УДК 621.391:004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 210-218

МЕТОД КРИПТОГРАФИЧЕСКОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ НА БАЗЕ ЭКВИВАЛЕНТНОГО КЛАССА СОВЕРШЕННЫХ ДВОИЧНЫХ РЕШЕТОК

Н.И. Кушниренко, В.Я. Чечельницкий

Одесский национальный политехнический университет,
пр. Шевченко, 1, Одесса, 65044, Украина; e-mail: natalka_kni@ukr.net

На основе свойств совершенных двоичных решеток эквивалентного класса предложен криптографический метод передачи информации, который позволяет уменьшить сложность декодера за счет применения единственного, перестраиваемого под порождающую решетку согласованного фильтра, обеспечить параметрическую скрытность передачи информации, помехоустойчивое кодирование и организовать многоканальную систему передачи информации.

Ключевые слова: криптографическая передача информации, совершенные двоичные решетки, метод модуляции, широкополосные сигналы

Введение

На радиоканал передачи данных, как на открытую систему, в общем случае воздействуют помехи и многолучевые замирания, вызванные естественным происхождением, а также канал подвержен воздействию помех искусственного происхождения от систем преднамеренного разрушения информации, подавления или перехвата данных.

Таким образом, современные системы передачи информации должны противостоять воздействию как естественных, так и специально организованных помех, т.е. обладать высокой помехозащищенностью.

Помехозащищенность – это главный комплексный показатель качества работы систем передачи информации, который включает [1]: помехоустойчивость, энергетическую скрытность, структурную или параметрическую скрытность, криптостойкость, имитостойкость, защиту информации от преднамеренных помех, подавления и перехвата сигналов, защиту информации от несанкционированного доступа. Поэтому главной проблемой телекоммуникационных систем является повышение помехозащищенности.

Обычно проблемы защиты передаваемой информации от влияния помех в каналах связи и защиты информации от несанкционированного доступа решаются независимо. Для защиты информации от воздействия природных и искусственно создаваемых помех используются методы помехоустойчивого кодирования, основанные на внесении передающим устройством в передаваемые цифровые сигналы избыточности и использовании этой избыточности приемником для исправления возникших в канале связи ошибок. А для защиты информации от несанкционированного доступа используются различные методы шифрования.

Для защиты передаваемой информации от влияния помех в каналах связи можно применить совершенные двоичные решетки – СДР. На базе СДР можно строить классы двумерных корректирующих кодов [2]. СДР можно применять и для криптографической передачи информации [3].

Цель статьи и постановка исследований

Целью настоящей статьи является разработка метода криптографической передачи информации с помощью объединения шифрования и канального кодирования на базе эквивалентного класса совершенных двоичных решеток.

Для достижения цели необходимо решить следующие *задачи*:

1. Рассмотреть свойства СДР эквивалентного класса при выполнении операций циклического сдвига строк и столбцов.
2. Разработать принцип и схему информационной модуляции и демодуляции на основе циклических сдвигов СДР эквивалентного класса.
3. Разработать схему модема для криптографической передачи информации.
4. Рассмотреть требования к блокам модема криптографической передачи информации.

Исследования, приведенные в данной статье, выполнены в рамках НИР «Методы защиты информации в широкополосных телекоммуникационных системах» проводимых кафедрой информационной безопасности Одесского национального политехнического университета.

Основная часть

Каждая СДР порядка N порождает класс эквивалентных матриц – $E(N)$-класс СДР [4], путем использования операций циклического сдвига строк и/или столбцов, при этом мощность $E(N)$-класса эквивалентных матриц определяется выражением

$$\Psi_{E(N)} = N^2. \tag{1}$$

Таким образом, если каким-либо способом построена СДР, то тем самым, по сути, задан класс эквивалентных СДР мощности (1), который можно построить из этой СДР как из порождающей.

В табл. 1, в качестве примера, представлен эквивалентный $E(4)$-класс СДР, который построен на базе порождающей матрицы

$$P(4) = \begin{bmatrix} + & + & - & - \\ + & + & + & + \\ - & + & + & - \\ - & + & - & + \end{bmatrix}. \tag{2}$$

Здесь символом «+» обозначен элемент СДР «+1», символом «–» обозначен элемент СДР «–1» для краткости. Далее мы будем применять те же обозначения.

