конференция РусКрипто

QApp

Схема цифровой подписи на решетках «Облепиха»

Антон Леевик
Криптограф-исследователь

qapp.tech

Участник

Актуальность

QApp

В России идет процесс стандартизации новых квантово-устойчивых схем цифровой подписи

На данный момент разработаны:

- Подпись на кодах «Шиповник»
- Подпись на хэш-функциях «Гиперикум»

Главные недостатки предложенных схем — большой размер подписи:

- «Гиперикум»: от ~ 18 Kb до ~ 57 Kb
- «Шиповник»: ~ 600 Kb

Задача: уменьшение размеров подписи при сохранении уровня стойкости

Решение: построение схемы на математическом аппарате теории решеток

Существующие подходы построения подписи на решетках

QApp

Парадигма Фиата-Шамира с прерываниями (схемы Dilithium, HAETAE)	**Парадигма Hash-and-Sign** (схемы Falcon, Mitaka)
Стойкость на основе сложности LWE и SIS	Стойкость на основе сложности SIS
Универсальный подход	Подходит для отдельных задач

Параметры	Dilithium	Falcon
Открытый ключ, байт	2 592	1 793
Подпись, байт	4 595	1 280
Выработка подписи, циклы	642 192	2 053 080
Проверка подписи, циклы	279 936	160 596

Существующие подходы построения подписи на решетках

QApp

Парадигма Фиата-Шамира с прерываниями (схемы Dilithium, HAETAE)	**Парадигма Hash-and-Sign** (схемы Falcon, Mitaka)
Стойкость на основе сложности LWE и SIS	Стойкость на основе сложности SIS
Универсальный подход	Подходит для отдельных задач

Параметры	Dilithium	Falcon	Hawk
Открытый ключ, байт	2 592	1 793	2 440
Подпись, байт	4 595	1 280	1 221
Выработка подписи, циклы	642 192	2 053 080	180 816
Проверка подписи, циклы	279 936	160 596	302 861

Hawk — новая схема на задаче **LIP**!

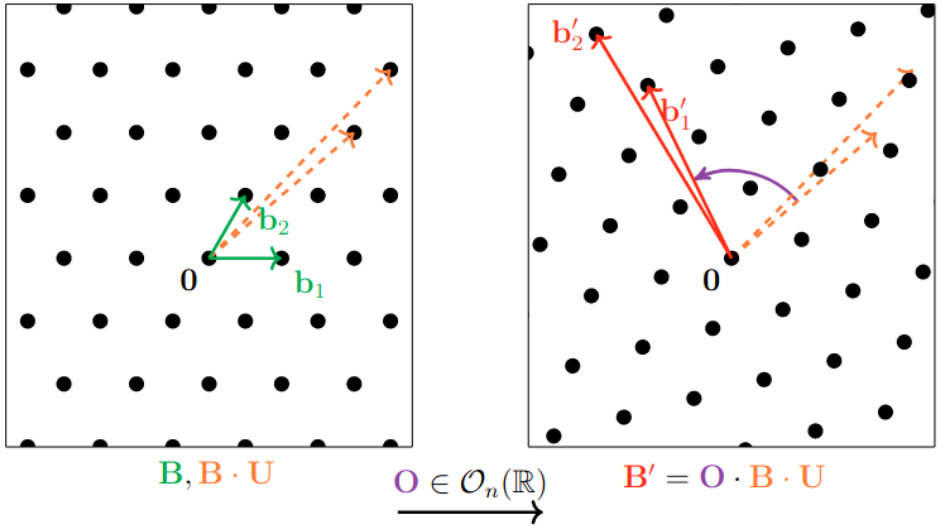
LIP vs LWE/SIS

QApp

LIP	SIS	LWE
• Активное изучение — 1997 год, Плескен и Сувень. Криптографические конструкции — 2022 год, работа Дюка и Ван Вёрдена • Есть сведение от задач GI (изоморфизма графов) и LCE (линейной эквивалентности кодов) • Есть потенциал для уменьшения размеров подписи благодаря использованию решеток с большим минимальным расстоянием	• 1996 год, Айтай • Есть сведение от задачи γ-SIVP • Сложно сократить размер подписи еще сильнее ввиду проблем со стойкостью	• LPN — 1993 год, LWE — 2005 год, Регев • Есть сведение от задач γ-SIVP и γ-GapSVP

