Модификация компактной версии криптосистемы Нидеррайтера

И. В. Чижов, А. В. Кирюткина

Аннотация—В работе предлагается модифицированная компактная версия криптосистемы Нидеррайтера, устраняющая уязвимости предложенной ранее компактной схемы. Задача обеспечения безопасности модифицированной криптосистемы сводится к задаче декодирования линейных кодов с дополнительным этапом перебора векторов ошибок в подпространстве размерности k. Доказано, что предложенная модификация сохраняет криптографическую стойкость, эквивалентную классической криптосистеме Нидеррайтера, при этом обеспечивая сокращение длины открытого ключа. Описаны алгоритмы генерации ключей, шифрования и расшифрования, проведен анализ их вычислительной сложности. Доказано, что стойкость модифицированной схемы к атакам на основе декодирования по информационным множествам превышает стойкость классической криптосистемы Нидеррайтера за счет дополнительного множителя 2^k в сложности атак.

Ключевые слова—криптосистемма Нидеррайтера, коды Гоппы, открытый ключ

I. Введение

Развитие квантовых вычислений представляет серьезную угрозу для современных криптографических систем. Квантовые компьютеры, использующие принципы суперпозиции и запутанности, способны эффективно решать задачи, лежащие в основе многих асимметричных криптосистем, таких как факторизация больших чисел и дискретное логарифмирование [1]. Это ставит под угрозу безопасность широко распространенных криптосистем, таких как RSA и ECC, и создает потребность в разработке и стандартизации алгоритмов постквантовой криптографии, устойчивых к атакам с использованием квантовых компьютеров.

Одним из перспективных направлений являются криптосистемы на основе кодов, исправляющих ошибки, в частности, схема Нидеррайтера. Ее стойкость основана на NP-трудной задаче декодирования линейных кодов [2], что делает ее устойчивой даже к квантовым атакам. Криптосистема Нидеррайтера [3] по своей стойкости эквивалентна более известной схеме Мак-Элиса, но в некоторых ситуациях предлагает преимущества.

Однако широкому практическому применению классической криптосистемы Нидеррайтера препятствует существенный недостаток — большой размер открытого ключа. Это делает актуальными исследования, направленные на создание компактных версий таких систем, которые сохраняли бы криптографическую стойкость, но при этом имели приемлемые для реальных приложений параметры.

В работе [4] была предложена одна из таких компактных версий, целью которой являлась оптимизация размера открытого ключа. Однако, дальнейший анализ демонстрирует наличие принципиального недостатка в предложенном методе, который компрометирует его криптографическую стойкость. Функция шифрования в данной схеме оказывается тривиальной, что позволяет восстанавливать исходное сообщение непосредственно из шифртекста без

Статья получена 10 сентября 2020

Иван Владимирович Чижов, МГУ им. М.В. Ломоносова, (email: chizhoviv@my.msu.ru).

Арина Владимировна Кирюткина, МГУ им. М.В. Ломоносова, (email: s02250444@gse.cs.msu.ru).

знания закрытого ключа.

Предлагается модифицированная компактная версия криптосистемы Нидеррайтера, устраняющая уязвимость исходной компактной схемы. Основная идея модификации состоит в изменении структуры проверочной матрицы и процедуры формирования вектора ошибок, что исключает возможность тривиального восстановления сообщения из шифртекста, присутствующую в схеме Халвана-Зали-Аттари [4]. При этом сохраняется ключевое преимущество компактной версии — существенно уменьшенный размер открытого ключа по сравнению с классической схемой Нидеррайтера.

Помимо этого, в работе представлены результаты анализа стойкости модифицированной схемы к атакам на основе информационного множества (ISD). Показано, что сложность ISD-атак возрастает до $O(2^{(n/20)+k})$ из-за невозможности прямого применения оптимизаций BJMM/Stern.

II. Криптосистема Нидеррайтера и ее компактная версия

A. Основные определения

Пусть $\mathbb{F}_q$ — конечное поле из q элементов, для произвольного натурального числа n через $\mathbb{F}_q^n$ обозначим линейное пространство векторов длины n над полем $\mathbb{F}_q$. Тогда $\mathbb{F}_q^{(n-k)\times n}$ — пространство матриц размера $(n-k)\times n$ над полем $\mathbb{F}_q$, а $\mathbb{F}_{q^m}[z]$ — кольцо полиномов от переменной z над полем $\mathbb{F}_{q^m}$.

Кодом называется множество $\mathscr{C} \subseteq \mathbb{F}_q^n$, где $\mathbb{F}_q$ — конечное поле из q элементов, а n — длина кода. Элементы кода называются кодовыми словами.

