УДК 621.391.8:519.725

ИСПОЛЬЗОВАНИЕ КВАДРАТИЧНО-ВЫЧЕТНОЙ КОНСТРУКЦИИ КОДА ДЛЯ ПЕРЕДАЧИ ИНФОРМАЦИИ В КАНАЛЕ ВАЙНЕРА

А.И. МИТЮХИН[1], П.П. УРБАНОВИЧ[2]

[1]*Институт информационных технологий*
Белорусского государственного университета информатики и радиоэлектроники
(г. Минск, Беларусь)
[2]*Белорусск*ого *государственный технологический университет*
(г. Минск, Беларусь)

E-mail: mityuhin@bsuir.by, p.urbanovich@belstu.by

Аннотация. Для повышения надёжности передачи информации в канале с шумами и защиты от несанкционированоого доступа предлагается осуществить кодирование с использованием нелинейного алгоритма формирования кода на основе квадратичных вычетов в конечном поле. Показано возможное применение кода не только для коррекции ошибок, но и для защиты информации от перехвата в многостанционных радиосистемах с расширением спектра.

Abstract. To increase the reliability of information transmission over a noisy channel and protect against unauthorized access, it is proposed to implement coding using a nonlinear code generation algorithm based on quadratic residues in a finite field. The possible application of the code is demonstrated not only for error correction but also for protecting information from interception in multi-station radio systems with spread spectrum.

Введение

В современных радиосистемах связи важнейшее значение имеют такие характеристики как помехозащищенность и защита от перехвата информации. Для многих применений повышение надежности связи решается за счет использования метода расширения спектра информационного сигнала, кодирования информации кодом, статистические и спектральные характеристики, которого приближаются к характеристикам фонового излучения типа белого шума [1]. Для специальных условий обеспечения связи радиосистемы должны надежно работать в каналах с активным радиоэлектронным подавлением, а также в условиях, когда в канале с подслушиванием [2] решаются задачи обнаружения сигнала, определения структуры сигнала и декодирования. В статье рассматривается метод нелинейного помехоустойчивого кодирования и способ защиты от несанкционированного доступа в радиосистеме на основе применения нелинейного метода формирования кода. Анализируются необходимые характеристики кодирования, повышающие уровень помехозащищенности и уровень защиты от перехвата.

Постановка задачи

Известно, что в системах с коррекцией ошибок широко используются линейные конструкции кодов, позволяюшие обеспечить передачу информации с высокой надежностью и наперед заданную вероятность ошибок [3]. В качестве примера можно привести коды максимальной длины (М-коды), коды Голда, линейные коды Адамара, коды Хэмминга и др. В задачах же связанных не только с коррекцией ошибок, но и защитой от перехвата, линейные коды даже сравнительно большой длины проявляют высокую степень уязвимости к структурному анализу перехватчика. При использовании линейных кодовых структур задача перехватчика по раскрытию параметров кодирования значительно упрощается.

Под перехватом кода будем понимать задачу восстановления порождающей матрицы $\mathbf{G}$ по принятым кодовым словам. В линейном пространстве кодовые слова есть линейная комбинация строк порождающей матрицы $\mathbf{G}$. Тогда линейные коды можно представить в виде системы линейных уравнений. Очевидно, используя методы линейной алгебры, например, метод Гаусса, можно построить порождающую или проверочную матрицы. Рассмотрим применение метода Гаусса для построения матрицы $\mathbf{G}$ и оценки вычислительной и временной сложности.

Чтобы построить матрицу $\mathbf{G}$ необходимо перехватить (принять) как минимум k кодовых слов длиной n, где k обозначает число информационный символов кода. Перехваченные слова образуют базис линейного

подпространства кода. Применяя метод Гаусса, можно получить матрицу $\mathbf{G}$ размером $(k \times n)$ в канонической форме

$$\mathbf{G}_{k\times n} = \left(\mathbf{I}_k \middle| \mathbf{G}^*_{k\times r} \right), \tag{1}$$

где r – число проверочных символов кода;

$\mathbf{G}^*_{k\times r}$ – проверочная часть порождающей матрицы кода.

