ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ / PHYSICS AND MATHEMATICS

Научная статья
УДК 519.852.64 + 004.056.55
https://doi.org/10.35266/1999-7604-2026-1-10

Обобщение кодов Уолша – Адамара

Михаил Сергеевич Беспалов[1], Кирилл Андреевич Фролов[2]✉
[1]Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ), Владимир, Россия
[2]АО «НПП «Исток» им. Шокина», Фрязино, Россия

Аннотация. Предлагается усовершенствование кодов Уолша – Адамара, дополненного кода Уолша и *p*-го варианта кода Уолша – Адамара, в виде матричного шифрования кодовой матрицей. Показано, что усовершенствование не влияет на процесс обнаружения и исправления ошибок. Разработаны алгоритмы декодирования по кодовой матрице как дополнение к декодированию по списку. Приведен пример, демонстрирующий, что в *p*-ном случае метод работает с ошибками разных типов: замещения, стирания и появления символа.

Ключевые слова: блочное кодирование, код Уолша – Адамара, дополненный код Уолша, код Рида – Маллера, линейная перестановка, конечное поле

Для цитирования: Беспалов М. С., Фролов К. А. Обобщение кодов Уолша – Адамара // Вестник кибернетики. 2026. Т. 25, № 1. С. 101–108. https://doi.org/10.35266/1999-7604-2026-1-10.

Original article

Generalized Walsh–Hadamard codes

Mikhail S. Bespalov[1], Kirill A. Frolov[2]✉
[1]Vladimir State University, Vladimir, Russia
[2]JSC "RPC "Istok" named after Shokin", Fryazino, Russia

Abstract. The paper proposes an optimization method of the Walsh–Hadamard codes, the augmented Walsh code and the *p*-ary Walsh–Hadamard code, via matrix encryption by a code matrix. The study shows that the upgrade does not affect the process of error detection and correction. Decoding algorithms using code matrices are developed as an addition to list decoding. In the *p*-ary case, the authors demonstrate the efficiency of the optimization method in handling errors of different types such as substitution, erasure, and appearance of a symbol.

Keywords: block coding, Walsh–Hadamard code, augmented Walsh code, Reed–Muller code, linear permutation, finite field

For citation: Bespalov M. S., Frolov K. A. Generalized Walsh–Hadamard codes. *Proceedings in Cybernetics*. 2026;25(1):101–108. https://doi.org/10.35266/1999-7604-2026-1-10.

ВВЕДЕНИЕ

В [1] введен усовершенствованный метод кодирования Уолша – Адамара в виде матричного шифрования. Наряду с кодом Уолша – Адамара известен [2] дополненный код Уолша, возможно обобщение [3] метода на базе p-го, а не двоичного, варианта исходного поля чисел. Уже для $p = 3$ это позволяет находить и исправлять ошибки не только типа замещение символа, но и типа стирание или появление символа. Дополненный код Уолша является также кодом Рида – Маллера первого порядка [4]. Покажем реализацию данного усовершенствования применительно к этим методам кодирования.

МАТЕРИАЛЫ И МЕТОДЫ

Усовершенствованный код Уолша – Адамара. В [1] предложено усовершенствование в виде дополнения (посредством матричного шифрования) к коду Уолша – Адамара. Приведем это усовершенствование кода Уолша – Адамара в более удобном виде, чем предложено в [1].

Зададим последовательность булевых (в поле $\mathbb{F}_2$) матриц C_n размера $n \times 2^n$ по схеме, предложенной в [5, 6], которая отлична от метода в [1]:

$$C_1 = (01),\ C_{n+1} = \begin{pmatrix} C_n & C_n \\ \mathbf{0}_n & \mathbf{1}_n \end{pmatrix}, \qquad (1)$$

где $\mathbf{0}_n = (0\,0\,\ldots 0)$, $\mathbf{1}_n = (1\,1\,\ldots\,1)$ – постоянные вектор-строки с 2^n отсчетами.

