УДК 003.26, 519.725.2
doi:10.31799/1684-8853-2025-1-23-28
EDN: IOKUXY

Научные статьи
Articles

Алгоритм построения матриц, уменьшающих расстояние кода

А. А. Воднев[a]*, аспирант, orcid.org/0009-0002-3539-4292, vodnev.98@mail.ru*
[a]*Московский институт электроники и математики им. А. Н. Тихонова Национального исследовательского университета «Высшая школа экономики», Таллинская ул., 34, Москва, 123458, РФ*

Введение: *уменьшение кодового расстояния представляет собой важный инструмент для решения некоторых задач в теории информации и криптографии. Например, в криптографических кодовых системах, таких как система Мак-Элиса, снижение кодового расстояния напрямую влияет на уменьшение длины открытого ключа, что является критически важным фактором для повышения эффективности и применимости кодовых криптосистем.* ***Цель:*** *разработать алгоритм построения матриц, способный эффективно уменьшать расстояние кода.* ***Результаты:*** *предложен итерационный алгоритм, который формирует ряд маскирующих матриц, успешно уменьшающих расстояние заданного кода. Для проверки изложенного подхода был выбран код Боуза — Чоудхури — Хоквингхема и криптографическая система Мак-Элиса. Проведен ряд экспериментов, показывающих эффективность разработанного алгоритма. Суть экспериментов заключалась в применении к коду Боуза — Чоудхури — Хоквингхема разработанного алгоритма, после чего полученный код внедрялся в систему Мак-Элиса. Полученная криптосистема подвергалась атакам на основе декодирования по информационным совокупностям. Результаты экспериментов показали, что к преобразованным кодам неприменима атака на основе декодирования по информационным совокупностям, а вес порождающей матрицы нового кода, которая является частью открытого ключа, стал меньше.* ***Практическая значимость:*** *невозможность применить декодирование по информационным совокупностям позволяет уменьшить объем открытого ключа в криптосистеме, что представляет значительный интерес для практики использования кодовых криптосистем.* ***Обсуждение:*** *приложение алгоритма не ограничивается только криптографией. Он может быть применен для преобразования каналов передачи данных, обладающих памятью. Отметим, что для полноценного внедрения матриц, уменьшающих расстояние кода, в криптографические системы необходима проверка декодируемости вектора ошибок после обратного преобразования, что является предметом дальнейших исследований.*

Ключевые слова *— корректирующие коды, кодовое расстояние, криптография, система Мак-Элиса, декодирование по информационным совокупностям, уменьшение размера ключа.*

Для цитирования: Воднев А. А. Алгоритм построения матриц, уменьшающих расстояние кода. *Информационно-управляющие системы*, 2025, № 1, с. 23–28. doi:10.31799/1684-8853-2025-1-23-28, EDN: IOKUXY
For citation: Vodnev A. A. Algorithm for constructing matrices that reduce code distance. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2025, no. 1, pp. 23–28 (In Russian). doi:10.31799/1684-8853-2025-1-23-28, EDN: IOKUXY

Введение

В криптографии есть два основных типа систем — алгебраические и кодовые. Алгебраические криптосистемы основаны на задаче факторизации [1] и вычислении дискретного логарифма [2]. Кодовые системы основаны на операциях линейной алгебры и методах помехоустойчивого кодирования [3]. Примером такой системы является система Мак-Элиса — криптографическая система с открытым ключом, основанная на проблеме декодирования кодов, корректирующих ошибки. Идея системы Мак-Элиса заключается в том, что вектор ошибки не меняет своего веса после применения обратной матрицы перестановок к шифротексту. Поэтому законному пользователю не нужно знать вектор ошибки для расшифровки, поскольку любой вектор ошибки с весом меньше половины кодового расстояния декодируется кодом с использованием того же алгоритма. Фактически безопасность системы основана на сложности декодирования для линейного кода с произвольной структурой. В работе [4] доказано, что декодирование произвольного линейного кода является NP-трудной задачей. Однако, несмотря на то, что кодовые криптосистемы имеют некоторые преимущества, особенно в том, что касается выигрыша по времени шифрования/дешифрования [5], а также устойчивости к декодированию в постквантовый период [6, 7], они имеют и недостатки.

