Math-Net.Ru
All Russian mathematical portal

V. A. Ivanov, Statistical estimation of the code noising efficiency,
Tr. Diskr. Mat., 2002, Volume 6, 48–63

https://www.mathnet.ru/eng/tdm92

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use
https://www.mathnet.ru/eng/agreement

Download details:
IP: 18.97.14.83
December 10, 2025, 10:51:10

Труды по дискретной математике
Том 6, с. 48–63
М.: ФИЗМАТЛИТ, 2002

СТАТИСТИЧЕСКИЕ МЕТОДЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ КОДОВОГО ЗАШУМЛЕНИЯ

В. А. ИВАНОВ

Изучаются вопросы применения случайных кодов для повышения уровня защиты информации от утечки по побочным каналам.

§ 1. ВВЕДЕНИЕ

Для увеличения надежности приема информации, передаваемой по двоичному симметричному каналу с заданным уровнем шума, широко используются методы помехоустойчивого кодирования, позволяющие увеличивать вероятность правильного приема передаваемых сообщений. При этом повышение надежности передачи информации достигается на каналах с тем же уровнем шума за счет уменьшения скорости ее передачи.

Для обеспечения надежной защиты информации от несанкционированного доступа, связанного с возникновением дополнительного (отводного, побочного) физического канала утечки информации (рис. 1), наряду с техническими

Схема одновременной передачи информации по двум каналам

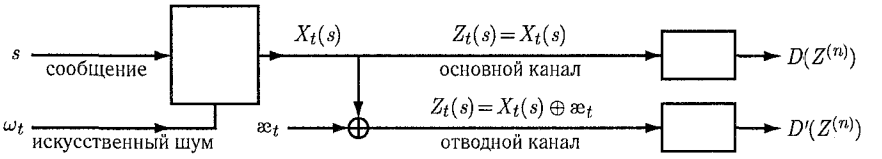

Рис. 1

методами воздействия на этот канал используются алгоритмические методы защиты. Суть этих методов состоит в применении специально подобранных преобразований передаваемой информации, которые гарантируют уменьшение вероятности правильного приема сообщений при оптимальном декоди-

© В. А. Иванов, 2002

ровании сигналов, получаемых из побочного канала. Один из таких методов, состоящий в применении случайного кодирования, получил в отечественной литературе (см. [2]) название метода кодового зашумления. Математическому обоснованию этого направления для двоичных симметричных каналов связи с шумами посвящены работы [1–6] и [8–10]. В частности, в работах [5] и [10] исследовалась эффективность способов кодирования одиночных битов случайными векторами длины $m \geq 1$, в работах [8] и [9] изучалась линейная модель случайного кодирования.

§ 2. МЕТОД СЛУЧАЙНОГО КОДИРОВАНИЯ

Пусть сообщение $s = (s_1, \ldots, s_k) \in \mathbf{Q}^k$, $\mathbf{Q} = \{0, \ldots, q-1\}$, кодируется в случайный вектор $\psi^{(n)}(s, \omega^{(n)}) = (\psi(s, \omega_1), \ldots, \psi(s, \omega_n))$, зависящий от последовательности $\omega^{(n)} = (\omega_1, \ldots, \omega_n)$ независимых случайных векторов $\omega_t = (\omega_{t1}, \ldots, \omega_{tr}) \in \mathbf{Q}^r$, $t = 1, \ldots, n$, каждый из которых распределен по закону $\mathbf{P}(w_t = w) = \rho(w)$, $w = (w_1, \ldots, w_r) \in \mathbf{Q}^r$, при любом значении параметра $t = 1, \ldots, n$. Везде далее под $\psi(s, w)$ будем понимать некоторую подстановку на множестве $\mathbf{Q}^m$ векторов (s, w), $m = k + r$, и считать, что $\rho(w) = q^{-r}$. На выходе побочного канала наблюдается последовательность $Z^{(n)} = Z^{(n)}(s) = (Z_1, \ldots, Z_n) = \psi^{(n)}(s, \omega^{(n)}) \oplus æ^{(n)}$, где $\oplus$ — покомпонентное сложение по модулю q, $Z_t = \psi(s, \omega_t) \oplus æ_t$, $æ^{(n)} = (æ_1, \ldots, æ_n)$ — последовательность независимых случайных векторов $æ_t = (æ_{t1}, \ldots, æ_{tm})$, $j = 1, \ldots, n$, каждый из которых при достаточно малых значениях Δ имеет распределение вероятностей

$$\mathbf{P}(æ_t = z) = q^{-m} \prod_{j=1}^{m} (1 + c(z_j)\Delta), \tag{1}$$

где $z = (z_1, \ldots, z_m) \in \mathbf{Q}^m$, $c(z_j)\colon \mathbf{Q} \to \mathbf{R}$, $\mathbf{R} = \{-\infty, +\infty\}$, $\sum_{j=1}^m c(z_j) = 0$, $\sum_{j=1}^m c^2(z_j) = 1$.

Обозначим через $f(z)\colon \mathbf{Q}^{mn} \to \mathbf{Q}^k$ функцию, с помощью которой производится декодирование наблюдаемых сигналов, так что на приеме получаем сообщение вида $s'(s) = f(Z^{(n)}) = f(\psi^{(n)}(s, \omega^{(n)}) \oplus æ^{(n)})$, $p_{ss} = \mathbf{P}(s'(s) = s)$ — вероятность правильного декодирования фиксированного сообщения $s \in \mathbf{Q}^k$, $P_{\text{пр}} = \sum_s \pi_s p_{ss}$ — вероятность правильного декодирования случайного сообщения S при условии, что сообщение S появляется на входе канала независимо с вероятностями $\mathbf{P}(S = s) = \pi_s$, $s \in \mathbf{Q}^k$.

Будем говорить, что функция $f(z)$ декодирует последовательность сигналов $Z^{(n)}$, получаемую после передачи фиксированного сообщения $s \in \mathbf{Q}^k$, с надежностью $1 - \alpha$, если $p_{ss} \geq 1 - a$, и что функция $f(z)$ декодирует последовательность сигналов $Z^{(n)}$, получаемую после передачи случайного сообщения

$S \in \mathbf{Q}^k$, с надежностью $1-\alpha$, если $P_{\text{пр}} \geq 1-a$. Заметим, что из $p_{ss} \geq 1-\alpha$ для всех $s \in \mathbf{Q}^k$ следует $P_{\text{пр}} \geq 1-\alpha$, однако обратное не верно, поскольку для надежного декодирования последовательности сигналов $Z^{(n)}$, получаемой после передачи случайного сообщения, не следует необходимость надежного декодирования сообщений, достаточно редко появляющихся на входе канала.

Введенная функция $f(z)$ задает критерий различения q^k гипотез, в котором в качестве области принятия гипотезы H_s, соответствующей поступлению на вход канала кодового слова сообщения s, используется множество $\mathbf{Q}^{mn}(s) = f^{-1}(s)$, $\cup_s \mathbf{Q}^{mn}(s) = \mathbf{Q}^{mn}$. При этом вероятность правильного приема сообщения при условии, что было передано сообщение s, равна $p_{ss} = \mathbf{P}(Z^{(n)}(s) \in \mathbf{Q}^{mn}(s))$, а вероятность ошибочного приема сообщения при условии, что было передано сообщение s, называемая вероятностью ошибки s-го рода, равна $\alpha_s = 1 - p_{ss}$. Обозначим еще через $N(\alpha)$ минимальный объем выборки, достаточный для правильной классификации сигналов с надежностью $1-\alpha$ ($\alpha_s \leq \alpha$ для любого $s \in \mathbf{Q}^k$); $N_{sg}(\alpha, \beta)$ — минимальный объем выборки, достаточный для различения гипотез H_s и H_g с вероятностями ошибок s-го и g-го рода, равными α и β соответственно.