По правила поля $\mathbb{F}_2$ вычислим квадратную матрицу порядка $N = 2^n$ (уровня n) – матрицу Уолша – Адамара в аддитивной форме

$$A_n = C_n^T \cdot C_n, \qquad (2)$$

строки которой составляют кодовое пространство в виде множества кодовых слов метода кодирования Уолша (или Уолша – Адамара). Если бы матрицу C_n определили по стандартно принятой в теории кодирования методике (повторенной в [1]) записи в столбцах чисел в двоичной системе в порядке возрастания, то по формуле (2) получили бы ту же матрицу A_n. Преимущества метода задания C_n по формуле (1) проявляются в процессе декодирования, когда процедура кодирования, описанная в [1], осуществляется через невырожденную (над полем $\mathbb{F}_2$) кодовую матрицу K по формуле

$$A(K) = C_n^T \cdot K \cdot C_n. \qquad (3)$$

Матрица $K \cdot C_n$ в (3) служит порождающей матрицей предлагаемого метода. Проверочную матрицу в случае метода кодирования Уолша не рекомендуется использовать из-за ее большого размера $(2^n - n) \times 2^n$.

При кодировании по формуле (3) (вместо (2)) кодовое пространство не меняется. Добавляется шифрование передаваемой информации за счет перестановки множества кодовых слов, что влечет изменение процесса декодирования.

Лемма 1. Верны два утверждения: 1) кодовая матрица K есть главная подматрица $A(K)$, выделенная выборкой (1, 2, 4, ..., 2^{n-1}); 2) позиции информационных символов в кодовых словах указаны в столбцах матрицы K^{-1}.

Первый пункт доказан в [5], второй – в [1]. Нумерация строк и столбцов ведется с нуля, а не с единицы. Термин «главная подматрица» означает, что как строки, так и столбцы выделены из исходной матрицы одной и той же выборкой.

Усовершенствованный дополненный код Уолша

В дополненном коде Уолша число кодовых слов удваивается с сохранением прежнего кодового расстояния, что достригается добавлением к матрице A_n дополнения матрицы $\overline{A_n}$. Матрица $\overline{A_n}$ получается из A_n заменой всех элементов матрицы на противоположные в поле $\mathbb{F}_2 = \{0,1\}$. Строки матрицы $\overline{A_n}$ назовем антистроками, а координаты антистрок – ложными.

В формуле (2) строки матрицы C_n составляют упорядоченный базис множества кодовых слов метода кодирования Уолша. Добавлением к C_n снизу строки $\mathbf{1}_n$ из единиц получаем базис дополненного кода Уолша. Эту матрицу, являющуюся правой половиной матрицы C_{n+1}, обозначим $\widetilde{C_n}$.

В качестве аналогичного (3) метода шифрования применительно к дополненному коду Уолша предложим усовершенствование:

$$B(K) = C_n^T \cdot K \cdot \widetilde{C_{n-1}} \qquad (4)$$

с невырожденной кодовой матрицей K.

Для усовершенствованного дополненного кода Уолша возникают те же вопросы:

1) Как восстановить кодирующую матрицу K по $B(K)$?

2) Является ли этот метод кодирования систематическим? Как найти информационные координаты в случае положительного ответа?

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Восстановление кодовой матрицы

Введем обозначение $\widehat{C_n}$ для левой половины матрицы C_{n+1}. Тогда матрицу C_n можно представить как блочную $C_n = \left(\widehat{C_{n-1}} | \widetilde{C_{n-1}}\right)$.

Лемма 2. Матрица $A(K) = (D(K)|B(K))$ формулы (3) есть блочная матрица с правым блоком $B(K)$ по формуле (4) и с левым блоком $D(K) = C_n^T \cdot \mathrm{K} \cdot \widehat{C_{n-1}}$.

Доказательство. В [7] предлагается трактовать j-ю строку произведения двух матриц как линейную комбинацию строк правого сомножителя с коэффициентами в j-й строке левого сомножителя, что и приводит к указанному соотношению.

