

Полный криптоанализ схемы подписи pqsigRM

4 июня 2026

Андрей Рубенков

- ▶ Парадигма **Hash-and-Sign** на кодах: схема CFS (Courtois–Finiasz–Sendrier, 2001) требует кода с большим кодовым расстоянием.
- ▶ Высокоскоростные коды Гоппы $\Rightarrow$ различитель; низкоскоростные $\Rightarrow$ проверка подписи непрактична.
- ▶ **pqsigRM** (Lee и др., 2020) — модификация кодов Рида–Маллера, подана на дополнительный раунд NIST и в KpqC.
- ▶ Атака Debris-Alazard–Loisel–Vasseur (ISIT 2024) требует $\sim 10^5$ подписей для наименьших размерностей.

Цель работы

Построить **структурную атаку** (только по открытому ключу) для всех параметров, предлагаемых авторами pqsigRM.

1. Коды в основе схемы подписи pqsigRM
2. Структурная атака при помощи произведения Адамара
3. Структурная атака с накоплением слов минимального веса

[1/3] Коды в основе схемы подписи pqsigRM

- ▶ $\mathbb{F}_2 = \{0, 1\}$ — поле из двух элементов $\mathbb{F}_2^n$ — линейное пространство векторов длины n над полем $\mathbb{F}_2$.
- ▶ **Линейный блочный $[n, k]$ -код** — линейное подпространство размерности k пространства $\mathbb{F}_2^n$.
- ▶ **Порождающая матрица** $[n, k]$ -кода $\mathcal{C}$ — $(k \times n)$ -матрица, строками которой являются базисные векторы $\mathcal{C}$.
- ▶ Любой $[n, k]$ -код $\mathcal{C}$ совпадает с линейной оболочкой строк своей порождающей матрицы $G_{\mathcal{C}}$, т.е.

$$\mathcal{C} = \{a \cdot G_{\mathcal{C}} \mid a \in \mathbb{F}_2^k\}.$$

- ▶ **Носитель** вектора: $\text{supp}(x) = \{i \mid x_i \neq 0\}$. Носитель кода: $\text{supp}(\mathcal{C}) = \bigcup_{c \in \mathcal{C}} \text{supp}(c)$.

- ▶ $\mathcal{RM}(r, m)$ — $[2^m, \sum_{i=0}^r \binom{m}{i}]$ -код, состоящий из векторов значений всех булевых функций от m переменных степени $\leq r$.
- ▶ Конструкция Плоткина:

$$\mathcal{RM}(r, m) = \{(u \mid u + v) : u \in \mathcal{RM}(r, m-1), v \in \mathcal{RM}(r-1, m-1)\}$$

- ▶ Порождающая матрица $G(r, m)$ задается рекурсивно:

$$G(r, m) = \left(\begin{array}{c|c} G(r, m-1) & G(r, m-1) \\ \hline 0 & G(r-1, m-1) \end{array} \right)$$

- ▶ Для $[n, k]$ -кода $\mathcal{C}$ с порождающей матрицей G и вектора $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_u) \in \mathbb{F}_2^u$ определим $[un, k]$ -код $\mathcal{C}_{(\alpha_1, \alpha_2, \dots, \alpha_u)}$ с порождающей матрицей:

$$G_\alpha = (G_{\alpha_1} | G_{\alpha_2} | \dots | G_{\alpha_u}),$$

где $G_{\alpha_i} = G$ при $\alpha_i = 1$ и $G_{\alpha_i} = 0^{k \times n}$ при $\alpha_i = 0$.

- ▶ Для $\mathcal{RM}(r, m)$ при $r > 1, m > 2$ выполнено:

$$\begin{aligned} \mathcal{RM}(r, m) &= \mathcal{RM}_{(1,1)}(r, m-1) + \mathcal{RM}_{(0,1)}(r-1, m-1) = \\ &= \mathcal{RM}_{(1,1,1,1)}(r, m-2) + \mathcal{RM}_{(0,1,0,1)}(r-1, m-2) + \\ &\quad + \mathcal{RM}_{(0,0,1,1)}(r-1, m-2) + \mathcal{RM}_{(0,0,0,1)}(r-2, m-2) \end{aligned}$$