Открытый ключ, например для системы Мак-Элиса, как правило, имеет бóльшую длину по сравнению с алгебраическими системами. Более того, система Мак-Элиса подвержена атакам, связанным с декодированием по информационным совокупностям (Information-Set Decoding, ISD) [8]. Среднее число попыток найти информационный набор без ошибок значительно меньше, чем для полного перебора по всем векторам ошибок. Таким образом, для достижения необходимого диапазона безопасности криптосистемы Мак-Элиса требуются коды с большей длиной n. В частности, Мак-Элис предложил использовать

код Гоппы (1024, 524, 101), исправляющий $t = 50$ ошибок, для которого длина открытого ключа составляет 536 576 [9].

Однако исследование кодовых криптосистем позволило существенно уменьшить размер открытого ключа [10, 11], а разработка новых методов решения задачи факторизации [12] привела к тому, что размер открытого ключа алгебраических систем увеличился. В результате размеры открытых ключей для разного типа систем стали соизмеримыми [13]. Помимо этого, кодовые криптосистемы выполняют меньше операций и опираются на линейную алгебру, которая реализуется эффективнее, чем арифметические операции. Таким образом, кодовые криптосистемы лучше подходят для реализации «легкой криптографии», которая способна обеспечить достаточный уровень безопасности в условиях ограниченных вычислительных систем [14, 15].

Существует множество подходов к уменьшению ключей кодовой криптосистемы [16–18], одним из возможных способов служит использование преобразующих матриц, не являющихся перестановками. В этом случае расстояние преобразованного кода может быть меньше, чем у исходного, и тогда преобразованный код не будет исправлять те ошибки, которые мог исправить исходный. В статье предлагается алгоритм получения преобразований, позволяющих уменьшить расстояние исходного кода. Идея уменьшения минимального кодового расстояния может быть полезна сразу по нескольким направлениям: во-первых, уменьшение размера открытого ключа, во-вторых, защита от атак, основанных на декодировании методом информационных совокупностей. Разработанный итерационный алгоритм маскирующих матриц формирует матрицу, которая при умножении на порождающую матрицу кода делает вес некоторых строк малым. При попытке декодировать полученный код методом информационных совокупностей будем получать ошибки, особенно если количество уменьшенных строк велико.

Алгоритм может быть применен не только для криптографических систем, но и, например, для построения более надежных каналов с памятью [19], а также в других задачах, требующих сокращения передаваемой информации без потери корректирующих свойств [20].

Формирование маскирующей матрицы и внедрение алгоритма в систему Мак-Элиса

Задачу уменьшения минимального кодового расстояния до величины l можно решить, уменьшив в порождающей матрице одну или несколько строк до веса l. После формирования порождающей матрицы $\mathbf{G}_0$ кода Боуза — Чоудхури — Хоквингхема (БЧХ) применим итерационный алгоритм, который уменьшит строки.

Алгоритм:

1) формируем маскирующую матрицу $\mathbf{M}_1$ для заданной строки $\mathbf{G}_0$;

2) перемножаем матрицы $\mathbf{G}_0$ и $\mathbf{M}_1$, получаем $\mathbf{GpM}_1$;

3) формируем маскирующую матрицу $\mathbf{M}_2$ для заданной строки $\mathbf{GpM}_1$;

4) перемножаем матрицы $\mathbf{GpM}_1$ и $\mathbf{M}_2$ и т. д.

Алгоритм продолжается до тех пор, пока не будет достигнут лимит на уменьшение строк либо не будет достигнуто требуемое количество «коротких» строк в порождающей матрице.

Умножение на маскирующую матрицу порождает новый код с уменьшенным расстоянием. Чем больше в порождающей матрице кода строк минимальной длины, тем больше слов минимального веса получаем в спектре всех слов для этого кода.

Алгоритм формирования маскирующей матрицы:

1) определяем позиции единиц заданной строки кода;

2) идем по позициям порождающей матрицы кода: если номер строки и номер столбца (больший или равный номеру строки) есть в выделенных позициях, то ставим на эту позицию единицу, в противном случае — ноль. Количество единиц в строке ограничено заданным параметром;

3) на остальных позициях ставим строки, как в единичной матрице.

Алгоритм разработан таким образом, что матрица, полученная на каждой итерации, не является вырожденной. Следовательно, для восстановления исходного кода достаточно найти матрицы, обратные $\mathbf{M}_1$, $\mathbf{M}_2$ и т. д.

