Способы разложения рекурсивных матриц и их применение к реализации линейных преобразований

С. А. Давыдов, В. А. Шишкин

***Аннотация*—В работе изучаются линейные преобразования, задаваемые рекурсивными матрицами. Рекурсивные линейные преобразования используются, например, в шифрсистеме Кузнечик и семействе хэш-функций PHOTON. Для обратимой рекурсивной матрицы S^m найдены все решения уравнения подобия $X^{-1}(S^T)^m X = S^m$. На основне найденных решений предлагаются способы разложения рекурсивных матриц и вытекающие из них способы программной реализации рекурсивных линейных преобразований. Предложенные реализации обладают хорошими трудоемкостными характеристиками в соотношении время выполнения – используемая память. Отмечается, что матрица $(S^T)^m$ реализует умножение на многочлен x^m в кольце многочленов $Q[x]/f(x)$, является максимально рассеивающей матрицей и также обладает сравнительно эффективной программной реализацией. Предлагаемая для рекурсивных матриц Реализация 4 по скорости зашифрования уступает известной реализации с использованием LUT-таблиц на 23%, при этом использует в 8 раз меньший объем памяти. Поскольку аналогичные разложения справедливы для обратной матрицы рекурсивного линейного преобразования, расшифрование также обладает эффективной программной реализацией. Авторы полагают, что предложенные реализации могут быть полезны для малоресурсных устройств с программной реализацией алгоритмов. В заключительном разделе приводится сводная таблица различных программных реализаций шифрсистемы Кузнечик.**

***Ключевые слова*—рекурсивные матрицы, максимально рассеивающие матрицы, линейные преобразования, блочные шифрсистемы, Кузнечик.**

I. Введение

В соответствии с принципами Клода Шеннона из работы «Communication Theory of Secrecy Systems» [1], используемые в шифрсистемах и функциях хэширования преобразования должны обеспечивать свойства перемешивания и рассеивания поступающих на вход данных. Для обеспечения свойств рассеивания используются, как правило, линейные преобразования. Высокие показатели рассеивания матрицы и транспонированной матрицы линейного преобразования необходимы для защиты от разностного [2] и линейного [3], [4] методов криптоанализа.

На текущий момент известны (см. [5]) несколько теоретических методов построения максимально рассеивающих матриц над полями $\mathbb{F}_{2^s}$ с использованием матриц Коши (хэш-функция Стрибог [6]), матриц Вандермонда, рекурсивных матриц (также называют серийными, хэш-функция PHOTON [7], шифрсистема Кузнечик [8]), матриц Адамара и др. Некоторые максимально рассеивающие матрицы получают переборными методами, например матрицы-циркулянты (шифрсистема AES [9], шифрсистема SM4 [10], хэш-функция Whirlpool [11]).

Помимо криптографической стойкости важным требованием к шифрсистемам и функциям хэширования является высокая скорость выполнения преобразований. Применение предвычисленных таблиц (LUT-таблицы, см. [12]) позволяет достигать высокой скорости программной реализации, однако, хранение таких таблиц требует определенного объема быстродоступной памяти. В случае отсутствия необходимого объема памяти на вычислителе, вопрос более «легких» программных реализаций становится актуальным.

В данной работе мы изучаем линейные преобразования, выполняемые рекурсивными матрицами, и предлагаем для них альтернативные варианты программной реализации. Предлагаемые реализации используют относительно небольшой объем быстродоступной памяти и обеспечивают достаточно высокую скорость выполнения преобразований. Реализации применимы к любой рекурсивной матрице, в частности, к матрицам шифрсистемы Кузнечик и семейству хэш-функций PHOTON. Отметим, что частный случай одного из вариантов разложения (см. раздел V) матрицы линейного преобразования шифрсистемы Кузнечик был получен в работе [13].

В разделе II мы введем основные определения и напомним некоторые свойства матриц. В разделе III мы рассмотрим общую концепцию построения матриц для линейных преобразований, задаваемых через умножение на элемент кольца (поля). В разделах IV и V мы получим два способа разложения рекурсивной матрицы общего вида. В разделе VI мы перечислим основные способы программной реализации рекурсивных матриц и предложим два новых способа. В разделе VII мы приведем сводную таблицу различных программных реализаций шифрсистемы Кузнечик с указанием числа операций, объема памяти и скорости зашифрования.

II. Основные определения

Всюду далее нумерацию координат векторов будем вести справа налево, а нумерацию строк матриц - снизу вверх. Все нумерации будем начинать с нуля.

Под раундом XSL-схемы мы понимаем последовательность следующих трех преобразований:

Статья получена 22 июня 2023

Степан Андреевич Давыдов, Лаборатория Криптографии АО НПК «Криптонит», (email: s.davydov@kryptonite.ru).

Василий Алексеевич Шишкин, Лаборатория Криптографии АО НПК «Криптонит», (email: v.shishkin@kryptonite.ru).

- Наложение ключа по модулю 2 (XOR).
- Применение нелинейного преобразования (слой S-боксов).
- Применение линейного преобразования (L-слой).

Линейное преобразование задаваемое (реализуемое) матрицей A будем обозначать $\widehat{A}$.

Пусть $Q = \mathbb{F}_{q^s}$ - конечное поле из q^s элементов, $f(x) = x^m - f_{m-1}x^{m-1} - ...f_1x - f_0$ - унитарный многочлен степени m над полем Q. *Сопровождающей матрицей* многочлена $f(x)$ назовем следующую матрицу над полем Q:

$$S_{m\times m} = S(f(x)) = \begin{pmatrix} f_{m-1} & 1 & 0 & ... & 0 \\ f_{m-2} & 0 & 1 & ... & 0 \\ ... & ... & ... & ... & ... \\ f_1 & 0 & 0 & ... & 1 \\ f_0 & 0 & 0 & ... & 0 \end{pmatrix}.$$

Матрица S обратима тогда и только тогда, когда $f_0 \neq 0$. Всюду далее считаем это условие выполненным.

При $k > 1$ матрицу $S^k = S(f)^k$ будем называть *рекурсивной матрицей*.