Код $\mathscr{C}$ называется линейным, если он образует подпространство векторного пространства $\mathbb{F}_q^n$ над полем $\mathbb{F}_q$. Размерность этого подпространства обозначается через k и называется размерностью кода. Линейный код с длиной n, размерностью k и минимальным расстоянием d будем называть $[n,k,d]_q$-кодом.

Весом Хэмминга $\mathrm{wt}(e)$ вектора $e \in \mathbb{F}_q^n$ называется количество его ненулевых координат.

Для произвольного $[n,k,d]_q$-кода $\mathscr{C}$ его дуальный код $\mathscr{C}^\perp$ определяется как:

$$\mathscr{C}^\perp = \{x \in \mathbb{F}_q^n \mid \langle x, c\rangle \stackrel{\text{def}}{=} x \cdot c^\top = 0 \ \forall c \in \mathscr{C}\}.$$

Дуальный код является линейным кодом с параметрами $[n, n-k, d^\perp]_q$, где $d^\perp$ — минимальное расстояние дуального кода, и выполняется $\dim(\mathscr{C}) + \dim(\mathscr{C}^\perp) = n$.

Порождающей матрицей G линейного кода $\mathscr{C}$ размерности k будем называть $(k\times n)$-матрицу над $\mathbb{F}_q$, строки которой образуют базис кода $\mathscr{C}$. Любое кодовое слово может быть представлено как $c = mG$, где $m \in \mathbb{F}_q^k$.

Проверочной матрицей H линейного кода $\mathscr{C}$ будем называть $(n-k)\times n$-матрицу над $\mathbb{F}_q$, такую что $Hc^\top = 0$ для любого $c \in \mathscr{C}$. Матрица H определяет синдром ошибки: $s = He^\top$, где e — вектор ошибки.

Определим код Гоппы $\Gamma(L,g)$ как линейный код над $\mathbb{F}_q$, задаваемый множеством $L = \{\alpha_1, ..., \alpha_n\} \subseteq \mathbb{F}_{q^m}$ и полиномом Гоппы $g(x) \in \mathbb{F}_{q^m}[z]$ степени t. При этом, полином выбирается таким образом, чтобы $g(\alpha_i) \neq 0, i = 1, \ldots, n$.

Кодовым словом является вектор $c = (c_1, ..., c_n)$, удовлетворяющий условию:

$$\sum_{i=1}^{n} \frac{c_i}{z-\alpha_i} \equiv 0 \pmod{g(z)}.$$

Криптосистемой Нидеррайтера называется криптосистема с открытым ключом, основанная на задаче декодирования линейных кодов, где открытым ключом является проверочная матрица $H' = SHP$, где H — проверочная матрица кода, S — случайная невырожденная матрица, P — матрица перестановки, а закрытым ключом тройка (S,H,P). В процесссе шифрования сообщение преобразовывается в вектор ошибки e веса t и вычисляется синдром $s = H'e^\top$. При расшифровании используется закрытый ключ для декодирования синдрома.

Задачей декодирования для линейного кода называется нахождение по матрице $H \in \mathbb{F}_q^{r\times n}$, вектору $s \in \mathbb{F}_q^r$ и числу t вектора $e \in \mathbb{F}_q^n$ веса Хемминга t, для которого выполняется равенство $He^\top = s^\top$. Для случайного кода эта задача является NP-трудной.

B. Классическая схема Нидеррайтера

Криптосистема Нидеррайтера относится к классу криптосистем с открытым ключом, основанных на задаче декодирования линейных кодов.

Пусть заданы:

- $\mathscr{C}$ – линейный $[n, k, d]_q$-код с исправляющей способностью $t = \lfloor \frac{d-1}{2} \rfloor$
- $\mathbb{F}_q$ – конечное поле характеристики q
- H – проверочная матрица кода $\mathscr{C}$ размера $(n-k) \times n$
- S – случайная невырожденная матрица размера $(n-k) \times (n-k)$
- P – перестановочная матрица размера $n \times n$
- Закрытый ключ: (S, H, P)
- Открытый ключ: $H' = SHP$

Рассмотрим, как будет выглядеть алгоритм шифрования в данной криптосистеме:

Алгоритм 1 Шифрование в криптосистеме Нидеррайтера

Вход: Сообщение $m \in \mathbb{F}_q^{n-k}$, открытый ключ $H' \in \mathbb{F}_q^{(n-k)\times n}$

Выход: Криптограмма $s \in \mathbb{F}_q^{n-k}$

1: Преобразовать сообщение m в вектор ошибок $e \in \mathbb{F}_q^n$ с весом Хэмминга $\mathrm{wt}(e) = t$

2: Вычислить синдром $s \leftarrow H' e^\top$

3: Возвратить: s

Тогда алгоритм расшифрования будет таким:

Алгоритм 2 Расшифрование в криптосистеме Нидеррайтера

Вход: Синдром $s \in \mathbb{F}_q^{n-k}$, закрытый ключ (S, H, P)

Выход: Исходное сообщение m

1: Вычислить $s' = S^{-1}s$

2: Найти вектор ошибок e' такой, что $He'^\top = s'$ и $\mathrm{wt}(e) = t$

3: Вычислить $e = e'P^\top$

4: Восстановить m из e

5: Возвратить: m

C. Параметры ключей в системе Нидеррайтера

- Открытый ключ:

$$\text{Длина} = (n-k) \times n \text{ бит}$$

где n – длина кода, k – размерность кода.

