УДК 621.391: 519.27

СИСТЕМА ПЕРЕДАЧИ ИНФОРМАЦИИ СО СЛУЧАЙНЫМ КОДИРОВАНИЕМ, ПОСТРОЕННАЯ НА ОСНОВЕ КОДОВ РИДА-СОЛОМОНА

Антон Алексейчук, Тарас Дроздовский, Юрий Сергиенко
Спецфакультет СБ Украины в составе ВИТИ НТУУ "КПИ"

Аннотация: **Предложены практически реализуемые способы случайного кодирования и декодирования сообщений с использованием кодов Рида-Соломона (РС) в системе передачи информации по каналу связи с отводом. Показано, что случайное кодирование на основе кодов РС обеспечивает (в ряде случаев существенно) более высокую стойкость защиты информации при большей скорости передачи по сравнению с рядом ранее исследованных классов двоичных линейных кодов.**
Summary: **Has been proposed practically implemented methods of random messages coding and decoding with usage of Reed-Solomon codes. Has been shown that the random coding by codes of Reed-Solomon into the system of transmission of information through the channel with a wire-tap channel provides (in some cases essentially) more efficient protection of information using higher speed of transmission in comparison with earlier investigated classes of binary linear codes.**
Ключевые слова: **Канал с отводом, случайное кодирование, код Рида-Соломона.**

I Введение

Классическая модель системы передачи информации по каналу связи с отводом (рис. 1) [1–4] представляет собой два статистически независимых канала с общим входом: основной канал – от источника к законному получателю и отводной – от источника к противнику. Источник вырабатывает случайные равновероятные двоичные векторы S^k длины k. Для защиты передаваемый сообщений в отводном канале применяется случайное кодирование, при котором вектору S^k ставится в соответствие случайный n-мерный двоичный вектор X^n ($n > k$), который при искажении в основном канале преобразуется в вектор $Y^n \in F^{(n)} \stackrel{\text{def}}{=} \{0, 1\}^n$, а в отводном канале – в вектор $Z^n \in F^{(n)}$.

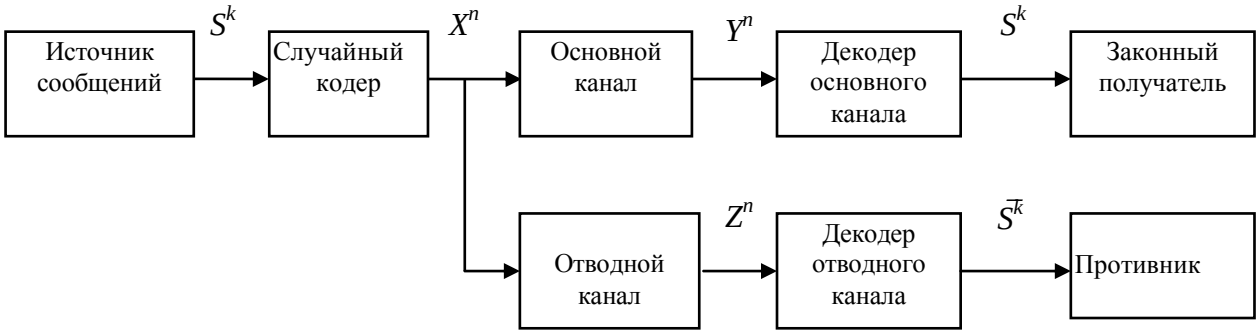

Рисунок 1 – Модель системы передачи информации по каналу связи с отводом

В частном случае, когда основной канал не имеет помех ($Y^n = X^n$), а отводной канал является двоичным симметричным каналом (ДСК) с вероятностью ошибки p ($0 < p < 0{,}5$) в [1] предложен способ, получивший название "случайного кодирования источника линейным кодом" [5, 6]. Согласно этому способу выбирается двоичный линейный код G с параметрами $(n, n–k)$, по которому строится так называемая кодовая книга [5–7], устанавливающая взаимно однозначное соответствие между информационными сообщениями длины k и смежными классами векторного пространства $F^{(n)}$ по коду G. При кодировании по кодовой книге вектор X^n, используемый для передачи информационного сообщения S^k, выбирается случайно и равновероятно в соответствующем S^k смежном классе по коду G. Поскольку основной канал не имеет помех, то законный получатель однозначно восстановит сообщение S^k по смежному классу, содержащему принятый вектор X^n.