Линейной рекуррентной последовательностью (ЛРП) над полем Q с характеристическим многочленом $f(x)$ и начальным вектором $\overrightarrow{u} = (u_{m-1}, ..., u_0) \in Q^m$ назовем последовательность, в которой $u_{i+m} = u_{i+m-1}f_{m-1} + ... + u_if_0$ при всех $i \geq 0$. Для всех $k > 0$ справедливо равенство:

$$(u_{k+m-1}, ..., u_k) = (u_{k+m-2}, ..., u_{k-1})S = \\ = ... = (u_{m-1}, ..., u_0)S^k \quad (1)$$

Многочлен

$$f^*(x) = (f(0))^{-1}x^m f(\frac{1}{x}) = \\ x^m + f_0^{-1}f_1x^{m-1} + ... + f_0^{-1}f_{m-1}x - f_0^{-1}$$

будем называть *двойственным многочленом* к многочлену $f(x)$. Если $f(x)$ - характеристический многочлен последовательности $(..., u_{i+m}, ..., u_1, u_0)$, то $f^*(x)$ - характеристический многочлен последовательности элементов u_i, взятых в обратном порядке: $(..., u_0, u_1, ..., u_{i+m-1}, u_{i+m})$.

Вектор $(0, ..., 0, 1, 0, ..., 0) \in Q^m$ с единицей на i-ом месте будем обозначать $\overrightarrow{E}_i$. Единичная матрица равна

$$E_{m\times m} = \begin{pmatrix} \overrightarrow{E}_{m-1} \\ \overrightarrow{E}_{m-2} \\ ... \\ \overrightarrow{E}_0 \end{pmatrix}.$$

Обозначим за T следующую перестановочную матрицу:

$$T_{m\times m} = \begin{pmatrix} \overrightarrow{E}_0 \\ \overrightarrow{E}_1 \\ ... \\ \overrightarrow{E}_{m-1} \end{pmatrix}.$$

Справедливы следующие факты:

1) $T = T^{-1}$.
2) Произведение TA меняет в матрице A порядок строк на противоположный, т. е. i-я строка матрицы A равна $(m-1-i)$-ой строке матрицы TA: $\overrightarrow{A}_i = \overrightarrow{(TA)}_{m-1-i}$.
3) Произведение AT меняет в матрице A порядок столбцов на противоположный, т. е. i-й столбец матрицы A равен $(m-1-i)$-ому столбцу матрицы TA: $A_i^{\downarrow} = (TA)_{m-1-i}^{\downarrow}$.
4) Произведение TAT отображает в матрице A все элементы относительно центра, т. е. $a_{i,j} = (tat)_{m-1-i,m-1-j}$, где tat - соответствующий элемент матрицы TAT.

Под умножением матрицы $A \in Q_{m,m}$ на элемент $a \in Q$ будем понимать умножение каждого элемента матрицы A на элемент a.

Весом $\omega(\overrightarrow{a})$ вектора $\overrightarrow{a} \in Q^m$ будем называть число ненулевых координат вектора $\overrightarrow{a}$.

Очевидно, что $\omega(\overrightarrow{E}_i) = 1$ при любом i.

Показателем рассеивания матрицы $A \in Q_{m,m}$ будем называть следующее число:

$$\tau(A) = \min_{\overrightarrow{a} \neq \overrightarrow{0}} [\omega(\overrightarrow{a}) + \omega(\overrightarrow{a}A)].$$

Нетрудно показать, что $\tau(A) = \tau(A^{-1})$ и $\tau(A) \leq m+1$. Если $\tau(A) = m+1$, матрицу A будем называть *максимально рассеивающей матрицей*.

При некоторых ограничениях, накладываемых на многочлен $f(x)$, матрица $S(f(x))^m$ является максимально рассеивающей матрицей. Линейные преобразования, реализуемые рекурсивными максимально рассеивающими матрицами, используются в качестве линейных преобразований в шифрсистеме Кузнечик и семействе хэш-функций PHOTON.

Линейные преобразования, задаваемые рекурсивными матрицами, можно выполнять как общим способом (умножением вектора на матрицу), так и рекурсивным способом, через вычисление элементов ЛРП с использованием формулы (1).

III. Линейные преобразования, реализуемые через умножение на элемент кольца

Пусть $f(x)$ - многочлен степени m над полем $Q = \mathbb{F}_{q^n}$, $R = Q[x]/f(x)$ - факторкольцо многочленов, которое можно также рассматривать как векторное пространство размерности m над полем Q с операциями сложения многочленов и умножения многочлена на элемент $a \in Q$. Пусть $\varphi : Q^m \to R$ - отображение, переводящее строку вектора в соответствующий многочлен:

$$\varphi(a_{m-1}, ..., a_1, a_0) = a_{m-1}x^{m-1} + ... + a_1x + a_0.$$

Нетрудно видеть, что φ - изоморфизм векторных пространств. Поскольку умножение на элемент $\alpha(x)$ кольца R является линейным преобразованием кольца R, соответствующее ему преобразование $\overrightarrow{a} \to \varphi^{-1}(\alpha(x) \cdot \varphi(\overrightarrow{a}))$ пространства Q^m можно задать матрицей $A \in Q_{m,m}$, которую будем обозначать A_α.

A. Критерий представимости матрицы через умножение на элемент кольца

Теорема III.1. *Пусть $f(x)$ - многочлен степени m над полем Q, $R = Q[x]/f(x)$ - факторкольцо многочленов. Матрица $A \in Q_{m,m}$ равна матрице A_α для некоторого $\alpha(x) \in R$ тогда и только тогда, когда для любого $i \in \overline{1, m-1} : \varphi(\overrightarrow{A_i}) = x^i\varphi(\overrightarrow{A_0})$ в кольце R. В условиях Теоремы $\alpha(x) = \varphi(\overrightarrow{A_0})$.*

□ **Необходимость.** Пусть $A = A_\alpha$. Заметим, что $\varphi(\overrightarrow{E_i}) = x^i$. Тогда $\varphi(\overrightarrow{A_i}) = \varphi(\overrightarrow{E_i}\cdot A) = \varphi(\varphi^{-1}(\alpha(x)\cdot\varphi(\overrightarrow{E_i}))) = \alpha(x)x^i$ при любом i. Подставив $i = 0$, получим $\alpha(x) = \varphi(\overrightarrow{A_0})$.