Утверждение 1. *Имеет место соотношение $N_{sg}(\alpha, \alpha) \leq N(\alpha)$ для любых s и g, $s \neq g$, из множества $\mathbf{Q}^k$.*

Доказательство. Доказательство следует из того, что разбиение $\cup_s \mathbf{Q}^{mn}(s) = \mathbf{Q}^{mn}$ для критерия различения q^k гипотез с надежностью $1-\alpha$ можно укрупнить до разбиения $\mathbf{Q}^{mn*}(s) \cup \mathbf{Q}^{mn*}(g)$, расширив произвольным образом подмножества $\mathbf{Q}^{mn}(s)$ и $Q^{mn}(g)$. Надежность полученного таким образом критерия различения двух гипотез будет не меньше надежности исходного критерия различения q^k гипотез, откуда следует утверждение 1. Таким образом, величина $\max\{N_{sg}(\alpha, \alpha),\ s,\ g \in \mathbf{Q}^k,\ s \neq g\}$ является оценкой снизу для минимального объема выборки $N(\alpha)$.

§ 3. АСИМПТОТИЧЕСКИЕ ХАРАКТЕРИСТИКИ КРИТЕРИЕВ ПРОВЕРКИ ГИПОТЕЗ

Пусть плотность распределения случайного вектора $Z_t = X_t(s) \oplus æ_t$, $t = 1, \ldots, n$, задана в виде

$$p_{s\Delta}(z) = p(z)(1 + \sum_{j=1}^{m} \Delta^j h_{sj}(z)), \tag{2}$$

где $s \in \mathbf{Q}^k$, $p(z) = q^{-m}$, $X_t(s) = \psi(s, \omega_t)$. Пусть

$$\begin{gathered} d_{sg} = \{d\colon h_{sj}(z) = h_{gj}(z) = h_j(z),\ j = 1, \ldots, d-1,\ h_{sd}(z) \neq h_{gd}(z)\}, \\ b_{sg} = \mathbf{E}(h_{sd}(Z_t) - h_{gd}(Z_t))^2, \end{gathered} \tag{3}$$

где $s, g \in \mathbf{Q}^k$, $z \in \mathbf{Q}^m$, $\mathbf{E}$ — математическое ожидание по равномерному распределению $p(z)$ на множестве $\mathbf{Q}^m$, которое реализуется при нулевом значении параметра Δ. Таким образом, значения коэффициентов при $\Delta, \ldots, \Delta^{d-1}$, где $d = d_{sg}$, не зависят от номера гипотезы. Поэтому плотность распределения вектора Z_t при справедливости гипотез H_s или H_g можно записать в виде

$$p_{v\Delta}(z) = p(z)\Big(1 + \sum_{i=1}^{d-1} \Delta^i h_i(z) + \sum_{j=d}^{m} \Delta^j h_{vj}(z)\Big), \tag{4}$$

$$v \in \mathbf{Q}^k, \quad p(z) = q^{-m}.$$

где $d = d_{sg}$ определено в (3), $v = s$ или $v = g$.

Теорема 1. *Пусть плотность распределения вероятностей случайного вектора $Z_t = X_t(s) \oplus æ_t$, $t = 1, \ldots, n$, при справедливости гипотез H_s или H_g, $s, g \in \mathbf{Q}^k$, имеет вид* (4). *Тогда минимальный объем $N_{sg}(\alpha, \beta)$ выборки, достаточный для различения гипотез H_s и H_g с вероятностями ошибок первого и второго α и β соответственно, асимптотически равен*

$$N_{sg}(\alpha, \beta) \sim \frac{(u_\alpha + u_\beta)^2}{b_{sg}\Delta^{2d}}, \tag{5}$$

где u_γ — верхняя квантиль уровня γ стандартного нормального распределения.

Доказательство. Первые $d - 1$ коэффициентов, $d = d_{sg}$, $z \in \mathbf{Q}^m$, $s, g \in \mathbf{Q}^k$, разложения (2) не зависят от индексов s и g гипотез H_s и H_g, $s, g \in \mathbf{Q}^k$. В силу $h_{sd}(z) \neq h_{gd}(z)$ и равновероятности меры, по которой проводится усреднение $\mathbf{E}$, выполняется неравенство $\mathbf{E}(h_{sd}(Z_t) - h_{gd}(Z_t))^2 = b_{sg} = b > 0$. Пусть

$$Q_{1d}(z) = \Delta^{-1} \sum_{i=1}^{d-1} \Delta^i h_i(z), \quad Q_{2ds}(z) = \Delta^{-d} \sum_{j=d}^{m} \Delta^j h_{sj}(z), \quad s \in \mathbf{Q}^k. \tag{6}$$

Тогда с учетом (6) плотность распределения вероятностей можно записать в виде $p_{s\Delta}(z) = p(z)(1 + \Delta Q_{1d}(z) + \Delta^d Q_{2ds}(z))$.

По предположению случайные величины $Z_1, \ldots, Z_n$ независимы. Поэтому логарифм отношения правдоподобия (ЛОП) представляется в виде суммы независимых одинаково распределенных случайных величин $L_n(Z^{(n)}) \times \sum_t l_{sgt}(Z_t)$, где

$$l_{sgt}(z) = l_{st}(z) - l_{gt}(z), \quad l_{st}(z) = \ln(p_{s\Delta}(z)/p(z)).$$

Отсюда следует, что для нахождения математического ожидания $\mathbf{E}$ и дисперсии $\mathbf{D}$ статистики ЛОП $L_n(Z^{(n)})$ достаточно получить математическое ожидание и дисперсию одного слагаемого $l_{sgt}(Z_t)$.

Заметим, что разложение функции $l_{xt}(z)$, $x \in \mathbf{B}^k$, по малому параметру Δ имеет вид $l_{st}(z) = \sum_{k=1}^{\infty}(-1)^{k+1}k^{-1}(\Delta Q_{1d}(z) + \Delta^d Q_{2ds}(z))^k$.

Поэтому

$$\mathbf{E}_s\, L_n(Z^{(n)}) - \mathbf{E}_g\, L_n(Z^{(n)}) = \sum\nolimits_t (\mathbf{E}_s\, l_{sgt}(Z_t) - \mathbf{E}_g\, l_{sgt}(Z_t)) =$$

$$= n\,\mathbf{E}\, l_{sgt}(Z_t)\Delta^d(Q_{2ds}(Z_t) - Q_{2dg}(Z_t)) =$$

$$= n\Delta^d\,\mathbf{E}(l_{st}(Z_t) - l_{gt}(Z_t))(Q_{2ds}(Z_t) - Q_{2dg}(Z_t)) =$$

$$= n\Delta^d\,\mathbf{E}(l_{st}(Z_t) - l_{gt}(Z_t))[(h_{sj}(Z_t) - h_{gj}(Z_t)) + O(\Delta)].$$

Функцию $l_{sgt}(z) = l_{st}(z) - l_{gt}(z)$ можно представить в виде $l_{sgt}(z) = \Delta^d(h_{sd}(z) - h_{gd}(z)) + O(\Delta^{d+1})$ и $\mathbf{E}_s\, L_n(Z^{(n)}) - \mathbf{E}_g\, L_n(Z^{(n)}) = n\Delta^{2d}\times \mathbf{E}(h_{sd}(Z_t) - h_{gd}(Z_t))^2 + O(\Delta^{2d+1}) = n\Delta^{2d}b_{sg}(1 + O(\Delta))$.