Обозначим $\tilde{K}$ следующую квадратную матрицу: последний столбец ее нулевой, а предыдущие столбцы есть подматрица матрицы $B(K)$, строки которой выделены выборкой (1, 2, 4, ..., 2^{n-1}), столбцы – выборкой 1, 2, 4, ..., 2^{n-2}). (Символом T обозначим квадратную матрицу того же порядка с одинаковыми столбцами, где образующий столбец выделен той же выборкой (1, 2, 4, ..., 2^{n-1}) из начального столбца матрицы $B(K)$.

Лемма 3. Кодовая матрица K восстанавливается по матрице $B(K)$ по правилу $K = \tilde{K} + T$ в поле $\mathbb{F}_2$.

Доказательство. По лемме 2 столбец с номером 2^{n-1} матрицы $A(K)$ есть начальный столбец матрицы $B(K)$. По лемме 1 последний столбец K выделяется выборкой (1, 2, 4, ..., 2^{n-1}) из начального столбца матрицы $B(K)$ и применяется для построения матрицы T, строки которой имеют вид $\mathbf{0}_{n-1}$ или $\mathbf{1}_{n-1}$.

По свойствам дискретных функций Уолша [6] и лемме 2 половина строк матрицы $B(K)$ повторяют те же строки матрицы $D(K)$, а вторая половина строк матрицы $B(K)$ служит антистроками соответствующих им строк матрицы $D(K)$. Антистрока $\bar{w}$ к строке w уровня $n-1$ получается сложением в поле $\mathbb{F}_2$ по формуле $w + \mathbf{1}_{n-1} = \bar{w}$, то есть ее координаты меняются на противоположные. Выделенная из $B(K)$ подматрица $\tilde{K}$ (без последнего нулевого столбца) при сравнении с матрицей K состоит из ее строк и антистрок, которым добавлением матрицы T возвращаем вид строк матрицы K.

Восстановление кодируемого сообщения

Дополненный код Уолша не является систематическим. Однако при декодировании этого кода выделяются информативные координаты (0, 1, 2, 4, ..., 2^{n-2}), которые рассматриваем в порядке (1, 2, 4, ..., 2^{n-2}, 0).

Если последняя координата с номером 0 имеет значение 0, то все координаты набора (1, 2, 4, ..., 2^{n-2}, 0) информационные, то есть на этих позициях записано кодируемое сообщение. Если же координата с номером 0 имеет значение 1, то все координаты набора (1, 2, 4, ..., 2^{n-2}) ложно-информационными, то есть на позициях (1, 2, 4, ..., 2^{n-2}) записана антистрока $\bar{w}$, кодируемого сообщения $w = \bar{w} + \mathbf{1}$ (которое здесь без последней координаты, равной 1).

Переформулируем теорему 3 из [1] применительно к принятому в данной статье определению матриц C_n в форме (1).

Лемма 4. Если кодовые сообщения являются строками матрицы C_n^T, то упорядоченными информационными координатами усовершенствованного метода кодирования Уолша – Адамара кодовыми словами $A(K)$ вида (3) будут упорядоченные двоичные числа в столбцах обратной матрицы K^{-1}, прочитанные в инверсной записи (разряды увеличиваются сверху вниз).

Доказательство остается прежним: из предположения $C_n^T = A(K) \cdot T$ вытекает, что $K^{-1} = C_n \cdot T$.

Представим матрицу K^{-1} как блочную, отделив последнюю строку (назвав ее p) и обозначив $\bar{K}$ оставшуюся верхнюю часть матрицы: $K^{-1} = \begin{pmatrix} \bar{K} \\ p \end{pmatrix}$. Координаты последней строки обозначим $p(0), p(1), \ldots, p(n-1)$.