Достаточность. Для произвольного $\overrightarrow{c} = (c_{m-1}, ..., c_0)$

$$(c_{m-1}, ..., c_0)A = \sum_{i=0}^{m-1} c_i\overrightarrow{A_i} = \varphi^{-1}(\sum_{i=0}^{m-1} c_i\varphi(\overrightarrow{A_i})) =$$
$$\varphi^{-1}(\varphi(\overrightarrow{A_0})\cdot\sum_{i=0}^{m-1} c_i x^i) = \varphi^{-1}(\varphi(\overrightarrow{A_0})\cdot\varphi(\overrightarrow{c})).$$

Значит по определению $A = A_\alpha$, где $\alpha(x) = \varphi(\overrightarrow{A_0})$.■

Пример III.1. *Матрица-циркулянт.*

Матрицу $A \in Q_{m,m}$ вида:

$$\begin{pmatrix} a_0 & a_{m-1} & ... & a_2 & a_1 \\ a_1 & a_0 & ... & a_3 & a_2 \\ ... & ... & ... & ... & ... \\ a_{m-2} & ... & a_1 & a_0 & a_{m-1} \\ a_{m-1} & ... & a_2 & a_1 & a_0 \end{pmatrix}$$

будем называть *матрицей-циркулянтом*. Матрица-циркулянт реализует умножение в кольце $R = Q[x]/(x^m - e)$ на элемент кольца $\varphi(a_{m-1}, ..., a_0) = a_{m-1}x^{m-1} + ... + a_1x + a_0$.

Для того, чтобы умножить $a(x)$ на $b(x)$ в R достаточно выполнить умножение $a(x)\cdot b(x) = c(x)$ в кольце $Q[x]$ и затем сложить младшую и старшую координатные половины результата $\varphi^{-1}(c(x)) : (c_{2m-1}, ..., c_m) + (c_{m-1}, ..., c_0)$. Применив отображение φ к полученному результату суммы, найдем результат умножения $a(x)$ на $b(x)$ в R.

Пример III.2. *Транспонирование сопровождающей матрицы.*

Пусть $S = S(f(x))$ - сопровождающая матрица многочлена $f(x)$, тогда матрица S^T имеет вид:

$$S^T = \begin{pmatrix} f_{m-1} & f_{m-2} & ... & f_1 & f_0 \\ 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & 1 & 0 \end{pmatrix}$$

Матрица S^T реализует умножение на элемент x в кольце $R = Q[x]/f(x)$. Матрица $(S^m)^T = (S^T)^m$ реализует умножение на элемент x^m в том же кольце. В случае неприводимости многочлена $f(x)$ кольцо R является полем.

B. Случай рекурсивных матриц

Поскольку матрицы S^m и $(S^m)^T$ являются подобными, рекурсивное преобразование $\widehat{S^m}$ также является умножением на элемент кольца x^m, но в другом базисе. Это означает, что выполнить рекурсивное преобразование $\widehat{S^m}$ можно в три этапа:

1) Перейти в базис, в котором матрица преобразования имеет вид $(S^T)^m = A_{x^m}$.
2) Выполнить умножение на элемент кольца x^m.
3) Вернуться в исходный базис.

Найдем всевозможные матрицы C, которые выполняют переход между вышеуказанными базисами.

Теорема III.2. *Для сопровождающей матрицы $S = S(f(x))$ выполняется равенство $S = C^{-1}S^TC$ тогда и только тогда, когда C - обратимая матрица вида:*

$$C = \begin{pmatrix} c_{2m-2} & c_{2m-3} & ... & c_m & c_{m-1} \\ c_{2m-3} & c_{2m-4} & ... & c_{m-1} & c_{m-2} \\ ... & ... & ... & ... & ... \\ c_m & c_{m-1} & ... & c_2 & c_1 \\ c_{m-1} & c_{m-2} & ... & c_1 & c_0 \end{pmatrix}, \qquad (2)$$

где $(c_{2m-2}, ..., c_0)$ - последовательные элементы ЛРП с характеристическим многочленом $f(x)$. Матрица вида (2) называется Ганкелевой матрицей [5].

□ Для обратимой матрицы C равенство $S = C^{-1}S^TC$ равносильно равенству $CS = S^TC$ или

$$\begin{pmatrix} \overrightarrow{C_{m-1}f^\downarrow} & C^\downarrow_{m-1} & ... & C^\downarrow_1 \\ \overrightarrow{C_{m-2}f^\downarrow} & ... & ... & ... \\ \overrightarrow{C_{m-3}f^\downarrow} & ... & ... & ... \\ ... & ... & ... & ... \\ \overrightarrow{C_0f^\downarrow} & ... & ... & ... \end{pmatrix} =$$
$$= \begin{pmatrix} \overrightarrow{f}C^\downarrow_{m-1} & \overrightarrow{f}C^\downarrow_{m-2} & ... & \overrightarrow{f}C^\downarrow_0 \\ \overrightarrow{C_{m-1}} & ... & ... & ... \\ \overrightarrow{C_{m-2}} & ... & ... & ... \\ ... & ... & ... & ... \\ \overrightarrow{C_1} & ... & ... & ... \end{pmatrix},$$

где $\overrightarrow{f} = (f_{m-1}, ..., f_0) = \varphi^{-1}(f(x))$ без m-ой координаты.

Рассмотрим подматрицы указанных выше матриц с номерами строк и столбцов от 0 до $m-2$:

$$\begin{pmatrix} c_{m-2,m-1} & c_{m-2,m-2} & ... & c_{m-2,1} \\ c_{m-3,m-1} & c_{m-3,m-2} & ... & c_{m-3,1} \\ ... & ... & ... & ... \\ c_{0,m-1} & c_{0,m-2} & ... & c_{0,1} \end{pmatrix} =$$
$$\begin{pmatrix} c_{m-1,m-2} & c_{m-1,m-3} & ... & c_{m-1,0} \\ c_{m-2,m-2} & c_{m-3,m-3} & ... & c_{m-2,0} \\ ... & ... & ... & ... \\ c_{1,m-2} & c_{1,m-3} & ... & c_{1,0} \end{pmatrix}.$$

Равенство указанных подматриц равносильно тому, что матрица C имеет вид (2). В силу симметричности матрицы C равенство $(m-1)$-ых строк матриц CS и S^TC равносильно равенству $(m-1)$-ых столбцов тех же матриц. Равенство $(m-1)$-ых строк указанных матриц равносильно системе уравнений:

$$\begin{cases} c_{m-1,m-1} = \overrightarrow{f}C^\downarrow_{m-2} \\ c_{m-1,m-2} = \overrightarrow{f}C^\downarrow_{m-3} \\ ... \\ c_{m-1,1} = \overrightarrow{f}C^\downarrow_0 \end{cases}$$

