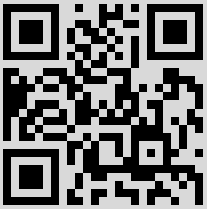

Math-Net.Ru
Общероссийский математический портал

В. А. Иванов, О методе случайного кодирования, *Дискрет. матем.*, 1999, том 11, выпуск 3, 99–108

DOI: http://dx.doi.org/10.4213/dm381

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
http://www.mathnet.ru/rus/agreement

Параметры загрузки:
IP: 89.252.8.95
15 июня 2017 г., 20:57:47



Дискретная математика

том 11 выпуск 3 * 1999

УДК 519.2

О методе случайного кодирования

© 1999 г. В. А. Иванов

Рассматривается система передачи информации с использованием случайного кодирования сообщений для достижения надежной передачи данных по основному каналу и надежной защиты информации в отводном канале. Получены формулы для вычисления различных вероятностных характеристик таких систем в предположении булевой параметризации поступающих на вход системы сообщений и передаваемых в канал связи сигналов.

1. Введение

В статье А. Вайнера [1], опубликованной в 1975 году, были изучены асимптотические свойства системы передачи информации по каналу связи с отводом. Затем В. И. Коржик и В. А. Яковлев в [2, 3] исследовали практические аспекты построения и анализа систем передачи данных при наличии отводного канала утечки информации. В настоящей работе находятся различные вероятностные характеристики таких систем в предположении, что сообщения, поступающие на вход системы, и сигналы, передаваемые в канал связи, представлены в виде векторов, координатами которых являются символы 0 и 1.

Рассмотрим стандартную модель передачи данных по двоичному симметричному каналу. Предположим, что множество

$$A = \{a^1, \dots, a^M\}$$

сообщений, поступающих на вход рассматриваемой системы передачи данных, совпадает с множеством B^m, где $B = (0, 1)$, всех двоичных векторов $a^i = (a^{i1}, \dots, a^{im})$ длины m, $i = 0, 1, \dots, M-1$, $M = 2^m$, а множество

$$X = \{x^1, \dots, x^N\}$$

сигналов, поступающих на вход канала связи, совпадает с множеством B^n всех двоичных векторов $x^j = (x^{j1}, \dots, x^{jn}) \in B^n$ длины n, $n \geqslant m$, $j = 0, 1, \dots, N-1$, $N = 2^n$.

Пусть на поступающий в канал связи в момент t сигнал

$$X = (x_{t1}, \dots, x_{tn}) \in B^n$$

воздействует аддитивная случайная помеха

$$\varkappa_t = (\varkappa_{t1}, \dots, \varkappa_{tn}) \in B^n,$$

не зависящая от каких бы то ни было сигналов и других помех, координаты которой независимы между собой и распределены по закону

$$\mathsf{P}(\varkappa_{tj} = 1) = p_0 = \frac{1-\Delta}{2}, \quad 0 \leqslant \Delta \leqslant 1, \quad j = 1, \ldots, n.$$

Таким образом, на выходе канала с помехами реализуется сигнал

$$x_t \oplus \varkappa_t = (x_{t1} \oplus \varkappa_{t1}, \ldots, x_{tn} \oplus \varkappa_{tn}),$$

по которому требуется восстановить с заданной достоверностью переданное в канал сообщение $a_t \in A$.

Для передачи сообщения $a \in A$ обычно используется сигнал x_a, который определяется с помощью инъективного отображения множества сообщений $A = B^m$ в множество сигналов $X = B^n$. На приемном конце для восстановления переданного в канал связи сообщения используется подходящее сюъективное отображение (декодер), задаваемое псевдобулевой функцией $g(x)\colon B^n \to A$, ставящее в соответствие каждому принятому сигналу x вполне определенное сообщение $a = g(x)$.

Рассмотрим теперь ситуацию, когда сообщения передаются одновременно по двум двоично симметричным каналам, основному и отводному (дополнительному, побочному). Предположим, что основной канал абсолютно надежен (то есть $\Delta = 1$ и, следовательно, $p_0 = 0$), в то время как отводной канал имеет ограниченную надежность ($\Delta \leqslant \Delta_0 < 1$, $(1 - \Delta_0)/2 \leqslant p_0 \leqslant 1/2$). Требуется построить систему передачи данных, которая бы обеспечивала абсолютно надежную передачу информации по основному каналу и достаточно надежную защиту информации в отводном (побочном) канале.