Индексы $[k1, k2]$ возле имени СДР (табл. 1) указывают, на какое количество позиций циклически сдвинуты строки и/или столбцы порождающей СДР – $P^{[0,0]}(4)$, причем $k1$ обозначает количество позиций сдвига строк вниз, а $k2$ — количество позиций сдвига столбцов вправо.

Введем понятие двумерной периодической взаимнокорреляционной функции (ДПВКФ) между произвольными СДР $P^0(N)$ и $P^1(N)$

$$B(N) = \left\| b_{m,n} \right\|, \tag{3}$$

при этом элементы ДПВКФ (3) между двумя СДР $P^0(N)$ и $P^1(N)$ вычисляются по формуле

$$b_{m,n} = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} p^0_{i,j} p^1_{i+m,j+n}. \qquad (4)$$

Таблица 1.

Эквивалентный $E(4)$-класс СДР

	$k2=0$	$k2=1$	$k2=2$	$k2=3$
$k1=0$	$P^{[0,0]}(4)=\begin{bmatrix}+&+&-&-\\+&+&+&+\\-&+&+&-\\-&+&-&+\end{bmatrix}$	$P^{[0,1]}(4)=\begin{bmatrix}-&+&+&-\\+&+&+&+\\-&-&+&+\\+&-&+&+\end{bmatrix}$	$P^{[0,2]}(4)=\begin{bmatrix}-&-&+&+\\+&+&+&+\\+&-&-&+\\-&+&-&+\end{bmatrix}$	$P^{[0,3]}(4)=\begin{bmatrix}+&-&-&+\\+&+&+&+\\+&+&-&-\\+&-&+&-\end{bmatrix}$
$k1=1$	$P^{[1,0]}(4)=\begin{bmatrix}-&+&-&+\\+&+&-&-\\+&+&+&+\\-&+&+&-\end{bmatrix}$	$P^{[1,1]}(4)=\begin{bmatrix}+&-&+&-\\-&+&+&-\\+&+&+&+\\-&-&+&+\end{bmatrix}$	$P^{[1,2]}(4)=\begin{bmatrix}-&+&-&+\\-&-&+&+\\+&+&+&+\\+&-&-&+\end{bmatrix}$	$P^{[1,3]}(4)=\begin{bmatrix}+&-&+&-\\+&-&-&+\\+&+&+&+\\+&+&-&-\end{bmatrix}$
$k1=2$	$P^{[2,0]}(4)=\begin{bmatrix}-&+&+&-\\-&+&-&+\\+&+&-&-\\+&+&+&+\end{bmatrix}$	$P^{[2,1]}(4)=\begin{bmatrix}-&-&+&+\\+&-&+&-\\-&+&+&-\\+&+&+&+\end{bmatrix}$	$P^{[2,2]}(4)=\begin{bmatrix}+&-&-&+\\-&+&-&+\\-&-&+&+\\+&+&+&+\end{bmatrix}$	$P^{[2,3]}(4)=\begin{bmatrix}+&+&-&-\\+&-&+&-\\+&-&-&+\\+&+&+&+\end{bmatrix}$
$k1=3$	$P^{[3,0]}(4)=\begin{bmatrix}+&+&+&+\\-&+&+&-\\-&+&-&+\\+&+&-&-\end{bmatrix}$	$P^{[3,1]}(4)=\begin{bmatrix}+&+&+&+\\-&-&+&+\\+&-&+&-\\-&+&+&-\end{bmatrix}$	$P^{[3,2]}(4)=\begin{bmatrix}+&+&+&+\\+&-&-&+\\-&+&-&+\\-&-&+&+\end{bmatrix}$	$P^{[3,3]}(4)=\begin{bmatrix}+&+&+&+\\+&+&-&-\\+&-&+&-\\+&-&-&+\end{bmatrix}$

В табл. 2, в качестве примера, приведены ДПВКФ между порождающей СДР (2) порядка $N=4$ с параметрами циклического сдвига строк и столбцов – $[0,0]$ и всеми остальными матрицами эквивалентного $E(4)$-класса СДР из табл. 1 с параметрами сдвига $[k1,k2]$.