или, с учетом элементов матрицы (2):

$$\begin{cases} c_{2m-2} = \overrightarrow{f} C_{m-2}^{\downarrow} \\ c_{2m-3} = \overrightarrow{f} C_{m-3}^{\downarrow} \\ ... \\ c_m = \overrightarrow{f} C_0^{\downarrow} \end{cases} \quad (3)$$

Условие (3) равносильно тому, что элементы $(c_{2m-2}, ..., c_0)$ есть последовательные элементы ЛРП с характеристическим многочленом $f(x)$. ■

IV. Выбор матрицы перехода C в уравнении подобия рекурсивной матрицы

Для эффективности реализации линейного преобразования рекурсивной матрицы в качестве матрицы подобия можно выбирать наиболее «легковесные» матрицы. Поскольку элементы матрицы подобия C лежат на ЛРП с характеристическим многочленом степени m, для однозначного задания матрицы C достаточно выбрать m последовательных элементов в последовательности $(c_{2m-2}, ..., c_0)$. Если выбрать m нулевых элементов, все элементы ЛРП будут равны нулю и матрица C будет нулевой. В данном пункте мы рассмотрим два варианта выбора последовательных элементов ЛРП, среди которых $m - 1$ нулевой и один единичный.

Предварительно докажем вспомогательное утверждение:

Утверждение IV.1. *Пусть многочлен над полем Q $f(x) = x^m - f_{m-1}x^{m-1} - ... - f_0$ - , $k \le m$ и матрицы $C \in Q_{k,k}$ и $C' \in Q_{k,k}$ имеют вид:*

$$C = \begin{pmatrix} c_{k-1} & c_{k-2} & ... & c_1 & c_0 \\ c_{k-2} & c_{k-3} & ... & c_0 & 0 \\ ... & ... & ... & ... & ... \\ c_1 & c_0 & ... & 0 & 0 \\ c_0 & 0 & ... & 0 & 0 \end{pmatrix},$$

$$C' = \begin{pmatrix} 0 & 0 & ... & 0 & c_0 \\ 0 & 0 & ... & c_0 & c_1 \\ ... & ... & ... & ... & ... \\ 0 & c_0 & ... & c_{k-3} & c_{k-2} \\ c_0 & c_1 & ... & c_{k-2} & c_{k-1} \end{pmatrix},$$

где $(c_{k-1}, ..., c_0, 0, ..., 0)$ - $m + k - 1$ последовательных элемента ЛРП с характеристическим многочленом $f(x)$. Тогда обратными матрицами к матрицам C и C' соответственно будут следующие матрицы:

$$C^{-1} = c_0^{-1} \cdot \begin{pmatrix} 0 & 0 & ... & 0 & 1 \\ 0 & 0 & ... & 1 & -f_{m-1} \\ ... & ... & ... & ... & ... \\ 0 & 1 & ... & -f_{m-k+3} & -f_{m-k+2} \\ 1 & -f_{m-1} & ... & -f_{m-k+2} & -f_{m-k+1} \end{pmatrix},$$

$$(C')^{-1} = c_0^{-1} \cdot \begin{pmatrix} -f_{m-k+1} & -f_{m-k+2} & ... & -f_{m-1} & 1 \\ -f_{m-k+2} & -f_{m-k+3} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ -f_{m-1} & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix}$$

□ Обозначим первую из указанных выше матриц как F и покажем, что $FC = E$. Заметим, что в i-ой строке матрицы F последние i элементов нулевые, а в j-ом столбце матрицы C первые $m-1-j$ элементов нулевые. Посчитаем элемент

$$(fc)_{ij} = \overrightarrow{F}_i C_j^{\downarrow} \quad (4)$$

в 3 случаях:

1) i > j. Тогда $i+m-1-j \ge m$ и в произведении (4) нет ненулевых слагаемых, поэтому произведение равно нулю.
2) i = j. Тогда $i + m - 1 - j = m - 1$ и единственное ненулевое слагаемое в произведении (4) есть $f_{i,i}c_{i,i} = c_0^{-1} \cdot c_0 = 1$.
3) i < j. Тогда (4) без учета нулевых слагаемых будет равно

$$c_0^{-1}[(1 \cdot c_{j-i} - f_{m-1}c_{j-i-1} - ... - f_{m-(j-i)} \cdot c_0) = (1 \cdot c_{j-i} - ... - f_{m-(j-i)} \cdot c_0 - f_{m-(j-i)-1} \cdot 0 - ... - f_0 \cdot 0)].$$

Последнее выражение равно нулю, поскольку вектор $(c_{j-i}, c_{j-i-1}, ..., c_1, c_0, 0, ..., 0)$ состоит из последовательных элементов ЛРП с характеристическим многочленом $f(x)$.

Таким образом, $(fc)_{ij} = 0$ при $i \ne j$ и $(fc)_{ij} = 1$ при $i = j$, значит матрица FC есть единичная матрица.

Заметим, что $C' = TCT$ (см. свойства матрицы T в разделе II). Тогда $(C')^{-1} = TC^{-1}T$. ■

Перейдем к выбору матрицы подобия C.

Утверждение IV.2. *Пусть в условиях Теоремы III.2 $m = 2k$ и $c_k = ... = c_{3k-2} = 0, c_{3k-1} = 1$, тогда матрицы C и C^{-1} в разложении*

$$C^{-1}(S^T)^m C = S^m \quad (5)$$

состоят из двух блоков размера $k \times k$ и имеют следующий вид:

$$C = diag\left(\begin{pmatrix} c_{2m-2} & c_{2m-3} & ... & c_{2m-k} & 1 \\ c_{2m-3} & c_{2m-4} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ c_{2m-k} & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & ... & 0 & c_{k-1} \\ 0 & 0 & ... & c_{k-1} & c_{k-2} \\ ... & ... & ... & ... & ... \\ 0 & c_{k-1} & ... & c_2 & c_1 \\ c_{k-1} & c_{k-2} & ... & c_1 & c_0 \end{pmatrix} \right) \quad (6)$$

$$C^{-1} = diag\left(\begin{pmatrix} 0 & 0 & ... & 0 & 1 \\ 0 & 0 & ... & 1 & -f_{m-1} \\ ... & ... & ... & ... & ... \\ 0 & 1 & ... & -f_{m-k+3} & -f_{m-k+2} \\ 1 & -f_{m-1} & ... & -f_{m-k+2} & -f_{m-k+1} \end{pmatrix}, \begin{pmatrix} f_{k-1} & f_{k-2} & ... & f_1 & f_0 \\ f_{k-2} & f_{k-3} & ... & f_0 & 0 \\ ... & ... & ... & ... & ... \\ f_1 & f_0 & ... & 0 & 0 \\ f_0 & 0 & ... & 0 & 0 \end{pmatrix} \right) \quad (7)$$