- ▶ Для любых $\alpha, \beta \in \mathbb{F}_2^u$ выполняется $\mathcal{C}_\alpha + \mathcal{C}_\beta = \mathcal{C}_{\alpha+\beta} + \mathcal{C}_\beta$.

$$\left(\begin{array}{cc|cc} G(r, m-2)^{\sigma_1^p} & G(r, m-2)^{\sigma_1^p} & G(r, m-2)^{\sigma_1^p} & G(r, m-2)^{\sigma_1^p} \\ 0 & G(r-1, m-2) & 0 & G(r-1, m-2) \\ \hline 0 & 0 & G(r-1, m-2) & G(r-1, m-2) \\ 0 & 0 & 0 & G(r-2, m-2)^{\sigma_2^p} \end{array} \right)$$

- ▶ Подстановки σ_i^p генерируются сначала выбором $p \leq 2^{m-2}$, а затем созданием подстановки случайных p координат.
- ▶ Определим $\mathcal{PQRM}_{\sigma_1, \sigma_2}(r, m)$ -код следующего вида:

$$\begin{aligned} \mathcal{PQRM}_{\sigma_1, \sigma_2}(r, m) = & \mathcal{RM}_{(1,1,1,1)}^{\sigma_1}(r, m-2) + \mathcal{RM}_{(0,1,0,1)}(r-1, m-2) + \\ & + \mathcal{RM}_{(0,0,1,1)}(r-1, m-2) + \mathcal{RM}_{(0,0,0,1)}^{\sigma_2}(r-2, m-2) \end{aligned}$$

¹Modified pqsigRM: RM Code-Based Signature Scheme. Y. Lee [и др.]. 2020.

Секретный ключ

- ▶ $G_{\sigma_1, \sigma_2}(r, m)$ — порождающая матрица кода $\mathcal{PQR}\mathcal{M}_{\sigma_1, \sigma_2}(r, m)$

Дано

- ▶ Открытый ключ $G'_{\sigma_1, \sigma_2}(r, m) = M \cdot G_{\sigma_1, \sigma_2}(r, m) \cdot P$

Найти

- ▶ Такие P' , σ'_1 и σ'_2 , что $M' \cdot G'_{\sigma_1, \sigma_2}(r, m) \cdot P' = G_{\sigma'_1, \sigma'_2}(r, m)$

[2/3] Структурная атака при помощи произведения Адамара

- ▶ Предложена В.М. Сидельниковым в 1994 году как альтернатива криптосистеме Мак-Элиса.
- ▶ Оригинальная криптосистема строится на основе кодов Рида–Маллера $\mathcal{RM}(r, m)$.
- ▶ Были предложены структурные атаки Миндера–Шокроллахи² и Чижова–Бородина³.

²Minder L., Shokrollahi A. Cryptanalysis of the Sidelnikov Cryptosystem. 2007.

³Бородин М., Чижов И. Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида–Маллера. 2014

- ▶ **Произведение Адамара** векторов $c, b \in \mathbb{F}_2^n$:

$$c \circ b = (c_1 b_1, \dots, c_n b_n).$$

- ▶ **Произведение Адамара кодов** $\mathcal{C}$ и $\mathcal{B}$:

$$\mathcal{C} \circ \mathcal{B} = \langle c \circ b \mid c \in \mathcal{C}, b \in \mathcal{B} \rangle.$$

- ▶ **Степень t Адамара** кода $\mathcal{C}$: $t\mathcal{C} = (t-1)\mathcal{C} \circ \mathcal{C}$, где $1\mathcal{C} = \mathcal{C}$.

- ▶ Для кодов Рида–Маллера:

$$q\mathcal{RM}(r, m) = \mathcal{RM}(\min(qr, m), m).$$

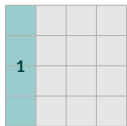
- ▶ Для кодов с масками: $\mathcal{C}_\alpha \circ \mathcal{B}_\beta = (\mathcal{C} \circ \mathcal{B})_{\alpha \circ \beta}$.

Структурная атака⁴ для $2r < m - 2$

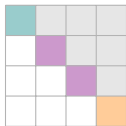
Идея: возведение $\text{PQRM}_{\sigma_1, \sigma_2}(r, m)$ в степень Адамара при $2r < m - 2$ выделяет блок 1, далее — остальные блоки.