Для вычисления дисперсии для $x \in \mathbf{B}^m$ заметим, что

$$\mathbf{D}_x\, L_n(Z^{(n)}) = n\,\mathbf{D}_x\, l_{sgt}(Z_t) = n\,\mathbf{E}_x(l_{sgt}(Z_t))^2 - n(\mathbf{E}_x\, l_{sgt}(Z_t))^2 =$$

$$= n\,\mathbf{E}(l_{sgt}(Z_t))^2(1 + \Delta Q_{1d}(Z_t) + \Delta^d Q_{2dx}(Z_t)) + O(\Delta) =$$

$$= n\Delta^{2d}\,\mathbf{E}(h_{sd}(z) - h_{gd}(z) + O(\Delta))^2(1 + O(\Delta)) = n\Delta^{2d}b_{sg}(1 + O(\Delta)).$$

Следовательно, при $\Delta \to 0$ выполняются асимптотические соотношения

$$\mathbf{E}_s\, L_n(Z^{(n)}) - \mathbf{E}_g\, L_n(Z^{(n)}) = n\Delta^{2d}b_{sg}(1 + O(\Delta),$$

$$\mathbf{D}\, L_n(Z^{(n)}) = n\Delta^{2d}b_{sg}(1 + O(\Delta)),$$

откуда стандартным способом (см., например, [4]), принимая во внимание асимптотическую нормальность статистики ЛОП, получается формула (5).

При доказательстве теоремы в разложениях со случайными аргументами существенно используется тот факт, что коэффициенты разложения (2) равномерно ограничены по абсолютной величине некоторой константой $|c_{uj}(z)| \leq C = \text{const}$, что следует из конечности множеств, из которых выбирается значения u, j, z.

Выражение (5) можно использовать в качестве оценки снизу минимального объема $N(\alpha)$ выборки, достаточного для правильной классификации сигналов с надежностью $1 - \alpha$. Действительно, обозначая $d^* = \max_{sg} d_{sg} = d_{s*g*}$, $b^* = b_{s*g*}$, если максимум достигается на сообщениях s^* и g^*, получаем асимптотическую оценку

$$N(\alpha) \geq N^*(\alpha) \sim \frac{4u_\alpha^2}{b^*\Delta^{2d*}}.$$

§ 4. ОЦЕНКИ НАДЕЖНОСТИ ОПТИМАЛЬНОГО ДЕКОДИРОВАНИЯ

Исследуем разложение плотности распределения вероятностей случайного вектора $Z_t = \psi(s, \omega_t) \oplus æ_t$, $t = 1, \ldots, n$, по малому параметру Δ при фиксированной гипотезе H_s, $s \in \mathbf{Q}^k$. Случайный вектор Z_t принимает значения $z = (z_1, \ldots, z_m)$ из множества $\mathbf{Q}^m$. Обозначим через $C^l(z)$ выражение

$$C^l(z) = \prod_{j=1}^{m} [c(z_j)]^{l_j},$$

где $C(z) = (C_1, \ldots, C_m) = (c(z_1), \ldots, c(z_m))$ — вектор с координатами $C_j = c(z_j)$, $c(z_j)$ — функция, принимающая действительные значения на элементах множества $\mathbf{Q}$, $l = (l_1, \ldots, l_m) \in \mathbf{B}^m$ — двоичный вектор.

Утверждение 2. *Плотность распределения случайного вектора $Z_t = \psi(s, \omega_t) \oplus æ_t$, $t = 1, \ldots, n$, при фиксированной гипотезе H_s, $s \in \mathbf{Q}^k$, может быть представлена в виде*

$$p_s(z) = p(z)\Big(1 + \sum_{j=1}^{m} \Delta^j h_{sj}(z)\Big), \tag{7}$$

где

$$p(z) = q^{-m}, \quad h_{sj}(z) = \operatorname{coef}_{\Delta^j} \mathbf{E} \prod_{i=1}^{m} (1 + c(\psi_i(s, \omega_t) \oplus z_i)\Delta) =$$

$$= \sum_{\|l\|=j} \mathbf{E}\, C^l(\psi, (s, \omega_t) \oplus z) =$$

$$= \sum_{\|l\|=j} \mathbf{E}[c^{l_1}(\psi_1(s, \omega_t) \oplus z_1) \ldots c^{l_m}(\psi_m(s, \omega_t) \oplus z_m)]. \tag{8}$$

Доказательство. Усреднение по случайному параметру ω_t с учетом формул $\mathbf{P}(æ_{tj} = z_j) = p(z_j)(1 + c(z_j)\Delta)$ приводит к следующим соотношениям:

$$p_s(z) = \mathbf{E}\mathbf{P}(æ_t = \psi(s, \omega_t) \oplus z | \omega_t) =$$

$$= p(z)\, \mathbf{E} \prod_{j=1}^{m} (1 + c(\psi_j(s, \omega_t) \oplus z_j)\Delta) =$$

$$= p(z)\Big(1 + \sum_{j=1}^{m} \Delta^j \sum_{\|l\|=j} [c(\psi(s, \omega_t) \oplus z_j)]^l\Big),$$

откуда следует (7). Для $j = 1, 2$ получаем

$$h_{s1}(z) = \sum_{j=1}^{m} \mathbf{E}\, c(\psi_j(s, \omega_t) \oplus z_j),$$

$$h_{s2}(z) = \sum_{i,j=1, i\neq j}^{m} \mathbf{E}\, c(\psi_i(s, \omega_t) \oplus z_i) c(\psi_j(s, \omega_t) \oplus z_j).$$

Из формулы (8) вытекает, что $h_{sj}(z) = h_{gj}(z)$ тогда и только тогда, когда

$$\sum_{\|l\|=j} \mathbf{E}\, C^l(\psi(s, \omega_t) \oplus z) = \sum_{\|l\|=j} \mathbf{E}\, C^l(\psi(g, \omega_t) \oplus z). \tag{9}$$

В важном для приложений случае $q = 2$ формула (9) упрощается. Рассмотрим неоднородный двоичный симметричный канал связи, в котором различные координаты кодового вектора передаются с разными вероятностями ошибок. Пусть вероятность ошибки в j-й координате кодового вектора равна

$$\mathbf{P}(æ_{tj} = 1) = (1 - a_j\Delta)/2, \quad \Delta \to 0, \quad 0 < a_j < \infty,$$
$$j = 1, \ldots, m, \quad a = (a_1, \ldots, a_m).$$

Утверждение 3. *Пусть $q = 2$ и случайные кодовые слова $\psi(s, \omega)$ передаются по неоднородному двоичному симметричному каналу связи с параметрами $a_1, \ldots, a_m$. Тогда равенства $h_{sj}(z) = h_{gj}(z)$, $j = 1, \ldots, d$, $s, g \in \mathbf{B}^k$, $s \neq g$, выполняются тогда и только тогда, когда справедливы соотношения $a^l\, \mathbf{E}[(l, \psi(s, \omega)) - (l, \psi(g, \omega))] = 0$ для всех $l = (l_1, \ldots, l_m)$ веса $\|l\| \leq d$.*