где $(c_{2m-1}, c_{2m-2}, ..., c_{2m-k+1}, 1, 0, ..., 0)$ - $m + k - 1$ последовательных элементов ЛРП с характеристическим многочленом $f(x)$, $(c_0, c_1, ..., c_{k-1}, 0, ..., 0)$ - $m+k-1$ последовательных элементов ЛРП с характеристическим многочленом $f^*(x)$ (см. раздел II).

□ Поскольку в матрице (2) элементы $c_k, ..., c_{3k-2}$ равны нулю, матрица C является блочно-диагональной с двумя блоками размера $k \times k$, причем блоки будут иметь вид, как в матрице (6). Поскольку в матрице (2) элементы $(c_{2m-2}, ..., c_0)$ образуют ЛРП с характеристическим многочленом $f(x)$, для того, чтобы найти элементы $(c_{2m-2}, c_{2m-3}, ..., c_{m+1}, 1, 0, ..., 0)$ и $(c_0, c_1, ..., c_{k-1}, 0, ..., 0)$ в матрице (6) достаточно рассчитать элементы ЛРП с начального состояния $c_k = ... = c_{3k-2} = 0$, $c_{3k-1} = 1$ в прямом направлении на $k-1$ тактов и обратном направлении на k тактов. В прямом направлении вычисление элементов происходит по закону рекурсии, задаваемому многочленом $f(x)$, в обратном – многочленом $f^*(x)$.

Обратная матрица C^{-1} будет состоять из двух блоков размера $k \times k$, каждый из которых является обратной матрицей к соответствующему блоку матрицы C.

В соответствии с Утверждением IV.1 верхний блок матрицы (7) будет обратной матрицей к верхнему блоку матрицы (6). Нижний блок матрицы (6) составлен из последовательных элементов ЛРП с начальным вектором $(c_{k-1} = f_0^{-1}, 0, ..., 0)$ и характеристическим многочленом $f^*(x) = x^m + f_0^{-1}(f_1 x^{m-1} + ... + f_{m-1}x - 1)$. Значит, в соответствии с Утверждением IV.1, нижний блок матрицы (7) будет обратной матрицей к нижнему блоку матрицы (6). ■

Утверждение IV.3. *Пусть в условиях Теоремы III.2 $c_0 = ... = c_{m-2} = 0, c_{m-1} = 1$, тогда матрицы C и C^{-1} соответственно имеют вид:*

$$C = \begin{pmatrix} c_{2m-2} & c_{2m-3} & ... & c_m & 1 \\ c_{2m-3} & c_{2m-4} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ c_m & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix},$$

$$C^{-1} = \begin{pmatrix} 0 & 0 & ... & 0 & 1 \\ 0 & 0 & ... & 1 & -f_{m-1} \\ ... & ... & ... & ... & ... \\ 0 & 1 & ... & -f_3 & -f_2 \\ 1 & -f_{m-1} & ... & -f_2 & -f_1 \end{pmatrix}, \quad (8)$$

где $(c_{2m-2}, c_{2m-3}, ..., c_m, 1, 0, ..., 0)$ - последовательные элементы ЛРП длины $2m-1$ с характеристическим многочленом
$f(x) = x^m - f_{m-1}x^{m-1} - ... - f_1 x - f_0$.

□ Утверждение IV.3 напрямую следует из Теоремы III.2 и Утверждения IV.1. ■

V. Разложение рекурсивных матриц

Теорема V.1. *Пусть $f(x) = x^m - f_{m-1}x^{m-1} - ... - f_0$ - многочлен над полем $Q = \mathbb{F}_{q^n}$, $S = S(f)$ - его сопровождающая матрица, $A = S^m$ - рекурсивная матрица. Пусть $\overrightarrow{E_{m-1}} \cdot S^{m-1} = (c_{m-1}, ..., c_1, 1)$. Тогда справедливо следующее разложение матрицы A в произведение матриц $F \cdot C$:*

$$A = \begin{pmatrix} f_{m-1} & f_{m-2} & ... & f_1 & f_0 \\ f_{m-2} & f_{m-3} & ... & f_0 & 0 \\ ... & ... & ... & ... & ... \\ f_1 & f_0 & ... & 0 & 0 \\ f_0 & 0 & ... & 0 & 0 \end{pmatrix} \cdot$$
$$\cdot \begin{pmatrix} c_{m-1} & c_{m-2} & ... & c_1 & 1 \\ c_{m-2} & c_{m-3} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ c_1 & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix} \quad (9)$$

□ В условиях Утверждения IV.3 с перенумерованием индексов элементов c_i разложение матрицы S^m имеет вид $S^m = C^{-1}(S^T)^m C =$

$$\begin{pmatrix} 0 & 0 & ... & 0 & 1 \\ 0 & 0 & ... & 1 & -f_{m-1} \\ ... & ... & ... & ... & ... \\ 0 & 1 & ... & -f_3 & -f_2 \\ 1 & -f_{m-1} & ... & -f_2 & -f_1 \end{pmatrix} (S^T)^m$$
$$\begin{pmatrix} c_{m-1} & c_{m-2} & ... & c_1 & 1 \\ c_{m-2} & c_{m-3} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ c_1 & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix}$$

Матрица $(S^T)^m$ реализует умножение на элемент кольца x^m. При умножении матрицы C^{-1} на матрицу $(S^T)^m$ каждая строка матрицы C^{-1} умножается на матрицу $(S^T)^m$, то есть каждый элемент $\varphi(\overrightarrow{C_i^{-1}})$ кольца $Q[x]/f(x)$ умножается на x^m.

$$\varphi(\overrightarrow{C_i^{-1}}) \cdot x^{i+1} \ mod \ f(x) =$$
$$(x^m - f_{m-1}x^{m-1} - ... - f_{i+1}x^{i+1}) -$$
$$- (x^m - f_{m-1}x^{m-1} - ... - f_1 x - f_0) =$$
$$f_i x^i + ... + f_1 x + f_0.$$