Основными параметрами, характеризующими стойкость защиты информации в описанной модели, являются неопределенность $\Delta(G) = k^{-1}H(S^k|Z^n)$ информационного сообщения относительно наблюдения Z^n [1 – 4, 8] и вероятность $P(G) \stackrel{\text{def}}{=} \mathbf{P}\{\delta^*(Z^n) = S^k\}$ правильного декодирования сообщений в отводном канале (с помощью оптимального декодера δ^*: $F^{(n)} \to F^{(k)}$) [7, 9]. Цель случайного кодирования состоит в максимизации

неопределенности $\Delta(G)$ или минимизация вероятности $P(G)$ путем выбора подходящего $(n, n-k)$-кода G при сохранении достаточно высокой скорости k/n передачи информации законному получателю.

Потенциальные возможности и асимптотические свойства теоретико-информационных характеристик эффективности случайного кодирования как способа криптографической защиты информации достаточно подробно исследованы в работах [1, 2, 4, 8] и других авторов. Еще в основополагающей статье [1] установлено существование "асимптотически надежных" систем со случайным кодированием, построенных на основе линейных кодов с параметрами $(n, n-k)$, имеющих при $n \to \infty$ ненулевую скорость передачи k/n и обеспечивающих сколь угодно близкое к 1 значение неопределенности в отводном канале. Вместе с тем, известные доказательства основных результатов [1, 2, 8] являются неконструктивными и не позволяют предложить конкретные способы построения линейных кодов, обладающих перечисленными выше свойствами.

Начало "конструктивному направлению" теории кодовой защиты информации [6], включающему в себя методы построения точных оценок стойкости систем со случайным кодированием и практически реализуемых процедур кодирования-декодирования сообщений, методики оценки и экспериментального подтверждения эффективности кодовой защиты и др., положила известная статья [3], в которой впервые для произвольного линейного кода G получено точное выражение неопределенности $\Delta(G)$ в отводном канале. Так как, согласно [3], для вычисления значений $\Delta(G)$ требуется знание спектров весов всех смежных классов по коду G, то на протяжении длительного времени основным критерием выбора кода для построения системы со случайным кодированием, допускающей теоретическое обоснование стойкости, являлся факт принадлежности данного кода G к совокупности двоичных линейных кодов с известными спектрами смежных классов. В настоящее время существует лишь ограниченное число таких кодов. К ним относятся $(2^r - 1, 2^r - r - 1)$-коды Хэмминга, $r \geq 1$; их расширения; коды Боуза-Чоундхури-Хоквингема (БЧХ) с параметрами $(2^r - 1, 2^r - 2r - 1)$, исправляющие двукратные ошибки; коды Голея (23, 12), (24, 12) и некоторые другие коды [10]. Все они не позволяют в полной мере реализовать на практике известные потенциальные возможности [1, 2, 4, 8] систем передачи информации со случайным кодированием.

II Постановка задачи

В настоящей статье предлагается конструкция двоичных линейных кодов, построенных на основе кодов Рида-Соломона (РС) над полем характеристики 2, обеспечивающих более высокую стойкость защиты информации (по критерию минимума вероятности правильного декодирования сообщений в отводном канале) при большей скорости передачи по сравнению с ранее исследованными классами кодов (Хэмминга, Голея, кодов БЧХ, исправляющих двукратные ошибки, кодов с большим дуальным расстоянием [3, 5–7, 11]). Для предложенных кодов разработаны практически реализуемые алгоритмы случайного кодирования и декодирования сообщений в системе передачи информации по каналу связи с отводом, основанные на вычислении дискретного преобразования Фурье в поле из 2^m элементов.

III Основная часть

Опишем конструкцию двоичных линейных кодов, предлагаемых для применения в системах передачи информации со случайным кодированием.

