

ОЦЕНКА ЭФФЕКТИВНОСТИ ПСЕВДОСЛУЧАЙНЫХ КОДОВ, СГЕНЕРИРОВАННЫХ С ПОМОЩЬЮ LFSR

Т.В. ЛАВРОВСКАЯ, О.И. ВОТЯКОВ, С.Г. РАССОМАХИН

Рассматривается возможность применения сдвиговых регистров с линейной обратной связью (LFSR) для генерации псевдослучайных помехоустойчивых кодов. Обоснована актуальность и проведена сравнительная оценка эффективности таких кодов путем сопоставления числовых характеристик спектров взаимных расстояний с аналогичными характеристиками равномерно случайных кодов. Сделано заключение о перспективности применения LFSR-кодов для снижения вычислительной сложности алгоритмов декодирования.

Ключевые слова: псевдослучайный код, LFSR, LFSR ПСК, равномерно случайный код, кодовое расстояние.

ВВЕДЕНИЕ

Постановка проблемы. В связи с глобализацией использования новых поколений сотовой связи и системы Интернет, для пользователей открываются новые горизонты применения данных сервисов, в частности все большую популярность набирают доверительные услуги, электронный документооборот, интернет-банкинг и другие. Это приводит к циркулированию в сети больших объемов информации, которая нуждается в надежной защите. Поэтому возникает проблема в разработке эффективных методов кодирования данных, которые будут обладать достаточным уровнем помехозащищенности. В связи с этим новый виток в развитии получили линейные блочные коды, использующие в качестве канальных символов псевдослучайные числа (псевдослучайные коды – ПСК) [1].

Основной преградой для широкого использования таких кодов является то, что декодирование, как правило, основывается на реализации принципа максимального правдоподобия и возможно лишь с использованием переборных алгоритмов.

Вычислительная сложность таких алгоритмов возрастает экспоненциально с длиной блока кода и при практически требуемых значениях длины блока является неприемлемой. Это является прямым следствием того, что существующие методы получения последовательностей псевдослучайных чисел основаны на применении нелинейных операций, к которым можно отнести и вычисление по модулю. Поэтому, была предпринята попытка получения ПСК с помощью применения линейного сдвигового регистра с обратной связью (LFSR), а также оценка эффективности кодов. При этом использование LFSR дает возможность реализации линейных алгебраических методов декодирования, например, с помощью алгоритма Берлекэмп-Мэсси или его модификаций [2].

Цель работы: разработка метода построения ПСК, который позволит реализовать декодирование, путем решения системы линейных уравнений, а также сравнение эффективности по

характеристикам спектра взаимных расстояний (весов) LFSR ПСК с равномерно случайными кодами (ПСК), полученными более сложными (нелинейными) алгоритмами.

1. АНАЛИТИЧЕСКАЯ МОДЕЛЬ ПСЕВДОСЛУЧАЙНОГО LFSR-КОДА

Линейные коды в контексте данной работы выступают как множество точек многомерного пространства, система координат которого обозначается вектором R . В качестве начальной инициализации для элементов вектора выбираются числа из диапазона $R_i \in [0, 2^n - 1]$, где n – это степень примитивного многочлена $P(x)$, который определяет структуру LFSR генератора. Элементы регистра при его инициализации представляются в двоичной системе счисления с алфавитом «-1» и «+1». Эти числа являются разрядами двоичного слова источника, подлежащего кодированию для формирования канального кодового слова ПСК.

Реализация регистра сдвига, обозначаемого в дальнейшем R , основывается на применении LFSR с базовой конфигурацией Фибоначчи. Основным отличием от традиционных рассмотрений LFSR структур в задачах формирования сложных сигнальных конструкций, является замена нелинейной операции суммирования по модулю два простым алгебраическим (с учетом знака) сложением.

Пусть

$$P(x) = \sum_{i=0}^n c_i \cdot x^i, \quad c_i \in [0, 1] \quad (1)$$

– полином структуры LFSR. Обозначим s – вектор, содержащий $m+1$ элементов из диапазона $[0, n]$, каждый из которых равен степени переменной x , входящей в (1) с ненулевым коэффициентом c_i . Величина m определяется числом резидентных обратных связей в структуре LFSR. Оправданным является название “вектор отводов”, используемое в дальнейшем для вектора s .

