3. R.J. Anderson "Solving a Class of Stream Ciphers" / Cryptologia, v. 14, n. 3, Jul 1990, pp. 285-288.

УДК 621.391:519.2

Алексейчук А. Н.

СЛУЧАЙНОЕ КОДИРОВАНИЕ В КАНАЛЕ СВЯЗИ С АДДИТИВНЫМ ШУМОМ, РАСПРЕДЕЛЕННЫМ НА КОНЕЧНОЙ АБЕЛЕВОЙ ГРУППЕ

Одним из известных эффективных способов повышения стойкости криптографических преобразований, применяемых в современных системах защиты информации, является случайное кодирование сообщений, при котором сигнал, используемый для передачи фиксированного сообщения $s \in S$, выбирается случайно из заданного множества сигналов (см., например, [1 – 4]). Достаточно общей математической моделью системы передачи информации со случайным кодированием является вероятностно-криптографическая система (ВКС) [5], представляющая собой совокупность дискретного источника, случайного кодера и произвольного дискретного канала. Указанная модель включает в себя в качестве частного случая понятие гомофонического (рандомизированного) шифра [2, 3] и может быть непосредственно использована при исследовании влияния случайного кодирования на неопределенность передаваемого сообщения [3, 5, 6], а также при анализе выходных последовательностей конечного автомата, функционирующего в условиях внешних помех и внутренних сбоев [7].

Центральной задачей анализа вероятностно-криптографических систем является разработка эффективных методов вычисления различных информационных или вероятностных характеристик реализуемых с использованием этих систем случайных отображений. Настоящая статья посвящена изучению одной из наиболее важных, с практической точки зрения, характеристик эффективности случайного кодирования дискретной информации в канале с аддитивным шумом, распределенным на конечной абелевой группе, – вероятности правильного приема сообщений оптимальным декодером канала.

Основные понятия и вспомогательные результаты.

Пусть S, X и Y – непустые конечные множества, $P_S = (p(s): s \in S)$ – распределение вероятностей (РВ) на множестве S, где $p(s) > 0$ для любого $s \in S$.

Вероятностно-криптографическая система определяется [5] как упорядоченная совокупность $\Re = (S, \sigma, W)$, состоящая из источника (S, P_S), сюръективного отображения σ: $X \to S$ и стохастической матрицы (канала) W с элементами $W(y/x)$, $y \in Y, x \in X$. Отображению σ ставится в соответствие случайный кодер – стохастическая матрица V с элементами $V(x/s)$, $x \in X, s \in S$ такая, что $V(x/s) > 0$ тогда и только тогда, когда $x \in C_s \overset{\text{def}}{=} \sigma^{-1}(s)$.

Предполагается, что источник вырабатывает случайное сообщение $s \in S$ с вероятностью $p(s)$, которое преобразуется в сообщение $x \in C_s$ с вероятностью $V(x/s)$. В свою очередь, x искажается в канале связи W и преобразуется с вероятностью $W(y/x)$ в доступное криптоаналитику выходное сообщение $y \in Y$.

Основная задача анализа эффективности рассматриваемого способа случайного кодирования информации состоит в вычислении или оценке вероятности $\pi(\sigma, \delta) \stackrel{\text{def}}{=} \mathbf{P}(\delta(y) = s)$ правильного приема сообщений в канале W ВКС $\mathfrak{R}$ с помощью данного декодера (отображения) δ: $Y \to S$ [8 – 10].

В дальнейшем рассматриваются исключительно вероятностно-криптографические системы $\mathfrak{R} = (S, \sigma, W)$, удовлетворяющие следующим условиям:

(а) множества S, X, Y являются абелевыми группами, $X = Y$;

(б) отображение σ есть равновероятная функция из Y в S, то есть

$$|C_s| = |Y|\,|S|^{-1},\ s \in S, \tag{1}$$

(в) для любых $s \in S$, $x \in C_s$ выполняются равенства

$$p(s) = |S|^{-1},\ V(x/S) = |C_s|^{-1}; \tag{2}$$

(г) существует РВ $\omega = (\omega(y):\ y \in Y)$ на группе Y такое, что

$$W(y/x) = \omega(y - x),\ x, y \in Y. \tag{3}$$

В соответствии с терминологией, принятой в [8 – 10], назовем способ случайного кодирования, отвечающий рассматриваемому частному случаю ВКС, равномерным случайным кодированием в канале с аддитивным шумом, распределенным на абелевой группе Y.

