ell\times m}$,
3. $\mathsf{T} = \mathsf{X} \cdot \mathbf{A} \bmod q$
4. $\mathsf{sk} = \mathsf{X}$, $\mathsf{vk} = (\mathbf{A}, \mathsf{T})$

II. Sign($\mathsf{sk} = \mathsf{X}, M \in \{0,1\}^\star$) :

1. $\mathsf{Y} \leftarrow \mathbb{Z}^{\ell\times m}$
2. $\mathsf{W} = \mathsf{Y} \cdot \mathbf{A} \bmod q$
3. $\mathsf{C} = \mathcal{H}(\mathsf{vk}, \mathsf{W}, M) \in \mathbb{Z}^{\ell\times\ell}$
4. $\mathsf{Z} = \mathsf{Y} + \mathsf{C} \cdot \mathsf{X}$
5. $\sigma = (\mathsf{Z}, \mathsf{C})$

Конструкция Lyubashevsky (упрощено)

Параметры: $n, m, \ell \in \mathbb{Z}$, $q \in \mathbb{Z}$ – модуль

Элементы малой $\|\cdot\|_\infty$ – Оранжевые

$\mathcal{H} : \{0,1\}^\star \to \mathbb{Z}^{\ell \times \ell}$ – хэш-функция, $\|\mathcal{H}()\|_\infty$–мала

I. KeyGen :

1. $\mathbf{A} \leftarrow \mathbb{Z}_q^{m \times n}$
2. $\mathsf{X} \leftarrow \mathbb{Z}^{\ell \times m}$,
3. $\mathsf{T} = \mathsf{X} \cdot \mathbf{A} \bmod q$
4. $\mathsf{sk} = \mathsf{X}$, $\mathsf{vk} = (\mathbf{A}, \mathsf{T})$

II. Sign$(\mathsf{sk} = \mathsf{X}, M \in \{0,1\}^\star)$:

1. $\mathsf{Y} \leftarrow \mathbb{Z}^{\ell \times m}$
2. $\mathsf{W} = \mathsf{Y} \cdot \mathbf{A} \bmod q$
3. $\mathsf{C} = \mathcal{H}(\mathsf{vk}, \mathsf{W}, M) \in \mathbb{Z}^{\ell \times \ell}$
4. $\mathsf{Z} = \mathsf{Y} + \mathsf{C} \cdot \mathsf{X}$
5. $\sigma = (\mathsf{Z}, \mathsf{C})$

III. Verify$(\mathsf{C}, M, \sigma = (\mathsf{Z}, \mathsf{C}))$:

1. $\mathsf{W}' = \mathsf{Z} \cdot \mathbf{A} - \mathsf{C} \cdot \mathsf{T}$
2. $\mathsf{C}' = \mathcal{H}(\mathsf{vk}, \mathsf{W}', M)$
3. Если $\mathsf{C}' == \mathsf{C}$ и $\|\mathsf{Z}\|_\infty$ – мала

   return "Accept"

   Иначе **return** "Reject"

Конструкция Lyubashevsky (упрощено)

Параметры: $n, m, \ell \in \mathbb{Z}$, $q \in \mathbb{Z}$ – модуль

Элементы малой $\|\cdot\|_\infty$ – Оранжевые

$\mathcal{H} : \{0,1\}^\star \to \mathbb{Z}^{\ell \times \ell}$ – хэш-функция, $\|\mathcal{H}()\|_\infty$–мала

I. KeyGen :

1. $\mathbf{A} \leftarrow \mathbb{Z}_q^{m \times n}$
2. $\mathsf{X} \leftarrow \mathbb{Z}^{\ell \times m}$,
3. $\mathsf{T} = \mathsf{X} \cdot \mathbf{A} \bmod q$
4. $\mathsf{sk} = \mathsf{X}$, $\mathsf{vk} = (\mathbf{A}, \mathsf{T})$

II. Sign($\mathsf{sk} = \mathsf{X}, M \in \{0,1\}^\star$) :

1. $\mathsf{Y} \leftarrow \mathbb{Z}^{\ell \times m}$
2. $\mathsf{W} = \mathsf{Y} \cdot \mathbf{A} \bmod q$
3. $\mathsf{C} = \mathcal{H}(\mathsf{vk}, \mathsf{W}, M) \in \mathbb{Z}^{\ell \times \ell}$
4. $\mathsf{Z} = \mathsf{Y} + \mathsf{C} \cdot \mathsf{X}$
5. $\sigma = (\mathsf{Z}, \mathsf{C})$