Из рассмотрения табл. 1 и табл. 2 следует важное свойство СДР эквивалентного $E(N)$-класса.

Свойство. ДПВКФ между порождающей СДР и СДР, чьи строки и/или столбцы циклически сдвинуты по отношению к ней, содержит один пик, энергия которого равна $E=N^2$. Сдвиги этого пика, по отношению к местоположению его в ДПАКВ, однозначно определяют количество циклических сдвигов строк и/или столбцов СДР относительно порождающей СДР.

Таблица 2.

ДПВКФ между СДР эквивалентного $E(4)$ -класса

$B^{[0,0]}(4) = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[0,1]}(4) = \begin{bmatrix} 0 & 16 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[0,2]}(4) = \begin{bmatrix} 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[0,3]}(4) = \begin{bmatrix} 0 & 0 & 0 & 16 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$
$B^{[1,0]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[1,1]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 16 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[1,2]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[1,3]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 16 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$
$B^{[2,0]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[2,1]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 16 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[2,2]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[2,3]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 16 \\ 0 & 0 & 0 & 0 \end{bmatrix}$
$B^{[3,0]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \end{bmatrix}$	$B^{[3,1]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 16 & 0 & 0 \end{bmatrix}$	$B^{[3,2]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \end{bmatrix}$	$B^{[3,3]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 16 \end{bmatrix}$

Установленное свойство имеет важное практическое значение, поскольку является, по сути, обоснованием метода передачи информации на основе циклических сдвигов порождающей СДР.

Рассмотрим более подробно метод передачи информации, основанный на циклических сдвигах СДР эквивалентного $E(N)$ -класса. Схема модулятора, функционирующая на его основе, показана на рис. 1.

Предположим, что сообщение состоит из дискретных символов, каждый из которых выбран из некоторого конечного множества – алфавита. Пусть

$$A \in \{a_0, a_1, a_2, \ldots, a_i, \ldots, a_{q-1}\} \tag{5}$$

алфавит, состоящий из q разных символов. Для передачи каждого символа a_i, где i – номер соответствующего символа из алфавита A (5), модулятор будет использовать одну порождающую СДР из $E(N)$ -класса.

Счетно-решающее средство определения количества циклических сдвигов строк и столбцов работает в модульной арифметике и, соответственно, рассчитывает параметры $k1$ и $k2$ по номеру i передаваемого символа a_i, для передаваемой СДР, следующим образом

$$k1 = Int(i / N), \tag{6}$$

где $Int(a/b)$ – означает целую часть от деления a на b;

$$k2 = Res(i/N), \tag{7}$$

где $Res(a/b)$ – означает остаток от деления a на b.

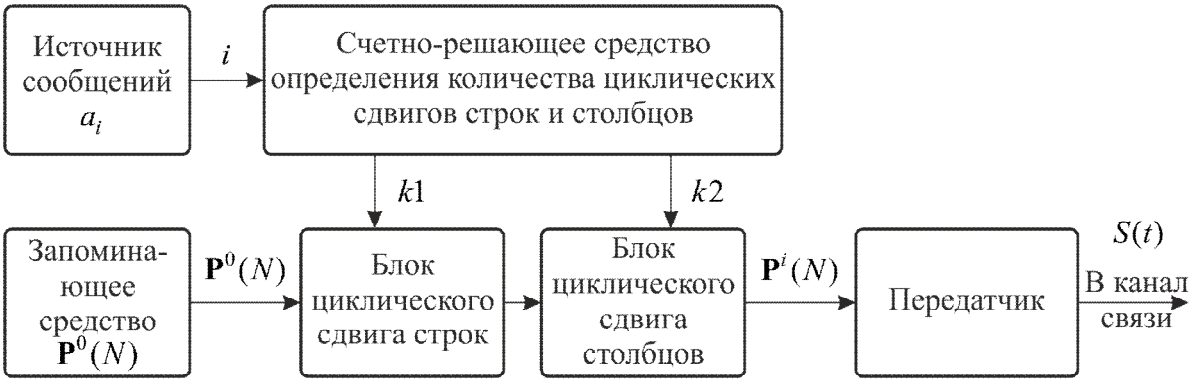

Рис. 1. Модулятор сигналов на основе СДР

Ясно, что порядок N для СДР $E(N)$-класса необходимо выбирать из условия $N^2 \geq q$.