- Закрытый ключ:

$$\text{Длина} = \underbrace{(n-k)^2}_{\text{Матрица } S} + \underbrace{n \times \lceil \log_2^n \rceil}_{\text{Перестановка } P} + \underbrace{t \times m + n \times m}_{\text{Матрица } H} \text{ бит}$$

D. Безопасность системы

Криптостойкость системы основана на двух вычислительно сложных задачах:

1) Задача декодирования произвольного линейного кода (NP-полная задача)
2) Задача нахождения эквивалентного кода (сложность зависит от класса кода)

На сегодняшний день не известно эффективных атак на криптосистему Нидеррайтера, в том числе атак на основе информационного множества и стукрурных атак.

E. Компактная версия криптосистемы Нидеррайтера

Основным параметром, ограничивающим применимость классической криптосистемы Нидеррайтера, является размер её открытого ключа. Поэтому сокращение его длины является актуальной исследовательской задачей. Рассмотрим компактную версию криптосистемы, предложенную в [4].

Генерация ключей

Алгоритм 3 Генерация ключевой пары

Вход: Параметры системы: n, m, t (длина кода, степень расширения поля, корректирующая способность)

Выход: Открытый ключ $pk = (H^{\top}_{cyclic}, t)$ и закрытый ключ $sk = (S_{ns}, H, P_{per})$

1: Выбрать случайную последовательность $(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$ из n различных элементов в поле $\mathbb{F}_{2^m}$

2: Выбрать случайный многочлен $g(x)$ такой, что $g(\alpha_i) \neq 0$ для всех $\alpha_i \in (\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$

3: Вычислить проверочную матрицу H размера $t \times n$:

$$H = \begin{bmatrix} 1/g(\alpha_0) & 1/g(\alpha_1) & \cdots & 1/g(\alpha_{n-1}) \\ \alpha_0/g(\alpha_0) & \alpha_1/g(\alpha_1) & \cdots & \alpha_{n-1}/g(\alpha_{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{t-1}/g(\alpha_0) & \alpha_1^{t-1}/g(\alpha_1) & \cdots & \alpha_{n-1}^{t-1}/g(\alpha_{n-1}) \end{bmatrix}$$

4: Сгенерировать случайный вектор длины $n-k$ и циклически сдвинуть его на k позиций направо для создания циклической матрицы P_{cyclic}

5: Дополнить P_{cyclic} единичной матрицей для вычисления H_{cyclic}:

$$H_{cyclic} = [P_{cyclic} | I_{(n-k)\times(n-k)}]$$

6: Сгенерировать случайную перестановочную матрицу $P_{per} \in F_{2^m}^{n\times n}$

7: Вычислить невырожденную матрицу $S_{ns} \in F_{2^m}^{(n-k)\times(n-k)}$

8: Возвратить: (sk, pk)

Дадим некоторые пояснения к алгоритму 3. Матрица H строится на основе кода Гоппы с последовательностью $\{\alpha_i\}$ и полиномом $g(x)$, циклическая структура P_{cyclic} позволяет оптимизировать вычисления, открытый ключ представляет собой модифицированную проверочную матрицу, закрытый ключ содержит информацию, необходимую для эффективного декодирования.

Шифрование сообщения

Алгоритм 4 Шифрование

Вход: Открытый ключ $pk = (H^{\top}_{\text{cyclic}}, t)$, сообщение $m \in \mathbb{F}_2^k$

Выход: Зашифрованное сообщение $c \in \mathbb{F}_2^n$

1: Преобразовать m в вектор ошибки $e_i = \varphi(m)$, длины $n-k$ и веса t, $\varphi(m)$ - функция преобразования сообщения в вектор e_iиз $\mathbb{F}_2^k$ в $\mathbb{F}_2^{n-k}$.