Используемая для построения LFSR ПСК схема сдвигового генератора представлена на рис. 1. В процессе генерации происходит потак-

товый сдвиг содержимого ячеек памяти регистра право на 1 позицию. При этом в отличие от традиционного алгоритма Фибоначчи каждая из ячеек памяти регистра сдвига способна хранить знаковые числа, абсолютная величина которых значительно превышает единицу. Кроме того, в отличие от обычных LFSR, в цепях обратных связей присутствует операция знакопереодевания, задаваемая множителями $(-1)^j$, $j \in \overline{1, (n-1)}$. Сумматоры на рис. 1 являются простыми алгебраическими устройствами сложения целых знаковых чисел. Содержимое младшей ячейки памяти регистра формируется в соответствии с вектором отводов s . Текущее значение символа ПСК считывается на каждом такте из старшей (ячейки) регистра R после завершения очередного сдвига вправо. В младшую ячейку заносится результат вычисления R_0 в соответствии со следующей формулой:

$$R_0 = \sum_{j=1}^m (-1)^j R_{(s_j-1)}, \quad (2)$$

где s — определенный выше вектор отводов.

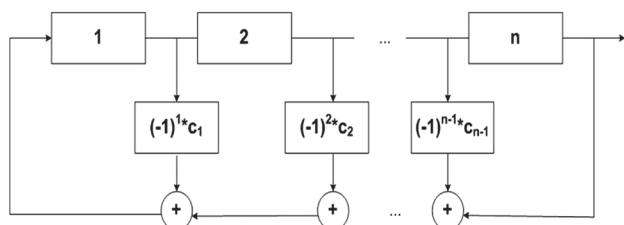


Рис. 1. Схема генератора ПСК с помощью LFSR

В результате инициализации вектора R двоичным числом i за конечное количество тактов N генерируется вектор, координатами которого являются псевдослучайные числа $Z_i = \{Z_{i,1}, Z_{i,2}, \dots, Z_{i,n}\}$. Перебор i от 0 до $2^n - 1$ дает возможность составления кортежей последовательностей Z_i , которые в последующем объединены в матрицу ZDV из транспонированных векторов Z_i :

$$ZDV = \text{augment}(Z_0, Z_1, \dots, Z_{2^n-1})^T, \quad (3)$$

где augment — функция объединения векторов Z_i в матрицу с размерностью $2^n \times n$.

Формирование кодовой книги осуществляется в два этапа.

На первом этапе производится выбор подматрицы $KB \in ZDV$, строки которой являются прототипами кодовых слов LFSR ПСК. Подматрица KB обладает размерностью $2^n \times n$, причем $\frac{n}{r} = V$ — скорость помехоустойчивого кода. Так как соотношение между n и r может быть произвольным, то допускаются значения скорости кода V как меньше, так и больше единицы, что является характерным для псевдослучайных кодов. В данной работе исследуются коды только для случая $V = 1$, т.е. $r = n$. Тогда функция извлечения подматрицы KB имеет вид:

$$KB = (\text{submatrix}(ZDV, 0, 2^n - 1, nc, nc + r - 1)), \quad (4)$$

где submatrix — функция, которая формирует подматрицу из ZDV , состоящую из строк с номерами от 0 до $2^n - 1$ и столбцов с номерами от nc до $nc + r - 1 = nc + n - 1$ включительно. Здесь параметр nc обозначает начальный номер столбца ZDV для формируемой подматрицы KB . Для исследований использован параметр $nc = n$.

На втором этапе производится нормировка символов (чисел) канального кода в соответствии с задаваемым бюджетом энергии. Смысл данной операции заключается в том, чтобы средний квадрат любого канального символа подматрицы KB не превышал заданного максимального значения $q_{\max}$. Для упрощения расчетов в представленной модели значение $q_{\max}$ положено единичным. На выходе генератора последовательности канальных символов образуют псевдохаотический поток из знаковых натуральных чисел.

Для минимизации канальных затрат энергии (в предположении использования многоуровневой амплитудной модуляции) целесообразна операция центрирования канальных символов (чисел) в относительно нуля. Для этого необходимо вычисление математического ожидания для элементов выбранной на первом этапе подматрицы:

$$MX = \frac{1}{n \cdot 2^n} \cdot \sum_{i=0}^{2^n-1} \sum_{j=0}^{n-1} (KB_i)_j. \quad (5)$$

После выполнения (5) производится перерасчет прототипов кодовых слов и строится модифицированная матрица из центрированных относительно нуля псевдослучайных элементов $KB0$:

$$KB0 = KB - MX. \quad (6)$$

Средняя мощность (дисперсия) канальных чисел может быть вычислена по формуле:

$$DX = \frac{1}{n \cdot 2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{n-1} ((KB0_i)_j)^2. \quad (7)$$

Финальной операцией второго этапа формирования кодовой книги является нормировка центрированной матрицы $KB0$ в соответствии с выделенным бюджетом энергии на передачу канального символа $q_{\max}$. При этом производится окончательное формирование кодовой книги LFSR ПСК $KB1$:

$$KB1 = \frac{KB0}{\sqrt{DX}} \cdot \sqrt{q_{\max}}. \quad (8)$$

Очевидно, что корректность энергетической нормировки может быть подтверждена проверкой выполнения следующего равенства:

$$\frac{1}{n \cdot 2^n} \cdot \sum_{i=0}^{2^n-1} \sum_{j=0}^{n-1} ((KB1_i)_j)^2 = q_{\max}, \quad (9)$$

которое является прямым следствием выражений (7) и (8) [3].