Далее декодер основного канала будем обозначать символом $f(x)$, а декодер отводного канала символом $g(x)$.

Заметим, что для повышения надежности защиты информации в отводном канале можно применять детерминированное кодирование, максимально размножающее канальные ошибки, неоднородное кодирование, при котором для передачи одного и того же символа $a \in A$ в разные моменты времени выбираются различные сигналы, или случайное кодирование, при котором сигнал, используемый для передачи фиксированного символа $a \in A$, выбирается случайно из заданного множества сигналов. Остановимся более подробно на последнем подходе.

2. Метод случайного кодирования

Следуя [1], используем для обеспечения надежной защиты информации в отводном канале метод случайного кодирования сообщений. Рассмотрим произвольную псевдобулеву функцию $f(x)$, задающую сюръективное отображение множества сигналов X на множество сообщений A. Введем обозначение

$$X_a = X_{af} = f^{-1}(a) = \{x\colon f(x) = a\}.$$

Разбиение

$$B^n = \bigcup_a X_a$$

множества всевозможных сигналов B^n на непересекающиеся классы назовем кодовой книгой основного канала, а множества $X_a = X_{af}$ страницами кодовой книги. В

такой интерпретации функция $f(x)$ определяет номер страницы, на которой записан сигнал x. Для того чтобы функция $f(x)$ могла быть использована как декодер основного канала, необходимо и достаточно лишь выполнение условия $f(x_a) = a$ для любого сигнала x_a, $a \in A$. Воспользуемся этим фактом для построения метода случайного кодирования.

Обозначим ξ_a случайный сигнал, равномерно распределенный на странице X_a кодовой книги, определяемой функцией $f(x)$. Ясно, что при таком выборе случайной величины ξ_a, который будем называть равномерным случайным кодированием, при любом $a \in A$ выполняется тождественное соотношение $f(\xi_a) = a$. Поэтому при передаче по основному каналу произвольного сообщения a с помощью случайного сигнала ξ_a на выходе декодера f получим с абсолютной достоверностью переданное сообщение a. Таким образом, псевдобулева функция f однозначно задает метод равномерного случайного кодирования и является декодером основного канала. Очевидно, что функция $f(x)$ будет также наилучшим декодером для отводного канала передачи в области достаточно малых помех. Однако в общем случае при использовании произвольной функции $g(x)$ для декодирования сигналов, поступающих на выход отводного канала, получаем сообщение $\hat{a} = g(\xi_a \oplus \varkappa)$, которое может оказаться более достоверным, чем сообщение $f(\xi_a \oplus \varkappa)$.

Далее будем полагать, что на вход системы передачи данных поступает последовательность назывисимых равномерно распределенных сообщений α_t, а функция $f(x)$, задающая случайное кодирование, является равновероятной функцией (каждый прообраз функции $f(x)$ имеет мощность N/M). Тогда случайная величина $\zeta = \xi_a$ при случайном равновероятном выборе сообщения α имеет равномерное распределение, то есть

$$\mathsf{P}(\zeta = x) = \sum_a \mathsf{P}(\xi_a = x) = \mathsf{P}(\alpha = f(x))\mathsf{P}(\xi_{f(x)} = x) = \frac{1}{N}$$

для всех $x \in X_a$. Поэтому, предполагая, что на вход системы поступает последовательность равновероятных независимых сообщений α_t, $t = 1, 2, \ldots$, на входе канала будем иметь равновероятную последовательность случайных векторов-сигналов X_t, $t = 1, 2, \ldots$

3. Оптимальное декодирование сигналов

Естественно, что при построении системы надежной передачи данных при небольшом уровне канальных помех (при $\Delta \to 1$) функция $g(x)$ должна удовлетворять соотношению $g(x_a) = a$. На остальных векторах $x \neq x_a$, $a \in A$, значения функции могут быть выбраны произвольно. В общем случае, когда интенсивность помех может принимать произвольные значения, никаких предварительных ограничений на функцию $g(x)$ не накладывается.