Значит $\varphi(\overrightarrow{C_i^{-1}}) \cdot x^m \ mod \ f(x) = f_i x^{m-1} + ... + f_0 x^{m-1-i}$ и $\varphi^{-1}[\varphi(\overrightarrow{C_i^{-1}}) \cdot x^m \ mod \ f(x)] = (f_i, ..., f_0, 0, ..., 0)$. ■

Следствие V.1. *Пусть выполнены условия Теоремы V.1, $g(x) = f^*(x)$ и $f_0^{-1}\overrightarrow{E_{m-1}}S(g)^{m-1} = (d_{m-1}, ..., d_1, d_0)$, $d_0 = f_0^{-1}$. Тогда обратной матрицей к матрице $A = S(f)^m$ будет следующая матрица:*

$$A^{-1} = \begin{pmatrix} 0 & 0 & ... & 0 & 1 \\ 0 & 0 & ... & 1 & -f_{m-1} \\ ... & ... & ... & ... & ... \\ 0 & 1 & ... & ... & -f_2 \\ 1 & -f_{m-1} & ... & -f_2 & -f_1 \end{pmatrix} \cdot$$
$$\begin{pmatrix} 0 & 0 & ... & 0 & d_0 \\ 0 & 0 & ... & d_0 & d_1 \\ ... & ... & ... & ... & ... \\ 0 & d_0 & ... & ... & d_{m-2} \\ d_0 & d_1 & ... & d_{m-2} & d_{m-1} \end{pmatrix} \quad (10)$$

□ Заметим, что первую матрицу в произведении (9) можно представить, как:

$$f_0 \cdot \begin{pmatrix} f_0^{-1}f_{m-1} & f_0^{-1}f_{m-2} & ... & f_0^{-1}f_1 & 1 \\ f_0^{-1}f_{m-2} & f_0^{-1}f_{m-3} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ f_0^{-1}f_1 & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix}$$

Тогда, в соответствии с Утверждением IV.1, первая и вторая матрицы в произведении (10) являются обратными матрицами ко второй и первой матрицам соответственно в произведении (9). ■

VI. Реализации рекурсивных матриц

A. Известные реализации

В этом пункте и всюду далее $q = 2$. На текущий момент авторам известны следующие варианты программной реализации линейных преобразований, задаваемых рекурсивными матрицами:

1) Реализация линейного регистра сдвига (вычисление элементов ЛРП на m тактов вперед).
2) Реализация линейного регистра сдвига с предвычисленной таблицей умножения в поле $\mathbb{F}_{2^n}$. Данная реализация отличается от Реализации 1 лишь тем, что вместо умножения в поле выполняется обращение в соответствующую область памяти. Поскольку при вычислении элементов ЛРП умножение выполняется только на коэффициенты многочлена f, в памяти необходимо хранить лишь m строк таблицы умножения ($m \cdot 2^n$ элементов поля).
3) Использование предвычисленных LUT-таблиц из $m^2 \cdot 2^n$ элементов поля $\mathbb{F}_{2^n}$ [12].

Первый вариант достаточно медленный ввиду очень большого числа выполняемых операций. Второй вариант существенно быстрее первого, но требует хранения небольшой таблицы в памяти. Третий вариант применим к любой XSL-схеме (не обязательно с рекурсивным линейным преобразованием) и является самым быстрым на современных процессорах с достаточным объемом кэш-памяти. Однако, в случае когда шифрование реализуется на вычислителе с небольшими ресурсами, третий вариант может не удовлетворять ограничениям по используемой памяти.

Разложения рекурсивной матрицы вида (5) и (9) позволяют предложить новые варианты выполнения SL-преобразования, являющиеся «компромиссными» по количеству операций и объему используемой памяти.

B. Реализация через разложение рекурсивной матрицы

Результат умножения вектора $\overrightarrow{a} = (a_{m-1}, ..., a_0)$ на матрицу A можно вычислить, посчитав линейную комбинацию строк матрицы A : $\overrightarrow{a}A = a_{m-1}\overrightarrow{A_{m-1}} + ... + a_0\overrightarrow{A_0}$. Для матриц F и C из (9) строки с номером i, умноженные на произвольный элемент поля $a_i \in Q$, могут быть получены сдвигом строки с номером $m-1$, умноженной на тот же элемент поля a_i на $m-1-i$ позиций влево. Если заранее вычислить произведение строки $\overrightarrow{F_{m-1}} = (f_{m-1}, ..., f_0)$ на все элементы поля Q, то при зашифровании вычислять $a_i\overrightarrow{F_i}$ можно путем обращения в соответсвующую область памяти и сдвигом на $(m-1-i)$ элементов влево. Аналогичный результат справедлив для матрицы C.

Для выполнения L-преобразования умножим поступивший вектор последовательно на матрицы F и C указанным выше способом. Для совмещения преобразований S и L в одно достаточно в предвычисленной таблице матрицы F по адресу $a \in Q$ хранить результат умножения $S(a) \cdot \overrightarrow{F_{m-1}}$.

Указанные таблицы для матриц F и C требуют хранения $2m \cdot 2^n$ элементов поля Q, что в $m/2$ раз меньше, чем в третьм варианте реализации и в 2 раза больше, чем во втором варианте реализации. При расшифровании можно использовать разложеине (10).

C. Реализация через умножение на элемент кольца (поля)

В указанной реализации необходимо последовательно выполнить умножение поступающего на вход L-преобразования вектора на 3 матрицы из равенства (5). Матрица $(S^T)^m$ реализует умножение в кольце R на элемент x^m. Матрицы C^{-1} и C реализуют переход в соответствующий базис и возврат в исходный базис.

Выполнять умножение на матрицы C^{-1} и C можно способом, указанным в предыдущем пункте. Для этого потребуется хранить $m \cdot 2^n$ элементов поля для каждой матрицы (в случае некоторых шифрсистем, например шифрсистемы Кузнечик, оценка может быть меньше).