С практической точки зрения представляют определенный интерес так называемые групповые вероятностно-криптографические системы [5], которые характеризуются условием

(д) отображение σ является эпиморфизмом группы Y в группу S.

Исследованию характеристик двоичных групповых ВКС (S и Y – элементарные абелевы 2-группы) посвящены работы [8, 11, 12] и ряд других. В [9] получены аналитическое выражение и оценки вероятности правильного приема сообщений оптимальным декодером групповой вероятностно-криптографической системы в предположении, что гомоморфизм σ удовлетворяет условию покоординатной невырожденности (см. [9]), а матрица W является n-й тензорной степенью матрицы переходных вероятностей q-ичного симметричного канала. В [10] ряд результатов [9] обобщен в на более широкий класс групповых ВКС.

В настоящей статье исследуется эффективность случайного кодирования (по критерию минимума вероятности правильного приема сообщений) в канале W произвольной вероятностно-криптографической системы, удовлетворяющей условиям (а) – (г). С использованием аппарата комплексных характеров и преобразования Фурье функций на конечной абелевой группе получены формулы для вычисления и оценки вероятности правильного декодирования сообщений в канале с аддитивным шумом вида (3). Установлены также общие достаточные (а в случае, когда Y является элементарной абелевой 2-группой, – необходимые и достаточные) условия, при которых оптимальный декодер канала групповой ВКС $\mathfrak{R} = (S, \sigma, W)$ совпадает с гомоморфизмом σ. В частности, получены обобщения основных результатов работ [8, 9].

Приведем основное соотношение для вероятности $\pi(\sigma, \delta)$ правильного приема декодером δ: $Y \to S$ сообщений в канале W ВКС $\mathfrak{R}$. На основнии (1) – (3) и формулы полной вероятности имеем

$$\pi(\sigma;\delta)=\sum_{y\in Y}p(\delta(y))\sum_{x\in C_{\delta(y)}}V(x/\delta(y))W(y/x)=|Y|^{-1}\sum_{y\in Y}\omega(y-C_{\delta(y)}),\qquad(4)$$

где по определению $\omega(y-C_{\delta(y)})=\sum_{x\in C_{\delta(y)}}\omega(y-x)$, $y\in Y$. Из равенства (4) следует, что отображение δ^*: $Y\to S$, определяемое соотношением

$$\omega(y-C_{\delta^*(y)})\geq\omega(y-C_s),\ s\in S,\qquad(5)$$

удовлетворяет условию $\pi(\sigma;\delta^*)\geq\pi(\sigma;\delta)$ для любого δ: $Y\to S$, то есть [8, 9] является оптимальным декодером канала W. Обозначим $\pi^*(\sigma)=\pi(\sigma;\delta^*)$ вероятность правильного приема сообщений в данном канале с помощью оптимального декодера δ^*. Также будем писать $\pi(\sigma)=\pi(\sigma;\sigma)$ при $\delta=\sigma$.

Ниже при анализе характеристик вероятностно-криптографических систем широко используется аппарат гармонического анализа (преобразования Фурье) функций, определенных на конечной абелевой группе. Приведем необходимую для дальнейшего изложения информацию о свойствах преобразования Фурье. Более подробные сведения можно найти в [13, 14].

Зафиксируем абелеву группу Y порядка Q и обозначим через T_Q группу корней степени Q из единицы. Существует изоморфизм $a\ \alpha\ \chi_a$, $a\in Y$ группы Y в ее группу характеров $\hat{Y}\overset{\text{def}}{=}\mathrm{Hom}(Y,T_Q)$ такой, что $\chi_a(y)=\chi_y(a)$, для любых a, $y\in Y$. В терминологии теории кодирования погруппы группы Y называются групповыми кодами. Каждой группе $G\subseteq Y$ соответствует группа $G^\perp=\{a\in Y:\ \chi_a(x)=1,\ x\in G\}$, которая называется дуальной к G [14]. Имеет место изоморфизм групп $G^\perp\cong\hat{Y}/G$, в силу которого выполняется равенство

$$|G^\perp|=|Y|\,|G|^{-1}.\qquad(6)$$

Характеры группы Y удовлетворяют следующим соотношениям ортогональности [13]: для любого группового кода G

$$\sum_{x\in G}\chi_a(x)=|G|,\ \text{если } a\in G^\perp;\ \sum_{x\in G}\chi_a(x)=0,\ \text{если } a\in Y\setminus G^\perp.\qquad(7)$$