Как видно из (1) получен закон кодирования информационных символов. Вычислительная сложность получения матрицы кода методом Гаусса составляет

$$O\left(k^2 n\right). \tag{2}$$

Если в радиосистеме применяются высокоскоростные коды, когда скорость кода $R = \frac{k}{n}$ приближается к единице и $k \approx n,$ сложность (2) асимптотически приближается к кубической сложности

$$O\left(n^3\right). \tag{3}$$

Возникает вопрос, как быстро можно осуществить перехват линейного кода над полем Галуа $GF(2)$ в канале с вероятностью ошибки p и сложностью (3). Для этого необходимо принять без ошибок k линейно независимых кодовых слов длиной $n.$ Перехватываемые кодовые слова могут быть и линейно зависимыми, поэтому необходимо учитывать это при оценке времени на перехват. Вероятность правильного приема слова определяется известным выражением

$$P_f = \left(1 - p\right)^n.$$

Метод Гаусса требует наличия только правильного множества кодовых слов, поэтому находим вероятность правильного приема всего множества из k кодовых слов

$$P_{\Sigma f} = P_f{}^k = \left(1 - p\right)^{kn}. \tag{4}$$

Используя формулу геометрического распределения, находим среднее количество попыток для получения перехвата множества из k кодовых слов без ошибок

$$E = \frac{1}{P_{\Sigma f}}. \tag{5}$$

Используя (3) и (5) можно получить оценку сложности перехвата линейного кода, используя метод Гаусса. Перехват требует выполнения

$$C = En^3 \tag{6}$$

вычислительных операций.

Используя (6) и физические характеристики канала, в табл. 1 представлены вычислительные и временные затраты на перехват линейного $[n,\ k]$-кода, (применялся метод Гаусса).

Таблица 1. Вычислительные и временные затраты на перехват линейного помехоусточивого кода

$[n,\ k]$	Вероятность ошибки p	Скорость канала, бит/с	Тактовая частота процессора, Гц	Число операций	Время на перехват, с
$[127,\ 120]$	10^{-4}	10^6	10^9	8640000	0,264

Поскольку в реальных радиосистемах связи длина линейного кода ограничивается временем на решение задач синхронизации (поиска) и требованием к вычислительной сложности декодирования, задача перехвата по раскрытию параметров линейного кодирования еще более упрощается. Это переводит задачу раскрытия параметров кода из разряда вычислительно невозможных в разряд тривиальных, реализуемых в реальном времени на стандартных процессорах. Хотя эти коды подходят для решения задачи синхронизации и устойчивости к шуму, они не обеспечивают никакой криптографической безопасности в каналах с низким уровнем шумов.

Утверждение. Линейные кодовые структуры любой практической длины или сложности $O\left(n^3\right)$ современными вычислительными средствами эффективно раскрываются за реальное время обработки.

Для устранения линейной уязвимости предлагается переход к нелинейному кодированию источника.

Задача передачи информации с коррекцией ошибок и одновременно задача защиты от перехвата должны решаться на нелинейном подходе или на крипто-кодовом подходе. Примерами крипто-кодового подхода являются криптосистемы Мак-Элиса и Нидеррайтера [4], [5]. Криптосистема Мак-Элиса основана на сложности декодирования случайного кода. Для случайного кода задача декодирования по зашумленному слову является NP-полной. Единственный способ для перехватчика получить матрицу $\mathbf{G}'$ – это полный перебор всех возможных комбинаций. Однако, недостатоком названных криптосистем является значительная техническая сложность. Криптосистема Мак-Элиса требует использования порождающих матриц $\mathbf{G}'$ большого размера. Например, матрица $\mathbf{G}'$ может состоять из $\approx 37 \cdot 10^6$ бит. Возникают ограничения по пропускной способности радиоканала, особенно для канала с шумами. Возникают также проблемы с передачей кодовых последовательностей, которые выступают в качестве секретных ключей криптосистемы. Названные проблемы делают внедрение крипто-кодовых систем в реальные радиосистемы, например, в системах связи с БПЛА сложным, техническая реализация системы с разумными временными параметрами вхождения в связь становится не реальной.