Теорема 1. При декодировании усовершенствованного дополненного кода Уолша с множеством кодовых слов $B(K)$ по формуле (4) номера j_m информативных координат записаны в инверсном порядке в столбцах с номерами m матрицы $\bar{K}$, составляющей верхний блок матрицы K^{-1}. Эти координаты с номерами j_m будут информативными в случаях:

1) $p(m) = 1$ – последняя координата m-го столбца K^{-1} равна 1;

2) $p(m) = 0$ и кодовое слово начинается с нуля ($B_j^0 = 0$), где i – номер наименее удаленного кодового слова.

В случае невыполнения этих условий $p(m) = 0$ и при условии, что наименее удаленное кодовое слово начинается с единицы $B_j^0 = 1$, координаты j_m будут ложно-информационными, что означает необходимость замены их значений на противоположные.

Доказательство. Согласно лемме 4, элементы последней строки $p(m)$ матрицы K^{-1} определяют, на какую часть блочной матрицы $A(K) = (D(K)|B(K))$указывает m-й столбец матрицы K^{-1}: если этот элемент равен 1, то верхние цифры столбца в инверсной записи есть номер информационного столбца матрицы $B(K)$; если же этот элемент равен 0, то верхние цифры в инверсной записи есть номер j информационного столбца матрицы $D(K)$, которой нет в нашем распоряжении. Зато мы можем указать правило вычисления этого столбца по аналогичному столбцу в матрице $B(K)$.

По правилам индуктивного определения дискретных функций Уолша, исследованным в [5] (представленных в аддитивной форме), столбец с номером $j + 2^{n-1}$ при $j < 2^{n-1}$ есть покоординатная сумма в поле $\mathbb{F}_2$ столбцов с номерами j и 2^{n-1}. Поскольку обратная операция к сложению по модулю два совпадает с исходной, то столбец с номером j есть аналогичная сумма столбцов с номерами $j + 2^{n-1}$ и 2^{n-1}, а данные столбцы присутствуют в матрице $B(K)$ с номерами j и 0. Отсюда вытекает процедура декодирования для усовершенствованного дополненного метода Уолша, которую опишем и продемонстрируем на примере.

Пример 1. Пусть осуществляется процедура кодирования по формуле (4) уровня $n = 4$ с кодовой матрицей

$$K = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix},$$

для которой

$$K^{-1} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$ – сразу вычислили и указали обратную.

Процедура кодирования на практике проводится не по формуле (4) сразу для всех возможных кодируемых сообщений C_n^T, а по формуле:

$$R \cdot K \cdot \widetilde{C_{n-1}} = S$$

для потока R входящих сообщений, разбитых на блоки. На выходе получаем не матрицу $B(K)$ всех возможных кодовых слов, а поток S упорядоченных кодовых слов, предназначенный для передачи по каналу связи.

При неустойчивом канале связи получатель принимает сообщение S_0, вместо S, которое обрабатывается методом декодирования по списку [4]. Сообщение S_0 разбивается на слова длиной 2^{n-1}, каждое из которых сравнивается по критерию минимума расстояния Хэмминга (число разрядов с различающимися символами) со всеми возможными кодовыми словами в виде строк матрицы $C_n \cdot \widetilde{C_{n-1}}$ (или матриц A_n, $\overline{A_n}$), и исправляем. На этапе исправления ошибок, когда по S_0 восстанавливаем S, матрица K не нужна.

Для примера предположим, что ошибки исправлены, и в потоке S получены два следующих кодовых слова: $w_1 = (0\ 1\ 1\ 0\ 1\ 0\ 0\ 1)$ и $w_2 = (1\ 0\ 1\ 0\ 1\ 0\ 1\ 0)$.

Матрицу K^{-1} разобьем на последнюю строку $p = 1010$ и оставшуюся часть матрицы

$$\bar{K} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

В столбцах матрицы $\bar{K}$ в инверсном порядке записан упорядоченный набор номеров информативных координат: 4, 7, 0, 5. Согласно распределению нулей и единиц в строке p, этот упорядоченный набор запишем в виде информационного кода $4\boxed{7}0\boxed{5}$.

