РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

КуАпп

От решёток Барнса–Уолла к стандарту: текущий статус разработки постквантовой схемы «Облепиха»

Артём Кунинец

Криптограф-исследователь «КуАпп»

По следам предыдущего года

РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

КуАпп

На Рускрипто 2025 была представлена «Облепиха» — постквантовая схема цифровой подписи на решетках

Представлено на Рускрипто 2025:

- Конструкция схемы на основе задачи LIP
- Решетки Барнса-Уолла и алгоритм гауссовой выборки
- Предварительный анализ стойкости схемы и предварительные параметры

За прошедший год выполнена следующая работа:

- Разработано теоретическое доказательство стойкости
- Осуществлена переоценка параметров схемы
- Модифицированы алгоритмы схемы подписи

LIP, $\triangle$LIP, ac-$\triangle$LIP

РусКрипто XXVIII научно-практическая конференция

КуАпп

LIP (поиск)	$\triangle\text{LIP}^{Q_0,Q_1}$ (различение)	ac-$\triangle\text{LIP}^{Q_0,Q_1}$ (средний случай)
Через базисы **Дано:** B, B' $$B' = OBU$$ **Найти:** $O \in O_n(\mathbb{R}),\ U \in GL_n(\mathbb{Z})$ **Через квадратичные формы** **Дано:** Q, Q' $$Q' = U^\top QU$$ **Найти:** $U \in GL_n(\mathbb{Z})$	**Дано:** $$Q' \xleftarrow{\$} [Q_b]$$ где Q_0, Q_1. **Найти:** $b \in \{0,1\}$	**Дано:** Q_0, Q_1, s и $$Q' \xleftarrow{\$} D_s([Q_b])$$ **Найти:** $b \in \{0,1\}$

Обозначения:

- $[Q] = \{\, U^\top QU \mid U \in GL_n(\mathbb{Z}) \,\}$ — класс эквивалентности квадратичной формы
- $D_s([Q])$ — гауссово распределение над формами из класса $[Q]$ с шириной s

Две решётки в конструкции схемы

Решётки Λ_S и Λ_Q соответствуют квадратичным формам S и Q

Решётка $\Lambda_{Q^{-1}}$ — дуальная Λ_Q

Λ_S

Используется в схеме подписи

- с её помощью **подписывается сообщение**
- существует алгоритм **гауссовой выборки**

Λ_Q

Используется в доказательстве стойкости

- S и Q^{-1} **изоморфны** над $\mathbb{Q}_p$ и над $\mathbb{R}$, но необязательно над $\mathbb{Q}$
- $[S] \neq [Q^{-1}]$
- существует **плотная подрешётка**

Ducas L., Van Woerden W. *On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography* // Advances in Cryptology -- EUROCRYPT 2022

Новые решётки Λ_S и Λ_Q

РусКрипто XXVIII научно-практическая конференция

КуАпп

Исходная решётка: решётка Барнса-Уолла BW_{2^n} размерности N с базисом $B(BW_{2^n})$, R — ее квадратичная форма

Λ_S

Решётка для подписи

Построение:

$$\Lambda_S = gBW_{2^n} \oplus (g+1)BW_{2^n}$$

Базис:

$$B(\Lambda_S) = \begin{pmatrix} gB(BW_{2^n}) & 0 \\ 0 & (g+1)B(BW_{2^n}) \end{pmatrix}$$

Квадратичная форма:

$$S = \begin{pmatrix} g^2R & 0 \\ 0 & (g+1)^2R \end{pmatrix}$$

Λ_Q

Решётка для стойкости

Построение:

$$\Lambda_{Q^{-1}} = BW_{2^n} \oplus g(g+1)BW_{2^n}$$

Базис:

$$B(\Lambda_{Q^{-1}}) = \begin{pmatrix} B(BW_{2^n}) & 0 \\ 0 & g(g+1)B(BW_{2^n}) \end{pmatrix}$$