Выполнять умножение на x^m в кольце R можно путем m-кратного умножения на x. Для умножения на x в кольце R необходимо сдвинуть элементы вектора $(a_{m-1}, ..., a_0)$ влево на одну позицию и привести результат по модулю $f(x)$. Для приведения по модулю, к результату сдвига необходимо добавить $f(x)$, умноженный на a_{m-1}. Поскольку старший коэффициент всегда сокращается, результат умножения на x равен $\varphi[(a_{m-2}, ..., a_0, 0) + (a_{m-1}f_{m-1}, ..., a_{m-1}f_0)]$.

Если заранее вычислить результаты умножения вектора $\overrightarrow{f} = (f_{m-1}, ..., f_0)$ на все элементы поля Q, то результат умножения на x можно вычислять за один нециклический сдвиг, одно обращение в память и одно сложение по модулю 2. Указанный способ умножения требует хранения $m \cdot 2^n$ элементов поля. Итого, реализация через умножение на элемент кольца требует хранения $3m \cdot 2^n$ элементов поля в общем случае. Объединение преобразований S и L выполняется аналогично предыдущему пункту.

D. Новые эффективные максимально рассеивающие преобразования

В предыдущем пункте мы рассмотрели реализацию рекурсивной матрицы $S^m = C^{-1}(S^T)^m C$ как последовательную реализацию матриц C^{-1}, $(S^T)^m$ и C. Заметим, что сама по себе матрица $(S^T)^m$ также является максимально рассеивающей матрицей и может быть использована в качестве линейного преобразования. Как было отмечено в предыдущем пункте, реализация такой матрицы требует хранения $m \cdot 2^n$ элементов поля, что в 3 раза меньше, чем в случае (VI-C) и в 2 раза меньше, чем в случае (VI-B). Число выполняемых при этом операций также сократится. Недостатком указанного подхода является невозможность объединения преобразований S и L в одно преобразование.

VII. Сравнение реализаций шифрсистемы Кузнечик

В данном пункте мы сравним 5 различных реализаций шифрсистемы Кузнечик. Все реализации выполнены на языке программирования C++. Авторы статьи не ставили перед собой цель добиться максимально быстрого шифрования в каждой из реализаций и не использовали каких-либо средств оптимизации, выходящих за рамки «разумного» написания кода программы. Цель авторов состояла именно в сравнении (приблизительном сравнении) указанных реализаций.

Реализации 1-3 совпадают с реализациями из пункта VI-A. Реализация 4 - реализация через разложение рекурсивной матрицы (см. VI-B), Реализация 5 - реализация через умножение на элемент кольца с переходом в соответствующий базис (см. VI-C).

Шифрсистема Кузнечик использует следующие параметры $n = 8$ (т. е. нелинейное преобразование S выполняется над 8-битными векторами) и $m = 16$ (т. е. линейное преобразование реализуется матрицей размера 16×16, состоящей из элементов поля $\mathbb{F}_{2^8}$).

Размер S-бокса составляет $2^8 \cdot 8$ бит или 256 байт. S-бокс необходимо хранить в реализациях 1-2. В реализациях 3-5 преобразования S и L объединены и хранение S-бокса не требуется. Поскольку у многочлена f всего 8 различных коэффициентов и один из них равен единице, размер таблицы умножения для Реализации 2 равен $7 \cdot 2^8 \cdot 8$ бит или 1,75 Кбайт. Размер предвычисленных таблиц для Реализации 3 равен $16 \cdot 16 \cdot 2^8 \cdot 8$ бит или 64 Кбайта. Размер предвычисленных таблиц для Реализации 4 равен $2 \cdot 16 \cdot 2^8 \cdot 8$ бит или 8 Кбайт. Для Реализации 5 предвычисленные таблицы $\{a\overrightarrow{f},\ a \in Q\}$ занимают 4 Кбайта. Эти же таблицы заменяют таблицы для матрицы C. В силу условия $f^*(x) = f(x)$ вектор $(c_{15}, ..., c_8)$ совпадает с вектором $(c_0, ..., c_7)$ и для матрицы C^{-1} таблицы занимают 2 Кбайта. Общий объем памяти для Реализации 5 равен 6 Кбайт.

Программы выполнялись на одном ядре процессора Intel Core i5-8265U с тактовой частотой 3.9 GHz в режиме Turbo Boost и размерами кэш-памяти первого, второго и третьего уровня соответственно 32 Кбайта, 256 Кбайт и 6 Мбайт(общий для 4 ядер). Для обобщения результатов рассчитана величина cycles per byte (cbp), равная отношению тактовой частоты процессора к скорости шифровашия.

Введем следующие обозначения для операций: XOR - покоординатное сложение по модулю 2, SHFT - сдвиг, MEM - обращение в память, MUL - умножение элементов в поле $\mathbb{F}_{2^8}$. В таблице приведено количество операций за один раунд шифрования для процессора с 64-битной разрядностью (например, наложение раундового ключа длины 128 бит требует одного обращения в память и двух операций XOR).

В объеме памяти учитываются предвычисленные таблицы и S-бокс и не учитываются вспомогательные переменные, указатели и пр. Выполнение развертывания ключа, считывание шифруемых данных в оперативную память и запись зашифрованных данных в файл не учитываются при замерах скорости зашифрования. Скорость зашифрования рассчитывалась как $1024/t$ (Мб/сек), где 1024 Мб - размер подаваемого на шифрование случайного файла, а t - время его зашифрования в режиме CBC в секундах.

Таблица I
Сравнение различных реализаций шифрсистемы Кузнечик.

Реализация линейного преобразования	XOR / SHFT / MEM	Объем памяти	Скорость шифрования	cpb
1. Вычисление ЛРП без таблицы умножения	242/32/17 + 208 MUL	256 байт	1,7 Мб/с	2188
2. Вычисление ЛРП с таблицей умножения	242/32/225	2 Кб	9,7 Мб/с	384
3. Использование предвычисленных LUT-таблиц	34/0/17	64 Кб	113,8 Мб/с	33
4. Разложение рекурсивной матрицы	50/42/33	8 Кб	87,1 Мб/с	43
5. Умножение на элемент кольца	66/76/49	6 Кб	27,9 Мб/с	133

VIII. Заключение

В работе предложены способы разложения рекурсивных матриц и вытекающие из них программные реализации XSL-схем с рекурсивным L-преобразованием. Предлагаемая Реализация 4 (см. VI-B) незначительно уступает в скорости зашифрования реализации с хранением LUT-таблиц (Реализация 3). При этом, объём используемой быстродоступной памяти существенно меньше, в связи с чем Реализация 4 может быть полезна для низкоресурсных устройств с программной реализацией XSL-схем, в частности для программной реализации шифрсистемы Кузнечик.