Поскольку начальная координата слова w_1 равна 0, то упорядоченный набор координат с номерами 4, 7, 0, 5 является информационным для w_1, что позволяет декодировать первое сообщение a_1 = (1 1 0 0). Так как начальная координата слова w_2 равна 1, то значения координат с номерами 7 и 5, которые выделены рамкой в информационном коде, являются ложно-информационными и подлежат замене на противоположные, что приводит к a_2 = (1 1 1 1).

Усовершенствование *p*-го варианта

Методы p-го кодирования для простого p, которые изучались в [8], рассмотрим на примере $p = 3$, поскольку основные видоизменения метода реализуются и в этом простейшем случае обобщения. Избыточность кода Уолша уже считается большой. В p-ном случае существенная избыточность, поскольку заменяем n-значные слова на p^n-значные. Будем, по возможности, сохранять прежние обозначения, наполненные новым содержанием.

Рекуррентным правилом, предложенным в [9], определим последовательность матриц C_n размера $n \times 3^n$, где операции в поле $\mathbb{F}_3 = \{0,1,2\}$:

$$C_1 = (0\ 1\ 2),\ C_{n+1} = \begin{pmatrix} C_n & C_n & C_n \\ \mathbf{0}_n & \mathbf{1}_n & \mathbf{2}_n \end{pmatrix}, \qquad (5)$$

здесь 0_n = (0 0 … 0), 1_n = (1 1… 1), 2_n = (2 2 … 2) – постоянные вектор-строки с 3^n отсчетами (уровня n).

Остановимся на p-ном аналоге метода Уолша и его усовершенствования, не привлекая дополненный код.

По правилам поля $\mathbb{F}_3$ вычислим квадратную порядка $N = 3^n$ (уровня n) матрицу

$$A_n = C_n^T \cdot C_n, \qquad (6)$$

строки которой составляют кодовое пространство в виде множества S кодовых слов данного метода кодирования.

Усовершенствование метода, состоящее в процедуре матричного шифрования, проведем через невырожденную над полем $\mathbb{F}_3$ кодовую матрицу K по формуле:

$$A(K) = C_n^T \cdot K \cdot C_n. \qquad (7)$$

В [9] доказан следующий обратный переход. В данном случае матрица $K \cdot C_n$ в (3) служит порождающей матрицей предлагаемого метода, так же как в случае $p = 2$.

Лемма 5. Кодовая матрица K выделяется из $A(K)$ в виде главной подматрицы выборкой $(1, 3, 9. \ldots, 3^{n-1})$ при нумерации с нуля.

Теорема 2. Кодирование по формуле (7) является систематическим. Информационные переменные указаны в столбцах матрицы K^{-1} в инверсном порядке в троичной системе счисления.

Доказательство. Анализируем в поле $\mathbb{F}_3$ соотношения $C_n^T = A(K) \cdot T$ и $K^{-1} = C_n \cdot T$, где матрица T размера $3^n \times n$, в каждом столбце которой одна единица (на разных позициях), а остальные – нули. Так как сомножитель T справа, то каждый столбец T выделяет из первого сомножителя (в виде $A(K)$ или C_n) столбец с указанным номером. В первом равенстве матрица T выделяет из матрицы $A(K)$ информационные столбцы в виде матрицы C_n^T. Поскольку столбцы матрицы C_n следуют в инверсном лексикографическом порядке в алфавите (0, 1, 2), а матрица T выделяет из C_n матрицу K^{-1}, в столбцах которой упорядочены инверсные номера информационных столбцов (координат), то теорема доказана.

Процедура исправления ошибок

Процедура обнаружения ошибок по критерию минимума расстояния Хэмминга (которое указывает количество ошибок) и в p-ном случае остается прежней. А процесс исправления ошибок становится в несколько раз длительнее даже в троичном случае.

Если обнаружена одна ошибка, то методом перебора она исправляется за один или два шага.

Если обнаружены две ошибки, то легко показать, что на их исправление требуется от одного до трех шагов.