III. Verify($\mathsf{C}, M, \sigma = (\mathsf{Z}, \mathsf{C})$) :

1. $\mathsf{W}' = \mathsf{Z} \cdot \mathbf{A} - \mathsf{C} \cdot \mathsf{T}$
2. $\mathsf{C}' = \mathcal{H}\left(\mathsf{vk}, \mathsf{W}', M\right)$
3. Если $\mathsf{C}' == \mathsf{C}$ и $\|\mathsf{Z}\|_\infty$ – мала

   return “Accept”

   Иначе **return** “Reject”

Корректность:

- $\mathsf{W}' == \mathsf{W}$ для корректной подписи
- $\|\mathsf{Z}\|_\infty$ – мала по построению

Безопасность

- Док-во безопасности аналогично док-ву подписи Шнорра
- Forking Lemma + сложность SIS + корректно подобранные пар-ры $\implies$ UF-CMA безопасность подписи
- Шаг 1. $T = \mathsf{X} \cdot \mathbf{A} \bmod q \sim \mathcal{U}(\mathbb{Z}_q^{\ell \times n})$ из-за SIS
- Шаг 2. Распределения C, Z симулируются без знания X, если распределение Z центрируется около 0 с помощью техники Rejection Sampling

Безопасность

- Док-во безопасности аналогично док-ву подписи Шнорра
- Forking Lemma + сложность SIS + корректно подобранные пар-ры $\implies$ UF-CMA безопасность подписи
- Шаг 1. $T = \mathsf{X} \cdot \mathbf{A} \bmod q \sim \mathcal{U}(\mathbb{Z}_q^{\ell \times n})$ из-за SIS
- Шаг 2. Распределения C, Z симулируются без знания X, если распределение Z центрируется около 0 с помощью техники Rejection Sampling

II. $\mathsf{Sign}(\mathsf{sk} = \mathsf{X}, M \in \{0,1\}^\star)$:

1. $\mathsf{Y} \leftarrow \mathbb{Z}^{\ell \times m}$
2. $\mathsf{W} = \mathsf{Y} \cdot \mathbf{A} \bmod q$
3. $\mathsf{C} = \mathcal{H}(\mathsf{vk}, \mathsf{W}, M) \in \mathbb{Z}^{\ell \times \ell}$
4. $\mathsf{Z} = \mathsf{Y} + \mathsf{C} \cdot \mathsf{X}$
5. $\sigma = (\mathsf{Z}, \mathsf{C})$

II. $\mathsf{Sign}(\mathsf{sk} = \mathsf{X}, M \in \{0,1\}^\star)$:

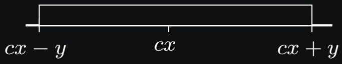
1. $\mathsf{Y} \leftarrow \mathbb{Z}^{\ell \times m}$
2. $\mathsf{W} = \mathsf{Y} \cdot \mathbf{A} \bmod q$
3. $\mathsf{C} = \mathcal{H}(\mathsf{vk}, \mathsf{W}, M) \in \mathbb{Z}^{\ell \times \ell}$
4. $\mathsf{Z} = \mathsf{Y} + \mathsf{X} \cdot \mathsf{C}$
5. $\sigma = (\mathsf{Z}, \mathsf{C})$
6. Если $\|\mathsf{Z}\|_\infty < B_z$:
7. Restart Sign

Безопасность

- Док-во безопасности аналогично док-ву подписи Шнорра
- Forking Lemma + сложность SIS + корректно подобранные пар-ры $\implies$ UF-CMA безопасность подписи
- Шаг 1. $T = \mathsf{X} \cdot \mathbf{A} \bmod q \sim \mathcal{U}(\mathbb{Z}_q^{\ell \times n})$ из-за SIS
- Шаг 2. Распределения C, Z симулируются без знания X, если распределение Z центрируется около 0 с помощью техники Rejection Sampling

II. $\mathsf{Sign}(\mathsf{sk} = \mathsf{X}, M \in \{0,1\}^\star)$:

1. $\mathsf{Y} \leftarrow \mathbb{Z}^{\ell \times m}$
2. $\mathsf{W} = \mathsf{Y} \cdot \mathbf{A} \bmod q$
3. $\mathsf{C} = \mathcal{H}(\mathsf{vk}, \mathsf{W}, M) \in \mathbb{Z}^{\ell \times \ell}$
4. $\mathsf{Z} = \mathsf{Y} + \mathsf{C} \cdot \mathsf{X}$
5. $\sigma = (\mathsf{Z}, \mathsf{C})$