2: Сформировать вектор $e = [0_k | e_i]$

3: Вычислить зашифрованное сообщение: $c = e \cdot H^{\top}_{\text{cyclic}}$

4: Возвратить: c

Расшифрование сообщения

Алгоритм 5 Расшифрование

Вход: Закрытый ключ $sk = (S_{ns}, H, P_{\text{per}})$, зашифрованное сообщение $c \in \mathbb{F}_2^n$

Выход: Исходное сообщение $m \in \mathbb{F}_2^k$

1: Вычислить: $c_1 = c \cdot (S_{ns})^{-1}$

2: Декодировать: $c_2 = \text{Decode}(c_1, H, t)$

3: Восстановить вектор ошибки: $e = c_2 \cdot (P_{\text{per}})^{-1}$

4: Извлечь сообщение: $m = \varphi^{-1}(e_i)$

5: Возвратить: m

F. Параметры ключей в компактной версии

- Открытый ключ:

$$\text{Длина} = (n-k) \text{ бит}$$

- Закрытый ключ:

$$\text{Длина} = \underbrace{(n-k)^2}_{\text{Матрица } S_{ns}} + \underbrace{n \times \lceil \log_2 n \rceil}_{\text{Перестановка } P_{per}} + \underbrace{(n-k) \times n}_{\text{Матрица } H} \quad \text{бит}$$

G. Недостаток компактной версии

Утверждение II.1 (Дефект компактной версии). В алгоритме 4 выполняется равенство $c = e$, т.е. шифртекст равен открытому тексту.

Доказательство. Посмотрим на представление матрицы H':

$$H'^{\top} = P_{per}^{\top} H^{\top} S_{ns}^{\top} = \left[\frac{P}{I}\right]_{n\times(n-k)}$$

Рассмотрим также матрицу H_{cyclic}:

$$H_{\text{cyclic}}^{\top} = \begin{bmatrix} P_{\text{cyclic}} \\ \hline I \end{bmatrix} = \begin{bmatrix} P \\ \hline I \end{bmatrix} + \begin{bmatrix} P_{\text{sec}} \\ \hline 0 \end{bmatrix} = \\ = H'^{\top} + H_{\text{sec}}^{\top}$$

Вектор ошибок e будет формироваться так:

$$e = [0_{1\times k} \mid e_i]_{1\times n}$$

Тогда в результате шифрования мы получим такой шифртекст:

$$\begin{aligned} c &= e \cdot H_{\text{cyclic}}^{\top} = \\ &= [0 \mid e_i] \cdot \begin{bmatrix} P \\ \hline I \end{bmatrix} + [0 \mid e_i] \cdot \begin{bmatrix} P_{\text{sec}} \\ \hline 0 \end{bmatrix} = \\ &= [0 \mid e_i] \cdot \begin{bmatrix} P \\ \hline I \end{bmatrix} = \\ &= e \end{aligned}$$

Соответственно получаем, что

$$c = e$$

Исходное сообщение не скрыто □

В результате вектор c будет равен вектору e, что позволяет однозначно восстановить исходное сообщение m без использования закрытого ключа. Таким образом, в [4] содержится ошибка. В связи с приведенной уязвимостью, данную криптосистему нельзя использовать на практике, однако ее можно модифицировать для устранения данного недостатка.

III. Модификация компактной версии криптосистемы Нидеррайтера

Для устранения данной уязвимости нами предложена модификация схемы, сохраняющая преимущество компактного ключа, но при этом обеспечивающая криптографическую стойкость. Ключевое нововведение заключается в изменении матричных компонент, участвующих в формировании ключа, не позволяющих однозначно восстановить вектор e, а также алгоритма шифрования и, вследствие этого, расшифрования.

A. Генерация ключа

Алгоритм генерации ключевой пары в модифицированной схеме представлен в листинге 6.

Алгоритм 6 Генерация ключевой пары (Модифицированная схема)

Вход: Системные параметры: n, m, k, t и s.
Выход: Открытый ключ $pk = (H_{\text{cyclic}}^{\top}, t, s)$ и закрытый ключ $sk = (S_{ns}, H, P_{\text{per}})$.