Блок циклического сдвига строк производит циклический сдвиг порождающей СДР $P^0(N)$ на $k1$ (9) строк вниз. Блок циклического сдвига столбцов производит циклический сдвиг полученной СДР на $k2$ (10) столбцов вправо.

При этом каждому передаваемому символу a_i из некоторого алфавита мощности N^2 ставится в соответствие одна СДР из используемого эквивалентного $E(N)$-класса. Номер i соответствующего символа a_i определяет количество циклических сдвигов строк и/или столбцов порождающей СДР $P^0(N)$.

В результате такой информационной модуляции получаем двумерное кодовое слово, которое последовательно строка за строкой подается на вход передатчика, где осуществляется (вторая ступень модуляции) частотная или фазовая модуляция (манипуляция) несущей частоты. Таким образом, в канал связи излучается одномерный дискретный сигнал $S(t)$, длины $n = N^2$ элементов. Ясно, что база такого сигнала определяется как

$$B = FT = N^2, \tag{8}$$

где N – порядок СДР.

Сложность радиотехнических устройств обычно оценивают количеством элементов памяти и количеством сумматоров, так как именно эти элементы влияют на быстродействие устройства и его цену. Заметим, что в передающем устройстве хранится одна порождающая СДР, вместо N^2 СДР эквивалентного класса, как это обычно происходит при традиционных методах передачи информации, поэтому ориентировочно сложность предложенного модулятора в N^2 меньше по количеству элементов в сравнении с модемами, которые построены по традиционным схемам.

В приемной части системы телекоммуникаций (рис. 2) осуществляется обработка принятого в условиях помех $\xi(t)$ сигнала $y(t)$

$$y(t) = S(t) + \xi(t).$$

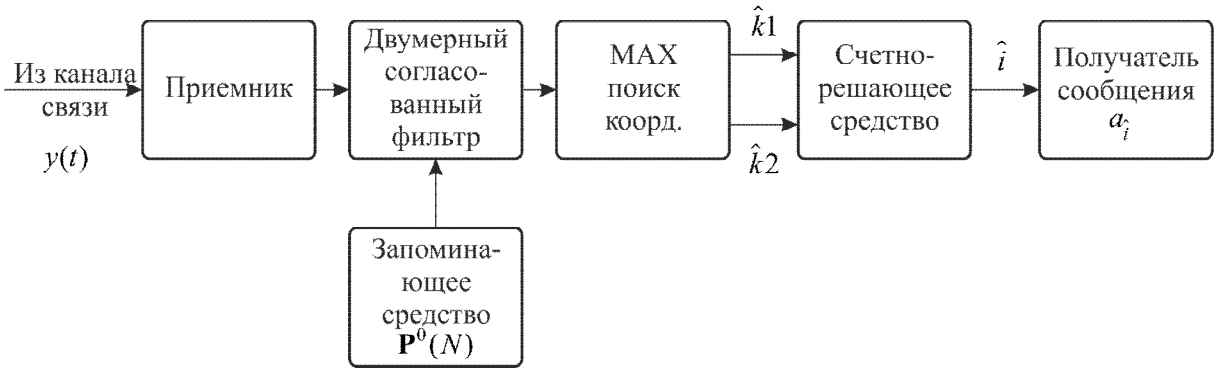

Рис. 2. Демодулятор сигналов на основе СДР

Вначале в приемнике осуществляется поэлементный прием сигнала $y(t)$ и формирование принятой решетки $Y(N)$. В демодуляторе (декодере) с корреляционным методом декодирования с помощью двумерного согласованного фильтра проводится расчет ДПВКФ между принятой решеткой $Y(N)$ и порождающей решеткой $P^0(N)$, параметры последней хранятся в запоминающем средстве. Затем решающее средство декодера осуществляет поиск максимального лепестка ДПВКФ и значений его максимально правдоподобных координат $\left(\hat{k}1, \hat{k}2\right)$.