Внедрение алгоритма в криптосистему происходит следующим образом:

1) так как $\mathbf{SG}_0$ дает тот же набор кодовых слов, что и $\mathbf{G}_0$, то матрицей $\mathbf{S}$ можно пренебречь;

2) матрица $\mathbf{P}$ заменяется маскирующей матрицей $\mathbf{M}$.

Получаем криптосистему вида

$$\mathbf{y} = \mathbf{xG}_0\mathbf{M} + \mathbf{e}.$$

Матрица $\mathbf{M}$ получена итерационным алгоритмом: $\mathbf{M} = \mathbf{M}_1\mathbf{M}_2\ldots\mathbf{M}_{k'}$, где k' — количество строк, вес которых необходимо изменить.

Если вес вектора ошибок $\mathbf{e}$ брать как подходящий для кода $\mathbf{G}_0$, то новый код $\mathbf{G}_0\mathbf{M}$ при условии, что матрица $\mathbf{M}$ уменьшает вес достаточно большого количества строк $\mathbf{G}_0$, с высокой вероятностью не сможет исправить все наложенные ошибки. Только легальный пользователь, знаю-

щий разложение $\mathbf{G}_0\mathbf{M}$, сможет корректно декодировать и восстановить $\mathbf{x}$.

Примеры применения алгоритма маскирующих матриц

Для проверки работы алгоритма проведем несколько экспериментов и проанализируем результаты.

За основу брали код БЧХ с порождающей матрицей $\mathbf{G}_0$. Характеристики кода: $n = 63$, $k = 18$, $t = 10$, где n — длина кода, k — длина кодового слова, t — количество исправляемых кодом ошибок.

Эксперимент 1.

Условие: три слова длины 1 на первых трех позициях матрицы кода.

Размерность строк матрицы $\mathbf{G}_0\mathbf{M}$: [1, 1, 1, 26, 20, 21, 23, 26, 28, 26, 28, 27, 27, 23, 22, 27, 23, 24]

Данный результат достигается путем последовательного умножения матрицы $\mathbf{G}_0$ на $\mathbf{M} = \mathbf{M}_1\mathbf{M}_2\mathbf{M}_3$, которая уменьшает размерность 1, 2 и 3-й строки соответственно до единицы.

Спектр по словам для кода БЧХ с маскирующей матрицей: [1, 3, 3, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 3, 6, 16...]

Из спектра видно, что минимальная длина слова, помимо нуля, равна 1. Количество слов, имеющих минимальную длину, равно трем. Следовательно, корректирующая способность нового кода стала равна 1.

Пробуем декодировать по информационной совокупности.

Кодируемое слово $\mathbf{x}$: [0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Кодовое слово $\mathbf{y}$: [0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Вектор ошибок $\mathbf{err}$: [1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Слово, полученное после декодирования: [1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Можно увидеть, что слова отличаются в трех битах (1, 2 и 3-м).

Эксперимент 2.

Условие: три слова длины 1 на случайных позициях матрицы кода.

Размерность строк матрицы $\mathbf{G}_0\mathbf{M}$: [31, 1, 24, 1, 20, 25, 23, 27, 27, 30, 24, 1, 25, 24, 26, 23, 23, 26]

Достигается последовательным умножением матрицы $\mathbf{G}_0$ на $\mathbf{M} = \mathbf{M}_1\mathbf{M}_2\mathbf{M}_3$, что уменьшает размерность 2, 4 и 12-й строки до единицы.

Спектр по словам для кода БЧХ с маскирующей матрицей: [1, 3, 3, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 8, 20...]

Первые четыре позиции полученного спектра совпадают со спектром из первого эксперимента. Следовательно, минимальное расстояние такое же.

Пробуем декодировать по информационной совокупности.

Кодируемое слово $\mathbf{x}$: [0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Кодовое слово $\mathbf{y}$: [0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Вектор ошибок $\mathbf{err}$: [1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Слово, полученное после декодирования: [0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Если сравнить два слова, изначальное и полученное, то они отличаются в нескольких позициях. Таким образом, ISD дает ошибку.

Эксперимент 3.

Условие: три слова длины 1 на трех подряд идущих позициях матрицы кода, смещение совокупности от начала.