1) Сгенерировать последовательность $L = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ из n различных элементов в поле $\mathbb{F}_{2^m}$.
2) Выбрать случайный полином Гоппы $g(x) \in \mathbb{F}_{2^m}[z]$ степени t, такой что $g(\alpha_i) \neq 0$ для всех $\alpha_i \in L$.
3) Построить проверочную матрицу H кода Гоппы $\Gamma(L, g)$ размера $t \times n$:
$$H = \begin{bmatrix} \frac{1}{g(\alpha_0)} & \frac{1}{g(\alpha_1)} & \cdots & \frac{1}{g(\alpha_{n-1})} \\ \frac{\alpha_0}{g(\alpha_0)} & \frac{\alpha_1}{g(\alpha_1)} & \cdots & \frac{\alpha_{n-1}}{g(\alpha_{n-1})} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_0^{t-1}}{g(\alpha_0)} & \frac{\alpha_1^{t-1}}{g(\alpha_1)} & \cdots & \frac{\alpha_{n-1}^{t-1}}{g(\alpha_{n-1})} \end{bmatrix}.$$
4) Сгенерировать два случайных вектора длины $n-k$ и циклическими сдвигами направо создать две циклические матрицы P_1 и P_2 размеров $(n-k)\times k$ и $(n-k)\times(n-k)$ соответственно.
5) Сформировать модифицированную проверочную матрицу для открытого ключа:
$$H_{\text{cyclic}} = [P_1|P_2]_{(n-k)\times n}.$$
6) Сгенерировать случайную перестановочную матрицу $P_{\text{per}} \in \mathbb{F}_{2^m}^{n\times n}$.
7) Вычислить невырожденную матрицу S_{ns} из уравнения:
$$S_{ns}^{\top} = B^{-1}P_2,$$
где $B \in \mathbb{F}_{2^m}^{(n-k)\times(n-k)}$ — обратимая нижняя подматрица матрицы $P_{\text{per}}^{\top}H^{\top}$.
8) Возвратить: $pk = (H_{\text{cyclic}}^{\top}, t, s)$, $sk = (S_{ns}, H, P_{\text{per}})$.

B. Процедура шифрования

Процедура шифрования в модифицированной схеме изменена для устранения уяз-

вимости. Отличие заключается в том, что вектор ошибок e теперь распределен по всему пространству $\mathbb{F}_2^n$, а его вес t разделен между двумя частями e_1 и e_2. Это исключает однозначное восстановление e_i из c.

Алгоритм 7 Шифрование (Модифицированная схема)

Вход: Открытый ключ $pk = (H_{\text{cyclic}}^{\top}, t, s)$, сообщение $m \in \mathbb{F}_2^k$.
Выход: Шифртекст $c \in \mathbb{F}_2^n$.

1) Отобразить сообщение m в вектор ошибок $e = [e_1|e_2]_{1\times n}$, где $e_1 \in \mathbb{F}_2^k$, $\text{wt}(e_1) = s$, а $e_2 \in \mathbb{F}_2^{n-k}$, $\text{wt}(e_2) = t - s$ (s - количество ненулевых битов в первой части вектора).
2) Вычислить шифртекст: $c = e \cdot H_{\text{cyclic}}^{\top}$.
3) Возвратить: c.

C. Процедура расшифрования

Процедура расшифрования усложнена в связи с необходимостью коррекции вносимых при шифровании изменений.

Алгоритм 8 Расшифрование (Модифицированная схема)

Вход: Закрытый ключ $sk = (S_{ns}, H, P_{\text{per}})$, шифртекст $c \in \mathbb{F}_2^n$.
Выход: Исходное сообщение $m \in \mathbb{F}_2^k$.

1) Вычислить вспомогательную матрицу P_{sec} как верхнюю подматрицу размера $k\times(n-k)$ матрицы $H_{\text{sec}}^{\top} = H_{\text{cyclic}}^{\top} + H'^{\top}$, где $H'^{\top} = P_{\text{per}}^{\top} H^{\top} S_{ns}^{\top}$.
2) Цикл: Подобрать вектор $e_1 \in \mathbb{F}_2^k$, $\text{wt}(e_1) = s$:
   a) Вычислить $c_1 = c - [e_1 \cdot P_{\text{sec}}|0]_{1\times(n-k)}$
   b) Вычислить $c_2 = c_1 \cdot (S_{ns}^{\top})^{-1}$
   c) Декодировать синдром: $c_3 = \text{Decode}(c_2, H, t)$.
   d) Если декодирование успешно — выход из цикла
3) Вычислить $c_4 = c_3 \cdot (P_{\text{per}}^{\top})^{-1} = e = [e_1|e_2]_{1\times n}$
4) Восстановить сообщение $m = \varphi^{-1}(e)$.
5) Возвратить: m.

На шаге 2 используется перебор по информационному множеству для нахождения корректного e_1. Сложность перебора оценивается как $\binom{k}{s}$, что является приемлемым при малых значениях s (например, $s = 3$), но создает вычислительный барьер для атакующего.

D. Стойкость модификации

Теорема III.1 (Стойкость модификации). Если существует полиномиальный алгоритм, решающий задачу восстановления вектора ошибок e по шифртексту

$$c = e \cdot H_{\text{cyclic}}^{T},$$

то существует полиномиальный алгоритм решения задачи синдромного декодирования для произвольного линейного кода.

Доказательство. Рассмотрим, как выглядит вектор ошибок $e = [e_1|e_2]_{1\times n}$, где $e_1 \in \mathbb{F}_2^k$ с весом s, $e_2 \in \mathbb{F}_2^{n-k}$ с весом $t - s$.