Обозначим C^Y множество всех комплекснозначных функций на группе Y. Множество C^Y является унитарным векторным пространством относительно скалярного произведения

$$(f,g)=\sum_{y\in Y}f(y)\overline{g(y)},$$

где $\overline{g(y)}$ – число, комплексно-сопряженное к числу $g(y)$. Преобразование Фурье $\hat{f}$ функции $f\in C^Y$ определяется по формуле

$$\hat{f}(a)=\sum_{x\in Y}\chi_a(x)f(x),\ a\in Y.$$

Обратное преобразование имеет вид

$$f(x) = Q^{-1}\sum_{a\in Y}\overline{\chi_a(x)}\,\hat{f}(a),\ x\in Y.$$

Введем в рассмотрение матрицу $A = (\chi_a(x))_{a,x\in Y}$, которую назовем матрицей Адамара группы Y (относительно данного изоморфизма $a\ \alpha\ \chi_a$, $a\in Y$) [15]. В силу (7) матрица $\sqrt{Q^{-1}}A$ является унитарной

$$\sqrt{Q^{-1}}A^* = (\sqrt{Q^{-1}}A)^{-1}, \tag{8}$$

где A^* есть матрица, сопряженная к A. Из равенства (8) следует соотношение

$$(f,g) = Q^{-1}(\hat{f},\hat{g}),\ f,g\in C^Y; \tag{9}$$

в частности, для любой функции $f\in C^Y$ выполняется равенство Парсеваля [14, 15]

$$(f,f) = Q^{-1}(\hat{f},\hat{f}). \tag{10}$$

Сопоставим функции $f\in C^Y$ квадратную матрицу M_f с элементами

$$(M_f)_{x,y} = f(y-x),\ x,y\in Y.$$

Нетрудно видеть, что матрицы M_f, $f\in C^Y$ одновременно приводятся к диагональному виду с помощью матрицы Адамара A

$$Q^{-1}(A^*M_fA) = \mathrm{diag}((\hat{f}(x))_{x\in Y}),\ f\in C^Y. \tag{11}$$

В силу (11) M_f является нормальной матрицей, и ее спектр представляет собой систему коэффициентов Фурье функции f. В частности, если f принимает вещественные значения, то соотношения $\hat{f}(x) \geq 0$, $x\in Y$ имеют место в том и только том случае, когда M_f является симметрической положительно полуопределенной матрицей [16].

Вероятность правильного приема сообщений в системе передачи информации с равномерным случайным кодированием.

Рассмотрим произвольную вероятностно-криптографическую систему $\mathfrak{R} = (S, \sigma, W)$, удовлетворяющую условиям (а) – (г). Для любого $s\in S$ обозначим соответсвенно $I_{\sigma,s}$, $I_{\delta,s}$ индикаторы множеств $C_s = \sigma^{-1}(s)$, $\delta^{-1}(s)$. Следующая теорема, обобщающая на случай произвольной конечной абелевой группы Y один из основных результатов работы [8], устанавливает аналитическое выражение вероятности $\pi(\sigma;\ \delta)$ правильного приема сообщений в канале ВКС $\mathfrak{R}$ с помощью декодера δ: $Y\to S$.

Теорема 1. Имеют место равенства

$$\pi(\sigma;\delta) = Q^{-2}\sum_{s\in S}\mathrm{tr}(M_{I_{\sigma,s}} W M^{*}_{I_{\delta,s}}), \tag{12}$$

$$\pi(\sigma;\delta) = Q^{-2}\sum_{s\in S}\sum_{a\in Y}\hat{\omega}(a)\,\hat{I}_{\sigma,s}(a)\overline{\hat{I}_{\delta,s}(a)}, \tag{13}$$

где для любой матрицы M запись $\mathrm{tr}(M)$ обозначает след M.