Изоморфные решетки

Пусть заданы решетки $\mathcal{L} \subset \mathbb{R}^n$ и $\mathcal{L}' \subset \mathbb{R}^n$ с базисами $\mathbf{B}$ и $\mathbf{B}'$ соответственно, а также ортогональное преобразование $\mathcal{O} : \mathbb{R}^n \to \mathbb{R}^n$ с соответствующей ей матрицей $\mathbf{O}$.
Тогда решетка $\mathcal{L}'$ изоморфна $\mathcal{L}$, если $\mathcal{L}' = \mathbf{O} \cdot \mathcal{L}$ и базис $\mathbf{B}' = \mathbf{O} \cdot \mathbf{B} \cdot \mathbf{U}$, где $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$



Задача LIP (решетчатая версия)

QApp

Задача LIP (задача поиска)

Для двух изоморфных решеток $\mathcal{L}, \mathcal{L}' \subset \mathbb{R}^n$ найти ортогональное линейное отображение $\mathcal{O}$ с соответствующей матрицей $\mathbf{O}$ такое, что $\mathbf{O} \cdot \mathcal{L} = \mathcal{L}'$

Пусть решетки $\mathcal{L}, \mathcal{L}'$ заданы двумя базисами $\mathbf{B}, \mathbf{B}'$, тогда задача LIP определяется следующим образом

Задача LIP (задача поиска)

Если даны два базиса $\mathbf{B}, \mathbf{B}'$ двух изоморфных решеток, то требуется найти ортогональную матрицу $\mathbf{O}$ и унимодулярную матрицу $\mathbf{U}$ такие, что

$$\mathbf{B}' = \mathbf{O} \cdot \mathbf{B} \cdot \mathbf{U}$$

Именно присутствие одновременно двух матриц $\mathbf{O}$ и $\mathbf{U}$ делает эту задачу сложной

Задача LIP (квадратичные формы)

Матрицы $\mathbf{O}, \mathbf{B}'$ используют вещественные коэффициенты $\Rightarrow$ Вместо базиса $\mathbf{B}$ рассмотрим матрицу Грама

$$\mathbf{Q} = \mathbf{B}^T\mathbf{B}$$

$\mathbf{Q}$ — положительно определена и задает квадратичную форму
Если $\mathbf{B}' = \mathbf{O} \cdot \mathbf{B} \cdot \mathbf{U}$, то для $\mathbf{Q} = \mathbf{B}^T\mathbf{B}$ имеем

$$(\mathbf{B}')^T\mathbf{B} = \mathbf{U}^T\mathbf{B}^T\mathbf{O}^T\mathbf{O}\mathbf{B}\mathbf{U} = \mathbf{U}^T\mathbf{B}^T\mathbf{B}\mathbf{U} = \mathbf{U}^T\mathbf{Q}\mathbf{U}$$

Будем считать, что $\mathbf{Q} \sim \mathbf{Q}'$, если $\exists \mathbf{U} \in \mathrm{GL}_n(\mathbb{Z}) : \mathbf{Q}' = \mathbf{U}^T\mathbf{Q}\mathbf{U}$

Задача LIP (квадратичные формы)

Для эквивалентных $\mathbf{Q}, \mathbf{Q}'$ необходимо найти такую унимодулярную матрицу $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$, что $\mathbf{Q}' = \mathbf{U}^T\mathbf{Q}\mathbf{U}$

Класс квадратичных форм, эквивалентных $\mathbf{Q}$, будем обозначать как $[\mathbf{Q}]$

Сложность задачи LIP

- С точки зрения теории: не легче задач GI и LCE
- С точки зрения практики: все существующие алгоритмы **требуют решения задачи SVP**

Лучший алгоритм **на практике** — перебирает все возможные изометрии между множествами коротких векторов изоморфных решеток

Лучший алгоритм **с доказанной сложностью** — использует короткие вектора примальной и дуальной решеток (требует $n^{O(n)}$ времени и памяти)

Сложность SVP и выбор решетки

Пусть $\mathcal{L}$ — решетка в $\mathbb{R}^n$, $\mathrm{Mk}(\mathcal{L}) = \sqrt{n}\det(\mathcal{L})^{1/n}$ — граница Минковского

Задача SVP

Найти кратчайший ненулевой вектор $v \in \mathcal{L}$ длины $\lambda_1(\mathcal{L}) \leq \mathrm{Mk}(\mathcal{L})$

Чем больше значение $f = \frac{\mathrm{Mk}(\mathcal{L})}{\lambda_1(\mathcal{L})}$, тем легче решить задачу SVP

Критерии выбора решетки:

- Малые значения f и $f^* = \frac{\mathrm{Mk}(\mathcal{L}^*)}{\lambda_1(\mathcal{L}^*)}$
- Наличие **эффективного** алгоритма выборки из Гауссова распределения над решеткой

Выбор решетки

QApp

Решетки $\mathbb{Z}^n$ (Hawk)	Решетки Барнса-Уолла BW_n («Облепиха»)
• $f, f^* = \Theta(\sqrt{n})$ • Алгоритмы Гауссовой выборки Кляйна, Пайкерта • SVP решается с помощью BKZ для блока $\beta \leq n/2 + o(n)$ для $n = 1024$ => $\beta \approx 440$	• $f, f^* = \Theta(\sqrt[4]{n})$ • Выборка на основе k-инговой конструкции • SVP решается с помощью BKZ для блока $\beta \approx 2n/3 + o(n)$ для $n = 1024$ => $\beta \approx 682$

Решетки Барнса-Уолла: базовое определение

Решетки Барнса-Уолла (BW) — бесконечная последовательность полноранговых решеток размерности $N = 2^n$ над $\mathbb{Z}[i]$:

$$BW_N = \begin{bmatrix} 1 & 1 \\ 0 & \theta \end{bmatrix}^{\otimes n}$$

где $\theta = 1 + i$, $\otimes n$ — произведение Кронекера.

Или

$$BW_N = \begin{bmatrix} BW_{N/2} & BW_{N/2} \\ \mathbf{O} & \theta \cdot BW_{N/2} \end{bmatrix}$$

где $BW_1 = [1]$

Решетки Барнса-Уолла: k-инговая конструкция

Решётка BW через проверочную конструкцию при $k = 2$:

$L = \theta \cdot \mathrm{BW}_N$, где $\theta = 1 + i$

$\beta = [\mathrm{BW}_N/\theta \cdot \mathrm{BW}_N]$ — множество представителей классов смежности $\mathrm{BW}_N/\theta \cdot \mathrm{BW}_N$

$$\begin{aligned}\mathrm{BW}_{2N} &= \Gamma(L, \beta, k) \\ &= \Gamma(\theta \cdot \mathrm{BW}_N, [\mathrm{BW}_N/\theta \cdot \mathrm{BW}_N], 2) \\ &= \{(u_1 + v; u_2 + v) : u_1, u_2 \in \theta \cdot \mathrm{BW}_N, v \in [\mathrm{BW}_N/\theta \cdot \mathrm{BW}_N]\}\end{aligned}$$

$$u_i + v \in \theta \cdot \mathrm{BW}_N + [\mathrm{BW}_N/\theta \cdot \mathrm{BW}_N] \Rightarrow u_i + v \in \mathrm{BW}_N \Rightarrow \mathrm{BW}_{2N} \subset \mathrm{BW}_N^2$$

Решетки Барнса-Уолла: k-инговая конструкция

Решётка BW через k-инговую конструкцию при $k = 4$:

$L = \theta^2 \cdot \mathrm{BW}_{\frac{N}{2}}$, где $\theta = 1 + i$

$\alpha = [\mathrm{BW}_{\frac{N}{2}}/\theta \cdot \mathrm{BW}_{\frac{N}{2}}]$

$\beta = [\theta \cdot \mathrm{BW}_{\frac{N}{2}}/\theta^2 \cdot \mathrm{BW}_{\frac{N}{2}}]$

$$\begin{aligned}\mathrm{BW}_{2N} &= \Gamma(L, \alpha, \beta, k) \\ &= \Gamma(\theta^2 \cdot \mathrm{BW}_{\frac{N}{2}}, [\mathrm{BW}_{\frac{N}{2}}/\theta \cdot \mathrm{BW}_{\frac{N}{2}}], [\theta \cdot \mathrm{BW}_{\frac{N}{2}}/\theta^2 \cdot \mathrm{BW}_{\frac{N}{2}}], 4) \\ &= \{(m + t_1, m + t_2, m + t_3, m + t_4) : m \in \theta^2 \cdot \mathrm{BW}_{\frac{N}{2}} + [\mathrm{BW}_{\frac{N}{2}}/\theta \cdot \mathrm{BW}_{\frac{N}{2}}], t_i \in \theta^2 \cdot \mathrm{BW}_{\frac{N}{2}} + [\theta \cdot \mathrm{BW}_{\frac{N}{2}}/\theta^2 \cdot \mathrm{BW}_{\frac{N}{2}}], \\ & t_1 + t_2 + t_3 + t_4 \in \theta^2 \cdot \mathrm{BW}_{\frac{N}{2}}\} \subseteq \mathrm{BW}^4_{\frac{N}{2}}\end{aligned}$$