Пусть R – (N, K, D)-код РС над полем $\mathbf{GF}(q)$, $q = 2^m$, $N = 2^m - 1$, $1 \leq K \leq N - 1$, $L = R^{\perp}$ – код, дуальный к коду R. Известно [10], что L является кодом РС с параметрами $(N, N - K, K + 1)$.

Зафиксируем базис $\alpha = \{\alpha_1, \ldots, \alpha_m\}$ поля $\mathbf{GF}(q)$ над полем $F = \mathbf{GF}(2)$ и обозначим через $\beta = \{\beta_1, \ldots, \beta_m\}$ базис поля $\mathbf{GF}(q)$, дуальный [10] к базису α. Определим отображения f: $\mathbf{GF}(q) \times F \to F^{(m+1)}$, h: $\mathbf{GF}(q) \to F^{(m+1)}$, полагая

$$f(x, \tau) = (x^{(1)} + \tau, \ldots, x^{(m)} + \tau, \tau), \; h(y) = (y^{(1)}, \ldots, y^{(m)}, y^{(m+1)}), \; x, y \in \mathbf{GF}(q), \; \tau \in F, \quad (1)$$

где $(x^{(1)}, \ldots, x^{(m)})$, $(y^{(1)}, \ldots, y^{(m)})$ – векторы координат элементов x и y в базисах α и β соответственно, $y^{(m+1)} = y^{(1)} + \ldots + y^{(m)}$. Рассмотрим двоичные коды

$$G = \{(f(x_0, \tau_0), \ldots, f(x_{N-1}, \tau_{N-1})) : (x_0, \ldots, x_{N-1}) \in L, (\tau_0, \ldots, \tau_{N-1}) \in F^{(N)}\}, \quad (2)$$

$$H = \{(h(y_0), \ldots, h(y_{N-1})) : (y_0, \ldots, y_{N-1}) \in R\}. \quad (3)$$

Непосредственно из (2), (3) следует, что G и H являются линейными кодами с параметрами $(N(m+1), (N-K)m + N)$ и $(N(m+1), Km)$ соответственно.

Утверждение 1. Справедливо равенство

$$H = G^{\perp}. \quad (4)$$

Доказательство. В силу равенства размерностей $\dim_F H = Km = \dim_F G^{\perp}$ для доказательства (4) достаточно убедиться в справедливости соотношения

$$H \subseteq G^{\perp}. \tag{5}$$

Рассмотрим скалярное произведение $\langle f(x, \tau), h(y)\rangle$ над полем F произвольных векторов $f(x, \tau) \overset{\text{def}}{=} (f(x_0, \tau_0), \ldots, f(x_{N-1}, \tau_{N-1}))$ и $h(y) \overset{\text{def}}{=} (h(y_0), \ldots, h(y_{N-1}))$, принадлежащих кодам G и H соответственно. Используя (1), получим

$$\langle f(x, \tau), h(y)\rangle = \sum_{i=0}^{N-1} f(x_i, \tau_i) h(y_i) = \sum_{i=0}^{N-1} \Big(\sum_{j=1}^{m} x_i^{(j)} y_i^{(j)}\Big) = \mathrm{Tr}\Big(\sum_{i=0}^{N-1} x_i y_i\Big) = 0, \tag{6}$$

где $\mathrm{Tr}(a) = \sum_{i=0}^{m-1} a^{2^i}$ – след элемента $a \in \mathbf{GF}(q)$, $(x_i^{(1)}, \ldots, x_i^{(m)})$ и $(y_i^{(1)}, \ldots, y_i^{(m)})$ – векторы координат элементов x_i и y_i в базисах α и β соответственно, $i \in \overline{0, N-1}$. Действительно, так как α и β – взаимно дуальные базисы, то $\mathrm{Tr}(x_i y_i) = \sum_{j=1}^{m} x_i^{(j)} y_i^{(j)}$, $i \in \overline{0, N-1}$ [10], и в силу ортогональности векторов $(x_0, \ldots, x_{N-1}) \in L$ и $(y_0, \ldots, y_{N-1}) \in R$ справедливо равенство (6). На основании (6) имеет место (5), что и требовалось доказать.