Размерность строк матрицы $\mathbf{G}_0\mathbf{M}$: [22, 1, 1, 1, 26, 20, 21, 23, 26, 28, 26, 28, 27, 27, 23, 22, 27, 23]

Этот результат достигается последовательным умножением матрицы $\mathbf{G}_0$ на $\mathbf{M} = \mathbf{M}_1\mathbf{M}_2\mathbf{M}_3$, что уменьшает размерность 2, 3 и 4-й строки до единицы.

Спектр по словам для кода БЧХ с маскирующей матрицей: [1, 3, 3, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 3, 6, 16...]

Представленный спектр полностью совпадает со спектром из эксперимента 1. Пробуем декодировать по информационной совокупности, но возьмем другое кодируемое слово.

Кодируемое слово $\mathbf{x}$: [1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Кодовое слово $\mathbf{y}$: [1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Вектор ошибок $\mathbf{err}$: [1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Слово, полученное после декодирования: [1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Как видим, полученное слово отличается от изначального, следовательно, ISD вновь допустило ошибку.

Эксперимент 4.

Условие: три слова длины 2 на трех подряд идущих позициях матрицы кода.

Размерность строк матрицы $\mathbf{G}_0\mathbf{M}$: [2, 2, 2, 24, 20, 17, 25, 24, 26, 24, 32, 23, 25, 30, 22, 25, 23, 21]

Данный результат достигается путем последовательного умножения матрицы $\mathbf{G}_0$ на $\mathbf{M} = \mathbf{M}_1\mathbf{M}_2\mathbf{M}_3$, что уменьшает размерность 2, 3 и 4-й строки до веса 2.

Спектр по словам для кода БЧХ с маскирующей матрицей: [1, 0, 3, 0, 3, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 5, 5, 26...]

Из спектра видно, что минимальная длина слова, помимо нуля, равна 2. Видна разница со спектрами предыдущих экспериментов.

Пробуем декодировать по информационной совокупности.

Кодируемое слово **x**: [0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0]

Кодовое слово **y**: [0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0]

Вектор ошибок **err**: [1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Слово, полученное после декодирования: [1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0]

Результат тот же. Примечательно, что метод ISD дает ошибку на позициях измененных строк порождающей матрицы.

Эксперимент 5.

Условие: три слова длины 2 расположить на первых трех позициях, так же как и на случайных позициях матрицы кода, не удается. Это приводит к увеличению уже уменьшенных строк кода.

Эксперимент 6.

Условие: два слова длины 3 на первых позициях.

Размерность строк матрицы $\mathbf{G}_0\mathbf{M}$: [3, 3, 30, 28, 25, 27, 21, 26, 20, 21, 25, 26, 21, 23, 26, 23, 29, 24]

Получить данную размерность можно, последовательно умножив матрицы $\mathbf{G}_0$ на $\mathbf{M} = \mathbf{M}_1\mathbf{M}_2$, уменьшающую размерность 1-й и 2-й строки до трех.

Спектр по словам для кода БЧХ с маскирующей матрицей: [1, 0, 0, 2, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 4, 2, 9, 33...]

Из спектра видно, что минимальная длина слова, помимо нуля, равна 2. Количество слов, имеющих минимальную длину, равно двум. Корректирующая способность нового кода стала равна трем.

Пробуем декодировать по информационной совокупности.

Кодируемое слово **x**: [0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Кодовое слово **y**: [0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Вектор ошибок **err**: [1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Слово, полученное после декодирования: [1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Метод информационных совокупностей смог исправить все ошибки, кроме одной. Это связано с увеличением минимального расстояния.

Эксперимент 7.

Условие: три слова длины 3 на первых трех позициях матрицы кода, как и на случайных позициях, не получается сделать.

Из проведенных экспериментов делаем два вывода:

1) ISD не дает нужного результата, метод ISD ошибается на тех же позициях, что и номера «укороченных» строк кода;

2) наиболее эффективным является сокращение длины нескольких строк до веса 1, так как это позволяет применять метод наибольшее количество раз без увеличения длины других строк при новом сокращении, что дает возможность минимизировать максимальное число строк.

Заключение

Разработка итерационного алгоритма маскирующих матриц, уменьшающего кодовое расстояние, представляет собой перспективный подход к усилению криптографической стойкости системы Мак-Элиса. Алгоритм также может быть успешно применен в приложениях, где необходимо уменьшить размер передаваемой информации.

Эксперименты с разработанным алгоритмом показали, что ISD плохо справляется с полученным кодом. Это позволяет бороться с проблемой большого размера ключа и способствует развитию направления кодовых криптосистем в криптографии.