Квадратичная форма:

$$Q^{-1} = \begin{pmatrix} R & 0 \\ 0 & g^2(g+1)^2R \end{pmatrix}$$

Новый алгоритм гауссовой выборки для Λ_S

РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

КуАпп

Шаг 1. Независимо сэмплируем

$$x_1 \xleftarrow{\$} D_{gBW_N,s} \qquad x_2 \xleftarrow{\$} D_{(g+1)BW_N,s}$$

Шаг 2. Собираем итоговый вектор

$$x = (x_1, x_2) \in gBW_N \oplus (g+1)BW_N$$

Алгоритм гауссовой выборки	Сложность алгоритма	Статистическое расстояние	Сглаживающий параметр
Алгоритм Кляйна	$O(N^2)$	ε	$\eta_\Sigma(\mathrm{BW}_N)$
n-уровневая квадратичная выборка	$O(N)$	2ε	$\eta_\Sigma((1+i)^n\mathrm{BW}_1)$
Итеративная k-инговая выборка	$O\left(2^{\frac{1}{2}\log^2 N}\right)$	2ε	$\eta_\Sigma((1+i)^n\mathrm{BW}_1)$

Kuninets A. et al. On the construction of Barnes-Wall lattices and their application in cryptography //Cryptology ePrint Archive. – 2025

Методы выбора матрицы U

Случайное блуждание

- высокая скорость работы
- сложно обосновать стойкость

Почти равномерная генерация при помощи алгоритма Евклида

- теоретически случаен
- практически недееспособен

Генерация через HNF

- сочетается с доказательством стойкости
- реализуем на практике, но скорость низкая

Из рассмотренных методов **окончательный выбор** делается в пользу **генерации через HNF**

Схема подписи «Облепиха»

РусКрипто XXVIII научно-практическая конференция

КуАпп

Генерация ключей

- Генерация формы $P \xleftarrow{\$} D_s[S]$ вместе с унимодулярной матрицей U
- Открытый ключ: P; секретный ключ: U

Подпись

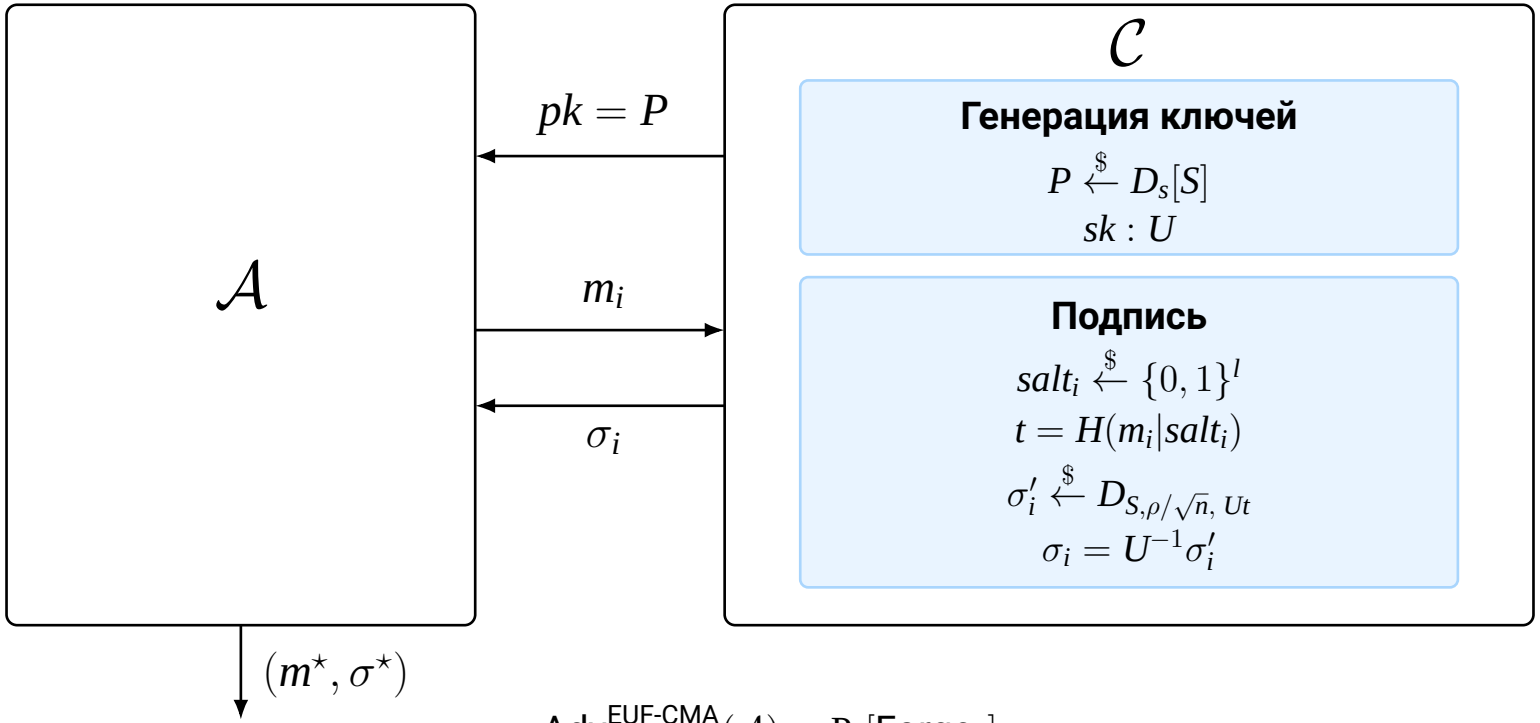
- Вычисляем $t = H(m|salt) \in \mathbb{T}_q$ — хэш сообщения
- Выбираем $\sigma_1 \xleftarrow{\$} D_{S,\rho/\sqrt{n},Ut}$
- Подпись: $(\sigma = U^{-1}\sigma_1, salt)$