Декодер источника вычисляет номер максимально правдоподобного передаваемого символа следующим образом

$$\hat{i} = \hat{k}1 \cdot N + \hat{k}2. \qquad (9)$$

Максимально правдоподобный номер $\hat{i}$ определяет переданное сообщение $a_{\hat{i}}$, которое поступает получателю сообщения.

Следует заметить, что декодирование сигналов, построенных на базе эквивалентного $E(N)$-класса СДР мощности N^2, можно осуществить с помощью единственного двумерного согласованного с порождающей СДР фильтра, вместо N^2 фильтров, как это требуется в общем случае при построении многоканального приемника и схемы поиска координат главного пика ДПВКФ.

Общая блок-схема модема на основе СДР показана на рис. 3.

На первый взгляд может показаться, что предложенный модем на базе СДР обеспечивает криптографический метод передачи информации. Ведь ни один бит передаваемого номера символа не связан никакими математическими преобразованиями с передаваемым по каналу связи кодом. Понятно, что если криптоаналитику не известно, какая СДР эквивалентного $E(N)$-класса была установлена в качестве базовой, то в этом случае невозможно определить какие были параметры циклического сдвига строк $(k1)$ и столбцов $(k2)$ и, соответственно, невозможно определить какой номер символа был передан.

Однако вскрытие представленного способа передачи информации, для криптоаналитика, не составляет больших трудностей, так как данный метод передачи информации представляет собой обычный шифр подстановки, т.е. код передаваемого символа заменяется на соответствующую СДР.

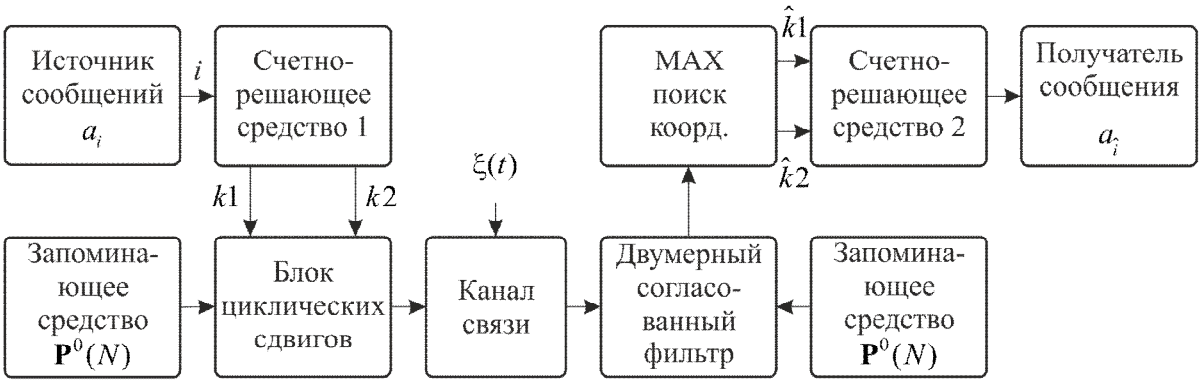

Рис. 3. Блок-схема модема на основе СДР

После приема некоторого кодированного сообщения, нетрудно определить относительную частоту появления различных СДР и поставить эту частоту в соответствие со среднестатистическими данными появления букв алфавита в тексте соответствующего языка.

Зная алгоритм передачи информации, алфавит, формулы для вычисления параметра сдвига строк и столбцов (6), (7), (9), по одному правильно определенному символу легко определить базовую СДР и после этого получить весь открытый текст.

Для того чтобы метод передачи информации не поддавался дешифрованию, необходимо, чтобы для каждого нового передаваемого символа открытого текста использовалась новая порождающая СДР. Это можно осуществить путем добавления в предложенную схему передатчика (рис. 1) и приемника (рис. 2) генератора эквивалентного класса СДР вместо запоминающего средства $P^0(N)$ (рис. 4).