В случае трех ошибок предлагается следующий алгоритм исправления. На двух по-

зициях из трех меняем значения и получаем один из трех ответов для d – расстояния Хэмминга между словами. Если $d = 1$ (значения поменяли правильно) или $d = 3$ (на обеих позициях поменяли неверно), то задача сводится к одной ошибке на третьей позиции. Если $d = 2$, то меняем значения на второй и третьей позициях. По пересчитанному значению d выдаем ответ: если $d = 0$, то исправление закончено; если $d = 1$, то исправляем третью позицию; если $d = 2$, то исправляем первую и вторую позиции; если $d = 3$, то исправляем все три позиции. Для исправления потребовалось от двух до трех шагов.

Пример процедуры декодирования

Пример 2. Пусть осуществляется процедура кодирования по формуле (7) уровня $n = 2$ над полем $\mathbb{F}_3$ с кодовой матрицей:

$$K = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}. \text{ Ее обратная } K^{-1} = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}.$$

Приведем матрицы (первая по формуле (5)):

$$C_2 = \begin{pmatrix} 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \end{pmatrix}$$

$$\text{и } KC_2 = \begin{pmatrix} 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \end{pmatrix}.$$

Предположим, что получатель декодирует следующий (разбитый на блоки) фрагмент потока полученного сообщения S_0:

...0|0 0 2 2 2 1 1 1 0|1 1 0 1 2 2 1 2 0|0...

По формуле (6) составим все 9 возможных кодовых слов

$$A_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \end{pmatrix} \quad (8)$$

и вычислим расстояние Хэмминга от слова w_1 = (0 0 2 2 2 1 1 1 0) до каждого из них σ_1 = (6 6 6 6 6 6 3 3 6) путем поэлементного сравнения со строками матрицы (8). Поскольку кодовое расстояние данного кода $d(K) = 6$, то данный код позволяет исправить 2 ошибки. В данном случае ошибок 3 и два кодовых слова на минимальном расстоянии от w_1. Это слова (000 222 111) и (012 201 120). Информационные координаты (7 1) вычисляются по матрице K^{-1} и составляют в первом слове сообщение (1 0), а во втором слове – (2 1). Видимо, предпочтение следует отдать сообщению (1 0), поскольку в первом варианте эти координаты не исправлялись, а во втором варианте именно их мы и заменили.

Для второго полученного слова w_2 = (1 1 0 1 2 2 1 2 0) аналогично вычисляем синдром σ_2 = (7 7 7 6 6 6 5 5 8), что не позволяет даже обнаружить ошибки и указать их число.

Вывод заключается в том, что если рассматриваем ошибки только вида замещения символа, то в данном месте произошел серьезный сбой при передаче информации. В качестве борьбы с подобным явлением запрашивается повтор сообщения.

Если же повтор невозможен, то можно рассмотреть вопрос о наличии ошибок другого вида: удаление или появление символа, что на практике встречается реже.

Для этого сдвинем сначала вправо на один разряд и вычислим σ, а потом влево, повторив вычисления. При сдвиге вправо значение синдрома будет большим, а при сдвиге на один разряд влево получим слова w_1 = (0 0 2 2 2 1 1 1 0), w_2 = (0 1 1 0 1 2 2 1 2) и σ_1 = (6 6 6 6 6 6 0 6 6), σ_2 = (7 2 6 5 6 5 6 7 5). Значит, слово w_1 является кодовым, а в слове w_2 две ошибки, которые легко исправляются до слова a_1 = (0 1 2 0 1 2 0 1 2).

Делаем вывод, что произошел сбой вида появление одного лишнего символа, за счет чего произошел сдвиг массива S_0 вправо на один разряд.

Информационные координаты с номерами 7 и 1 дают исходные сообщения (1 0) и (1 1).

Таким образом, излишняя избыточность данного метода позволяет работать с ошибками разного типа.

Число вариантов кодирования

Главное преимущество предложенного усовершенствования – в большом числе способов шифрования. В [9] вычислено число возможных невырожденных матриц K в качестве кодовой матрицы.