Гауссова выборка из решетки Барнса-Уолла

Для выборки элемента $v \leftarrow \mathcal{D}_{BW_N,\mathbf{c},\Sigma}$, где $N = 2^{2s+1}$, используется итеративный алгоритм, в основе которого лежит k-инговая выборка*

Алгоритм

1. Выборка в решётке $\theta^2 BW_1$, где $BW_1 = \mathbb{Z}[i] \cong \mathbb{Z}^2$(алгоритм Кляйна или Пайкерта)

2. Последовательное применение s раз k-инговой выборки с $k = 4$:

   - $k = 4$:
     Вход: $\theta^2 BW_{N/2} \subsetneq \theta BW_{N/2} \subsetneq BW_{N/2}$, алгоритм выборки $\mathcal{D}_{\theta^2 BW_{N/2},\cdot,\Sigma}$ с $\Sigma > \eta_\epsilon(BW_{N/2})$, $\mathbf{c} \in BW_{N/2}^4 \otimes \mathbb{R}$
     Выход: вектор из BW_{2N}

3. Для $N = 2s$ применяем k-инговую выборку с $k = 2$:

   - $k = 2$:
     Вход: $\theta BW_N \subsetneq BW_N \subsetneq BW_{N/2}^2$, алгоритм выборки $\mathcal{D}_{\theta BW_N,\cdot,\Sigma}$ с $\Sigma > \eta_\epsilon(BW_{N/2}^2)$, $\mathbf{c} \in (BW_{N/2}^2)^2 \otimes \mathbb{R}$
     Выход: вектор из BW_{2N}

* Espitau T., Wallet A., Yu Y. On Gaussian sampling, smoothing parameter //ASIACRYPT 2023-29th International Conference on the Theory and Application of Cryptology and Information Security. – 2023. – С. 1-56.

Гауссова выборка из $[S]$

Алгоритм 1: Выборка $\mathcal{D}_s([S])$

Input: Квадратичная форма $\mathbf{S} \in \mathcal{S}_n^{>0}$, соответствующая базису $\mathbf{B}$ решётки $\mathcal{L}$, параметр $s \geq \max\{\lambda_n(\mathbf{S}), \eta_\epsilon(\mathbf{S})\}$

Output: Квадратичная форма $\mathbf{P} = \mathbf{U}^T\mathbf{S}\mathbf{U}$, изоморфизм $\mathbf{U}$

1: $\mathbf{Y} \leftarrow (\mathbf{y}_1, \ldots, \mathbf{y}_n) \in \mathcal{D}^n_{\mathbf{S},0,s}$ // n линейно независимых векторов решётки

2: Вычислить эквивалентный базис $\mathbf{R}$ и матрицу перехода $\mathbf{U}$ // **EqBasis**$(\mathbf{B}, \mathbf{Y}) \to \mathbf{R} = \mathbf{B}\mathbf{U}^{-1}$

3: $\mathbf{P} \leftarrow \mathbf{R}^T\mathbf{R}$ // $\mathbf{P} = \mathbf{U}^T\mathbf{S}\mathbf{U}$

4: Вернуть $(\mathbf{P}, \mathbf{U})$

Идея

- Исходная квадратичная форма $\mathbf{S}$ — короткая
- Для решёток BW_N выполняется $s > \lambda_N(\mathbf{S}) \sim \sqrt{N}$
- Эффективная выборка «коротких» векторов возможна из $\mathbf{S}$, но невозможна из $\mathbf{P}$ (без знания матрицы $\mathbf{U}$)

Схема цифровой подписи «Облепиха»

QApp

Формирование ключей

На вход: системный параметр N, $\mathbf{S} = \mathbf{B}^*\mathbf{B}$

На выход: $(\mathrm{sk}, \mathrm{vk})$, где

- sk — секретный ключ (унимодулярная матрица $\mathbf{U}$, преобразующая базис исходной решетки)
- vk — открытый ключ (квадратичная форма $\mathbf{P} = \mathbf{U}^T\mathbf{S}\mathbf{U}$ изоморфной решетки)

Алгоритм 2: Алгоритм KeyGen

Input: системный параметр N, $\mathbf{S} = \mathbf{B}^*\mathbf{B}$

Output: $(\mathrm{sk}, \mathrm{vk})$ — пара секретный/открытый ключ

1: Выбираем $\mathbf{P} \leftarrow \mathcal{D}_s([\mathbf{S}])$ вместе с $\mathbf{U}$, такой что $\mathbf{P} = \mathbf{U}^T\mathbf{S}\mathbf{U}$