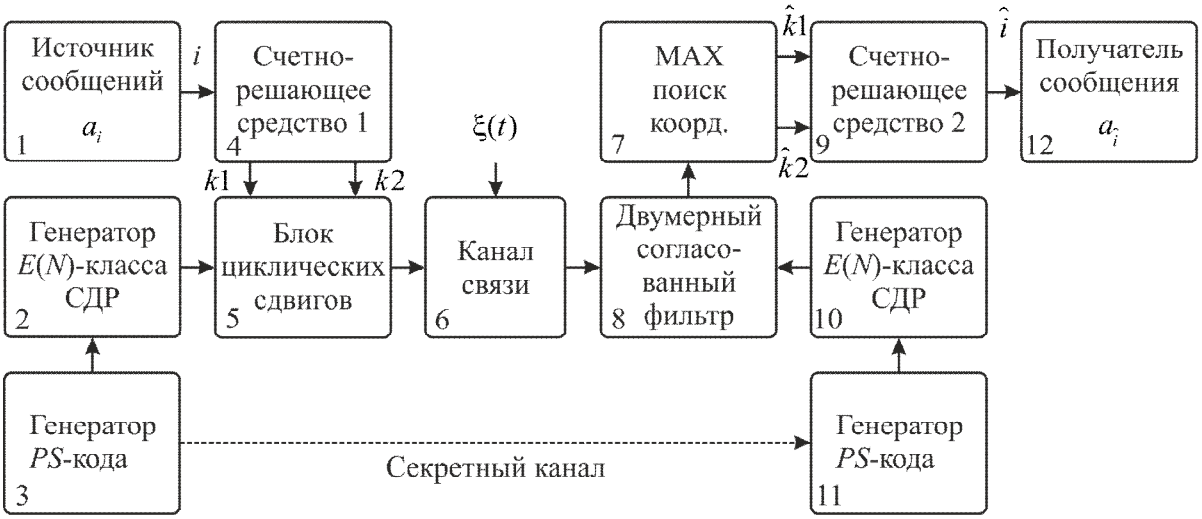

Рис. 4. Блок-схема модема на основе $E(N)$ -класса СДР

Генератор $E(N)$ -класса СДР (блок 2, блок 10), который управляется генератором PS -кода (блок 3, блок 11), для каждого очередного символа открытого сообщения (блок 1) генерирует новую порождающую СДР. Генератор PS -кода (блок 3, блок 11) формирует псевдослучайные числа, последовательность которых управляется закрытым ключом, передающимся на приемную сторону по секретному каналу.

Закрытый ключ изменяет параметры генератора PS-кода. Остальная часть схемы работает так же, как было описано ранее.

Рассмотрим требования к генератору $E(N)$-класса СДР (блок 2 и блок 10). Данный генератор должен генерировать все СДР заданного эквивалентного класса, который определяется порождающей СДР. Структура генерируемой СДР определяется ее номером, который является целочисленным значением и подается на генератор от внешнего устройства в двоичном виде. СДР нумеруются от 0 до $\Psi_{E(N)} - 1$ (1), поэтому количество разрядов двоичного номера генерируемой СДР определяется выражением

$$l_{E(N)} = \log_2 \Psi_{E(N)}. \qquad (10)$$

Генератор PS-кода (блок 3, блок 11) должен формировать псевдослучайную последовательность, каждое значение которой должно иметь количество разрядов, которое определено в (10). Генератор PS-кода должен вырабатывать неповторяющуюся последовательность большой длины. После того, как будет осуществлена передача символов открытого текста (блок 1), количество которых равно длине последовательности, необходимо сформировать новый закрытый ключ, который изменит параметры генераторов PS-кода (блоки 3 и 11).

В связи с тем, что для передачи очередного символа открытого текста каждый раз используется новая порождающая СДР, в канале связи (блок 6) появляются статистически независимые СДР. Криптоаналитик может получить информацию только о том, что по каналу связи передан какой-то символ из заданного алфавита (5). Другая информация ему не доступна.

При достаточной базе (8) шумоподобного сигнала, который сформирован на основе СДР и передается по каналу связи (блок 6), мощность сигнала может быть ниже мощности естественных шумов канала связи. Простым энергетическим приемником в таких условиях невозможно определить даже факт передачи информации. Для перехвата таких сигналов необходимо знать структуру этих сигналов, а она для каждого передаваемого символа открытого текста постоянно изменяется. Кроме того, необходимо обратить внимание на то, что шумоподобные сигналы, которые построены на базе СДР, обладают большой избыточностью.