Проверка

- Вычисляем $t = H(m|salt)$
- Проверяем неравенство $\|\sigma - t\|_P \leq \rho$
- Если условие выполняется — подпись принимается

Теоретическое обоснование:

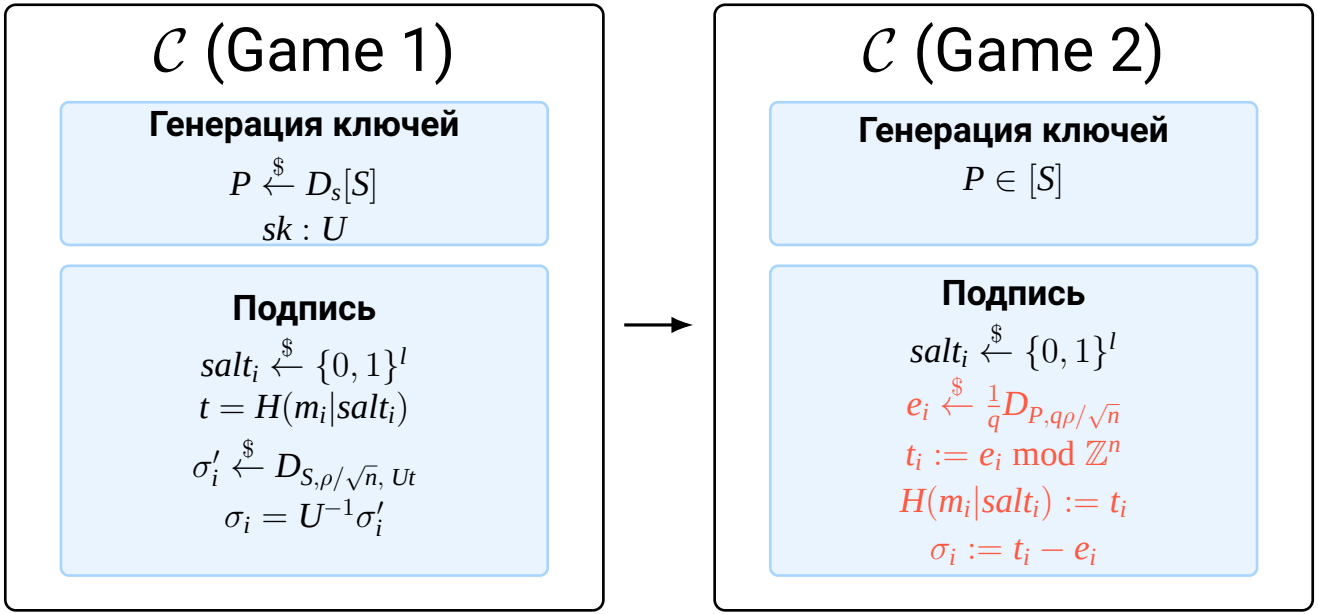
$Game_1$



$$\mathrm{Adv}_{\Sigma}^{\text{EUF-CMA}}(\mathcal{A}) = \Pr[\text{Forge}_1]$$