2: Вернуть $(\mathrm{sk}, \mathrm{vk}) = (\mathbf{U}, \mathbf{P}) \in \mathrm{GL}_N(\mathbb{G}) \times \mathbb{G}^{N\times N}$

Схема цифровой подписи «Облепиха»

QApp

Формирование подписи

На вход: сообщение m и секретный ключ sk

На выход: вектор σ, близкий к $\mathbf{t}$ относительно формы $\mathbf{P}$, полученный с помощью квадратичной формы $\mathbf{S}$ и секретного преобразования $\mathbf{U}$

Алгоритм 3: Алгоритм Sign

Input: сообщение m, секретный ключ $\text{sk} = \mathbf{U}$

Output: подпись $\sigma \in BW_N$

1: $\mathbf{t} \leftarrow \mathcal{H}(m)$

2: выбираем $\sigma' \leftarrow \mathcal{D}_{\mathbf{S},\rho/\sqrt{N},\mathbf{Ut}}$

3: $\sigma \leftarrow \mathbf{U}^{-1}\sigma'$

4: Вернуть σ

Схема цифровой подписи «Облепиха»

QApp

Проверка подписи

На вход: сообщение m, открытый ключ vk и подпись σ
На выход: подпись принимается в случае принадлежности σ решётке BW_n и выполнении $\|\mathbf{t} - \sigma\|_{\mathbf{P}} \leq \rho$, в противном случае, отклоняется

Алгоритм 4: Алгоритм Verify

Input: открытый ключ vk $= \mathbf{P}$, сообщение m и подпись σ
Output: принять/отклонить подпись

1: $\mathbf{t} \leftarrow \mathcal{H}(m)$
2: **if** $\sigma \in BW_N$ и $\|\mathbf{t} - \sigma\|_{\mathbf{P}} \leq \rho$ **then**
3: Вернуть: принять подпись
4: **else**
5: Вернуть: отклонить подпись
6: **end if**

Атаки на схему

QApp

Восстановление секретного ключа

Восстановление секретного ключа = решение задачи search-LIP, то есть нахождение **любой** матрицы $\mathbf{V} \in \mathrm{GL}(\mathbb{Z})$ такой, что $\mathbf{P} = \mathbf{V}^T\mathbf{S}\mathbf{V}$

- Лучшая атака требует решение SVP $\Rightarrow$ уровень стойкости схемы = сложность решения SVP (core-SVP)
- Hull-атака — рассмотрение задачи SVP в $\mathcal{L} \cap s\mathcal{L}^*$. Для решеток с $\det \mathcal{L} = 1$ не облегчает перебор. Решетки Барнса-Уолла размерности $N = 2^n$ для нечетных n — унимодулярны

Подделка подписи

Подделка подписи — нахождение близкого вектора к $\mathcal{H}(m)$

- Выборка из Гауссова распределения $\Rightarrow$ редукция базиса
- Решение задачи BDD для решетки Барнса-Уолла по квадратичной форме $\mathbf{P}$ $\Rightarrow$ решение SVP

Сложность SVP и параметры схемы

QApp

Сложность лучшего алгоритма решения SVP для размерности β:

- Классический алгоритм: $\approx 2^{0.292\beta}$
- Квантовый алгоритм: $\approx 2^{0.265\beta}$

Схема	Размер подписи, байт	Классическая стойкость	Квантовая стойкость
Falcon	666	120	108
Hawk	555	≈ 121	≈ 110
«Облепиха»	≈ 1000	≈ 138	≈ 125
Dilithium	4595	252	229
Falcon	1280	273	248
Hawk	1221	≈ 252	≈ 229
«Облепиха»	≈ 2000	≈ 258	≈ 234

Открытые вопросы

QApp

- Какова эффективность Hull-атак в контексте $\mathbb{Z}[i]$ для решеток Барнса-Уолла размерности 2^n, где n — четное?
- EUF-CMA стойкость схемы основана на задаче ΔLIP. Насколько сложна эта задача?
- Как компактно представить открытый ключ?

Соавторы доклада

QApp

Антон Леевик

Криптограф-исследователь

Екатерина Малыгина

Криптограф-исследователь, PhD

Евгений Мельничук

Криптограф-исследователь

Денис Набоков

Специалист по защите информации

QApp

Антон Леевик
Криптограф-исследователь

aleevik@qapp.tech
@f_o_rest

qapp.tech

Участник