Для устранения линейной уязвимости, технической сложности криптосистем типа Мак-Элиса предлагается переход к нелинейному помехоустойчивому кодированию источника. Рассматриваемый подход строится на намеренно внесенные ошибки кодирования как в системе типа Мак-Элиса. Построение же порождающей матрицы выполняется на нелинейных функциях.

Решение задачи

В кодовый вектор намеренно вносится вектор $\mathbf{e} = \left(e_0, e_1, ..., e_{n-1}\right)$ случайных ошибок. В этом случае передача данных моделируется информационным каналом Вайнера (канал с подслушиванием), рис. 1. Модель такого канала гарантирует информационно-теоретическую (абсолютную) безопасность [6].

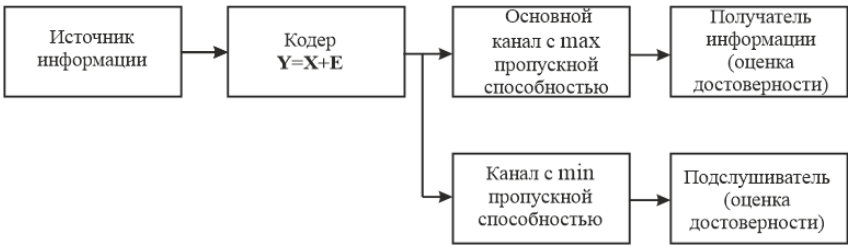

Рис. 1. Модель канала с подслушиванием

$\mathbf{X}$ – кодированное сообщение, $\mathbf{E}$ – случайный вектор ошибок в канале с минимальной пропускной способностью.

Ошибки в канале подслушивания или большой уровень шума в принятом им сигнале мешают декодированию кодированных сообщений, передаваемых по основному каналу. Кодер-декодер основного канала должны быть построены так, чтобы обеспечивать надежную защиту информации от перехвата. При этом необходимо обеспечить не только невозможность доступа к передаваемой информации, но и передачу данных с наибольшей скоростью *R.* Требования надежности и секретности означают, что должна быть обеспечена максимально возможная ненадежность данных, поступающих к подслушивающему приемному устройству (декодеру). По основновну каналу принимается искаженное кодовое слово и декодируется на основе принципа максимального правдопобия или минимума расстояния Хэмминга. Одновременно исправляются как намеренно внесенные ошибки в кодовое слово, так и ошибки из-за шумов, возникших в канале связи. В канале перехватчика

обеспечить оптимальное декодирования невозможно из-за значительного уровня шума и нелинейного кодирования, когда сообщение превращается случайный набор символов.

Теоретические принципы

Существуют коды, которые строятся на квадратичных вычетах на полем $GF(p)$, где p – простое нечетное целое число.

Определение 1. Ненулевые квадраты чисел, вычисленные по модулю p называются квадратичными вычетами по модулю p.

Для нахождения квадратичных вычетов достаточно рассмотреть только квадраты чисел до

$$\left(\frac{p-1}{2}\right)^2 \bmod p. \tag{7}$$

Количество всех квадратичных вычетов вычетов по модулю p равно

$$(p-1)/2.$$

Оставшиеся $(p-1)/2$ чисел по модулю p называются невычетами.

Операция вычисления квадратов чисел и нахождение вычетов является нелинейной. Выбор функций квадратичных вычетов и невычетов для построения нелинейного кода, связан с тем, что они не удовлетворяет принципу суперпозии (линейности), когда

$$T\left(x_1 + x_2\right) \neq T\left(y_1\right) + T\left(y_2\right),$$

где x_1 и x_2 – входные данные, y_1 и y_2 выходные данные, оператор $T[*]$ определяет характер математических операций при отображении входных данных в выходные.