Лемма 6. Число невырожденных над полем $\mathbb{F}_3$ матриц K порядка n равно $(3^n - 1)\,(3^n - 3)(\,3^n - 9)\,\ldots\,(3^n - 3^{n-1})$.

В частности, число линейных перестановок уровня 2, совпадающее с числом возможных кодовых матриц, над полем $\mathbb{F}_3$ равно 48; а уровня 3 – равно 11 232. Для уровня 4 число кодовых матриц равно 2 426 112.

ЗАКЛЮЧЕНИЕ

Предложенное усовершенствование кода Уолша – Адамара в различных видах, сохраняя прежние возможности обнаружения и исправления ошибок типа замещения, добавляет процесс шифрования информации. Кодовая матрица служит секретным ключом, что также позволяет организовать многоканальную систему передачи информации. Если для каждого блока информации применять свой ключ, выбранный истинно случайным образом, то согласно теореме Шеннона данный алгоритм будет являться абсолютно криптостойким. Если менять матрицу-ключ достаточно часто (не реже чем через каждые $2^{n-1} - 1$ слов для двоичного случая), то вероятность успешной атаки на алгоритм путем шифрования 2^n сообщений e_i, где i-я координата равна 1, остальные равны 0, будет ниже ½.

Большая избыточность кода нивелируется широким спектром возможностей для оптимизации, основанных на структуре кодов Уолша – Адамара. К таким методам оптимизации можно отнести быстрое преобразование Адамара [10], применение PD и s-PD множеств [11–14] для декодирования. В случае p-го варианта кодирования даже при $p = 3$ метод хорошо работает для обнаружения и исправления единичных ошибок других типов, а именно стирания или появления символа.

Дополненный код Уолша встречается также под названием проколотый код Адамара в статье [15], где установлены нижние оценки его арифметической сложности, допускающие перенос на рассмотренное в статье усовершенствование.

Список источников

1. Беспалов М. С., Фролов К. А. Кодирование информации линейными перестановками дискретного преобразования Уолша // Вестник кибернетики. 2024. Т. 23, № 3. С. 90–95.
2. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М. : Связь, 1979. 744 с.
3. Heng I., Cooke C. H. Error correcting codes associated with complex Hadamard matrices // Applied Mathematics Letters. 1998. Vol. 11, no. 4. P. 77–80.
4. Кузнецов Ю. В., Шкарин С. А. Коды Рида – Маллера (обзор публикаций) // Математические вопросы кибернетики. Вып. 6. М. : Наука, 1996. С. 5–50.
5. Беспалов М. С. Собственные подпространства дискретного преобразования Уолша // Проблемы передачи информации. 2010. Т. 46, № 3. С. 60–79.
6. Беспалов М. С., Скляренко В. А. Дискретные функции Уолша и их приложения. Владимир : Изд-во ВлГУ, 2014. 68 с.
7. Малоземов В. Н. Линейная алгебра без определителей. Квадратичная функция. СПб. : Изд-во С.-Петербург. ун-та, 1997. 80 с.
8. Delsarte P., Goethals J. M. Tri-weight codes and generalized Hadamard matrices // Information and Control. 1969. Vol. 15, no. 2. P. 196–206.

References

1. Bespalov M. S., Frolov K. A. Information encoding by linear permutations of discrete Walsh transform. *Proceedings in Cybernetics*. 2024;23(3):90–95. (In Russ.).
2. MacWilliams F. J., Sloane N. J. A. The theory of error-correcting codes. Trans. Moscow: Svyaz; 1979. 744 p. (In Russ.).
3. Heng I., Cooke C. H. Error correcting codes associated with complex Hadamard matrices. *Applied Mathematics Letters.* 1998;11(4):77–80.
4. Kuznetsov J. V., Shkarin S. A. Kody Rida – Mallera (obzor publikatsiy). *Matematicheskie voprosy kibernetiki*. Moscow: Nauka; 1996. No. 6. p. 5–50. (In Russ.).
5. Bespalov M. S. Eigenspaces of the discrete Walsh transform. *Problems of Information Transmission.* 2010;46(3):60–79. (In Russ.).
6. Bespalov M. S., Sklyarenko V. A. Diskretnye funktsii Uolsha i ikh prilozheniya. Vladimir: Izd-vo VISU; 2014. 68 p. (In Russ.).
7. Malozemov V. N. Lineynaya algebra bez opredeliteley. Kvadratichnaya funktsiya. St. Petersburg: Izd-vo SPbSU; 1997. 80 p. (In Russ.).
8. Delsarte P., Goethals J. M. Tri-weight codes and generalized Hadamard matrices. *Information and Control*. 1969;15(2):196–206.