Надежность передачи данных будем характеризовать вероятностью правильного приема сообщения

$$P_c = \mathsf{P}(f(X) = g(X \oplus \varkappa)). \tag{1}$$

Определение 1. Функцию $g^f(x)$ назовем оптимальным декодером отводного канала в системе передачи информации со случайным кодированием, задаваемой функцией $f(x)$, если для любой псевдобулевой функции $g(x)$, переводящей множество B^n

в множество B^m, выполняется соотношение

$$\mathbf{P}(f(X) = g^f(X \oplus \varkappa)) \geqslant \mathbf{P}(f(X) = g(X \oplus \varkappa)). \tag{2}$$

Лемма 1. *Для того чтобы функция $g(x)$ была оптимальным декодером отводного канала, достаточно, чтобы на любом наборе $s \in B^n$ она принимала значение $g(s) = a \in B^m$, для которого справедливы неравенства*

$$\mathbf{P}(f(s \oplus \varkappa = a) \geqslant \mathbf{P}(f(s \oplus \varkappa = b) \tag{3}$$

при любом $b \in B^m$, $b \neq a$.

Доказательство. Заметим, что в силу равновероятности X для любых псевдобулевых функций f и g справедливо равенство

$$\mathbf{P}(f(X) = g(X \oplus \varkappa)) = \mathbf{P}(f(X \oplus \varkappa) = g(X)).$$

Поэтому в силу неравенств (3) справедливы соотношения

$$\begin{aligned}\mathbf{P}(f(X) = g(X \oplus \varkappa)) &= \sum_s \mathbf{P}(X = s)\mathbf{P}(f(s \oplus \varkappa) = g(s)) \\ &\geqslant \sum_s \mathbf{P}(X = s)\mathbf{P}(f(s \oplus \varkappa) = g'(s)) = \mathbf{P}(f(X) = g'(X \oplus \varkappa))\end{aligned}$$

для любой псевдобулевой функции $g'(x)$, откуда следует (2).

Следует заметить, что вид оптимального декодера зависит от параметра канала связи Δ. Проиллюстрируем это на примере.

Пример 1. Пусть бинарный символ $a \in B$ передается по отводному каналу с помощью случайного кода, задаваемого булевой функцией

$$\begin{aligned}f(x) &= f(x_1, x_2, x_3, x_4) \\ &= x_1x_2(x_3 \oplus x_4 \oplus 1) \oplus x_1x_3(x_4 \oplus 1) \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4.\end{aligned}$$

В [4] показано, что в различных зонах изменения параметра Δ оптимальное декодирование достигается на различных функциях. Так, в области изменения вероятности помехи $0 \leqslant p = p_0 = (1 - \Delta)/2 \leqslant p_1$ наилучшее декодирование достигается на функции $g^f(x) = f(x)$, а в области $p_1 \leqslant p \leqslant p_2$ наилучшее декодирование достигается на функции $g^f(x) = f_1(x)$, в области $p_2 \leqslant p \leqslant 1/2$ наилучшее декодирование достигается на функции $g^f(x) = f_2(x)$, где

$$\begin{aligned}p_1 &\approx 0{,}259, \\ p_2 &\approx 0{,}352, \\ f_1(x) &= f(x)x_1x_2x_3x_4, \\ f_2(x) &= x_2x_3 \oplus x_2x_4 \oplus x_3x_4.\end{aligned}$$

Граничные значения p_1 и p_2 являются корнями кубических уравнений

$$2p^3 - 4p + 1 = 0, \qquad 2p^3 - 4p^2 + 4p + 1 = 0$$

соответственно. Вероятность правильного декодирования в этих областях выражается формулой

$$\mathbf{P}(g^f(x \oplus \varkappa) = f(x)) = d_0 + d_1\Delta + d_2\Delta^2 + d_3\Delta^3 + d_4\Delta^4,$$

где для функции $g^f(x) = \psi(x)$ коэффициенты $d(\psi) = (d_0, d_1, d_2, d_3, d_4)$ принимают следующие значения:

$$\begin{aligned} d(f) &= \frac{1}{16}(8, 3/2, 7/2, 5/2, 1/2), \\ d(f_1) &= \frac{1}{16}(8, 9/4, 9/4, 7/4, 3/4), \\ d(f_2) &= \frac{1}{16}(8, 3, 0, 1, 0). \end{aligned}$$