Свойство нелинейности квадратичных вычетов можно использовать для построения помехоустойчивого кода, обеспечивающего защиту от перехвата.

Определение 2. Пусть p – простое нечетное число. Функция χ называется символом Лежандра, если

$$\chi(i) = \begin{cases} 0, \text{ если } i \text{ кратно } p \text{ (делится на } p); \\ 1, \text{ если } i \text{ квадратичный вычет по модулю } p; \\ -1, \text{ если } i \text{ квадратичный невычет по модулю } p, \end{cases}$$

где $i = 0,1,...,p-1.$

При помощи квадратичных вычетов и функция χ можно построить нелинейный помехоустойчивый код с необходимым кодовым расстоянием d.

Элемент кодового слова вычисляется по формуле

$$l(i) = \begin{cases} 1, \text{ если } i \text{ квадратичный вычет по модулю } p; \\ -1, \text{ если } i \text{ квадратичный невычет по модулю } p, \end{cases} \tag{8}$$

В рассматриваемой системе кодирования длина кода $n = p$. Кроме свойства нелинейности последовательности (8), выбор данного метода кодирования связан с тем, что минимальное расстояние кода определяется алгебраическим пределом и позволяет работать в каналах с высоким зашумлением.

Таким образом, помехоустойчивая передача информации будет строится на нелинейном алгоритме кодирования и криптоподходе, обеспечивающем защиту от перехвата. Однако, нелинейность кода спасает только от линейного криптоанализа и не решает проблемы стойкости. Криптостойкость радиосистемы определяется тем, как использовать нелинейный помехоустойчивый код. Предлагается криптостойкость обеспечить дополнительным кодированием нелинейного кода М-кодом большой длины. Для каждого нелинейного слова формируется случайный поток вида

$$\mathbf{c}^j = \mathbf{l}^j \oplus \mathbf{m}^j, j = 0,1,...,n-1,$$

где $\mathbf{c}$ – вектор, элементами которого являются выборочные оценки входного процесса, $\mathbf{l}$ – вектор нелинейного кода, $\mathbf{m}$ – вектор-сегмент М-кода.

В качестве сегмента М-кода выбирается состояние регистра сдвига, в котором формируется последовательность длиной

$$n = 2^k - 1.$$

Рассматривается система сигналов, состоящая из n различных нелинейных кодовых слов, построенных на квадратичных вычетах. Все кодовые слова описываются циркулянтной матрицей

$$\mathbf{L} = \begin{pmatrix} l_0 & l_1 & \cdots & l_{n-1} \\ l_{n-1} & l_0 & \cdots & l_{n-2} \\ \cdot & \cdot & \cdot & \cdot \\ l_1 & l_2 & \cdots & l_0 \end{pmatrix}. \quad (9)$$

Коэффициентами матрицы являются числа $1, -1$.

Исходя из понятия теоретико-информационной стойкости, предлагается реализовать динамическое соответствие между строками матрицы (9) и сегментами (состояниями регистра) М-кода. В этом случае появляется возможность получить уровень стойкости, приближающийся к стойкости одноразового шифр-блокнота. При этом необходимо обеспечить тактовую синхронизацию генераторов М-кода передатчика и приемника по основному каналу, рис. 1. Задача синхронизации может решаться с использованием подхода, примененного в системе NAVSTAR. Кроме того, применение микротермостатированных кварцевых генераторов тактовой частоты на передающей и приемной стороне также снимает проблему синхронизации за реальное время работы радиосистемы.

На премной стороне в основном канале после снятия сегмента, декодирование кода можно реализовать на основе согласованной фильтрации или корреляционной обработки. В этом случае вычисляется произведение вида

$$\mathbf{Z} = \mathbf{LY},$$

где $\mathbf{Y} = (y_0, y_1, ..., y_{n\text{-}1})$ – вектор, коэффициенты которого есть выборочные значения входного процесса декодера, $\mathbf{Z} = (z_0, z_1, ..., z_{n\text{-}1})$ – вектор, значения коэффициентов которого описывают корреляционную функцию.