Тогда посмотрим на представление матрицы H':

$$H' = P_{per}^{\top} H^{\top} S_{ns}^{\top} = F S_{ns}^{\top},$$

где

$$F = \left[\frac{A}{B}\right]_{n\times(n-k)}, S_{ns}^{\top} = B^{-1} \cdot P_2$$

Таким образом,

$$H'^{\top} = F \cdot S_{ns}^{\top} = \left[\frac{A \cdot S_{ns}^{\top}}{B \cdot S_{ns}^{\top}}\right] = \\ = \left[\frac{A \cdot S_{ns}^{\top}}{B \cdot B^{-1} \cdot P_2}\right] = \left[\frac{P}{P_2}\right]_{n\times(n-k)}$$

Посмотрим на то, какую структуру будет иметь матрица H_{sec}:

$$H_{sec}^{\top} = H_{cyclic}^{\top} + H'^{\top} = \\ = \left[\frac{P_1}{P_2}\right] + \left[\frac{P}{P_2}\right] \\ = \left[\frac{P_{sec}}{0}\right]_{n\times(n-k)}$$

Тогда шифртекст c будет считаться так:

$$c = e \cdot H_{cyclic}^{\top} = e \cdot H'^{\top} + e \cdot H_{sec}^{\top} =$$
$$= \underbrace{[e_1|e_2]}_{1\times n} \cdot \left[\frac{P}{P_2}\right] + [\underbrace{e_1}_{1\times k}|e_2] \cdot \left[\frac{P_{sec}}{0}\right]$$

Восстановление вектора ошибок e по шифртексту c требует решения задачи синдромного декодирования, что является NP-трудной задачей для случайных линейных кодов [3]. □

Теорема III.2 (Корректность модификации). Для секретного ключа $sk = (S, H, P)$ и любого вектора ошибок $e \in \mathbb{F}_2^n$ с весом $\leq t$ выполняется:

$$D_{sk}(E_{pk}(e)) = e,$$

где E_{pk} и D_{sk} — процедуры шифрования и расшифрования соответственно.

Доказательство. При нахождении корректного вектора e_1, вычисляем матрицу P_{sec} из уравнения $P_{\text{sec}} = P + P_1$ (матрицы имеют размерность $k \times (n-k)$), где P_1 – компонента открытого ключа, а P находится из

$$\begin{cases} H'^{\top} = P_{per}^{\top} H^{\top} S_{ns}^{\top}, \\ H'^{\top} = \left[\dfrac{P}{P_2}\right] \end{cases}$$

Считаем

$$c' = e \cdot H_{sec}^{\top} = [e_1 \cdot P_{sec}|0]_{1\times(n-k)}$$

А затем вычисляем

$$\begin{aligned} c_1 &= c - c' = e \cdot H_{\text{cyclic}}^{\top} - c' \\ &= e \cdot H'^{\top} + e \cdot H_{\text{sec}}^{\top} - e \cdot H_{\text{sec}}^{\top} \\ &= e \cdot H'^{\top} = e \cdot P_{\text{per}}^{\top} \cdot H^{\top} \cdot S_{ns}^{\top} \end{aligned}$$

Далее применяем оригинальный алгоритм расшифрования, используемый в криптосистеме Нидеррайтера. Таким образом, мы получим корректное сообщение m. □

Следовательно, для модифицированной криптосистемы Нидеррайтера выполняются стойкость и корректность.

E. Параметры ключей

Модифицированная схема сохраняет компактность открытого ключа:

- Открытый ключ:

$$\text{Длина} = 2 \times (n-k) \times m \text{ бит}$$

- Закрытый ключ:

$$\text{Длина} = \underbrace{(n-k)^2}_{\text{Матрица } S_{ns}} + \underbrace{n \times \lceil \log_2 n \rceil}_{\text{Перестановка } P_{per}} + \underbrace{t \times m + n \times m}_{\text{Матрица } H} \text{ бит}$$

Таким образом, предложенная модификация позволяет устранить критический недостаток исходной компактной схемы, сохранив ее преимущества и обеспечив криптографическую стойкость, основанную на сложности задачи синдромного декодирования.

IV. Оценка сложности алгоритмов

В данном разделе приводится оценка вычислительной сложности основных алгоритмов модифицированной криптосистемы: генерации ключей, шифрования и расшифрования. Сложность оценивается в двух аспектах: количество битовых операций и количество операций в поле $\mathbb{F}_{2^m}$, что позволяет более точно оценить производительность как программных, так и аппаратных реализаций.

На основе сложности базовых операций оценим сложность основных алгоритмов модифицированной криптосистемы.

Утверждение IV.1 (Сложность генерации ключей). Алгоритм генерации ключей имеет сложность $O((n-k)^3 \cdot m^2)$ битовых операций или $O((n-k)^3)$ операций в поле $\mathbb{F}_{2^m}$

Оценка следует из анализа операций генерации матриц S_{ns}, H, P_{per} и циклических матриц P_1, P_2. Доминирующей операцией является вычисление матрицы S_{ns} методом Гаусса.