Обозначим через w примитивный элемент поля $\mathbf{GF}(q)$ и рассмотрим матрицу A с элементами w^{ij}, $i, j \in \overline{0, N-1}$. Как известно [10, 12], матрица A является обратимой, при этом обратная матрица имеет вид

$$A^{-1} = \left(w^{-ij}\right)_{i, j \in \overline{0, N-1}}. \tag{7}$$

Ниже используется следующий известный результат о строении кодов Рида-Соломона (см., например, [10], стр. 295).

Утверждение 2. Пусть порождающий многочлен кода L равен $g(z) = (z - w)(z - w^2)\ldots(z - w^K)$. Тогда L состоит из всех векторов $x = (x_0, \ldots, x_{N-1})$, удовлетворяющих условиям $x = A^{-1}t$, $t = (t_0, \ldots, t_{N-1}) \in \mathbf{GF}(q)^{(N)}$, $t_1 = \ldots = t_K = 0$.

Следствие. Пусть $t = (t_0, \ldots, t_{N-1})$, $t' = (t_0', \ldots, t_{N-1}') \in \mathbf{GF}(q)^{(N)}$. Тогда векторы $x = A^{-1}t$ и $x' = A^{-1}t'$ принадлежат одному смежному классу пространства $\mathbf{GF}(q)^{(N)}$ по коду L в том и только том случае, когда $t_1 = t_1', \ldots, t_K = t_K'$.

Опишем процедуры случайного кодирования сообщений линейным кодом G вида (2) и декодирования их в основном канале системы передачи информации по каналу связи с отводом.

Пусть $s = (s_1, \ldots, s_K)$ – входной (информационный) вектор длины K над полем $\mathbf{GF}(q)$, $(t_0, t_{K+1}, \ldots, t_{N-1})$ и $\tau = (\tau_0, \ldots, \tau_{N-1})$ – случайные равновероятные векторы, распределенные на множествах $\mathbf{GF}(q)^{(N-K)}$ и $F^{(N)}$ соответственно. Далее будем отождествлять элементы поля $\mathbf{GF}(q)$ с m-векторами их координат в базисе α.

Алгоритм случайного кодирования сообщений кодом G

1. Находим вектор $x = (x_0, \ldots, x_{N-1}) \in \mathbf{GF}(q)^{(N)}$, полагая

$$x^T = A^{-1}(t_0, s_1, \ldots, s_K, t_{K+1}, \ldots, t_{N-1})^T, \tag{8}$$

где матрица A^{-1} определяется по формуле (7).

2. Находим двоичный вектор

$$y = f(x, \tau) \overset{\text{def}}{=} (f(x_0, \tau_0), \ldots, f(x_{N-1}, \tau_{N-1})), \tag{9}$$

где отображение f в правой части (9) определяется по формуле (1), и передаем y по основному каналу связи.

Алгоритм декодирования сообщений в основном канале

1. Разбиваем принятый вектор $y = f(x, \tau)$ на подвекторы длины $m + 1$. С использованием (1) восстанавливаем по y вектор $x = (x_0, \ldots, x_{N-1})$.

2. Находим вектор

$$(t_0, s_1, \ldots, s_K, t_{K+1}, \ldots, t_{N-1})^T = Ax^T \tag{10}$$

(см. (8)), по которому восстанавливаем информационное сообщение $s = (s_1, \ldots, s_K)$.

Покажем, что предложенные алгоритмы являются корректными, то есть реализуют способы случайного кодирования и декодирования сообщений по кодовой книге, соответствующей коду G [1, 5 – 7]. В силу равновероятности случайных векторов $(t_0, t_{K+1}, \ldots, t_{N-1})$ и τ достаточно показать, что для любых $s, s' \in \mathbf{GF}(q)^{(K)}$ двоичные векторы $y = f(x, \tau)$ и $y' = f(x', \tau')$, используемые для передачи сообщений s и s' соответственно, принадлежат одному смежному классу по коду G в том и только том случае, когда выполняется равенство $s = s'$.