Разложим вероятность P_c правильного приема сообщения (1) в ряд по параметру Δ:

$$P_c = p^{fg}(\Delta) = \mathbf{P}(f(x) = g(x \oplus \varkappa)) = \sum_{k=0}^{n} d_k(f, g)\Delta^k.$$

Найдем представление для коэффициентов $d_k = d_k(f, g)$ с помощью преобразований Фурье–Адамара подходящих булевых функций. Пусть $f_y(x)$ — булева функция, принимающая значение единица на наборах, на которых псевдобулева функция $f(x)$ принимает значение y, и значение нуль на остальных наборах,

$$\hat{\psi}(u) = \frac{1}{2}\sum_x \psi(x)(-1)^{(u,x)}, \quad u, x \in B^n,$$

— преобразование Фурье–Адамара булевой функции $\psi(x)$.

Теорема 1. *Вероятность правильного приема сообщения на выходе отводного канала с помощью декодера $g(x)$ в системе передачи со случайным кодированием, задаваемым псевдобулевой функцией $f(x)$, может быть представлена в виде*

$$P_c = P^{fg}(\Delta) = \mathbf{P}(f(x) = g(x \oplus \varkappa)) = \sum_{k=0}^{n} d_k(f, g)\Delta^k, \tag{4}$$

где

$$d_k(f, g) = \sum_y \sum_{\|u\|=k} \hat{f}_y(u)\hat{g}_y(u), \qquad \|u\| = u_1 + \ldots + u_n.$$

Доказательство. Справедлива цепочка равенств

$$
\begin{aligned}
P^{fg}(\Delta) &= \mathbf{P}(f(X) = g(X \oplus \varkappa)) = \sum_{y \in A} \mathbf{P}(f(X) = g(X \oplus \varkappa) = y) \\
&= \sum_{y \in A} \mathbf{P}(f(X) = y, g(X \oplus \varkappa) = y) = \sum_{y \in A} \mathbf{P}(f_y(X) = 1, g_y(X \oplus \varkappa) = 1) \\
&= \sum_{y \in A} \mathbf{P}(f_y(X) g_y(X \oplus \varkappa) = 1) = \sum_{y \in A} \mathbf{E} f_y(X) g_y(X \oplus \varkappa) \\
&= \sum_{y \in A} \mathbf{E} \left(\sum_{u \in X} \hat{f}_y(u) (-1)^{(u,X)} \right) \left(\sum_{v \in X} \hat{g}_y(v) (-1)^{(v, X \oplus \varkappa)} \right) \\
&= \sum_{y \in A} \sum_{u \in X} \hat{f}_y(u) \hat{g}_y(u) \mathbf{E} (-1)^{(u,\varkappa)} \\
&= \sum_{y \in A} \sum_{k=0}^{n} \sum_{\|u\|=k} \hat{f}_y(u) \hat{g}_y(u) \Delta^k \\
&= \sum_{k=0}^{n} d_k(f, g) \Delta^k,
\end{aligned}
$$

где $\mathbf{E}$ — символ математического ожидания. Таким образом, с учетом равенства

$$\mathbf{E}(-1)^{(u,\varkappa)} = \Delta^{\|u\|}$$

получаем (4).

4. Оптимизация метода случайного кодирования

С точки зрения обеспечения защиты информации в отводном канале предпочтение следует отдавать методам случайного кодирования, для которых вероятность правильного декодирования переданного сообщения принимает наименьшее значение. С учетом этого введем понятие оптимального случайного кодирования.

Определение 2. Случайное кодирование сообщений, задаваемое функцией $\lambda(x)$, будем называть оптимальным, если для любой псевдобулевой функции f, отображающей множество B^n в множество B^m, выполняется неравенство

$$\mathbf{P}(\lambda(X) = g^{\lambda}(X \oplus \varkappa)) \leqslant \mathbf{P}(f(X) = g^{f}(X \oplus \varkappa)). \tag{5}$$

Исследуем наиболее простой случай $m = 1$, $n \geqslant 2$.