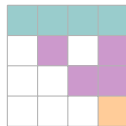
Труды CTCrypt 2025



Этап 1. Разделение блока 1
Теоремы 1-2, шаги 1-2



Этап 2. Разделение блоков 1-4
Теорема 2, шаги 3-7



Этап 3. Атака Чижова-Бородина + Очистка подблоков
Предложение 8

■ $G(r, m-2)^{\sigma_1}$ ■ $G(r-1, m-2)$ ■ $G(r-2, m-2)^{\sigma_2}$ ■ неизвестно/*

Ограничение: $2r < m - 2$ — не покрывает параметры авторов pqsigRM.

⁴ Рубенков А., Чижов И. Эффективная структурная атака на схему постквантовой подписи pqsigRM. XIV симпозиум CTCrypt 2025. Стр. 475–493

Дуальный код $\mathcal{PQR}\mathcal{M}^\perp(r, m)$

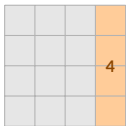
- ▶ **Дуальный код** $\mathcal{C}^\perp = \{h \in \mathbb{F}_2^n \mid \langle h, c \rangle = 0 \ \forall c \in \mathcal{C}\}$. Для кодов РМ:
 $\mathcal{RM}(r, m)^\perp = \mathcal{RM}(m-r-1, m)$.
- ▶ Пусть $r' = m - r - 1$. Порождающая матрица кода $\mathcal{PQR}\mathcal{M}^\perp$ имеет вид:

$$\left(\begin{array}{ccc|c} G(r' - 2, m - 2)^{\sigma_1^p} & 0 & 0 & 0 \\ G(r' - 1, m - 2) & G(r' - 1, m - 2) & 0 & 0 \\ G(r' - 1, m - 2) & 0 & G(r' - 1, m - 2) & 0 \\ \hline G(r', m - 2)^{\sigma_2^p} & G(r', m - 2)^{\sigma_2^p} & G(r', m - 2)^{\sigma_2^p} & G(r', m - 2)^{\sigma_2^p} \end{array} \right)$$

- ▶ Отсюда возведение дуального кода в степень Адамара выделяет блок 4 при $2r > m$.

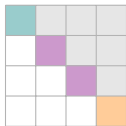
Модификация атаки⁵ для $2r > m$

Идея: при $2r > m$ квадрат самого кода заполняет все пространство и не несет информации. Переход к $\mathcal{PQR}^\perp_{\sigma_1, \sigma_2}(r, m)$ меняет соотношение параметров и степень Адамара выделяет блок 4.



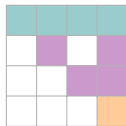
Этап 1. Выделение блока 4
через дуальный код

Различитель: степень Адамара
 $\mathcal{PQR}^\perp$



Этап 2. Разделение блоков
1–4

Укорочение + квадрат $\mathcal{PQR}^\perp$,
 $O(\log \log n \cdot n^4)$



Этап 3. Восстановление
ключа

Атака Чижова–Бородина +
Очистка подблоков

■ $G(r, m-2)^{\sigma_1}$ ■ $G(r-1, m-2)$ ■ $G(r-2, m-2)^{\sigma_2}$ ■ неизвестно/*

Ограничение: $2r > m$. Вместе со случаем $2r < m - 2$ остается зазор $m - 2 \leq 2r \leq m$.

⁵Разделы 3–4 работы.

Теорема

Задача криптоаналитика решается за

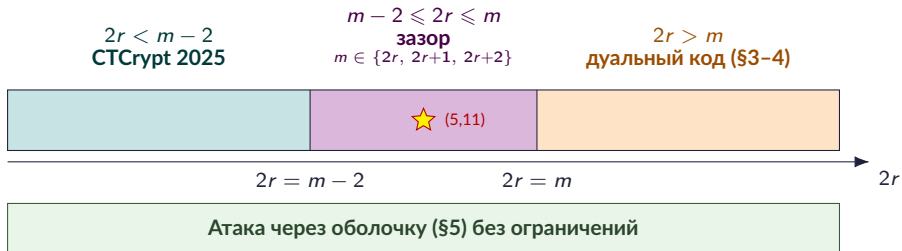
$$O\left(\log_2(\log_2(n)) \cdot n^4 + n^2 \cdot \text{DecRM}(n) + \max_{i \in \{r, r-1, r-2\}} L(i, m-2)\right) = \\ = \exp\{O((\log_2 n)^{d_{\max}})\}$$