Дальнейшие исследования этого алгоритма могут быть направлены на уточнение параметров, а также на разработку новых методов защиты кодовых криптосистем, способных обеспечить высокий уровень безопасности в эпоху квантовых вычислений.

Финансовая поддержка

Статья подготовлена в результате проведения исследования в рамках Программы фундаментальных исследований Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ).

Литература

1. **Rivest R. L., Shamir A., Adleman L. M.** A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, vol. 21, no. 2, pp. 120–126. doi.org/10.1145/ 359340.359342
2. **El Gamal T.** A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 1985, vol. 31, no. 4, pp. 469–472. doi.org/10.1109/TIT.1985.1057074
3. **Рацеев С. М., Череватенко О. И., Чернявская В. А.** О некоторых криптосистемах, основанных на алгебраических кодах. *Вестник Самарского университета. Естественнонаучная серия*, 2021, т. 27, № 1, с. 62–73. doi.org/10.18287/2541-7525-2021-27-1-62-73
4. **Berlekamp E., McEliece R., van Tilborg H.** On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 1978, vol. 24, no. 3, pp. 384–386. doi.org/10.1109/TIT.1978.1055873
5. **V´eron P.** Code based cryptography and steganography. *5th International Conference, CAI 2013*, Porquerolles, France, 3–6 September, 2013, pp. 9–46. doi.org/10.1007/978-3-642-40663-8_5
6. **Ovchinnikov A. A.** The variant of post-quantum cryptosystem based on burst-correcting codes and on the complete decoding problem. *Информационно-управляющие системы*, 2022, № 3, с. 45–54. doi:10.31799/1684-8853-2022-3-45-54
7. **Bavdekar R., Chopde E. J., Bhatia A., Tiwari K., Daniel S. J., Atul.** Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. *Cryptography and Security (cs.CR)*, 2202. doi.org/10.48550/arXiv.2202.02826
8. **Давыдов В. В., Беляев В. В., Кустов Е. Ф., Леевик А. Г., Беззатеев С. В**. Современные вариации криптосистем Мак-Элиса и Нидеррайтера. *Научно-технический вестник информационных технологий, механики и оптики*, 2022, т. 22, № 2, с. 324–331. doi:10.17586/2226-1494-2022-22-2-324-331, EDN: CFSCVT
9. **McEliece R. J.** *A Public-Key Cryptosystem Based on Algebraic Coding Theory.* DSN Progress Report, 1978, pp. 42–44.
10. **Berger T. P., Cayrel P. L., Gaborit P., Otmani A.** Reducing key length of the McEliece cryptosystem. *Second International Conference on Cryptology in Africa*, Gammarth, Tunisia, 21–25 June, 2009, pp. 77–97. doi.org/10.1007/978-3-642-02384-2_6
11. **Faug`ere J. C., Otmani A., Perret L., Tillich J. P.** Algebraic cryptanalysis of McEliece variants with compact keys. *29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, French Riviera, May 30–June 3, 2010, pp. 279–298. doi.org/10.1007/978-3-642-13190-5_14
12. **Kocher P. C.** Timing attacks on implementations of Diffie — Hellman, RSA, DSS, and other systems. *16th Annual International Cryptology Conference*, Santa Barbara, California, USA, 18–22 August, 1996, pp. 104–113. doi.org/10.1007/3-540-68697-5_9
13. **Barker E.** *NIST Special Publication 800-57. Part 1: Revision 4, Recommendation for Key Management, Part 1: General*. National Inst. of Standards and Technology, Gaithersburg, MD, USA, 2016. doi.org/10.6028/NIST.SP.800-57pt1r4
14. **Eisenbarth T., Kumar S., Paar C., Poschmann A., Uhsadel L.** A survey of lightweight-cryptography implementations. *IEEE Design & Test of Computers*, 2007, vol. 24, no. 6, pp. 522–533. doi.org/10.1109/MDT.2007.178
15. **Ivanov F., Krouk E., Kreshchuk A.** On the lightweight McEliece cryptosystem for low-power devices. *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)*, Moscow, Russia, 21–25 October, 2019, pp. 133–138. doi.org/10.1109/REDUNDANCY48165.2019.9003324
16. **Zyablov V. V., Ivanov F. I., Krouk E. A., Sidorenko V. R.** On new problems in asymmetric cryptography based on error-resistant coding. *Problems of Information Transmission*, 2022, vol. 58, no. 2, pp. 184–201. doi:10.1134/S0032946022020077
17. **Ivanov F., Krouk E., Kabatiansky G., Rumenko N.** New code-based cryptosystem. *8th International Workshop "Code-Based Cryptography" (CBCrypto 2020)*, Zagreb, Croatia, 9–10 May, 2020, LNSC, vol. 12087, pp. 41–49 doi:10.1007/978-3-030-54074-6_3
18. **Красавин А. А.** Использование модифицированной (U|U+V)-конструкции в криптосистеме McEliece. *Труды МФТИ*, 2018, т. 10, № 2, с. 109–113. EDN: XTWBRZ
19. **Сухоруков А. С.** Пропускная способность дискретного многомерного канала связи с памятью. *T-Comm: Телекоммуникации и транспорт*, 2018, т. 12, № 3, с. 13–21. doi:10.24411/2072-8735-2018-10048, EDN: XOHIUP
20. **Кудряшова А. Ю.** Минимизация искажений сигнала при локально-оптимальном способе цифрового преобразования. *T-Comm: Телекоммуникации и транспорт,* 2020, т. 14, № 5, с. 27–34. doi:10.36724/2072-8735-2020-14-5-27-34, EDN: AIOUOJ