Доказательство. Необходимым и достаточным условием выполнения соотношения $h_{sj}(z) = h_{gj}(z)$ является равенство (9), которое с учетом выражения $c(z_j) = (-1)^{z_j} a_j$ принимает вид

$$\sum_{\|l\|=j} (-1)^{(l,z)} a^l\, \mathbf{E}[(-1)^{(l,\psi(s,\omega_t))} - (-1)^{(l,\psi(g,\omega))}] =$$
$$= 2 \sum_{\|l\|=j} (-1)^{(l,z)} a^l\, \mathbf{E}[(l, \psi(g, w)) - (l, \psi(s, \omega))] = 0. \tag{10}$$

Здесь под скалярным произведением понимается сумма произведений координат $(l, \psi) = l_1\psi_1 \oplus \ldots \oplus l_m\psi_m$ по модулю два, $a^l = a_1^{l_1} \ldots a_m^{l_m}$. Принимая во внимание (10) и тот факт, что 2^m функций

$$\varphi(l, z) = \varphi_1(z) = (-1)^{(l,z)}, \quad l \in \mathbf{B}^m,$$

образуют базис в пространстве действительных функций, заданных на множестве аргументов $z \in \mathbf{B}^m$, убеждаемся в справедливости утверждения 3.

Заметим, что достаточным условием для выполнения равенств $h_{sj}(z) = h_{gj}(z)$, $s \neq g$, $s, g \in \mathbf{B}^k$, $j = 1, \ldots, d$, является справедливость соотношений $\mathbf{E}(-1)^{(l,\psi_s(\omega))} = 0$ или $\mathbf{P}((l, \psi_s(\omega)) = 0) = 1/2$.

Определение 1. Под уровнем защиты случайного кодирования $\psi(s, \omega)$ будем понимать число $d(\psi) = \max\limits_{s \neq g} d_{sg}$.

Утверждение 4. *Уровень защиты $d(\psi)$ случайного кодирования $\psi(s, \omega)$ равен d тогда и только тогда, когда минимальный объем $N(\alpha)$ выборки, достаточный для различения 2^k гипотез H_s, $s \in \mathbf{B}^k$, с надежностью $1 - \alpha$ при $\Delta \to 0$ имеет порядок $N(\alpha) \asymp \Delta^{-2d}$, где символ $\asymp$ обозначает эквивалентность с точностью до мультипликативной константы.*

Доказательство. С одной стороны, значение $N(\alpha)$ ограничено снизу величиной $N_{sg}(\alpha, \beta)$. Поэтому справедливы соотношения $N(\alpha) \geq \max\limits_{s \neq q} N_{sg}(\alpha, \alpha) \asymp \Delta^{-2d(\psi)}$. С другой стороны, если $\max_{s \neq g} N_{sg}(\alpha, \alpha) \asymp \Delta^{-2d(\psi)}$, то, проводя последовательное различение гипотез H_s и H_g, $s \neq g$, можно за конечное число M шагов определить с заданной достоверностью правильную гипотезу по выборке, объем которой не превосходит $M \max N_{sg}(\alpha, \alpha) \asymp \Delta^{-2d(\psi)}$.

Сопоставим случайному вектору $X = (X_1, \ldots, X_m) \in \mathbf{B}^m$ и детерминированному вектору $l = (l_1, \ldots, l_m) \in \mathbf{B}^m$ веса $\|X\| = \nu$ случайный вектор $X_{\langle l \rangle} = (X_{j(1)}, \ldots, X_{j(\nu)}) \in \mathbf{B}^\nu$, где $1 \leq j(1) < j(2) < \ldots < j(\nu - 1) < j(\nu) \leq m$ — номера единичных координат вектора l.

Введем по аналогии с [13] понятия ν-равновероятного, (ν, μ)-равновероятного и строго ν-равновероятного случайного вектора $X = (X_1, \ldots, X_m) \in \mathbf{B}^m$.

Определение 2. Случайный вектор $X = (X_1, \ldots, X_m) \in \mathbf{B}^m$ называется ν-равновероятным, если любой его подвектор $X_{\langle l \rangle}$, для которого $\|l\| = \nu$, имеет равновероятное распределение, (ν, μ)-равновероятным, если он ν-равновероятен и существует подвектор $X_{\langle l \rangle}$ с $\|l\| = \mu$, распределение которого не является равновероятным, и, наконец, строго ν-равновероятным, если он $(\nu, \nu + 1)$-равновероятен. Уровнем равновероятности $\nu(X)$ случайного вектора $X = (X_1, \ldots, X_m) \in \mathbf{B}^m$ будем называть целое число ν, для которого вектор X является $(\nu, \nu + 1)$-равновероятным.

Заметим, что некоторые алгоритмы построения таких случайных векторов упоминаются в работе [13].

Для примера укажем, что уровень равновероятности вектора $X = (X_1, X_2)$ с распределением $p(x) = p(x_1, x_2)$, где $p(0, 0) = p(1, 1) = 1/4 + \alpha$, $p(0, 1) = p(1, 0) = 1/4 - \alpha$, равен $\nu(X) = 2$ при $\alpha = 0$ и равен $\nu(X) = 1$ при $a \neq 0$, что следует из равенств $\mathbf{P}(X_1 = 0) = p(0, 0) + p(0, 1) = 1/2$, $\mathbf{P}(X_2 = 0) = p(0, 0) + p(1, 0) = 1/2$, $p(0, 0) \neq 1/4$.

Утверждение 5. *Случайный вектор $X = (X_1, \ldots, X_m) \in \mathbf{B}^m$ ν-равновероятен тогда и только тогда, когда для всех векторов $l \in \mathbf{B}^m$, $l \neq 0$, $\|l\| \leq \nu$, случайные величины $(l, X) = l_1 X_1 \oplus \ldots \oplus l_m X_m$ равновероятны.*

Доказательство. Пусть $\mathbf{P}(X = x) = 2^{-m}$, где $x = (x_1, \ldots, x_m) \in \mathbf{B}^m$. Тогда при $l \neq 0$ и $\sigma \in \mathbf{B}$ получаем $\mathbf{P}((l, X) = \sigma) = \Sigma^* \mathbf{P}(X_1 = x_1, \ldots, X_m = x_m)$, где Σ^* обозначает суммирование по векторам x, удовлетворяющим условию $l_1 x_1 \oplus \ldots \oplus l_m x_m = \sigma$. Отсюда $\mathbf{P}((l, X) = \sigma) = 1/2$, так как число наборов x, для которых $(l, x) = \sigma$, равно 2^{m-1}.

Пусть теперь $\mathbf{P}((l, X) = \sigma) = 1/2$ для любого $l \neq 0$. Для $m = 1$ из $\mathbf{P}((l, X) = \sigma) = 1/2$ следует $\mathbf{P}(X = \sigma) = 1/2$. Предположим теперь, что утверждение 5 справедливо для случайных векторов с m координатами. Покажем, что тогда утверждение будет справедливо и для случайных векторов с $m + 1$ координатами. Действительно, обозначая $p_m(\sigma_1, \ldots, \sigma_m) = \mathbf{P}(X_1 = \sigma_1, \ldots, X_m = \sigma_m)$, получаем $p_m(0, \sigma_2, \ldots, \sigma_m) + p_m(1, \sigma_2, \ldots, \sigma_m) = p_{m-1}(\sigma_2, \ldots, \sigma_m)$, откуда следует, что все векторы с четным или нечетным числом единиц имеют одинаковые вероятности. Принимая во внимание, что множества таких векторов имеют мощности 2^{m-1}, а суммарные вероятности их равны по 1/2, поскольку они равны $\mathbf{P}(X_1 \oplus \ldots \oplus X_m = 0) = 1/2$ или $\mathbf{P}(X_1 \oplus \ldots \oplus X_m = 1) = 1/2$, убеждаемся в справедливости утверждения 5.