Действительно, пусть $x' = (x_0', \ldots, x_{N-1}')$ и y' определяются аналогично x и y в соответствии с равенствами (8), (9). В силу линейности отображения f имеем

$$y + y' = (f(x_0 + x_0', \tau_0 + \tau_0'), \ldots, f(x_{N-1} + x_{N-1}', \tau_{N-1} + \tau_{N-1}')).$$

Отсюда на основании (2) заключаем, что условие $y + y' \in G$ равносильно условию $x + x' \in L$, которое согласно следствию утверждения 2 и равенству (8) выполнятся тогда и только тогда, когда совпадают векторы s и s'. Итак, описанные алгоритмы корректно реализуют процедуры случайного кодирования и декодирования сообщений в смежных классах по коду G.

Отметим, что в силу равенства (1) для нахождения вектора y на шаге 2 алгоритма случайного кодирования (вектора x на шаге 1 алгоритма декодирования) достаточно выполнить Nm сложений в поле F или, что то же самое, N операций сложения элементов поля $\mathbf{GF}(q)$. Следовательно, трудоемкость каждого из предложенных алгоритмов определяется по существу трудоемкостью нахождения векторов в левых частях равенств (8), (10), то есть сложностью вычисления дискретного преобразования Фурье длины $N = q - 1$ в поле из $q = 2^m$ элементов [12]. В настоящее время известны различные "быстрые" алгоритмы решения этой задачи [12, 13], временная сложность лучших из которых (зависящая от арифметических свойств числа N) оценивается величиной порядка Nm операций умножения и сложения в поле $\mathbf{GF}(q)$. Таким образом, предложенные алгоритмы случайного кодирования/декодирования сообщений кодом G вида (2) могут быть практически эффективно реализованы (с использованием как программных, так и аппаратных средств) при подходящих значениях параметра m.

Оценим стойкость защиты информации в системе передачи со случайным кодированием кодом G, принимая в качестве показателя стойкости вероятность $p(G)$ правильного декодирования (оптимальным декодером) сообщения Z_n в отводном канале (см. рис. 1). На основании результатов, полученных в статьях [9, 11], справедливы соотношения

$$p(G) = q^{-K} \sum_{u \in G^{\perp}} \Delta^{\|u\|} \le q^{-K}(1 + (q^K - 1)\Delta^{d'}), \tag{11}$$

где $\Delta = 1 - 2p$, $\|u\|$ – вес Хэмминга вектора $u \in G^{\perp}$, d' – дуальное расстояние кода G. Непосредственно из равенств (3), (4), (11) и оценки $d' \ge 2D = 2(N - K + 1)$ [10] вытекает следующее утверждение, устанавливающее верхнюю границу вероятности $p(G)$.

Утверждение 3. Для вероятности правильного декодирования сообщений в системе передачи информации со случайным кодированием кодом G имеет место неравенство

$$p(G) \le p_{m,K} \stackrel{\text{def}}{=} q^{-K} + \Delta^{2(N - K + 1)}. \tag{11}$$

В частности, при $K = 2^{m-1}$, $m \to \infty$ вероятность $p(G)$ экспоненциально стремится к нулю при скорости передачи $R_G \stackrel{\text{def}}{=} Km \big/ N(m+1) \to 1/2$.

В табл. 1 для различных значений вероятности p искажения в ДСК и $\varepsilon > 0$ представлены результаты сравнительного анализа стойкости защиты информации (по критериям $p(G) < \varepsilon$, $p(H_r) < \varepsilon$) и, соответственно, скорости передачи в системах со случайным кодированием кодом G (при $K = 2^{m-1}$, $m = 3, 4, \ldots$) и двоичным кодом Хэмминга H_r (с параметрами $(2^r - 1, 2^r - r - 1)$, $r = 3, 4, \ldots$). (В таблице приведены минимальные значения m и r, удовлетворяющие условиям $p_{m,K} < \varepsilon$, $p(H_r) < \varepsilon$ соответственно). Для расчета вероятности $p(H_r)$ использовано известное выражение [3]

$$p(H_r) = \frac{1}{2^r}(1 + (2^r - 1)\Delta^{2^{r-1}}), \ \Delta = 1 - 2p;$$

через $R_r = r \big/ (2^r - 1)$ обозначена скорость передачи информации при случайном кодировании кодом H_r.

