# Цифровая подпись на алгебраических решётках

Елена Киршанова, Никита Колесников, Екатерина Малыгина,
Семён Новосёлов

Заседание рабочей группы ТК 26 "Постквантовые криптографические механизмы"

**Балтийский федеральный университет имени Иммануила Канта**

# Основные критерии дизайна

- наличие док-ва безопасности
- простота в реализации
- возможность выбора параметров для разных уровней безопасности
- возможность реализации быстрой арифметики

# 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: Bai-Gabraith, Dilithium, Tesla, наше предложение

Преимущество: простая реализация

Недостаток: более длинные подписи

## Наше предложение

1. Взять за основу эффективные конструкции Фиат-Шамира (Dilithium)
2. Упростить процедуру генерации ключа (за счет меньшего числа выборок)
3. Адаптировать параметры и док-во схемы

Мы используем

- $R = \mathbb{Z}[x]/(x^n + 1), n = 256,\ R_q = R/(qR), q = 2^{23}$
- задачу LWR (Learning with Rounding) для безопасности ключевой пары. Это основное отличие от Dilithium.
- LWR сводится к задаче нахождения короткого вектора в решётках

# Конструкция (упрощено)

$B_w = \{\mathbf{x} \in \{-1, 0, 1\}^n \mid \|\mathbf{x}\|^2 = w\}$. MSB$(x, \tau)$ – $\tau$ старших бит $x$

$\mathcal{H} : \{0,1\}^\star \to B_w$ – криптографическая хэш-функция.

$R -$ кольцо, $R \simeq \mathbb{Z}^n$, $R_q = R/(qR), q = 2^{23}, p = 2^{19}, k = 4, \ell = 3, \tau = 2$

## Конструкция (упрощено)

$B_w = \{\mathbf{x} \in \{-1, 0, 1\}^n \mid \|\mathbf{x}\|^2 = w\}$. MSB$(x, \tau)$ – $\tau$ старших бит $x$

$\mathcal{H} : \{0,1\}^\star \to B_w$ – криптографическая хэш-функция.

$R -$ кольцо, $R \simeq \mathbb{Z}^n$, $R_q = R/(qR), q = 2^{23}, p = 2^{19}, k = 4, \ell = 3, \tau = 2$

I. KeyGen :

1. $\mathbf{A} \leftarrow R_q^{k \times \ell}$
2. $\mathbf{s} \leftarrow [-4, 4]^\ell$
3. $\mathbf{t} = \text{Round}\left(\frac{p}{q} \cdot \mathbf{As}\right)$
4. sk $= \mathbf{s}$, vk $= (\mathbf{A}, \mathbf{t})$

## Конструкция (упрощено)

$B_w = \{\mathbf{x} \in \{-1, 0, 1\}^n \mid \|\mathbf{x}\|^2 = w\}$. MSB$(x, \tau)$ – $\tau$ старших бит $x$

$\mathcal{H} : \{0,1\}^\star \to B_w$ – криптографическая хэш-функция.

$R$ – кольцо, $R \simeq \mathbb{Z}^n$, $R_q = R/(qR), q = 2^{23}, p = 2^{19}, k = 4, \ell = 3, \tau = 2$

### I. KeyGen :

1. $\mathbf{A} \leftarrow R_q^{k \times \ell}$
2. $\mathbf{s} \leftarrow [-4, 4]^\ell$
3. $\mathbf{t} = \text{Round}\left(\frac{p}{q} \cdot \mathbf{As}\right)$
4. sk $= \mathbf{s}$, vk $= (\mathbf{A}, \mathbf{t})$

### II. Sign(sk, $m$) :

1. $\mathbf{y} \leftarrow [-q/8, q/8]^\ell$
2. $\mathbf{c} = \mathcal{H}\left(\text{MSB}(\mathbf{A} \cdot \mathbf{y}, \tau), m\right)$
3. $\mathbf{z} = \mathbf{y} + \mathbf{sc}$
4. $\sigma = (\mathbf{c}, \mathbf{z})$

## Конструкция (упрощено)

$B_w = \{\mathbf{x} \in \{-1, 0, 1\}^n \mid \|\mathbf{x}\|^2 = w\}$. MSB$(x, \tau)$ – $\tau$ старших бит $x$

$\mathcal{H} : \{0,1\}^\star \to B_w$ – криптографическая хэш-функция.

$R$ – кольцо, $R \simeq \mathbb{Z}^n$, $R_q = R/(qR), q = 2^{23}, p = 2^{19}, k = 4, \ell = 3, \tau = 2$

### I. KeyGen :

1. $\mathbf{A} \leftarrow R_q^{k \times \ell}$
2. $\mathbf{s} \leftarrow [-4, 4]^\ell$
3. $\mathbf{t} = \text{Round}\left(\frac{p}{q} \cdot \mathbf{As}\right)$
4. sk $= \mathbf{s}$, vk $= (\mathbf{A}, \mathbf{t})$

### II. Sign(sk, $m$) :

1. $\mathbf{y} \leftarrow [-q/8, q/8]^\ell$
2. $\mathbf{c} = \mathcal{H}\left(\text{MSB}(\mathbf{A} \cdot \mathbf{y}, \tau), m\right)$
3. $\mathbf{z} = \mathbf{y} + \mathbf{sc}$
4. $\sigma = (\mathbf{c}, \mathbf{z})$

### III. Verify(vk, $m, \sigma = (\mathbf{c}, \mathbf{z})$) :

1. $\mathbf{w} = \mathbf{Az} - \mathbf{t} \cdot \frac{q}{p} \cdot \mathbf{c}$
2. $\mathbf{c}' = \mathcal{H}(\text{MSB}(\mathbf{w}, \tau)), m)$
3. Если $\mathbf{c}' == \mathbf{c}$ и $\|\mathbf{z}\|_\infty$ – мала
   **return** “Accept”
   Иначе **return** “Reject”

## Конструкция (упрощено)

$B_w = \{\mathbf{x} \in \{-1, 0, 1\}^n \mid \|\mathbf{x}\|^2 = w\}$. MSB$(x, \tau)$ – $\tau$ старших бит $x$

$\mathcal{H} : \{0,1\}^\star \to B_w$ – криптографическая хэш-функция.