Теорема 2. *Пусть $m = 1$, $n > 1$. Тогда наилучшую защиту информации в отводном канале дает метод случайного кодирования, задаваемый булевой функцией $f(x) = x_1 \oplus \ldots \oplus x_n$. В этом случае вероятность правильного приема равна*

$$\mathbf{P}(f(\xi_a \oplus \varkappa) = a) = \frac{1 + \Delta^n}{2}.$$

Доказательство. Воспользуемся формулой

$$\mathbf{P}(f(X) \neq g(X \oplus \varkappa)) = \hat{f}(0) + \hat{g}(0) - 2\sum_{k=0}^{n} \alpha^{f,g}(k)\Delta^k, \tag{6}$$

где

$$\alpha^{f,g}(k) = \sum_{\|u\|=k} \hat{f}(u)\hat{g}(u), \quad \hat{f}(u) = \frac{1}{N}\sum_{x} f(x)(-1)^{(u,x)}, \quad N = 2^n.$$

Из формулы (6) следует, что разложение (4) по степеням Δ будет иметь максимальный порядок Δ^n для любой функции $g(x)$, если будут выполняться соотношения

$$\alpha^{f,g}(k) = 0, \qquad k = 1, \ldots, n-1.$$

Для этого достаточно потребовать выполнения равенства $\hat{f}(u) = 0$ для всех наборов u веса $k = 1, \ldots, n-1$, или, другими словами, потребовать, чтобы функция $f(x)$ допускала представление

$$f(x) = \hat{f}(0) + (-1)^{\delta(x)}\hat{f}(e),$$

где $e = (1, \ldots, 1)$ — вектор, состоящий из n единиц, $\delta(x) = (e, x) = x_1 \oplus \ldots \oplus x_n$. Такой функцией будет линейная функция $f(x) = x_1 \oplus \ldots \oplus x_n$, либо функция $f(x) = x_1 \oplus \ldots \oplus x_n \oplus 1$. Заметим, наконец, что из соотношения

$$f(x \oplus \varkappa) \oplus g(x) = f(x) \oplus g(x) \oplus \varkappa_1 \oplus \ldots \oplus \varkappa_n$$

следует равенство $g^f(x) = f(x)$. Теорема доказана.

Введем следующую общую характеристику метода случайного кодирования.

Определение 3. Назовем коэффициентом защищенности информации для случайного кодирования с декодером основного канала f и декодером отводного канала g натуральное число $r = r(f, g)$, для которого выполняются соотношения

$$d_k(f, g) = 0, \quad k = 1, \ldots, r-1, \quad d_r(f, g) > 0. \tag{7}$$

Исследуем коэффициент защищенности информации в случае $m > 1$ для некоторых конкретных псевдобулевых функций $f(x)$ для случая $f(x) = g(x)$. Как показали вычисления на ЭВМ, оптимальный декодер для рассмотренных примеров с $m = 4$, $n = 8$ для значений параметра $\Delta = 0{,}2; 0{,}1; 0{,}01$ совпадает с функцией $g^f(x) = f(x)$.

Найдем непосредственным вычислением на ЭВМ по формулам (3) и (4) коэффициенты защищенности информации для некоторых конкретных систем передачи сообщений (полубайтов)

$$a = (a_1, \ldots, a_4) \in B^4$$

с помощью сигналов (байтов)

$$x = (x_1, \ldots, x_8) \in B^8$$

при значениях параметра $\Delta = 0{,}2; 0{,}1; 0{,}01$.

Пример 2. Пусть

$$f^1(x_1,\dots,x_8) = (x_1 \oplus x_5,\dots,x_4 \oplus x_8).$$

Для случайного кодирования сообщения a применим отображение $x = (\xi, a \oplus \xi)$, где искусственный шум $\xi = (\xi_1,\dots,\xi_4) \in B^4$ представляет собой последовательность независимых и равномерно распределенных бинарных случайных векторов. Для указанных значений параметра Δ получаем $g^f = f$, и коэффициенты $d(f^j) = (d_0(f^j),\dots,d_n(f^j))$ в разложении (3) принимают вид $d(f^1) = \frac{1}{16}(1,0,4,0,6,0,4,0,1)$, вероятность правильного приема $P_c = P(\Delta)$ равна

$$P(0{,}2) = 0{,}073116, \quad P(0{,}1) = 0{,}065038, \quad P(0{,}01) = 0{,}062525,$$

и $g^f = f$, $r(f,f) = 2$.