Таблица 1 – Характеристики эффективности систем со случайным кодированием кодами G и H_r

ε		10^{-4}	10^{-8}	10^{-12}	10^{-15}	10^{-20}
p						
0,01	$p(H_r)$	$6{,}1 \cdot 10^{-5}$	$7{,}5 \cdot 10^{-9}$	$9{,}1 \cdot 10^{-13}$	$8{,}9 \cdot 10^{-16}$	$6{,}8 \cdot 10^{-21}$
	$p_{m,K}$	$3{,}2 \cdot 10^{-5}$	$1{,}0 \cdot 10^{-9}$	$1{,}1 \cdot 10^{-18}$	$1{,}1 \cdot 10^{-18}$	$1{,}2 \cdot 10^{-36}$
	R_r	$8{,}5 \cdot 10^{-4}$	$2{,}0 \cdot 10^{-7}$	$3{,}6 \cdot 10^{-11}$	$4{,}4 \cdot 10^{-14}$	$4{,}5 \cdot 10^{-19}$
	R_G	$4{,}5 \cdot 10^{-1}$	$4{,}6 \cdot 10^{-1}$	$4{,}6 \cdot 10^{-1}$	$4{,}6 \cdot 10^{-1}$	$4{,}6 \cdot 10^{-1}$

Продолжение Таблицы 1

	r	14	27	40	50	67
	m	9	10	11	11	12

0,1	$p(H_r)$	$6{,}1\cdot 10^{-5}$	$7{,}5\cdot 10^{-9}$	$9{,}1\cdot 10^{-13}$	$8{,}9\cdot 10^{-16}$	$6{,}8\cdot 10^{-21}$
	$p_{m,K}$	$6{,}3\cdot 10^{-7}$	$3{,}9\cdot 10^{-13}$	$3{,}9\cdot 10^{-13}$	$1{,}6\cdot 10^{-25}$	$1{,}6\cdot 10^{-25}$
	R_r	$8{,}5\cdot 10^{-4}$	$2{,}0\cdot 10^{-7}$	$3{,}6\cdot 10^{-11}$	$4{,}4\cdot 10^{-14}$	$4{,}5\cdot 10^{-19}$
	R_G	$4{,}4\cdot 10^{-1}$	$4{,}4\cdot 10^{-1}$	$4{,}4\cdot 10^{-1}$	$4{,}5\cdot 10^{-1}$	$4{,}5\cdot 10^{-1}$
	r	14	27	40	50	67
	m	6	6	7	8	8
0,2	$p(H_r)$	$6{,}1\cdot 10^{-5}$	$7{,}5\cdot 10^{-9}$	$9{,}1\cdot 10^{-13}$	$8{,}9\cdot 10^{-16}$	$6{,}8\cdot 10^{-21}$
	$p_{m,K}$	$8{,}0\cdot 10^{-8}$	$6{,}3\cdot 10^{-15}$	$6{,}3\cdot 10^{-15}$	$4{,}0\cdot 10^{-29}$	$4{,}0\cdot 10^{-29}$
	R_r	$8{,}5\cdot 10^{-4}$	$2{,}0\cdot 10^{-7}$	$3{,}6\cdot 10^{-11}$	$4{,}4\cdot 10^{-14}$	$4{,}5\cdot 10^{-19}$
	R_G	$4{,}3\cdot 10^{-1}$	$4{,}4\cdot 10^{-1}$	$4{,}4\cdot 10^{-1}$	$4{,}4\cdot 10^{-1}$	$4{,}4\cdot 10^{-1}$
		14	27	40	50	67
		5	6	6	7	7