$R$ – кольцо, $R \simeq \mathbb{Z}^n$, $R_q = R/(qR), q = 2^{23}, p = 2^{19}, k = 4, \ell = 3, \tau = 2$

I. KeyGen :

1. $\mathbf{A} \leftarrow R_q^{k \times \ell}$
2. $\mathbf{s} \leftarrow [-4, 4]^\ell$
3. $\mathbf{t} = \text{Round}\left(\frac{p}{q} \cdot \mathbf{As}\right)$
4. sk $= \mathbf{s}$, vk $= (\mathbf{A}, \mathbf{t})$

II. Sign(sk, $m$) :

1. $\mathbf{y} \leftarrow [-q/8, q/8]^\ell$
2. $\mathbf{c} = \mathcal{H}\left(\text{MSB}(\mathbf{A} \cdot \mathbf{y}, \tau), m\right)$
3. $\mathbf{z} = \mathbf{y} + \mathbf{sc}$
4. $\sigma = (\mathbf{c}, \mathbf{z})$

III. Verify(vk, $m, \sigma = (\mathbf{c}, \mathbf{z})$) :

1. $\mathbf{w} = \mathbf{Az} - \mathbf{t} \cdot \frac{q}{p} \cdot \mathbf{c}$
2. $\mathbf{c}' = \mathcal{H}(\text{MSB}(\mathbf{w}, \tau)), m)$
3. Если $\mathbf{c}' == \mathbf{c}$ и $\|\mathbf{z}\|_\infty$ – мала
   **return** “Accept”
   Иначе **return** “Reject”

Корректность:

- $\mathbf{c}' == \mathbf{c}$ т.к. MSB$(\mathbf{w}, \tau) =$ MSB$(\mathbf{Ay}, \tau)$ (с большой вероятностью).
- $\|\mathbf{z}\|_\infty$ – мала по построению

# Безопасность

$$R - \text{кольцо}, R \simeq \mathbb{Z}^n. \quad R_q = R/(qR), q = 2^\nu, p = 2^\mu$$

Задача Short Integer Solution (SIS):

Дано: $\mathbf{A} \in R_q^{k \times \ell}, \mathbf{t} \in R_q^\ell$ т.ч. $\mathbf{Az} = \mathbf{t}$

Найти: $\mathbf{z}$, т.ч. $\|\mathbf{z}\|_\infty \ll q$.

## Безопасность

$$R - \text{кольцо}, R \simeq \mathbb{Z}^n. \quad R_q = R/(qR), q = 2^\nu, p = 2^\mu$$

Задача Short Integer Solution (SIS):

$$\text{Дано: } \mathbf{A} \in R_q^{k \times \ell}, \mathbf{t} \in R_q^\ell \text{ т.ч. } \mathbf{Az} = \mathbf{t}$$

$$\text{Найти: } \mathbf{z}, \text{ т.ч. } \|\mathbf{z}\|_\infty \ll q.$$

Задача Learning With Rounding (LWR):

$$\text{Дано: } \mathbf{A} \in R_q^{k \times \ell}, \mathbf{t} = \mathsf{Round}\left(\frac{p}{q} \cdot \mathbf{As}\right) \in R_p^\ell$$

$$\text{Найти: } \mathbf{s}.$$

SIS + LWR $\Longrightarrow$ подпись, стойкая к атакам UF-CMA в модели квантового случайного оракула (QROM).

# Параметры

- SIS, LWR $\geq$ задача нахождения короткого вектора (SVP) в $\mathcal{L}, \mathcal{L}^{\perp}$
- предложенные параметры достигают (консервативно)

  классического уровня безопасности в 109 бит.
  SVP в размерности $\beta$ решается за время $2^{0.292\beta+16.4}$ [ACD+ 18]

  квантовго уровня безопасности в 85 бит
  SVP в размерности $\beta$ решается за время $2^{0.265\beta}$ в модели QRAM, [KMPS19]

| \|sk\| | \|vk\| | \|sig\| | KeyGen | Sign | Verify |
|---|---|---|---|---|---|
| 3k | 2.4k | 1.9k | 2.08M | 24.6M | 2.6M |

$\star$ размеры ключей/подписи – в байтах

$\star\star$ время работы – в тактах Intel Xeon(R) E-2146G 3.50GHz

# ToDo

- Оптимизация реализации
- Несколько наборов параметров для разных уровней безопасности

Детальное описание схемы и док-во:

`https://crypto-kantiana.com/main_papers/main_Signature.pdf`

Реализация (обновляется):

`https://github.com/ElenaKirshanova/pqc_LWR_signature`

# Ссылки


- [ACD+18] M.R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E.W. Postlethwaite, F. Virdia, T. Wunderer. Estimate all the lwe, ntru schemes!
- [GPV08] G. Gentry, C. Peikert, V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions.
- [FS87] A. Fiat, Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems
- [Dil] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, D. Stehle. Crystals-dilithium: A lattice-based digital signature scheme.
- [BDGL] A. Becker, L. Ducas, N. Gama, T. Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving.
- [KMPS19] E. Kirshanova, E. Martensson, E.W. Postlethwaite, S.R. Moulik. Quantum Algorithms for the Approximate k-List Problem and their Application to Lattice Sieving