Для достижения требуемого уровня помехозащищенности необходимо использовать коды, которые обладают достаточно большим расстоянием между всеми парами кодовых слов. Поэтому

вычисление характеристик кодовой книги, количественно оценивающих взаимную удаленность кодовых слов (точек m -мерного пространства) является эффективным способом оценки характеристик помехоустойчивости LFSR ПСК. Для реализации этой цели в рассматриваемой модели используется функция оценки эффективности кодов по характеристикам спектра взаимных расстояний (весов) $GD1$:

$$GD1 = \left\{ gd_0^1, gd_1^2, \dots, gd_{2^n-2}^{2^n-1} \right\}, \quad (10)$$

$$C_{2^n}^2 = \frac{2^n!}{(2^n-2)!2!} - \text{элементов}$$

где $gd_i^j = |KB1_i - KB1_j|$ — взаимное расстояние между словами с номерами i и j в кодовой книге LFSR ПСК.

Результаты тестирования рассматриваемой модели LFSR ПСК представлены на рис. 2, 3 в виде гистограмм, которые отображают распределение взаимных расстояний кодовых слов $GD1$, полученных описанным выше способом при разных порождающих полиномах. Для осуществления возможности сравнительной оценки на этих же рисунках представлены гистограммы распределения весов для псевдослучайных кодов, символы которых генерируются программным датчиком с нелинейным алгоритмом формирования равномерно распределенных в заданном диапазоне чисел. Такие коды можно использовать в качестве эталона для сравнения, поскольку их свойства достаточно хорошо изучены и обеспе-

чивают в определенных диапазонах отношений сигнал/шум монотонное убывание вероятности декодирования с ошибкой при увеличении длины блока [4]. Для обеспечения корректных условий сравнения спектров взаимных расстояний LFSR ПСК и ПСК последние нормированы на одинаковую с (8) среднюю энергию канального символа.

В качестве основных числовых параметров для сравнения использованы вычисления:

- математического ожидания взаимного евклидова расстояния между парами кодовых слов $mean(GD1)$ и $mean(GD2)$;
- среднеквадратического отклонения для гистограмм исследуемых распределений $stdev$;
- медианы распределения спектров $median(GD1)$ и $median(GD2)$.

Сопоставление полученных числовых характеристик для LFSR ПСК и ПСК свидетельствует о их достаточной близости. Коды, получаемые с помощью линейного алгоритма LFSR, безусловно уступают по числовым параметрам спектров весов равномерно случайным кодам. Однако отсутствие возрастания этого проигрыша при увеличении степени порождающего многочлена LFSR, а также простота линейной алгебраической генерации, как предпосылка реализации вычислительно легких алгоритмов декодирования, дают возможность для констатации перспективности рассмотренных кодов.

ВЫВОДЫ

Построенная модель и проведенный вычислительный эксперимент позволяют сделать оптимистический прогноз о дальнейшем использовании ПСК сгенерированных на основе LFSR. Хотя по полученным характеристикам (математическое ожидание, дисперсия и среднеквадратическое отклонение) коды сгенерированные на основе LFSR, и проигрывают равномерно случайным кодам. Однако эти недостатки можно компенсировать, за счет использования порождающего неприводимого многочлена более высокой степени. Такие коды, в силу линейности алгоритма формирования символов кодовых слов являются легко декодируемыми с использованием линейных алгебраических методов. Это дает возможность увеличения длины блока, до практически требуемых значений, а также открывает перспективу для решения проблемы декодирования ПСК. В качестве направления дальнейших исследований целесообразно выбрать рассмотрение линейных алгебраических методов декодирования LFSR ПСК, например, с помощью алгоритма Бэрлекэмп — Мэсси или его модификаций.