Следствие. *Уровень равновероятности $\nu(X)$ случайного вектора $X = (X_1, \ldots, X_m) \in \mathbf{B}^m$ равен ν тогда и только тогда, когда для любого вектора $l \in \mathbf{B}^m$, $l \neq 0$, $\|l\| \leq \nu$, случайные величины $(l, X) = l_1 X_1 \oplus \ldots \oplus l_m X_m$ равновероятны и существует вектор $l \in \mathbf{B}^m$ веса $\|l\| = \nu + 1$, для которого случайная величина (l, X) не является равновероятной.*

Теорема 2. *Для того, чтобы уровень защиты $d(\psi)$ случайного кодирования $\psi(s, w) = (\psi_1(s, \omega), \ldots, \psi_m(s, \omega))$ удовлетворял соотношению $d(\psi) \geq d$, достаточно, чтобы уровень равновероятности $\nu(\psi)$ случайного вектора $\psi(s, \omega)$ удовлетворял условию $\nu(\psi(s, \omega)) \geq d - 1$.*

Доказательство следует непосредственно из утверждений 3 и 5.

§ 5. ЛИНЕЙНАЯ МОДЕЛЬ СЛУЧАЙНОГО КОДИРОВАНИЯ

Рассмотрим случай аддитивного наложения искусственной помехи $\psi(s, \omega) = a(s) \oplus \chi(\omega)$, где $a(s)$ — отображение из $\mathbf{B}^k$ в $\mathbf{B}^m$, $\chi(\omega)$ — случайное отображение из $\mathbf{B}^r$ в $\mathbf{B}^m$ и отображение $\psi(s, \omega)$ из $\mathbf{B}^m$ в $\mathbf{B}^m$ обратимо по s.

Утверждение 6. *Пусть случайное кодирование задается с помощью обратимого отображения $\psi(s, \omega) = a(s) \oplus \chi(\omega)$, где $s \in \mathbf{B}^k$, $\omega \in \mathbf{B}^r$, $a(s) \in \mathbf{B}^m$, $\chi(\omega) \in \mathbf{B}^m$, $k + r = m$. Тогда уровень защиты $d(\psi) \geq d$ в том и только том случае, когда выполняется равенство*

$$\left[(l, a(s)) - (l, a(g))\right] \mathbf{E}(-1)^{(l, \chi(\omega_t))} = 0,$$

для всех векторов $l \in \mathbf{B}^m$ веса $\|l\| \leq d - 1$. Выполнение равенства $\mathbf{E}(-1)^{(l, \chi(\omega_t))} = 0$ для всех векторов $l \in \mathbf{B}^m$ веса $\|l\| \leq d - 1$ обеспечивает уровень защиты по меньшей мере $d(\psi) = d$.

Доказательство. Для выполнения соотношения $d(\psi) = d$ в соответствии с утверждением 3 необходимо и достаточно выполнение равенств $\mathbf{E}(l, \psi(s,\omega)) = \mathbf{E}(l, \psi(g,\omega))$ для всех $l = (l_1, \ldots, l_m)$ веса $\|l\| \leq d-1$, что эквивалентно утверждению 6.

Как следует из утверждения 6, уровень защиты введенного выше случайного кодирования $\psi(s,\omega)$ удовлетворяет соотношению $d(\psi) \geq d$, если для вектора искусственной помехи $\chi(\omega)$ выполняется соотношение $\nu(\chi) \geq d - 1$. В более простом случае $\psi(s,\omega) = (s \oplus \Psi(\omega), \omega)$, когда $a(s) = (s, 0) \in \mathbf{B}^m$, $\chi(\omega) = (\Psi(\omega), \omega)$, где $\Psi(\omega)$ — произвольное отображение из $\mathbf{B}^r$ в $\mathbf{B}^k$, условие $[(l, a(s)) - (l, a(g))]\,\mathbf{E}(-1)^{(l,\chi(\omega_t))} = 0$ переходит в условие $[(l', s) - (l', g)]A_l = 0$, где $A_l = \mathbf{E}(-1)^{(l',\Psi(\omega))\oplus(l'',\omega)}$, $l = (l', l'')$, $l' \in \mathbf{B}^k$, $l'' \in \mathbf{B}^r$, для всех $l \in \mathbf{B}^m$ веса $\|l\| \leq d-1$. Таким образом, условие $\mathbf{P}((l', \Psi(\omega)) = (l'', \omega)) = \mathbf{P}((l, \chi(\omega) = 0) = 1/2$, эквивалентное условию $A_l = 0$, является достаточным для того, чтобы обеспечить уровень защиты информации $d(\psi) \geq d$.

Определение 3. Равновероятная функция $\Psi(\omega) = (\Psi_1(\omega), \ldots, \Psi_k(\omega))$, отображающая множество $\mathbf{B}^r$ в множество $\mathbf{B}^k$, называется τ-устойчивой, если любая функция от $r - \tau$ переменных, полученная из $\Psi(\omega)$ путем фиксации любых τ входных переменных, сохраняет свойство равновероятности.

Из определения 3 следует, что нельзя нарушить независимость и равномерную распределенность выходных случайных величин $\Psi_1(\omega), \ldots, \Psi_k(\omega)$ любой τ-устойчивой функции $\Psi(\omega) = (\Psi_1(\omega), \ldots, \Psi_k(\omega))$ путем замены не более τ входных переменных константами. Очевидно, что $\tau \leq r - k$.

Максимальное значение τ, при котором функция $\Psi(\omega)$ остается τ-устойчивой, будем обозначать $\tau(\Psi(\omega))$.

Утверждение 7. *Пусть* $\Psi(\omega)\colon \mathbf{B}^r \to \mathbf{B}^k$ *есть* τ*-устойчивая функция,* $\tau \leq r - k$, $k \geq 1$. *Тогда случайный вектор* $\chi(\omega) = (\Psi(\omega), \omega) \in \boldsymbol{B}^m$, $m = k + r$, *является* $\tau + 1$*-равновероятным.*