9. Беспалов М. С. Дискретное преобразование Крестенсона // Проблемы передачи информации. 2010. Т. 46, № 4. С. 91–115.
10. Abbe E., Shpilka A., Ye M. Reed-Muller codes: Theory and algorithms // IEEE Transactions on Information Theory. 2020. Vol. 67, no. 6. P. 3251–3277.
11. Key J. D., McDonough T. P., Mavron V. C. Reed-Muller codes and permutation decoding // Discrete Mathematics. 2010. Vol. 310, no. 22. P. 3114–3119.
12. Barrolleta R. D., Villanueva M. Partial permutation decoding for binary linear and Z_4-linear Hadamard codes // Designs, Codes and Cryptography. 2018. Vol. 86, no. 3. P. 569–586.
13. Bernal J. J., Simón J. J. New advances in permutation decoding of first-order Reed-Muller codes // Finite Fields and Their Applications. 2023. Vol. 88.
14. Bernal J. J., Simón J. J. Permutation decoding of first-order generalized Reed-Muller codes // Journal of Algebra and Its Applications. 2025. https://doi.org/10.48550/arXiv.2509.11757.
15. Li Z., Lin S.-J., Hu H. On the arithmetic complexities of Hamming codes and Hadamard codes // Journal of Latex Class Files. 2018. https://doi.org/10.48550/arXiv.1804.09903.

Информация об авторах

М. С. Беспалов – доктор физико-математических наук;
https://orcid.org/0000-0003-0661-337X,
bespalov@vlsu.ru
К. А. Фролов – сотрудник;
https://orcid.org/0000-0001-8691-8151,
golegoga33rus@gmail.com✉

9. Bespalov M. S. Discrete Chrestenson transform. *Problems of Information Transmission*. 2010;46(4):91–115. (In Russ.).
10. Abbe E., Shpilka A., Ye M. Reed-Muller codes: Theory and algorithms. *IEEE Transactions on Information Theory*. 2020;67(6):3251–3277.
11. Key J. D., McDonough T. P., Mavron V. C. Reed-Muller codes and permutation decoding. *Discrete Mathematics*. 2010;310(22):3114–3119.
12. Barrolleta R. D., Villanueva M. Partial permutation decoding for binary linear and Z_4-linear Hadamard codes. *Designs, Codes and Cryptography*. 2018;86(3):569–586.
13. Bernal J. J., Simón J. J. New advances in permutation decoding of first-order Reed-Muller codes. *Finite Fields and Their Applications*. 2023;88.
14. Bernal J. J., Simón J. J. Permutation decoding of first-order generalized Reed-Muller codes. *Journal of Algebra and Its Applications*. 2025. https://doi.org/10.48550/arXiv.2509.11757.
15. Li Z., Lin S.-J., Hu H. On the arithmetic complexities of Hamming codes and Hadamard codes. *Journal of Latex Class Files*. 2018. https://doi.org/10.48550/arXiv.1804.09903.

About the authors

M. S. Bespalov – Doctor of Sciences (Physics and Mathematics);
https://orcid.org/0000-0003-0661-337X,
bespalov@vlsu.ru
K. A. Frolov – Employee;
https://orcid.org/0000-0001-8691-8151,
golegoga33rus@gmail.com✉