UDC 003.26, 519.725.2
doi:10.31799/1684-8853-2025-1-23-28
EDN: IOKUXY

Algorithm for constructing matrices that reduce code distance

A. A. Vodnev[a], Post-Graduate Student, orcid.org/0009-0002-3539-4292, vodnev.98@mail.ru
[a]Higher School of Economics, Tikhonov Moscow Institute of Electronics and Mathematics, 34, Tallinskaya St., 123458, Moscow, Russian Federation

Introduction: Reducing code distance is an important tool for addressing certain problems in information theory and cryptography. For example, in cryptographic coding systems such as McEliece, reducing the code distance directly affects the reduction of the public key length, which is a critically important factor for increasing the efficiency and applicability of coding-based cryptosystems. **Purpose:** To develop a matrix construction algorithm which is capable to effectively reduce code distance. **Results:** We propose an iterative algorithm that generates a series of masking matrices, successfully reducing the distance of the given code. To validate this approach, we choose the BCH code and the McEliece cryptographic system. We have conducted a series of experiments demonstrating the effectiveness of the developed algorithm. The experiments involve applying the developed algorithm to the BCH code, after which the resulting code is integrated into the McEliece system. The resulting cryptosystem is subjected to attacks based on information set decoding. The experimental results show that the transformed codes are not susceptible to attacks based on information set decoding, and the weight of the generator matrix of the new code, which is part of the public key, is reduced. **Practical relevance:** The inability to apply information set decoding makes it possible to reduce the public key size in a cryptosystem, which is of significant interest for the practical application of coding-based cryptosystems. **Discussion:** The application of this algorithm is not limited to cryptography. The proposed approach can also be applied to transforming communication channels with memory. It is important to note that, for the full integration of matrices that reduce code distance into cryptographic systems, verification of the error vector's decodability after applying the reverse transformation is necessary, which is a subject for further research.

Keywords — error-correcting codes, code distance, cryptography, McEliece system, information set decoding, key size reduction.

For citation: Vodnev A. A. Algorithm for constructing matrices that reduce code distance. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2025, no. 1, pp. 23–28 (In Russian). doi:10.31799/1684-8853-2025-1-23-28, EDN: IOKUXY

Financial support

The article was prepared as a result of research conducted within the framework of the Fundamental Research Program of the National Research University Higher School of Economics (HSE).