Доказательство. Пусть вектор $l = (l', l'') \in \mathbf{B}^m$, где $l' \in \mathbf{B}^k$, $l'' \in \mathbf{B}^r$, $k + r = m$, имеет вес $\|l\| = \tau + 1$. Тогда если $\|l''\| = \tau + 1 \leq r \leq \tau + k$, то $l' = 0$ и $\mathbf{P}((l'', \omega) = 0) = 1/2$, если $\|l\| = j \leq \tau$,то $\|l'\| = j' = \tau + 1 - j \geq 1$. В этом случае заметим, что функция $f(\omega) = (l', \Psi(\omega)) = l'_1\Psi_1(\omega) \oplus \ldots \oplus l'_m\Psi_m(\omega)$, полученная суммированием некоторых координат τ-устойчивой функции $\Psi(\omega)$, также будет τ-устойчивой, поскольку сумма независимых равновероятных величин имеет равновероятное распределение. Из того, что $\mathbf{P}(f(\omega) = (\alpha, \omega)) = 1/2 - f^\wedge(\alpha)$ при $\alpha \neq 0$, где через $f^\wedge(\alpha)$ обозначено преобразование Фурье–Адамара $f^\wedge(\alpha) = \mathbf{E}\, f(\omega)(-1)^{(\alpha,\omega)}$ булевой функции $f(x)$ в точке $\alpha \in \mathbf{B}^r$, и преобразование Фурье–Адамара τ-устойчивой функции $f(x)$ удовлетворяет (см. [15]) условию $f^\wedge(\alpha) = 0$ для любого вектора $\alpha \in \mathbf{B}^r$, $\alpha \neq 0$, $\|\alpha\| \leq t$, получаем соотношение $\mathbf{P}(f(\omega) = (l'', \omega)) = 1/2$ при $\|l''\| \leq \tau$ и, следовательно, $\mathbf{P}((l, \chi(\omega)) = 0) = 1/2$ для любого вектора $l \neq 0$ веса $\|l\| \leq \tau + 1$.

Таким образом, если $\psi(s,\omega) = (s \oplus \Psi(\omega), \omega)$, $\chi(\omega) = (\Psi(\omega), \omega)$ и $\tau(\Psi(\omega)) \geq \geq \tau$, то $\nu(\chi(\omega)) \geq \tau + 1$ и $d(\psi(s,\omega)) \geq \tau + 2$. Заметим еще, что условие τ-устойчивости функции $\Psi(\omega)$ является достаточно сильным ограничением на способ случайного кодирования. В частности, число координатных функций τ-устойчивой функции от r аргументов ограничено сверху величиной $k \leq r - - \tau$ и для получения $\tau(\Psi) \geq \tau$. потребуется иметь $r \geq k + \tau$. Так, например, полагая $\tau = r - 1$, получаем $k = 1$ и, выбирая в качестве функции $\Psi(\omega)$ $(r-1)$-устойчивую функцию $\Psi(\omega) = \omega_1 \oplus \ldots \oplus \omega_r$, получаем $m = r + 1$, $\tau(\Psi(\omega)) = r - 1$, $\nu(\chi(\omega)) = r$ и $d(\psi(s,\omega)) = r + 1$ при скорости передачи информации $1/m$. Для увеличения скорости передачи при фиксированном r потребуется увеличить параметр k.

Рассмотрим теперь (m, k, d)-линейный код над полем $\mathbf{GF}(2)$ с k информационными символами, $r = m - k$ проверочными символами и кодовым расстоянием d. Обозначим через $G = (G^1, \ldots, G^m)$ порождающую матрицу кода размер $k \times m$, через $B = (B^1, \ldots, B^m)$ — двоичную матрицу того же размера, через $H = (H^1, \ldots, H^m)$ — проверочную матрицу кода размера $r \times m$, G^j, B^j, H^j — вектор-столбцы матриц G, B, H высоты k, k, r соответственно. Пусть $\gamma(H)$ — максимальное натуральное d, при котором любые $d-1$ столбцов матрицы H линейно независимы. Известно (см. [14]), что кодовое расстояние (минимальный вес кодового слова) рассматриваемого кода равно $d = \gamma(H)$.

Заметим, что первые k строк матрицы $F = \begin{pmatrix} B \\ H \end{pmatrix}$ в случае $B = G$ являются строками порождающей матрицы G и составляют базис линейного кода, и следовательно, линейно независимы. Строки проверочной матрицы H являются базисными векторами линейного подпространства, ортогонального к линейному коду, и поэтому также линейно независимы. Если полученная таким образом матрица F окажется невырожденной матрицей размера $m \times m$, то порождаемое ею отображение $\psi(s,w) = (s,w)F$ будет представлять собой подстановку на множестве $\mathbf{B}^m$. В этом случае на вход канала связи подаются векторы $X(s) = \psi(s,\omega_t) = sG \oplus \omega_t H$ и на выходе побочного канала реализуется случайные векторы $Z_t = sG \oplus \omega_t H \oplus æ_t$.

Если матрица F окажется вырожденной, то следует заменить в ней подматрицу G на подматрицу B таким образом, чтобы матрица F стала невырожденной, и использовать полученную матрицу для реализации случайного кодирования.

Для оценки снизу уровня защиты $d(\psi)$ случайного кода, задаваемого подстановкой $\psi(s,w) = (s,w)F$, достаточно установить уровень равновероятности случайного вектора $X(s) = \psi(s,\omega_t) = sB \oplus \omega_t H$, который совпадает с уровнем равновероятности случайного вектора $\chi_t = \omega_t H$.

Утверждение 8. *Уровень равновероятности $\nu(\chi)$ случайного вектора $\chi = = \omega H = ((\omega H)_1, \ldots, (\omega H)_m)$ равен $\gamma(H)$.*

Доказательство. Выберем произвольный вектор $l \in \mathbf{B}^m$, имеющий вес Хэмминга $\|l\| = j \leq \gamma(H)$. Обозначим через $(\omega H)_{\langle l \rangle}(H_{\langle l \rangle})$ подвектор вектора ωH (подматрицу матрицы H), составленный из координат (составленную из столбцов), номера которых совпадают с номерами единичных координат вектора l. Дополним матрицу $H_{\langle l \rangle}$ размера $r \times j$ до невырожденной матрицы H' размера $r \times r$. Это можно сделать, поскольку при $j \leq \gamma(H)$ ранг матрицы $H_{\langle l \rangle}$ равен j. Тогда из равновероятности вектора ω следует равновероятность вектора $\omega H'$ и его подвектора $(\omega H)_{\langle l \rangle}$. Кроме того, при $j > \gamma(H)$ существует вектор l с $\|l\| = j$, для которого выполняется равенство $l_1 H_1 \oplus \ldots \oplus l_m H_m = 0$, откуда следует, что $(l, \omega H) = l_1(\omega H)_1 \oplus \ldots \oplus l_m(\omega H)_m = 0$ и что распределение линейной комбинации, состоящей из j координат вектора ωH, не является равновероятным. Утверждение доказано.

Теорема 3. *Любому линейному коду (m, k, d) можно сопоставить случайный код $\psi(s, \omega)$ с уровнем защиты $d(\psi) \geq d$.*

Доказательство. Из утверждениий 6 и теоремы 2 следует, что случайный код $\psi(s, \omega_t) = a(s) \oplus \chi(\omega_t)$, где $a(s) = sB$, $\chi(\omega_t) = \omega_t H$, построенный с помощью проверочной матрицы H линейного кода (m, k, d) и матрицы B, обеспечивающей обратимость преобразования $\psi(s, \omega_t)$, имеет уровень защиты $d(\psi) = d$.

Приведем несколько примеров.