Доказательство. На основании соотношения (4) справедливы равенства

$$\pi(\sigma;\delta) = Q^{-1}\sum_{\substack{x,y\in Y:\\ \sigma(x)=\delta(y)}}\omega(y-x) = Q^{-1}\sum_{s\in S}\sum_{\substack{x,y\in Y:\\ I_{\sigma,s}(x)=1,\\ I_{\delta,s}(y)=1}}\omega(y-x),$$

которые могут быть также записаны в виде

$$\pi(\sigma;\delta) = Q^{-1}\sum_{s\in S}\sum_{x,y\in Y}\omega(y-x)\,I_{\sigma,s}(x)\,I_{\delta,s}(y). \tag{14}$$

Непосредственно из (14) следует равенство (12). Сопрягая с помощью матрицы Адамара A каждую из трех матриц под знаком функции "след" в правой части (12) и используя (11), с учетом равенства $W = M_{\omega}$ получим равенство (13). Теорема доказана.

Соотношения (12), (13) позволяют получать разнообразные оценки вероятности $\pi(\sigma;\delta)$. Приведем одну из простейших оценок такого типа.

Теорема 2. Предположим, что матрица W является положительно определенной, то есть выполняется условие

$$\hat{\omega}(a) > 0,\ a\in Y. \tag{15}$$

Обозначим

$$\hat{\omega}_m = \min\{\hat{\omega}(a) : D_{\sigma}(a) > 0, a\in Y\},\ \hat{\omega}_M = \max\{\hat{\omega}(a) : D_{\sigma}(a) > 0, a\in Y\setminus 0\},$$

где

$$D_{\sigma}(a) = Q^{-2}\sum_{s\in S}\left|\hat{I}_{\sigma,s}(a)\right|^2,\ a\in Y. \tag{16}$$

Тогда для вероятности $\pi(\sigma)$ правильного приема с помощью декодера $\delta = \sigma$ сообщений в канале ВКС $\Re = (S, \sigma, W)$ справедливы следующие неравенства:

$$|S|^{-1}(1+\hat{\omega}_m(|S|-1)) \le \pi(\sigma) \le |S|^{-1}(1+\hat{\omega}_M(|S|-1)). \tag{17}$$

При этом каждая из границ (17) достигается, если W является Q-ичным симметричным каналом

$$\omega(0) = Q^{-1}(1+(Q-1)\Delta),\ \omega(a) = Q^{-1}(1-\Delta),\ a \in Y \setminus 0, \tag{18}$$

где $\Delta \in [0, 1]$.

Доказательство. Убедимся в справедливости нижней оценки (17). На основании равенства (13) и условия теоремы имеют место соотношения

$$\pi(\sigma) = \sum_{a \in Y} \hat{\omega}(a) D_\sigma(a) = D_\sigma(0) + \sum_{a \in Y \setminus 0} \hat{\omega}(a) D_\sigma(a) \geq D_\sigma(0) + \hat{\omega}_m \Big(\sum_{a \in Y \setminus 0} D_\sigma(a) \Big). \tag{19}$$

Используя (16), равенство Парсеваля (10) (при $f = I_{\sigma,s}$, $s \in S$) и условие равновероятности функции σ получим, что

$$\sum_{a \in Y} D_\sigma(a) = Q^{-2} \sum_{s \in S} \sum_{a \in Y} \left| \hat{I}_{\sigma,s}(a) \right|^2 = Q^{-1} \sum_{s \in S} \left| \sigma^{-1}(s) \right| = 1. \tag{20}$$

Далее, поскольку для любого $s \in S$ $\hat{I}_{\sigma,s}(0) = \left| \sigma^{-1}(s) \right| = Q|S|^{-1}$, то в силу (16)

$$D_\sigma(0) = |S|^{-1}. \tag{21}$$

Непосредственно из (19) – (21) следует нижняя оценка (17). Аналогично устанавливается верхняя граница вероятности $\pi(\sigma)$.

Наконец, если РВ ω удовлетворяет условию (18), то, как нетрудно убедиться с помощью непосредственных вычислений,

$$\hat{\omega}(a) = \Delta,\ a \in Y \setminus 0. \tag{22}$$

Следовательно, в силу (13), (19)

$$\pi(\sigma) = |S|^{-1}(1 + \Delta(|S| - 1)), \tag{23}$$

что и требовалось доказать.