References

1. Rivest R. L., Shamir A., Adleman L. M. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, vol. 21, no. 2, pp. 120–126. doi.org/10.1145/ 359340.359342
2. El Gamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 1985, vol. 31, no. 4, pp. 469–472. doi.org/10.1109/TIT.1985.1057074
3. Ratseev S. M., Cherevatenko O. I., Chernyavskaya V. A. On some cryptosystemsbased on algebraic codes. *Vestnik of Samara University. Natural Science Series*, 2021, vol. 27, no. 1, pp. 62–73. doi.org/10.18287/2541-7525-2021-27-1-62-73 (In Russian).
4. Berlekamp E., McEliece R., van Tilborg H. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 1978, no. 24(3), pp. 384–386.
5. V´eron P. Code based cryptography and steganography. *5th International Conference, CAI 2013*, Porquerolles, France, 3–6 September, 2013, pp. 9–46. doi.org/10.1007/978-3-642-40663-8_5
6. Ovchinnikov A. A. The variant of post-quantum cryptosystem based on burst-correcting codes and on the complete decoding problem. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 3, pp. 45–54. doi:10.31799/1684-8853-2022-3-45-54
7. Bavdekar R., Chopde E. J., Bhatia A., Tiwari K., Daniel S. J., Atul. Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. *Cryptography and Security (cs.CR)*, 2202. doi.org/10.48550/arXiv.2202.02826
8. Davydov V. V., Beliaev V. V., Kustov E. F., Leevik A. G., Bezzateev S. V. Modern variations of McEliece and Niederreiter cryptosystems. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 2, pp. 324–331 (In Russian). doi:10.17586/2226-1494-2022-22-2-324-331, EDN: CFSCVT
9. McEliece R. J. *A Public-Key Cryptosystem Based on Algebraic Coding Theory.* DSN Progress Report, 1978, pp. 42–44.
10. Berger T. P., Cayrel P. L., Gaborit P., Otmani A. Reducing key length of the McEliece cryptosystem. *Second International Conference on Cryptology in Africa*, Gammarth, Tunisia, 21–25 June, 2009, pp. 77–97. doi.org/10.1007/978-3-642-02384-2_6
11. Faug`ere J. C., Otmani A., Perret L., Tillich J. P. Algebraic cryptanalysis of McEliece variants with compact keys. *29th Annual International Conference on the Theory and Applications of Cryptographic Techniques,* French Riviera, May 30–June 3, 2010, pp. 279–298. doi.org/10.1007/978-3-642-13190-5_14
12. Kocher P. C. Timing attacks on implementations of Diffie — Hellman, RSA, DSS, and other systems. *16th Annual International Cryptology Conference,* Santa Barbara, California, USA, 18–22 August, 1996, pp. 104–113. doi.org/10.1007/3-540-68697-5_9
13. Barker E. *NIST Special Publication 800-57. Part 1: Revision 4, Recommendation for Key Management, Part 1: General*. National Inst. of Standards and Technology, Gaithersburg, MD, USA, 2016. doi.org/10.6028/NIST.SP.800-57pt1r4
14. Eisenbarth T., Kumar S., Paar C., Poschmann A., Uhsadel L. A survey of lightweight-cryptography implementations. *IEEE Design & Test of Computers*, 2007, vol. 24, no. 6, pp. 522–533. doi.org/10.1109/MDT.2007.178
15. Ivanov F., Krouk E., Kreshchuk A. On the lightweight McEliece cryptosystem for low-power devices. *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)*, Moscow, Russia, 21–25 October, 2019, pp. 133–138. doi.org/10.1109/REDUNDANCY48165.2019.9003324
16. Zyablov V. V., Ivanov F. I., Krouk E. A., Sidorenko V. R. On new problems in asymmetric cryptography based on error-resistant coding. *Problems of Information Transmission,* 2022, vol. 58, no. 2, pp. 184–201. doi:10.1134/S0032946022020077
17. Ivanov F., Krouk E., Kabatiansky G., Rumenko N. New code-based cryptosystem. *8th International Workshop "Code-Based Cryptography" (CBCrypto 2020)*, Zagreb, Croatia, 9–10 May, 2020, LNSC, vol. 12087, pp. 41–49. doi:10.1007/978-3-030-54074-6_3
18. Krasavin A. A. (U|U+V) modification for McEliece cryptosystem. *Proceedings of MIPT*, 2018, vol. 10, no. 2, pp. 109–113 (In Russian). EDN: XTWBRZ
19. Sukhorukov A. S. Bandwidth multidimensional discrete communication channel with memory. *T-Comm*, 2018, vol. 12, no. 3, pp. 13–21 (In Russian). doi:10.24411/2072-8735-2018-10048, EDN: XOHIUP
20. Kudryashova A. Yu. Minimizing signal distortions at the most optimal choice of digital conversion method. *T-Comm*, 2020, vol. 14, no. 5, pp. 27–34 (In Russian). doi:10.36724/2072-8735-2020-14-5-27-34, EDN: AIOUOJ