Каждая СДР может содержать максимум N^2 бит информации, однако фактически переносит только $\log_2 N^2$. Таким образом, относительная скорость r передачи информации рассмотренной схемы составляет

$$r = \frac{\log_2 N^2}{N^2}.$$

Такая избыточность кода позволяет исправлять ошибки, которые могут возникнуть в канале связи при передаче информации.

Рассмотренный метод криптографической передачи информации позволит создать и многоканальную систему передачи информации, если в качестве порождающих использовать минимаксные совершенные двоичные решетки.

Выводы

В работе рассмотрены свойства СДР при выполнении операций циклического сдвига строк и/или столбцов и свойства двумерных периодических взаимнокорреляционных функций между СДР эквивалентного $E(N)$-класса.

На основе рассмотренных свойств СДР обоснован выбор метода информационной модуляции на базе эквивалентного класса СДР. Приведены структурные схемы модулятора и демодулятора сигналов на основе СДР. Показано, что сложность построения модулятора и демодулятора (модема) уменьшена приблизительно в N^2 по сравнению с традиционными схемами.

Предложена модификация указанного модема для осуществления криптографической передачи информации.

Результаты, полученные в данной работе, могут быть использованы при построении многоканального криптографического модема, который может обеспечить параметрическую скрытность передачи информации и исправление ошибок, которые могут возникнуть в канале связи.

Список литературы

1. Варакин, Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. — М.: Радио и связь, 1985. — 384 с.
2. Баранов, П.Е. Класс двумерных корректирующих кодов на основе совершенных двоичных решеток / П.Е. Баранов, М.И. Мазурков, В.Я. Чечельницкий, А.А. Яковенко // Радиоэлектроника (Изв. вузов).— 2009.— Т. 52, № 2.— С. 29–35.
3. Мазурков, М.И. Метод защиты информации на основе совершенных двоичных решеток / М.И. Мазурков, В.Я. Чечельницкий, П. Мурр // Радиоэлектроника (Изв. вузов).— 2008.— Т. 51, № 11.— С. 53–57.
4. Мазурков, М.И. Классы эквивалентных и порождающих совершенных двоичных решеток для CDMA-технологий / М.И. Мазурков, В.Я. Чечельницкий // Радиоэлектроника (Изв. вузов).— 2003.— Т. 46, № 5.— С. 54–63.

МЕТОД КРИПТОГРАФІЧНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ НА БАЗІ ЕКВІВАЛЕНТНОГО КЛАСУ ДОСКОНАЛИХ ДВІЙКОВИХ РЕШІТОК

Н.І. Кушніренко, В.Я. Чечельницький

Одеський національний політехнічний університет,
пр. Шевченка, 1, Одеса, 65044, Україна; e-mail: natalka_kni@ukr.net

На основі властивостей досконалих двійкових решіток еквівалентного класу запропоновано криптографічний метод передачі інформації, який дозволяє зменшити складність декодера за рахунок застосування єдиного узгодженого фільтра, який перебудовується під породжуючу решітку, забезпечити параметричну скритність передачі інформації, завадостійке кодування і організувати багатоканальну систему передачі інформації.

Ключові слова: криптографічна передача інформації, досконалі двійкові решітки, метод модуляції, широкосмугові сигнали

METHOD OF CRYPTOGRAPHIC DATA TRANSFER BASED ON EQUIVALENT CLASS OF PERFECT BINARY LATTICES

N.I. Kushnirenko, V. Ia. Chechelnytskyi

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: natalka_kni@ukr.net

A cryptographic data transfer method was developed based on the features of perfect binary lattices of equivalent class. This method allows for the following: (1) simplification of the decoder structure due to the use of single matched filter redeveloped for generic lattice, (2) parametric data transfer security, (3) robust coding, and (4) organization of multichannel data transfer.

Keywords: cryptographic data transfer, perfect binary lattices, modulation method, broadband signals.