Теоретическое обоснование:

$Game_1 \to Game_2$

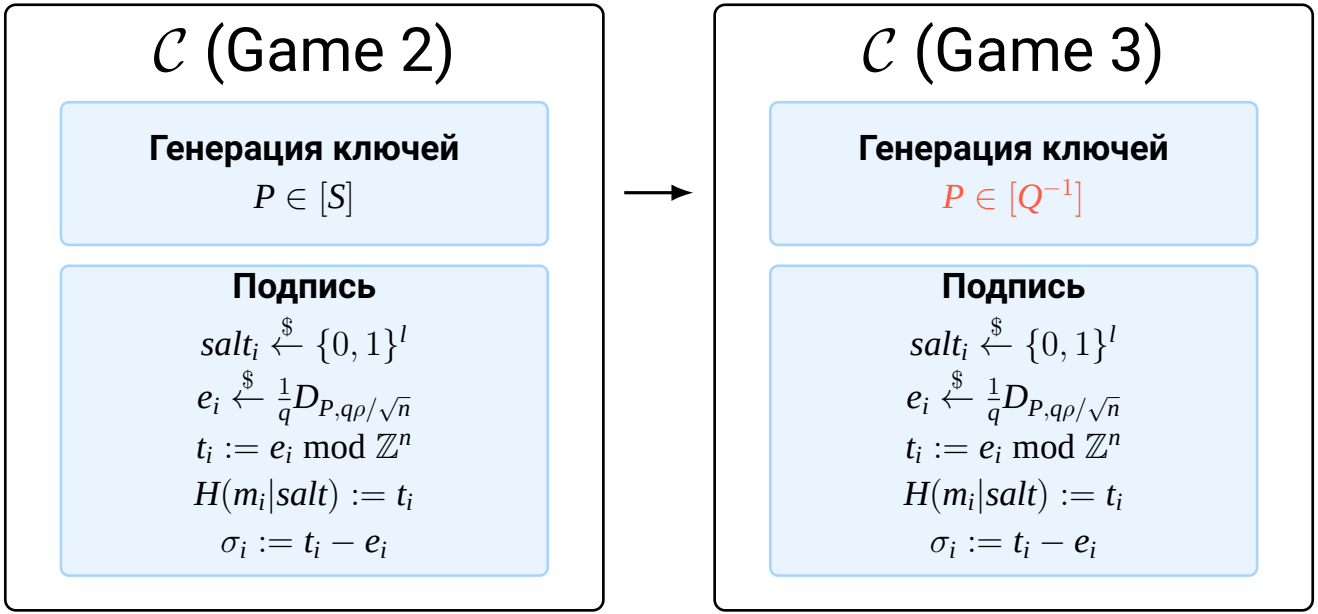


$$|\Pr[\text{Forge}_1] - \Pr[\text{Forge}_2]| \le q_s \cdot \varepsilon_{\text{smooth}} + \varepsilon_{\text{RO}}$$

$$\varepsilon_{\text{RO}} \le \left(q_s q_h + \frac{q_s^2}{2}\right) \cdot 2^{-\ell}$$

Теоретическое обоснование:

$Game_2 \to Game_3$



$$|\Pr[\text{Forge}_2] - \Pr[\text{Forge}_3]| \leq \text{Adv}_{\text{ac-}\Delta\text{LIP}^{S,Q^{-1}}}(\mathcal{B})$$

$$\Pr[\text{Forge}_3] \leq 2^{-N}$$

Теоретическое обоснование: итоговая оценка

РусКрипто XXVIII научно-практическая конференция

КуАпп

$$\mathrm{Adv}_{\mathcal{A}}^{\text{EUF-CMA}} \leq \underbrace{|\Pr[\text{Forge}_1] - \Pr[\text{Forge}_2]|}_{\text{вероятность обнаружения симуляции}} + \underbrace{|\Pr[\text{Forge}_2] - \Pr[\text{Forge}_3]|}_{\mathrm{Adv}_{\mathcal{B}}^{\text{ac-}\Delta\text{LIP}}} + \underbrace{\Pr[\text{Forge}_3]}_{\text{вероятность подписи в разряженной решетке}} + \underbrace{\frac{(q_h + q_s)^2}{2q^{2N}}}_{\text{вероятность коллизии}}$$

$$\mathrm{Adv}_{\Sigma}^{\text{EUF-CMA}}(\mathcal{A}) \leq q_s \cdot \varepsilon_{\text{smooth}} + \left(q_s q_h + \frac{q_s^2}{2}\right) \cdot 2^{-\ell} + \mathrm{Adv}_{\text{ac-}\Delta\text{LIP}^{S,Q^{-1}}}(\mathcal{B}) + \frac{(q_h + q_s)^2}{2q^{2N}} + 2^{-N}$$

Сложность Δ-LIP

Простое решение Δ-LIP

Если у двух классов решёток различаются **легко вычислимые инварианты**,
то задачу различения можно решить тривиально

Арифметические инварианты

- определитель
- род решётки
- чётность
- НОД коэффициентов

вычисляются эффективно

Геометрические инварианты

- минимумы решетки
- контактное число
- Тета-ряды $\Theta_Q(q) = \sum_{l \geq 0} N_l q^l$,
  $N_l = |\{x_Q \in \mathbb{Z}^n : \|x\|_Q = l\}|$

вычисляются сложно

Для решёток Λ_S и Λ_Q **арифметические инварианты специально выбраны совпадающими**,
поэтому задачу Δ-LIP нельзя решить просто

Анализ практической стойкости

РусКрипто XXVIII научно-практическая конференция

КуАпп

Hull-атаки

- Решётки Барнса-Уолла размерности $N = 2^n$ для чётных n устойчивы к hull-атакам[1]
- Решётки Λ_S также устойчивы

Оценка стойкости схемы

- практическая стойкость оценивается через **сложность решения SVP**
- размер блока BKZ оценивается в модели **Core-SVP**
- для оценок используются эвристики для случайных решёток

Уровень	$\dim \Lambda_S$	g	s_{pk}	s_{sig}	ρ	q	Секр. ключ, КБ	Откр. ключ, КБ	Подпись, КБ
192	1024	31	798	233	7456	50	1053	2195	721

[1] Kuninets A. et al. On the construction of Barnes-Wall lattices and their application in cryptography //Cryptology ePrint Archive. – 2025

Итоги и дальнейшая работа

РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

КуАпп

Сделано

- разработано формальное доказательство стойкости в модели **ROM**
- произведён практический анализ стойкости схемы
- определены параметры схемы **«Облепиха»**

Дальнейшая работа

- разработка теоретического доказательства стойкости в модели **QROM**
- уменьшение размера **подписи** и **открытого ключа**
- уточнение практических параметров с учётом специфики решёток, используемых в схеме

Соавторы доклада

Артём Кунинец

Криптограф-исследователь

Антон Леевик

Криптограф-исследователь

Екатерина Малыгина

Криптограф-исследователь

к.ф.-м.н.

Евгений Мельничук

Криптограф-исследователь

Спасибо за внимание!

РусКрипто XXVIII научно-практическая конференция

КуАпп

Артём Кунинец

Криптограф-исследователь «КуАпп»

akuninec@tech.com

@Arkaft

qapp.tech