Пример 3. Рассмотрим код Хэмминга $(7,4,3)$ (см. [5]), сопоставляющий двоичным сообщениям $a = (a_1,\dots,a_4)$, занумерованным числами $0,1,\dots,15$, где номер $j(a)$ сообщения a определяется по формуле

$$j(a) = a_1 + 2a_2 + 4a_3 + 8a_4,$$

кодовые слова

$$x^j = (x_1^j,\dots,x_7^j), \qquad j = 0,1,\dots,15,$$

вида

$$\begin{aligned}
x^0 &= 0 \to 0000000, & x^8 &= 67 \to 1000011,\\
x^1 &= 15 \to 0001111, & x^9 &= 76 \to 1001100,\\
x^2 &= 22 \to 0010110, & x^{10} &= 85 \to 1010101,\\
x^3 &= 25 \to 0011001, & x^{11} &= 90 \to 1011010,\\
x^4 &= 37 \to 0100101, & x^{12} &= 102 \to 1100110,\\
x^5 &= 42 \to 0101010, & x^{13} &= 105 \to 1101001,\\
x^6 &= 51 \to 0110011, & x^{14} &= 112 \to 1110000,\\
x^7 &= 60 \to 0111100, & x^{15} &= 127 \to 1111111.
\end{aligned}$$

Построим псевдобулеву функцию $f_H(x) = f_H(x_1,\dots,x_7)$, принимающую значения $y = (y_1,\dots,y_4) \in B^4$ или равносильные им значения $j(y) = 0,1,\dots,15$ на наборах x, для которых выполняется условие $\|x \oplus x^j\| \leqslant 1$, где символом $\|x\|$ обозначается вес Хэмминга $x_1 + \dots + x_7$ вектора x. По функции $f_H(x)$ построим псевдобулеву функцию

$$f^2(x) = f_H(x) \oplus (x_8, x_8, x_8, x_8) = (y \oplus x_8,\dots,y_4 \oplus x_8)$$

от восьми булевых аргументов $x_1,\dots,x_8$. Вероятностные характеристики случайного кода, порождаемого псевдобулевой функцией $f^2(x)$, принимают значения

$$d(f^2) = \frac{1}{16}(1;0;9{,}1875;0;2{,}1875;0;3{,}0625;0;0{,}5625),$$

$$P(0{,}2) = 0{,}085700, \quad P(0{,}1) = 0{,}068256, \quad P(0{,}01) = 0{,}062557,$$

$$g^f = f, \qquad r(f,f) = 2.$$

Пример 4. Пусть

$$f^3(x_1,\dots,x_8)=(x_2\oplus x_3\oplus x_4\oplus x_5, x_3\oplus x_4\oplus x_1\oplus x_6, x_4\oplus x_1\oplus x_2\oplus x_7, x_1\oplus x_2\oplus x_3\oplus x_8).$$

Для случайного кодирования сообщения a можно применить отображение

$$x=(\xi_1,\dots,\xi_4,a_1\oplus\xi_2\oplus\dots\oplus\xi_4,\dots,a_4\oplus\xi_1\oplus\dots\oplus\xi_3),$$

где искусственный шум $\xi=(\xi_1,\dots,\xi_4)\in B^4$ представляет собой последовательность независимых и равномерно распределенных бинарных случайных векторов. При указанных значениях параметра Δ получаем, что $g^f=f$ и

$$d(f^3)=\frac{1}{16}(1,0,0,0,14,0,0,0,1),$$
$$P(0{,}2)=0{,}063900,\quad P(0{,}1)=0{,}062587,\quad P(0{,}01)=0{,}062500,$$
$$g^f=f,\qquad r(f,f)=4.$$

Заметим, что линейные функции, определяющие координаты псевдобулевой функции $f^4(x)=(\psi_1(x),\dots,\psi_4(x))$, представляют собой скалярные произведения

$$\psi_j(x)=(l_j,x),\qquad j=1,2,3,4,$$

векторов l_j базиса кода Хэмминга $(8,4,4)$ (см. [5]) и векторов $x=(x_1,\dots,x_8)$.