Утверждение IV.2 (Сложность шифрования). Алгоритм шифрования имеет сложность $O(n \cdot t \cdot m^2)$ битовых операций или $O(n \cdot t)$ операций в поле $\mathbb{F}_{2^m}$

Сложность определяется операцией умножения вектора ошибок e на матрицу $H^{\top}_{\text{cyclic}}$ и созданием вектора ошибок веса t.

Утверждение IV.3 (Сложность расшифрования). Алгоритм расшифрования имеет сложность $O\left(\binom{k}{s} \cdot ((n-k)^3 \cdot m^2 + t^3 \cdot m^2 + n \cdot t \cdot m)\right)$ битовых операций или $O\left(\binom{k}{s} \cdot ((n-k)^3 + t^3 + n \cdot t)\right)$ операций в поле $\mathbb{F}_{2^m}$

Сложность обусловлена перебором векторов e_1 веса s, операциями матричных умножений и декодированием с использованием проверочной матрицы H. Сложность нахождения вектора ошибок e по синдрому s составляет $O(t^3 + n \cdot t)$ операций в поле $\mathbb{F}_{2^m}$ или $O(t^3 \cdot m^2 + n \cdot t \cdot m)$ битовых операций [5, 6].

A. Сравнение с классической схемой Нидеррайтера

Таблица I
Сравнительный анализ сложности алгоритмов

	Классическая	Модифицированная
Генерация ключа		
Битовые	$O((n-k)n^2m^2)$	$O((n-k)^3m^2)$
Операции в поле	$O((n-k)n^2)$	$O((n-k)^3)$
Шифрование		
Битовые	$O(tnm^2)$	$O(tnm^2)$
Операции в поле	$O(tn)$	$O(tn)$
Расшифрование		
Битовые	$O((n-k)^3m^2)$	$O(\binom{k}{s}(n-k)^3m^2)$
Операции в поле	$O((n-k)^3)$	$O(\binom{k}{s}(n-k)^3)$

Проведенный анализ позволяет сделать следующие выводы:

1) Сложность генерации ключей в модифицированной схеме сравнима с классической, а в некоторых случаях может быть ниже за счет уменьшения размерности используемых матриц.
2) Сложность процедуры шифрования практически идентична в обеих схемах.
3) Основное увеличение сложности наблюдается в процедуре расшифрования, что обусловлено необходимостью перебора $\binom{k}{s}$ вариантов вектора e_1. Однако при малых значениях s (например, $s = 3$) это является допустимым компромиссом, обусловленным необходимостью устранения критической уязвимости в исходной компактной схеме.
4) Предложенная модификация обеспечивает существенное сокращение размера открытого ключа при сохранении приемлемой вычислительной сложности базовых операций.

Полученные оценки сложности подтверждают практическую реализуемость предложенной модификации и ее конкурентоспособность по сравнению с классической схемой Нидеррайтера.

V. Сложность взлома модифицированной криптосистемы

В данном разделе рассматриваются известные атаки на криптосистему Нидеррайтера и проводится анализ их эффективности против предложенной модификации. Внимание уделяется как специализированным криптографическим атакам, эксплуатирующим алгебраическую структуру кодов Гоппы, так и универсальным алгоритмам декодирования линейных кодов.

A. Формальная постановка задачи

Задача взлома криптосистемы Нидеррайтера формулируется следующим образом:

Даны открытые параметры - $n, k, t \in \mathbb{N}, q = 2^m$, открытый ключ: $H' \in \mathbb{F}_q^{(n-k)\times n}$, зашифрованное сообщение: $s \in \mathbb{F}_q^{n-k}$

Найти: вектор $e \in \mathbb{F}_q^n$ такой, что $\mathrm{wt}(e) = t, H' \cdot e^\top = s^\top$

B. Атака на основе декодирования по информационным множествам

Метод декодирования по информационным множествам (Information Set Decoding, ISD) является одним из наиболее эффективных универсальных методов решения задачи синдромного декодирования. Идея ISD заключается в приведении матрицы H к систематическому виду $[I_{n-k}|P]$ с помощью перестановки столбцов и последующем решении упрощенной подзадачи.