операций, где $\text{DecRM}(n)$ — сложность декодирования кода Рунда-Маллера, а $L(r, m)$ — сложность восстановления структуры $\mathcal{RM}(r, m)$,

$d_{\max} = \max_{i \in \{r, r-1, r-2\}} \gcd(i, m-3)$, если выполнены следующие условия:

- Размерности r и m кода $\mathcal{PQR}_{\sigma_1, \sigma_2}(r, m)$ удовлетворяют условию $2r > m$.
- Подстановки $\sigma_1, \sigma_2 \in S_{2^{m-2}}$ таковы, что $\mathcal{A}^q = \mathcal{B}^q = \mathcal{V}_{2^{m-2}}$, где $q = \lceil \frac{m-2}{m-r-1} \rceil - 1$.

Ландшафт параметров атаки



- ▶ Зазор $m - 2 \leq 2r \leq m$ — единственный, где обе атаки произведением Адамара не применимы.
- ▶ Предлагаемые авторами параметры pqsigRM лежат **ровно в зазоре**.
- ▶ Атака через оболочку (§5) закрывает зазор и не имеет ограничений на (r, m) .

[3/3] Структурная атака с накоплением слов минимального веса

- ▶ **Оболочка кода** — «самодуальная часть»:

$$\mathcal{H}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^\perp.$$

- ▶ **Вес Хемминга** $\text{wt}(x)$ — число ненулевых координат.
- ▶ **Минимальное расстояние**: $d_{\min}(\mathcal{C}) = \min_{c \in \mathcal{C} \setminus \{0\}} \text{wt}(c)$.
- ▶ **Укорочение** кода $\mathcal{C}$ по множеству I — подкод слов, обнуляющихся на I :

$$\mathcal{C}_I = \{c \in \mathcal{C} \mid \text{supp}(c) \cap I = \emptyset\}.$$

Пусть $\mathcal{A} = \mathcal{RM}^{\sigma^1}(r, m-2)$, $\mathcal{B} = \mathcal{RM}(r-1, m-2)$, $\mathcal{C} = \mathcal{RM}^{\sigma^2}(r-2, m-2)$.

$$\begin{aligned} \mathcal{H}(\mathcal{PQRM}(r, m)) = & \underbrace{(\mathcal{A} \cap \mathcal{C}^\perp)_{(1,1,1,1)}}_{\text{блоки 1-4}} + \underbrace{\mathcal{H}(\mathcal{B})_{(0,1,1,0)}}_{\text{блоки 2 и 3}} + \\ & + \underbrace{(\mathcal{A} \cap \mathcal{H}(\mathcal{B}))_{(1,1,0,0)}}_{\text{блоки 1-2}} + \underbrace{(\mathcal{H}(\mathcal{B}) \cap \mathcal{C}^\perp)_{(0,0,1,1)}}_{\text{блоки 3-4}} + \dots \end{aligned}$$

- ▶ Слагаемое с маской $(0, 1, 1, 0)$ содержит код $\mathcal{RM}(\min(r-1, m-r-2), m-2)$ с **фиксированным** числом слов минимального веса.
- ▶ Остальные слагаемые — пересечения вида $\mathcal{RM}(r', m-2)^{\sigma'} \cap \mathcal{RM}(r'', m-2)^{\sigma''}$, содержащие **существенно меньше** слов минимального веса.

Шаг 0: открытый ключ

$$G_{\text{pub}} = M \cdot G_{\sigma_1, \sigma_2}(r, m) \cdot \gamma$$

?	?	?	?
?	?	?	?
?	?	?	?
?	?	?	?

Строки и столбцы перемешаны подстановками M и γ

Блочная структура 4×4 полностью скрыта

Шаг 1: слова минимального веса оболочки кода

Строим $\mathcal{H}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^\perp$ и ищем слова веса $d_{\min}$

?	Блоки 2, 3	?
?	Блоки 2, 3	?
?	Блоки 2, 3	?
?	Блоки 2, 3	?