Список литературы

[1] Shannon Claude E. Communication theory of secrecy systems // Bell Syst. Tech. J. — 1949. — Vol. 28. — P. 656–715.

[2] Biham Eli, Shamir Adi. Differential cryptanalysis of des-like cryptosystems // Journal of Cryptology. — 1990. — Vol. 4. — P. 3–72.

[3] Matsui Mitsuru. Linear cryptanalysis method for des cipher // International Conference on the Theory and Application of Cryptographic Techniques. — 1994.

[4] Малышев Ф. М. Двойственность разностного и линейного методов в криптографии // Матем. вопр. криптогр. — 2014. — Vol. 5. — P. 35–47. — URL: https://doi.org/10.4213/mvk128.

[5] Cryptographically significant mds matrices over finite fields: A brief survey and some generalized results / Kishan Chand Gupta, Sumit Kumar Pandey, Indranil Ghosh Ray, Susanta Samanta // Adv. Math. Commun. — 2019. — Vol. 13. — P. 779–843.

[6] Информационная технология. Криптографическая защита информации. Функция хэширования. — no. ГОСТ 34.11 - 2018. — URL: https://protect.gost.ru/v.aspx?control=7&id=232143.

[7] Guo Jian, Peyrin Thomas, Poschmann Axel. The photon family of lightweight hash functions. — Vol. 2011. — 2011. — 08. — P. 222–239.

[8] Информационная технология. Криптографическая защита информации. Блочные шифры. — no. ГОСТ 34.12 — 2018. — URL: https://protect.gost.ru/v.aspx?control=7&id=232146.
[9] Advanced encryption standard (aes) // Federal Information Processing Standards. — November 26, 2001. — no. Publication 197. — URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf.
[10] Diffie Whitfield, Ledin George. Sms4 encryption algorithm for wireless networks // IACR Cryptol. ePrint Arch. — 2008. — Vol. 2008. — P. 329. — URL: https://eprint.iacr.org/2008/329.pdf.
[11] Information technology – security techniques – hash-functions – part 3: Dedicated hashfunctions // ISO/IEC. — 2004. — no. 10118-3. — URL: https://www.iso.org/standard/39876.html.
[12] Дорохин СВ, Качков СС, Сидоренко АА. Реализация блочного шифра "Кузнечик" с использованием векторных инструкций // Труды Московского физико-технического института. — 2018. — Vol. 10, no. 4 (40).
[13] Tolba Mohamed F., Youssef A. Improved meet-in-the-middle attacks on reduced round kuznyechik // ICISC. — 2017.

Decompositions of the recursive matrices and its application to the implementation of the linear transformations

S. Davydov, V. Shishkin

***Abstract*—We study linear transformations defined by the recursive matrices in this article. Such transformations are used, for example, in the Kuznyechik block cipher and the PHOTON family of lightweight hash functions. We have found all solutions of the equation $X^{-1}(S^T)^m X = S^m$ for any invertible recursive matrix S^m. We propose two ways of recursive matrices decomposition and its application to the software implementation of the linear transformations. Our implementations are sufficiently fast and require rather small amount of memory. We note, matrix $(S^T)^m$ implements multiplication by polynomial x^m over the ring $Q[x]/f(x)$. This matrix is also MDS matrix and has rather efficient software implementation. Proposed for recursive matrices Implementation 4 is 23% slower then implementation with LUT-tables, but it uses 8 times less memory. Since the inverse of the recursive matrix has the same decomposition, decryption software implementation is also efficient. We consider, our implementations may be useful for low-resource devices with software implementation of algorithms. We demonstrate the table with different software implementation results of the block cipher Kuznyechik in conclusion.**

***Keywords*—recursive matrices, MDS matrices, linear transformations, block ciphers, Kuznyechik.**

References

[1] Shannon Claude E. Communication theory of secrecy systems // Bell Syst. Tech. J. — 1949. — Vol. 28. — P. 656–715.

[2] Biham Eli, Shamir Adi. Differential cryptanalysis of des-like cryptosystems // Journal of Cryptology. — 1990. — Vol. 4. — P. 3–72.

[3] Matsui Mitsuru. Linear cryptanalysis method for des cipher // International Conference on the Theory and Application of Cryptographic Techniques. — 1994.

[4] Malyshev F. M. The duality of differential and linear methods in cryptography, in russian // Mathematical Aspects of Cryptography. — 2014. — Vol. 5. — P. 35–47. — URL: https://doi.org/10.4213/mvk128.

[5] Cryptographically significant mds matrices over finite fields: A brief survey and some generalized results / Kishan Chand Gupta, Sumit Kumar Pandey, Indranil Ghosh Ray, Susanta Samanta // Adv. Math. Commun. — 2019. — Vol. 13. — P. 779–843.

[6] V. Dolmatov A. Degtyarev. Gost r 34.11-2012: Hash function // Request for Comments. — 2013. — no. RFC: 6986. — URL: https://datatracker.ietf.org/doc/html/rfc6986.

[7] Guo Jian, Peyrin Thomas, Poschmann Axel. The photon family of lightweight hash functions. — Vol. 2011. — 2011. — 08. — P. 222–239.

[8] Gost r 34.12-2015: Block cipher «kuznyechik» // Request for Comments. — 2016. — no. RFC: 7801. — URL: https://datatracker.ietf.org/doc/html/rfc7801.

[9] Advanced encryption standard (aes) // Federal Information Processing Standards. — November 26, 2001. — no. Publication 197. — URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf.

[10] Diffie Whitfield, Ledin George. Sms4 encryption algorithm for wireless networks // IACR Cryptol. ePrint Arch. — 2008. — Vol. 2008. — P. 329. — URL: https://eprint.iacr.org/2008/329.pdf.

[11] Information technology – security techniques – hash-functions – part 3: Dedicated hashfunctions // ISO/IEC. — 2004. — no. 10118-3. — URL: https://www.iso.org/standard/39876.html.

[12] S. V. Dorokhin S. S. Kachkov A. A. Sidorenko. Implementation of «kuznyechik» cipher using vector instructions, in russian // MIPT works. — 2018. — Vol. 10, no. 4 (40).

[13] Tolba Mohamed F., Youssef A. Improved meet-in-the-middle attacks on reduced round kuznyechik // ICISC. — 2017.