Алгоритм 9 Классический ISD

Вход: $H_0 \in \mathbb{F}_q^{n\times(n-k)}$ — проверочная матрица, $s \in \mathbb{F}_q^{n-k}$ — синдром, w — целевой вес ошибки, $l \in [0, n-k]$, $p \in [\max\{0, w-(n-k-l)\}, \min\{w, k+l\}]$ — параметры

Выход: $e \in \mathbb{F}_q^n : eH_0^\top = s$ и $\mathrm{wt}(e) = w$, либо $\perp$ при неудаче

1) Выбрать случайную подстановку π; $H \leftarrow \pi(H_0)$
2) Привести H к систематическому виду методом Гаусса:

$$H = \begin{pmatrix} I_{n-k-\ell} & H' \\ 0 & H'' \end{pmatrix}, \begin{array}{l} H' \in \mathbb{F}_q^{(n-k-\ell)\times(k+\ell)}, \\ H'' \in \mathbb{F}_q^{(k+\ell)\times\ell}, \\ s = (s' \parallel s'') \in \mathbb{F}_q^{n-k} \end{array}$$

3) Решить подзадачу $\mathrm{SD}(H'', s'', p)$
4) Для каждого найденного e'':
   a) Восстановить $e = (e'\|e'')$, где $e' = s' - e''(H')^\top$
   b) Если $\mathrm{wt}(e) = w$ и $eH^\top = s$, тогда вернуть $e_0 = \pi^{-1}(e)$
5) Вернуть $\perp$

Проведенный анализ позволяет сделать следующий вывод о стойкости предложенной модификации - сложность декодирования возрастает до $O(2^{(n/20)+k})$ из-за невозможности прямого применения оптимизаций BJMM/Stern

Таким образом, к сложности реализации рассмотренных атак добавляется дополнительный шаг — подбор вектора $e_1 \cdot P_{\mathrm{sec}}$, который требует 2^k операций.

VI. Заключение

В данной работе проведено комплексное исследование модификации компактной версии криптосистемы Нидеррайтера. Основной целью работы было устранение критической уязвимости исходной компактной схемы при сохранении преимуществ в размере открытого ключа и обеспечении криптографической стойкости, соответствующей современным требованиям постквантовой криптографии.

Рассмотренная модификация демонстрирует устойчивость к ISD-атакам с сложностью $O(2^{(n/20)+k})$. Результаты подтверждают возможность практического применения предложенной модификации в системах защиты информации, требующих устойчивости к квантовым атакам.

Библиография

[1] P. W. Shor, «Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,» SIAM Journal on Computing, т. 26, № 5, с. 1484—1509, 1997.

[2] E. R. Berlekamp, Algebraic Coding Theory, Revised. Aegean Park Press, 1978.

[3] H. Niederreiter, «Knapsack-type cryptosystems and algebraic coding theory,» Problems of Control and Information Theory, т. 15, № 2, с. 157—166, 1986.

[4] A. Khalvan, A. Zali и M. A. Attari, «A Tiny Public Key Scheme Based on Niederreiter Cryptosystem,» arXiv preprint, 2023, arXiv:2310.06724.

[5] F. J. MacWilliams и N. J. A. Sloane, The Theory of Error-Correcting Codes. North-Holland, 1977.

[6] N. Patterson, «The Algebraic Decoding of Goppa Codes,» IEEE Transactions on Information Theory, т. 21, № 2, 1975.

Modification of Niederreiter cryptosystem compact version

Ivan Chizhov, Arina Kiryutkina

***Abstract*—This work proposes a modified compact version of the Niederreiter cryptosystem that eliminates vulnerabilities inherent in a previously suggested compact scheme. The security of the modified cryptographic system is reduced to the problem of decoding linear codes with an additional step of exhaustive search over error vectors in a subspace of dimension k.**

It is rigorously proven that the proposed modification preserves cryptographic strength equivalent to the classical Niederreiter cryptosystem while providing a substantial reduction in public key length. The paper provides formal descriptions of key generation, encryption, and decryption algorithms, accompanied by a detailed analysis of their computational complexity.

Furthermore, we establish that the modified scheme's resistance to Information Set Decoding (ISD) attacks exceeds that of the classical Niederreiter cryptosystem. This enhanced security is achieved through the introduction of an additional multiplicative factor of 2^k in the attack complexity, significantly raising the security level against state-of-the-art cryptanalytic techniques.

***Keywords*—Niederreiter cryptosystem, Goppa codes, public key**

References

[1] P. W. Shor, «Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer», *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[2] E. R. Berlekamp, *Algebraic Coding Theory*, Revised. Aegean Park Press, 1978.

[3] H. Niederreiter, «Knapsack-type cryptosystems and algebraic coding theory», *Problems of Control and Information Theory*, vol. 15, no. 2, pp. 157–166, 1986.

[4] A. Khalvan, A. Zali, and M. A. Attari, «A tiny public key scheme based on niederreiter cryptosystem», *arXiv preprint*, 2023, arXiv:2310.06724.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[6] N. Patterson, «The algebraic decoding of goppa codes», *IEEE Transactions on Information Theory*, vol. 21, no. 2, 1975.