1. Рассмотрим $(m, 1, m)$-код, состоящий из двух кодовых слов $\mathbf{0} = (0, \ldots, 0) \in \mathbf{B}^m$ и $\mathbf{e} = (1, \ldots, 1) \in \mathbf{B}^m$. В соответствующем случайном коде сообщение $s \in \mathbf{B}$ преобразуется в вектор $X(s) = (X_1, \ldots, X_m)$, который случайно и равновероятно выбирается из множества векторов, удовлетворяющих условию $X_1 \oplus \ldots \oplus X_m = s$. В этом случае $\gamma(H) = m - 1$ и $d(\psi) = m$ при скорости передачи информации по каналу $R = 1/m$. Вероятность правильного декодирования сигнала на выходе отводного канала при вероятности канальной ошибки $\mathbf{P}(æ_{tj} = 1) = p = (1 - \Delta)/2$ равна $P^* = \Sigma^* C_m^k p^k (1 - p)^{m-k}$, где Σ^* означает суммирование по нечетным индексам k. Аналогично обозначим $P^{**} = \Sigma^{**} C_m p^k (1 - p)^{m-k}$, где Σ^{**} означает суммирование по четным индексам k. Из формул $(p + q)^m = P^* + P^{**} = 1$, $(q - p)^m = \Delta^m = P^* - P^{**}$ получаем $P^* = (1/2)(1 + \Delta^m)$.

2. Пусть случайный код задается отображением $\psi(s, \omega) = (s \oplus \omega, \omega)$, $s, \omega \in \mathbf{B}^4$, чему соответствует линейный (8,4,2)-код. Уровень равновероятности вектора $X = (\omega, \omega)$ равен $\nu(X) = 1$, поэтому $d(\psi) = 2$ при скорости передачи информации по каналу $R = 1/2$.

3. Рассмотрим расширенный код Хэмминга (8,4,4). В этом случае, поскольку код Хэмминга (8,4,4) является самодуальным (см. [14]), при построении способа случайного кодирования необходимо подобрать матрицу B так, чтобы отображение $\psi(s, \omega_t)$ было обратимо. При этом из того, что $\gamma(H) = 3$, следует, что уровень защиты равен $d(\psi) = 4$ при скорости передачи информации по каналу, равной $R = 1/2$. Таким образом, при передаче информации по

двоичному симметричному каналу со скоростью 1 минимальный объем выборки для различения двух гипотез H_s и H_g с вероятностями ошибок первого и второго рода α и β соответственно асимптотически равен

$$N_{sg}(\alpha,\beta) \sim \frac{(u_\alpha + u_\beta)^2}{b_{sg}\Delta^2},$$

а при передаче информации со скоростью 1/2 с использованием случайного кода, соответствующего расширенному коду Хэмминга, минимальный объем выборки оценивается величиной

$$N_{sg}(\alpha,\beta) \sim \frac{(u_\alpha + u_\beta)^2}{b_{sg}\Delta^8}.$$

4. В случае использования кода Голея (24, 12, 8) (см. [14]) при скорости передачи информации $R = 1/2$ уровень защиты достигает значения $d(\psi) = 8$.

§ 6. ИССЛЕДОВАНИЕ КОНКРЕТНЫХ МОДЕЛЕЙ КОДОВОГО ЗАШУМЛЕНИЯ

Коэффициенты $h_{sj}(z)$ в формуле (7) в случае $q = 2$ могут быть представлены в виде $h_{sj}(z) = \mathbf{E}\, R_{sj}(\omega_t, z)$, где

$$R_{sj}(\omega_t, z) = \sum_{v=0}^{j} (-1)^v \binom{a}{v}\binom{b}{j-v}, \tag{11}$$

$a = a(s,\omega_t,z) = \|\psi(s,\omega_t) \oplus z\|$, $b = m - a$, и, как показывают непосредственно проведенные для значений $j = 1,2,3$ вычисления, с учетом соотношений $\binom{r}{s} = 0$ при $r < s$ принимают значения $h_{s1}(z) = \mathbf{E}\, R_{s1}(\omega_t, z)$, где

$$R_{s1}(\omega_t, z) = m - 2a(s,\omega_t,z), \tag{12}$$

$$h_{s21}(z) = (1/2)[\mathbf{E}\, R_{s1}^2(\omega_t, z) - m], \tag{13}$$

$$h_{s3}(z) = (1/6)[\mathbf{E}\, R_{s1}^3(\omega_t, z) - (3m-2)h_{s1}(z)]. \tag{14}$$

Заметим, что уровень защиты случайного кодирования будет равен $d(\psi) = d$ в случае $h_{s1}(z) = \ldots = h_{s,d-1}(z) = 0$ и $\mathbf{E}_0\, h_{sg}^2(Z_t) = b_{sg} > 0$ для всех s и g.

Рассмотрим алгоритм случайного кодирования, порождаемый подстановкой вида $\psi(s,w) = (g(s,w), w)$, где $s \in \mathbf{B}^k$, $w \in \mathbf{B}^r$, $g(s,w)$ — набор подстановок на множестве $\mathbf{B}^k$, занумерованных символами w.

Пусть $\|\psi(s,\omega_t)\|^* = \|\psi(s,\omega_t)\| - \mathbf{E}\|\psi(s,\omega_t)\|$, $a^*(s,\omega_t,z) = a(s,\omega_t,z) - \mathbf{E}\,a(s,\omega_t,z)$.

Теорема 4. *Пусть вектор w имеет длину $r = lk$ и состоит из l подвекторов $w^j \in \mathbf{B}^k$, $j = 1,\dots,l$, $w = (w^1,\dots,w^l) \in \mathbf{B}^{lk}$, $m = (l+1)k$, преобразование $g^l(s,w) = g_l(g_{l-1}(\dots g_2(g_1(s,w^1),w^2)\dots,w^{l-1}),w^l)$ представляет собой суперпозицию l квазигрупповых операций $g_1(s,w^1),\dots,g_l(s,w^l)$, $g'^l(u,\lambda) = s\oplus w^1\oplus\dots\oplus w^l$ — трансляция вектора s, $\psi^l(s,w) = (g^l(s,w),w)$, $\psi'^l(s,w) = (g'^l(s,w),w)$. Тогда для алгоритма $\psi^l(s,w)$ выполняются соотношения $d(\psi^1) \geq 2$, $d(\psi^1) = 2$, если $\mathbf{E}\|g^1(s,\omega_t)\oplus z^0\|^*\|\omega_t\oplus z^1\|^* \neq 0$, $d(\psi^2) \geq 3$, $d(\psi^2) = 3$, если $\mathbf{E}\|g^1(s,\omega_t)\oplus z^0\|^*\|\omega_t^1\oplus z^1\|^*\|w_t^2\oplus z^2\|^* \neq 0$; для алгоритма $\psi'^l(s,w)$ справедливы соотношения $d(\psi'^0) = 1$, $d(\psi'^1) = 2$, $d(\psi'^2) = 3$ и минимальный объем выборки для различения гипотез H_s и H_g при $s \neq g$, $s \in \mathbf{B}^k$, $g \in \mathbf{B}^k$, с вероятностями ошибок первого и второго рода α и β соответственно при $\delta \to 0$ асимптотически равен*

$$N_{sg}(\alpha,\beta) \sim \frac{(u_\alpha + u_\beta)^2}{4\|s\oplus g\|\Delta^{2(l+1)}}. \tag{15}$$

Доказательство. При $l = 0$, $m = k$, $g(s,w) = s$, $s,w \in \mathbf{B}^k$, $a(s,z) = \|s\oplus z\|$ получаем

$$h_{s1}(z) = k - 2\|s\oplus z\|, \quad b_s = \mathbf{E}_0\,h_{s1}^2(Z_t) = \mathbf{E}_0(k - 2\|s\oplus Z_t\|)^2 = k,$$

$$b_{sg} = \mathbf{E}_0(h_{g2}(g,Z_t) - h_{s2}(s,Z_t))^2 = 4\,\mathbf{E}_0(\|s\oplus Z_t\|^* - \|g\oplus Z_t\|^*)^2 =$$

$$= 2k - 8\,\mathbf{E}_0\|s\oplus Z_t\|^*\|g\oplus Z_t\|^* = 2k - 8\,\mathrm{Cov}(\|s\oplus Z_t\|,\ \|g\oplus Z^t\|) = 4\|s\oplus g\|,$$

так как $\mathrm{Cov}(\|Z_t\|,\ \|Z_t\oplus z\|) = k/4 - \|d\|/2$. Поэтому асимптотическое значение минимального объема выборки можно определить по формуле (15).