Носитель I блоков 2 и 3 найден, $|I| = 2^{m-1}$

Блоки 1 и 4 еще не разделены

Шаги 2–3: укорочение кода и произведение Адамара

Укорочение по l , затем $\mathbb{C}_1 \circ \mathbb{C}_2$

Бл. 1	Бл. 2, 3	Бл. 4
Бл. 1	Бл. 2, 3	Бл. 4
Бл. 1	Бл. 2, 3	Бл. 4
Бл. 1	Бл. 2, 3	Бл. 4

Носители блоков 1 и 4 разделены

Блоки 2 и 3 еще не разделены между собой

Шаг 4: преобразование Гаусса по блоку 1

Переставляем столбцы блока 1, применяем метод Гаусса

$G(r, m-2)^{\sigma_1 \gamma_1}$	*	*	*
0	*	*	*
0	*	*	*
0	0	0	*

Подматрица на пересечении строк и столбцов 2, 3 (выделена)
содержитconcatenацию кодов Рида-Маллера

Шаг 5: разделение блоков ⁶ 2 и 3

Все 4 носителя найдены, блочно-треугольный вид

$G(r, m-2)^{\sigma_1 \gamma_1}$	*	*	*
0	$G(r-1, m-2)^{\gamma_2}$	0	*
0	0	$G(r-1, m-2)^{\gamma_3}$	*
0	0	0	$G(r-2, m-2)^{\sigma_2 \gamma_4}$

Произведение Адамара в подматрице разделило блоки 2 и 3

Наддиагональные подблоки еще не очищены

⁶Чижов И. В., Конюхов С. А., Давлетшина А. М., Эффективная структурная атака на криптосистему Мак-Элиса–Сидельникова. 2020

Шаг 6: атака на коды Риды–Маллера и очистка⁷

Секретный ключ $G_{\sigma_1, \sigma_2}(r, m)$ восстановлен

$G(r, m-2)^{\sigma_1}$	$G(r, m-2)^{\sigma_1}$	$G(r, m-2)^{\sigma_1}$	$G(r, m-2)^{\sigma_1}$
0	$G(r-1, m-2)$	0	$G(r-1, m-2)$
0	0	$G(r-1, m-2)$	$G(r-1, m-2)$
0	0	0	$G(r-2, m-2)^{\sigma_2}$

Атака Чижова–Бородина раскрывает подстановки на диагонали

Декодирование очищает наддиагональные подблоки

⁷Рубенков А., Чижов И. Эффективная структурная атака на схему постквантовой подписи pqsigRM. XIV симпозиум CTCrypt2025. Стр. 475–493

Теорема

Задача криптоаналитика для $\mathcal{PQR}\mathcal{M}_{\sigma_1, \sigma_2}(r, m)$ -кода решается за

$$O(n \cdot W_0(r', m-2) + n^4 + n^2 \cdot \text{DecRM}(n) + \max_{i \in \{r, r-1, r-2\}} L(i, m-2)) = \exp\{O((\log_2 n)^s)\},$$

где $r' = \min(r-1, m-r-2)$, $s = \max(r', \max_{i \in \{r, r-1, r-2\}} \gcd(i, m-3))$,
 $\text{DecRM}(n)$ – сложность декодирования РМ-кода, $L(r, m)$ – сложность
восстановления структуры $\mathcal{RM}(r, m)$, а W_0 – оценка сложности поиска
слов минимального веса.

Замечание

Практическая реализация атаки для набора $(r, m) = (5, 11)$ занимает
5–7 часов работы на компьютере с Intel Core i7-13700H без
параллелизации.

1. Существующая структурная атака расширена для размерностей $2r > m$
2. Построена **структурная атака без ограничений** на размерности кода, покрывающая все оригинальные параметры pqsigRM.
3. Сложность обеих атак **эквивалентна** сложности атаки на криптосистему непосредственно на кодах Рида-Маллера.

Таким образом модификация кодов Рида-Маллера в конструкции pqsigRM **не обеспечивает дополнительной защищенности.**

Готов ответить на вопросы

Рубенков Андрей Дмитриевич

Специалист-исследователь
лаборатории криптографии



a.rubenkov@kryptonite.ru

- ▶ Получение точной вероятностной оценки успеха атаки с использованием слов минимального веса.
- ▶ Нахождение границы значения p , при котором подстановки σ_1 и σ_2 такие, что атака 2 неприменима.
- ▶ Построение атаки для случая, когда σ_i не автоморфизм, но атака не применима.
- ▶ Решение задачи эффективного нахождения носителя блоков 2 и 3 при наличии «зашумленных» слов минимального веса.