Моделирование и анализ криптографической стойкости метода

Моделирование проводилось с использованием математического программного продукта MATLAB. Использовались квадратичными вычеты по модулю $p = 257$. Полная матрица $\mathbf{L}$ помехоустойчивого кода имела размерность (257×257). В качестве кода, вносившего высокую степень случайности канального потока кодированных данных, использовался М-код длиной $n = 2^{511} - 1 \approx 6,7 \cdot 10^{153}$. Такое значение длины исключает повторение состояние регисто сдвига за реальное время передачи радиосигнала. Вычислительная сложность полного перебора М-кода составляет $2^{511} - 1$ операций. Каждая строка матрицы $\mathbf{L}$ кодировалась динамическим сегментом длиной 511. Фактически сегменты вырезались длиной 257 бит. Без априорного знания двоичного состояния регистра сдвига, вычислить, какой именно сегмент М-кода был использован в текущий момент времени математически невозможно за реальное время. Тем самым обеспечивается высокая вычислительная стойкость. Выбор этих значений кодирования полностью скрывал алгебраическое соответствие между матрицей $\mathbf{L}$ и сегментами. Чтобы симуляция была приближена к реальности, в модель генератора тактовой частоты в MATLAB добавлялся блок случайных блужданий фазы имитирующий температурный уход.

Результаты и их обсуждение

1. Поскольку символы неповторяемых сегментов М-кода смешиваются поэлементно с нелинейной циркулянтной матрицей кода, перехватчик никогда не вычислит исходные состояния генератора-регистра М-кода. Алгоритм Берлекэмпа-Месси, используемый с целью быстрого декодировани М-кода, в этом случае перестает работать.
2. Предложенный метод передачи информации в канале Вайнера характеризуется абсолютной практической безопасностью.
3. Осуществить декодирование информации методом перебора или на основе математического анализа за реальное время невозможно.
4. Нелинейные свойства помехоустойчивого кода, построенного на квадратичных вычетах, намеренно внесенные ошибки кодирования позволяют обеспечить практически нулевую пропускную способность в канале подслушивателя.
5. Помехоустойчивый код, построенный на квадратичных вычетах, позволяет иметь максимальную пропускную способнось в основном канале.
6. Хотя вычислительна стойкость метода уступает теоретико-информационной стойкости, радиосистема, построенная на предлагаемом принципе неуязвима для существующих вычислительных систем. Возникает вычислительно невыполнимая задача правильного декодирования в канале подслушивателя.
7. Можно утверждать, что защита от декодирования в канале подслушивания, построенная на основе применения рассмотренных двух этапов кодирования реализуется на понятии вычислительной стойкости, когда систему можно взломать не за реальное время, имея не бесконечную вычислительную производительность процессора.

Заключение

Приведенное рассмотрение использования квадратично-вычетной конструкции кода для передачи информации в канале Вайнера обеспечивает помехоустойчивость и защиту от перехвата. Если имеются ограничения на время передачи информации, радиосистема остается секретной с практической точки зрения. Описанные конструкции могут быть использованы в системах крипто-кодового класса.

Список использованных источников

1. Mitsiukhin A. Detection and Analysis of Moving Objects. International Journal on Applied Physics and Engineering, Volume 4, 2025, 62–71.
2. Bloch M., R., Barros J. Physical-Layer Security: From Information Theory to Security Engineering. Cambridge University Press, 2011.
3. Мак-Вильямс Ф. Дж., Слоен Н. Дж. А. Теория кодов, исправляющих ошибки. М. Связь, 1979.
4. Тилборг ван Х. К. А. Основы криптологии. М. Мир, 2006.
5. Bernstein D. J., Buchmann J., Dahmen E. Post-Quantum Cryptography. Springer, 2009.
6. Смарт Н. Криптография. М. Техносфера, 2006.