При $l = 1$, $m = 2k$, $a(s,w,z) = \|s\oplus w\oplus z^0\| + \|w\oplus z^1\|$, $z = (z^0,z^1)$

$$h_{s1}(z) = -2\,\mathbf{E}\,a^*(s,\omega_t,z) = 0,$$

$$h_{s2}(z) = 2\,\mathbf{E}(a(s,\omega_t,z) - k)^2 - k = 2\,\mathbf{E}\,a^{*2}(s,\omega_t,z) - k.$$

Поэтому $d(\psi^1) \geq 2$. Для алгоритма $\psi'^1(s,w)$ получаем

$$h_{s2}(z) = 2\,\mathbf{E}(a(\omega) - k)^2 - k = k - 2\|s\oplus z^0\oplus z^1\|,$$

так как

$$\mathbf{E}\|\omega\|^2 = k(k+1)/4,$$

$$\mathbf{E}\|\omega\|\,\|\omega\oplus z\| = \mathrm{Cov}(\|\omega\|,\|\omega\oplus z\|) + k^2/4 = k(k+1)/4 - \|z\|/2.$$

Следовательно, при $l = 1$ имеем $d(\psi'^1) = 2$ и

$$b_{sg} = \mathbf{E}_0(h_{g2}(Z_t) - h_{s2}(Z_t))^2 =$$
$$= 4\,\mathbf{E}_0(\|s \oplus Z_t^0 \oplus Z_t^1\| - \|g \oplus Z_t^0 \oplus Z_t^1\|)^2 = 4\|s \oplus g\|,$$

откуда следует (15).

При $l = 2$, $m = 3k$, $w = (w^1, w^2)$, $z = (z^0, z^1)$, $a(s, w, z) = \|g(s, w) \oplus z^0\| + \|w^1 \oplus z^1\| + \|w^2 \oplus z^2\|$

$$h_{s1}(z) = -2\,\mathbf{E}\,a^*(s, \omega_t, z) = 0, \quad h_{s2}(z) = 2\,\mathbf{E}\,a^{*2}(s, \omega_t, z) - m/2 = 0,$$
$$h_{s3}(z) = -8\,\mathbf{E}\|g(s, \omega_t) \oplus z^0\|^*\|\omega_t^1 \oplus z^1\|^*\|\omega_t^2 \oplus z^2\|^*.$$

Поэтому $d(\psi^2) \geq 3$. Для алгоритма $\psi'^1(s, w)$ имеем

$$h_{s3}(z) = -8\,\mathbf{E}\|s \oplus \omega_t \oplus z^0\|^*\|\omega_t^1 \oplus z^1\|^*\|\omega_t^2 \oplus z^2\|^* = k - 2\|s \oplus z^0 \oplus z^1 \oplus z^2\|,$$

$d(\psi'^1) = 2$, и для $l = 2$ из равенства

$$b_{sg} = \mathbf{E}_0(h_{s3}(Z_t) - h_{g3}(Z_t^t))^2 =$$
$$= 4\,\mathbf{E}_0(\|s \oplus Z_t^0 \oplus Z_t^1 \oplus Z_t^2\| - \|g \oplus Z_t^0 \oplus Z_t^1 \oplus Z_t^2\|)^2 = 4\|s \oplus g\|$$

получаем (15).

В заключение заметим, что, вообще говоря, для любого значения d, $0 < d < d(\psi)$, множество всех 2^k сообщений делятся на классы d-эквивалентности по признаку $s \sim g$, если $h_{sj}(z) = h_{gj}(z)$, $j = 1, \ldots, d$. Поэтому по выборке объема $N \asymp \Delta^{-2d}$ переданные сообщения могут определяться лишь с точностью до d-эквивалентности. Наибольший практический интерес представляют методы случайного кодирования, для которых $k(1) = \ldots = k(d-1) = 1$, $k(d) = 2^k$, где $k(l)$ — число классов l-эквивалентности. Некоторые из таких способов кодового зашумления рассмотрены выше.

СПИСОК ЛИТЕРАТУРЫ

1. *Wyner A.* The Wire-Tap Channal. — Bell Syst. Tech. J., 1975, v. 54, p. 1355–1387.
2. *Коржик В. И., Яковлев В. А.* Неасимптотические оценки эффективности кодового зашумления одного канала. — Пробл. передачи информ., 1981, т. 17, в. 4, с. 11–18.
3. *Коржик В. И., Яковлев В. А.* Защита информации от утечки за счет побочных электромагнитных излучений и наводок на основе способа кодового зашумления. — Информ. вычислит. тех., 1993, в. 1, 2, с. 61–66.
4. *Иванов В. А.* Проверка статистических гипотез по случайно преобразованной реализациию. — Дискрет. матем., 1994, т. 6, в. 2, с. 150–158.
5. *Ошкин И. Б., Проскурин Г. В.* Нижние оценки вероятности различения подмножеств единичного куба. — Пробл. передачи информ., 1994, т. 30, в. 3, с. 15–22.

6. *Иванов В. А.* Об эффективности методов случайного кодирования. — Обозр. прикл. промышл. матем., 1998, т. 5, в. 2, с. 220–221.

7. *Пазизин С. В.* Обнаружение и прием последовательности сигналов, искаженных случайной помехой и независимым шумом. — Пробл. передачи информ., 1998, т. 34, в. 1, с. 46–55.

8. *Иванов В. А.* О методе случайного кодирования. — Дискрет. матем., 1999, т. 11, в. 3, с. 99–108.

9. *Пазизин С. В.* О характеристиках случайных блоковых кодов, порождающих ошибки. — Обозр. прикл. промышл. матем., 2000, т. 7, в. 2, с. 520–521.

10. *Пазизин С. В.* Вероятности правильного декодирования для канала с аддитивным нормальным шумом и двоичного симметричного канала при случайном выборе кодовых слов. — Дискрет. матем., 2000, т. 12, в. 2, с. 93–98.

11. *Иванов В. А.* Вероятностные характеристики алгоритмов случайного кодирования. — Обозр. прикл. промышл. матем., 2001, т. 8, в. 1, с. 187–188.

12. *Иванов В. А.* Асимптотические характеристики критериев проверки гипотез по случайно преобразованной выборке. — В сб.: Труды по дискретной математике. Т. 5. — М.: ФИЗМАТЛИТ, 2002, с. 61–72.

13. *Гладков Б. В.* Суммы случайных величин, любые r из которых независимы. — Матем. заметки, 1982, т. 32, № 3, с. 385–399.

14. *Мак-Вильямс Ф. Дж, Слоэн Н. Дж.* Теория кодов, исправляющих ошибки. — М.: Связь, 1979.

15. *Xiao G.-Z., Massey J. E.* A spectral characterisation of correletion immune combining function. — IEEE Trans. Inform. Theory, 1988, v. 34, p. 569–571.