II. $\mathsf{Sign}(\mathsf{sk} = \mathsf{X}, M \in \{0,1\}^\star)$:

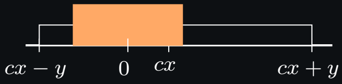
1. $\mathsf{Y} \leftarrow \mathbb{Z}^{\ell \times m}$
2. $\mathsf{W} = \mathsf{Y} \cdot \mathbf{A} \bmod q$
3. $\mathsf{C} = \mathcal{H}(\mathsf{vk}, \mathsf{W}, M) \in \mathbb{Z}^{\ell \times \ell}$
4. $\mathsf{Z} = \mathsf{Y} + \mathsf{X} \cdot \mathsf{C}$
5. $\sigma = (\mathsf{Z}, \mathsf{C})$
6. Если $\|\mathsf{Z}\|_\infty < B_z$:
7. Restart Sign

Безопасность

- Док-во безопасности аналогично док-ву подписи Шнорра
- Forking Lemma + сложность SIS + корректно подобранные пар-ры $\implies$ UF-CMA безопасность подписи
- Шаг 1. $T = \mathsf{X} \cdot \mathbf{A} \bmod q \sim \mathcal{U}(\mathbb{Z}_q^{\ell \times n})$ из-за SIS
- Шаг 2. Распределения C, Z симулируются без знания X, если распределение Z центрируется около 0 с помощью техники Rejection Sampling

II. $\mathsf{Sign}(\mathsf{sk} = \mathsf{X}, M \in \{0,1\}^\star)$:

1. $\mathsf{Y} \leftarrow \mathbb{Z}^{\ell \times m}$
2. $\mathsf{W} = \mathsf{Y} \cdot \mathbf{A} \bmod q$
3. $\mathsf{C} = \mathcal{H}(\mathsf{vk}, \mathsf{W}, M) \in \mathbb{Z}^{\ell \times \ell}$
4. $\mathsf{Z} = \mathsf{Y} + \mathsf{C} \cdot \mathsf{X}$
5. $\sigma = (\mathsf{Z}, \mathsf{C})$



II. $\mathsf{Sign}(\mathsf{sk} = \mathsf{X}, M \in \{0,1\}^\star)$:

1. $\mathsf{Y} \leftarrow \mathbb{Z}^{\ell \times m}$
2. $\mathsf{W} = \mathsf{Y} \cdot \mathbf{A} \bmod q$
3. $\mathsf{C} = \mathcal{H}(\mathsf{vk}, \mathsf{W}, M) \in \mathbb{Z}^{\ell \times \ell}$
4. $\mathsf{Z} = \mathsf{Y} + \mathsf{X} \cdot \mathsf{C}$
5. $\sigma = (\mathsf{Z}, \mathsf{C})$
6. Если $\|\mathsf{Z}\|_\infty < B_z$:
7. Restart Sign

На практике

- Недостатки схемы подписи:
  1. Размер ключей/подписи (матрица над $\mathbb{Z}_q$ занимает $n^2 \log q$ бит)
  2. Время операция (умножение матриц)

- Вместо $\mathbb{Z}_q^n$ на практике используем для неприводимого над $\mathbb{Q}$ многочлена $f, \deg(f) = n$:

$$R = \mathbb{Z}[x]/(f(x)) \cong \mathbb{Z}^n, \quad R_q/R/(qR) \cong \mathbb{Z}_q^n$$

  1. Матрица $n \times n$ над $\mathbb{Z}_q$ $\to$ многочлен $g \in R_q$ (храним $n \log q$ бит)
  2. Умножение матриц $\to$ произведение многочленов

- Это дает малые размеры ключей/подписей и эффективные алгоритмы.

  Пример: в Dilithium при уровне без-ти в 128 бит:
  $|\mathsf{vk}| = 1.5k, |\sigma| = 2.7k$

- Задачи LWE, SIS, SVP формулируется для “идеальных” или “модульных” решёток (идеал в кольце целых R – решётка в $\mathbb{C}^n$)

Открытые вопросы

1. Улучшенные алгоритмы SVP для “идеальных” решёток
2. Алгоритмы SVP для других норм, например, ℓ_∞.
3. Практическая реализация алгоритмов: расширение библиотек `fplll`, `g6k`[1]
4. "Assessing the security of lattice-based submissions: the 10 questions that NIST should be asking the community": `http://prometheuscrypt.gforge.inria.fr/2018-06-04.assessing-security`

[1] `https://github.com/fplll/fplll`
`https://github.com/fplll/g6k`

Открытые вопросы

1. Улучшенные алгоритмы SVP для “идеальных” решёток
2. Алгоритмы SVP для других норм, например, ℓ_∞.
3. Практическая реализация алгоритмов: расширение библиотек `fplll`, `g6k`[1]
4. "Assessing the security of lattice-based submissions: the 10 questions that NIST should be asking the community": `http://prometheuscrypt.gforge.inria.fr/2018-06-04.assessing-security`

?

[1] `https://github.com/fplll/fplll`
`https://github.com/fplll/g6k`