Как видно из таблицы, в достаточно больших диапазонах изменения p и ε эффективность (по трем основным показателям: вероятности правильного декодирования в отводном канале, скорости передачи и длине передаваемых сообщений) системы со случайным кодированием кодом G существенно выше по сравнению с эффективностью аналогичной системы, построенной на основе кода Хэмминга. Так, например, при "зашумлении" отводного канала с вероятностью искажения $p = 0{,}1$ кодами Хэмминга минимальная длина кодовых слов, при которой вероятность правильного декодирования $p(H_r)$ меньше значения $\varepsilon = 10^{-8}$, равна $2^{27} - 1$ ($r = 27$). При этом скорость передачи $R_r = 2\cdot 10^{-7}$; $p(H_r) = 7{,}5\cdot 10^{-9}$. В аналогичной ситуации применение кода G длины $7(2^6 - 1) = 441$ ($m = 6$) обеспечивает вероятность правильного декодирования $p(G) < 3{,}9\cdot 10^{-13}$ при скорости передачи $R_G = 0{,}44$. С ухудшением качества отводного канала повышение эффективности (по каждому из трех упомянутых выше показателей) случайного кодирования кодами вида (2) становится еще более значительным. К аналогичным результатам приводит сравнение указанных кодов с другими линейными кодами, имеющими большое дуальное расстояние [11].

В табл. 2 представлены результаты расчетов вероятности правильного декодирования сообщений в системах со случайным кодированием некоторыми кодами БЧХ с известными спектрами весов, кодом Голея и (186, 106)-кодом G ($m = 5$, $K = 16$) соответственно (для вероятности $p(G)$ указаны значения верхней границы (11)).

Таблица 2 – Значения вероятности правильного декодирования в отводном канале

p	0,01	0,1	0,2	
код $(n, n-k)$				$R = k/n$
Голея (24, 12)	$7{,}857\cdot 10^{-1}$	$7{,}977\cdot 10^{-2}$	$4{,}778\cdot 10^{-3}$	0,5
БЧХ (31, 16, 7)	$7{,}323\cdot 10^{-1}$	$3{,}815\cdot 10^{-2}$	$1{,}009\cdot 10^{-3}$	0,49
БЧХ (31, 21, 5)	$7{,}323\cdot 10^{-1}$	$3{,}836\cdot 10^{-2}$	$1{,}787\cdot 10^{-3}$	0,33
БЧХ (31, 26, 3)	$7{,}324\cdot 10^{-1}$	$5{,}852\cdot 10^{-2}$	$3{,}152\cdot 10^{-2}$	0,17
БЧХ (63, 45, 7)	$5{,}309\cdot 10^{-1}$	$1{,}312\cdot 10^{-3}$	$4{,}622\cdot 10^{-6}$	0,29
БЧХ (63, 51, 5)	$5{,}309\cdot 10^{-1}$	$1{,}505\cdot 10^{-3}$	$2{,}446\cdot 10^{-4}$	0,19
БЧХ (63, 57, 3)	$5{,}313\cdot 10^{-1}$	$1{,}644\cdot 10^{-2}$	$1{,}563\cdot 10^{-2}$	0,09
G (186, 106)	$5{,}233\cdot 10^{-1}$	$7{,}922\cdot 10^{-4}$	$7{,}958\cdot 10^{-8}$	0,43

Согласно данным, приведенным в таблице, при относительно плохом качестве отводного канала ($p \geq 0{,}1$) стойкость защиты информации в отводе с использованием кода G оказывается на 1–2 порядка выше по сравнению со стойкостью, обеспечиваемой лучшим из представленных в таблице кодов (БЧХ с параметрами (63, 45, 7)). При этом код G имеет приблизительно в 1,48 раза большую скорость передачи.

IV Выводы

Центральная задача теории кодовой защиты информации состоит в разработке конструктивных методов построения линейных кодов, обеспечивающих требуемую стойкость защиты передаваемых сообщений, имеющих приемлемую скорость передачи и допускающих эффективные (практически реализуемые) процедуры случайного кодирования и декодирования сообщений в основном канале. Традиционный подход к построению систем со случайным кодированием, основанный на применении линейных кодов с известными спектрами весов смежных классов, не позволяет в полной мере реализовать на практике потенциально

достижимые характеристики эффективности случайного кодирования как способа криптографической защиты информации.