Литература

- [1] Григорьев, В.А. Сети и системы радиодоступа [Текст] / В. А. Григорьев, О. И. Лагутенко., Ю.А. Распаев. — М.: Эко-Трендз, 2005. — 384 с.
- [2] Скляр, Б. Цифровая связь. Теоретические основы и практическое применение [Текст] / Б. Скляр //

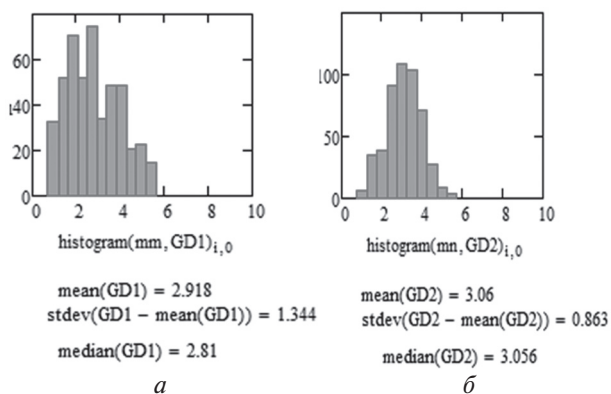


Рис. 2. Распределение кодовых слов ПСК LFSR (а) и ПСК (б) при $P(x) = x^5 + x^2 + 1$

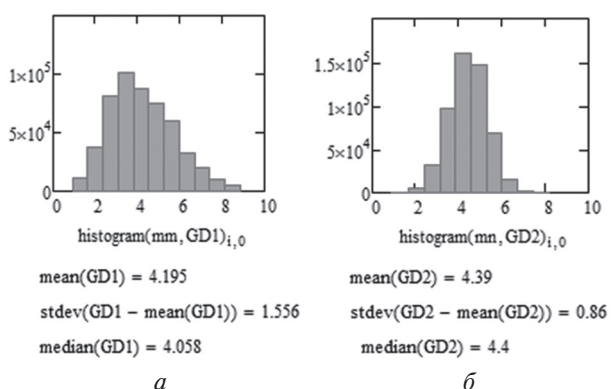


Рис. 3. Распределение кодовых слов ПСК LFSR (а) и ПСК (б) при $P(x) = x^{10} + x^3 + 1$

Изд. 2-е» испр. : Пер. с англ. — М. : Издательский дом “Вильямс”, 2003. — С. 354–378.

- [3] *Гихман, И.И.* Теория вероятностей и математическая статистика [Текст] / И.И. Гихман, А.В. Скороход, Н.И. Ядренко. — К.: Высшая шк., 1982. — 439 с.
- [4] *Лавровская, Т.В.* Анализ применения правила простого округления для получения вычислительно реализуемых методов декодирования / С.Г. Рассомахин, Т.В. Лавровская // Системы обработки информации. — 2015. — Вып. 5 (151). — С. 115–117.

Поступила в редколлегию 9.11.2015



Лавровская Тамила Валериевна, аспирант кафедры безопасности информационных систем и технологий ХНУ имени В. Н. Каразина. Научные интересы: информационная безопасность, теория передачи информации.

Вотяков Олег Иванович, кандидат технических наук, директор ЦКБ «Протон», г. Харьков. Научные интересы: информационная безопасность, системы радиомониторинга и радиоконтроля.



Рассомахин Сергей Геннадиевич, доктор технических наук, доцент, заведующий кафедрой БИСТ ХНУ им. В.Н. Каразина. Научные интересы: информационная безопасность, теория передачи информации.

УДК 621.391

Оцінка ефективності псевдовипадкових кодів згенерованих за допомогою LFSR / Т.В. Лавровська, О.І. Вотяков, С.Г. Рассомахин // Прикладна радіоелектроніка: наук.-техн. журнал. — 2015. — Том 14. — № 4. — С. 339–342.

Розглядається можливість застосування зсувних регістрів з лінійним зворотним зв'язком (LFSR) для генерації псевдовипадкових завадостійких кодів. Обґрунтовано актуальність і проведено порівняльну оцінку ефективності таких кодів шляхом зіставлення числових характеристик спектрів взаємних відстаней з аналогічними характеристиками рівномірно випадкових кодів. Зроблено висновок про перспективність застосування LFSR-кодів для зниження обчислювальної складності алгоритмів декодування.

Ключові слова: псевдовипадковий код, LFSR, LFSR ПСК, рівномірно випадковий код, кодова відстань.

Рис.: 3. Бібліогр.: 4 найм.

UDC 621.391

Evaluating the effectiveness of pseudorandom codes generated by LFSR / T.V. Lavrovskaya, O.I. Votyakov, S.G. Rassomakhin // Applied Radio Electronics: Sci. Journ. — 2015. — Vol. 14. — № 4. — P. 339–342.

The paper considers a possibility of linear shift feedback registers (LFSR) application for generation of pseudorandom error-correction codes. The actuality has been substantiated and comparative estimation of such codes effectiveness via numerical characteristics comparison of mutual distances spectra with the same characteristics of uniformly random codes has been carried out. A conclusion about the prospectiveness of LFSR-codes application for decoding algorithms computation complexity reduction has been made.

Keywords: pseudo random code, LFSR, LFSR PRC, evenly random code, code distance.

Fig.: 3. Ref.: 4 items.