5. Системы с линейным декодированием в основном канале

Запишем функцию $f(x)$ в виде

$$f(x)=(\psi_1(x),\dots,\psi_m(x)).$$

Обозначим

$$l_j(x)=(l_j,x)=l_{j1}x_1\oplus\dots\oplus l_{jn}x_n,\quad j=1,\dots,m,$$

скалярное произведение двоичного вектора $l_j=(l_{j1},\dots,l_{jn})$ на двоичный вектор $x=(x_1,\dots,x_n)$, являющееся линейной булевой функцией от n аргументов, $\|x\|=x_1+\dots+x_n$ — вес Хэмминга вектора x,

$$d=d(l_1,\dots,l_m)=\min_{c\neq 0}\|c_1l_1\oplus\dots\oplus c_ml_m\|,$$

где $c=(c_1,\dots,c_m)$ — двоичный вектор длины m.

Теорема 3. *Пусть для декодирования случайного кода по основному и отводному каналам используется линейная функция*

$$f(x)=l(x)=(l_1(x),\dots,l_m(x)).$$

Тогда коэффициент защищенности информации равен $r(f,f)=d(l_1,\dots,l_m)$.

Доказательство. Представим функцию $f_y(x)$ в виде

$$f_y(x) = \frac{1}{2^m} \prod_{j=1}^{m} (1 + (-1)^{y_j \oplus \psi_j(x)}). \tag{8}$$

Полагая в (8) $\psi_j(x) = (l_j, x)$ и перемножая скобки, получим разложение функции $f_y(x)$ в ряд Фурье–Адамара. После перемножения скобок в (8) получим сумму слагаемых вида

$$(-1)^{y_{j(1)} \oplus \ldots \oplus y_{j(k)} \oplus (l_{j(1)}, x) \oplus \ldots \oplus (l_{j(k)}, x)} \tag{9}$$

для всевозможных наборов натуральных чисел

$$j(1), j(2), \ldots, j(k), \quad 1 \leqslant j(1) < j(2) < \ldots < j(k) \leqslant m, \quad k = 0, 1, \ldots, m.$$

Из того, что для любого двоичного вектора $c = (c_1, \ldots, c_m)$ выполняются неравенства

$$\|c_1 l_1 \oplus \ldots \oplus c_m l_m\| \geqslant d,$$

где $d = d(l_1, \ldots, l_m)$, следует справедливость соотношений $\hat{f}_y(u) = 0$ для $\|u\| \leqslant d$ и $\hat{f}_y(u) \neq 0$ для любого набора u веса $\|u\| = d$, вид которого задается вектором c, на котором достигается равенство $\|c_1 l_1 \oplus \ldots \oplus c_m l_m\| = d$. Теорема доказана.

Следствие 1. *Для любого линейного двоичного кода (n, m, d) существует псевдобулева функция $f(x)$, отображающая множество B^n в множество B^m так, что порождаемое ею случайное кодирование имеет коэффициент защищенности информации $r(f, f) = d$.*

Таким образом, для построения метода случайного кодирования сообщений $a \in B^m$ с помощью сигналов $x \in B^n$ с коэффициентом защищенности информации $r(f, f) = d$ достаточно найти код (n, m, d), по векторам его базиса $l_1, \ldots, l_m$ построить псевдобулеву функцию $f(x) = ((l_1, x), \ldots, (l_m, x))$, задающую алгоритм случайного кодирования и проверить оптимальность $g^f = f$ декодирования в отводном канале в заданной зоне изменения параметра Δ.

Список литературы

1. Wyner A., The wire-tap channal. *Bell System Technical J.* (1975) **54**, 1355–1387.
2. Коржик В. И., Яковлев В. А., Пропускная способность канала связи с внутренним случайным кодированием. *Пробл. передачи информации* (1992) **28**, №4, 24–34.
3. Коржик В. И., Яковлев В. А., Защита информации от утечки за счет побочных электромагнитных излучений и наводок на основе способа кодового зашумления. *Информатика и вычислительная техника* (1993) **1–2**, 61–66.
4. Иванов В. А., Автоматные преобразования случайных последовательностей. *Труды по дискретной математике* (1998) **2**, 151–168.
5. Питерсон У., Уэлдон Э., *Коды, исправляющие ошибки.* Мир, Москва, 1976.

Статья поступила 15.09.**1998**.