В настоящей статье предложена конструкция двоичных линейных кодов, построенных на основе кодов РС над полем **GF**(2^m), обеспечивающих по основным показателям (стойкости защиты информации в отводном канале, скорости передачи, длине кодовых слов) существенно более высокую эффективность случайного кодирования по сравнению с эффективностью систем, построенных на основе кодов Хэмминга и других линейных кодов с большим дуальным расстоянием. Показано также, что при относительно плохом качестве одводного канала ($p \geq 0{,}1$) применение предложенных кодов в системах со случайным кодированием информации обеспечивает меньшую вероятность правильного декодирования в отводе при большей скорости передачи по сравнению с некоторыми другими ранее исследованными кодами.

Разработанные и описанные в статье алгоритмы случайного кодирования и декодирования сообщений с использованием предложенных кодов основываются на дискретном преобразовании Фурье в поле **GF**(2^m), позволяют осуществлять случайное кодирование (декодирование в основном канале) с временной сложностью (измеряемой количеством операций сложения и умножения в поле **GF**(2^m)), пропорциональной длине кодовых слов, и могут быть практически эффективно реализованы в перспективных системах кодовой защиты информации.

Литература: ***1.*** *Wyner A. D. The Wire-Tap Channel // Bell System Techn. J. – 1975. – V. 54. – № 8. – P. 1355–1388.* ***2.*** *Csiszar I., Korner J. Broadcast Channels with Confidential Messages // IEEE Trans. Inform. Theory. – 1978. – V. 24. – № 3. – P. 339–348.* ***3.*** *Коржик В. И., Яковлев В. А. Неасимптотические оценки кодового зашумления одного канала // Проблемы передачи информации. – 1981.– Т.17.– В.4.– С.11-18.* ***4.*** *Maurer U. M. Provable Security in Cryptography: Diss. ETH № 9260. – 1990. – 120 p.* ***5.*** *Коржик В. И., Яковлев В. А. Пропускная способность канала связи с внутренним случайным кодированием // Проблемы передачи информации. – 1992. – Т. 28. – В. 4. – С. 24-34.* ***6.*** *Горицкий В. М. Вероятностная криптография в системах защиты информации: кодовая защита // Электроника и связь. – 1998. – В. 5. – С. 140-145.* ***7.*** *Иванов В. А. О методе случайного кодирования // Дискретная математика. – 1999. – Т. 11. – В. 3. – С. 99–108.* ***8.*** *Чисар И. Почти независимость случайных величин и пропускная способность криптостойкого канала // Проблемы передачи информации. – 1996. – Т. 32. – В. 1. – С. 48–57.* ***9.*** *Алексейчук А. Н. О вероятности безошибочного декодирования в отводном канале с аддитивным шумом, распределенным на конечной абелевой группе // Защита информации: сборник научных трудов Национального авиационного ун-та. – К.: КМУГА, 2001. – С. 9–16.* ***10.*** *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. – М.: Связь, 1979. – 743 с.* ***11.*** *Алексейчук А. Н. Оценки эффективности кодовой защиты дискретных сообщений с использованием линейных кодов с большим дуальным расстоянием // Реєстрація, зберігання і обробка даних. – 2001. – Т. 3 – № 2. – С. 99–106.* ***12.*** *Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов: Пер. с англ. – М.: Мир, 1989. – 448 с.* ***13.*** *Ноден П., Китте К. Алгебраическая алгоритмика: Пер. с франц. – М.: Мир, 1999. – 719 с.*

УДК 681.3.06:519.248.681

ТЕСТИРОВАНИЕ ЧИСЕЛ НА ПРОСТОТУ: ТЕОРИЯ И ПРАКТИКА

Иван Горбенко, Виталий Вервейко
Харьковский национальный университет радиоэлектроники

Анотація: **Наводиться класифікація та огляд основних алгоритмів тестування чисел на простоту, а також їх порівняльний аналіз та рекомендації з побудови практичних засобів.**
Summary: **Classification, review of main primality test algorithms, comparative analysis and recommendation of mean building are given in the article.**
Ключові слова: **Прості числа, тестування чисел на простоту, асиметричні криптосистеми.**

Введение

Задача определения, является ли заданное число простым или составным, есть одной из фундаментальных проблемных задач теории чисел. Поиском решения данной задачи математики занимались много веков, однако до появления криптографии с открытым ключом [1] эффективных алгоритмов проверки чисел на простоту найдено не было.