Рассмотрим одно применение теоремы 2. Предположим, что группа Y является прямым произведением абелевых групп $Y = F_1 \times \ldots \times F_n$, $|F_i| = q_i$, $i \in \overline{1, n}$, а РВ ω имеет следующий вид:

$$\omega(y) = \prod_{i=1}^{n} \omega_i(y_i),\ y = (y_1, \ldots, y_n) \in Y, \tag{24}$$

где

$$\omega_i(0) = \frac{1}{q_i}(1+(q-1)\Delta_i),\ \omega_i(y_i) = \frac{1}{q_i}(1-\Delta_i),\ y_i \in F_i \backslash 0,\ \Delta_i \in [0,1],\ i \in \overline{1,n}. \qquad (25)$$

Используя (24), (25), находим $\hat{\omega}(a_1,\ldots,a_n) = \prod_{i=1}^{n} \hat{\omega}_i(a_i) = \prod_{i:a_i \neq 0} \Delta_i \geq \Delta_1 \ldots \Delta_n$, $(a_1, \ldots, a_n) \in Y$.

Таким образом, по теореме 2 вероятность $\pi^*(\sigma)$ правильного приема (с помощью оптимального декодера) сообщений в канале связи вида (24) удовлетворяет следующему неравенству:

$$\pi^*(\sigma) \geq |S|^{-1}(1 + \Delta_1 \ldots \Delta_n(|S| - 1)). \qquad (26)$$

Ниже показано, что при условии $F_i = S,\ i \in \overline{1,n}$ неравенство (26) обращается в равенство, если отображение σ имеет вид $\sigma(y_1, \ldots, y_n) = y_1 + \ldots + y_n$, $(y_1, \ldots, y_n) \in Y$. Этот результат обобщает аналогичное утверждение, полученное в [8, 17] для случая $S = (\mathbf{GF}(2), +)$, $\Delta_i \equiv \Delta \in [0, 1]$.

Оптимальное декодирование сообщений в групповых вероятностно-криптографических системах.

Рассмотрим подробнее важный частный случай, в котором отображение σ является эпиморфизмом группы Y в группу S, то есть $\mathfrak{R} = (S, \sigma, W)$ представляет собой групповую вероятностно-криптографическую систему.

Обозначим $G = \{y \in Y: \sigma(y) = 0\}$ ядро гомоморфизма σ. Нетрудно видеть, что множества $C_s = \sigma^{-1}(s)$, $s \in S$ являются различными смежными классами (СК) группы Y по подгруппе G. Отсюда на основании (4), (5) заключаем, что оптимальный декодер δ^* канала W групповой ВКС $\mathfrak{R}$ определяется равенством

$$y - C_{\delta^*(y)} = C_{s^*},\ y \in Y, \qquad (27)$$

где C_{s^*} есть наиболее вероятный СК группы Y по подгруппе G

$$\omega(C_{s^*}) = \max\{\omega(y + G):\ y \in Y\}. \qquad (28)$$

Вероятность правильного приема сообщений в канале W равна при этом

$$\pi^*(\sigma) = \omega(C_{s^*}). \qquad (29)$$

В связи с результатами, полученными в [7 – 9], представляет определенный теоретический и практический интерес описание распределений вероятностей ω на группе Y, удовлетворяющих условию

$$\omega(C_{s^*}) = \omega(G) \qquad (30)$$

для любой подгруппы $G \subseteq Y$.

Назовем группу G регулярной относительно РВ ω [10], если для любого СК $y + G$, $y \in Y$ выполняется неравенство $\omega(y + G) \leq \omega(G)$. Распределение вероятностей ω на группе Y

назовем регулярным, если каждая подгруппа $G \subseteq Y$ является регулярной относительно РВ ω, то есть удовлетворяет равенству (30).

В силу (28), (29) для регулярных распределений ω (и только для них) оптимальный декодер δ^* канала W совпадает с отображением σ (каким бы ни был эпиморфизм σ: $Y \to S$). Следовательно, "в условиях регулярности" оптимальный прием сообщения $y \in Y$ в канале W состоит в определении смежного класса $y + G$, содержащего y.

Лемма 1. Для любой подгруппы $G \subseteq Y$ имеют место равенства

$$\omega(G + a) = \left|G^{\perp}\right|^{-1} \sum_{x \in G^{\perp}} \hat{\omega}(x)\overline{\chi_a(x)}, \; a \in Y. \tag{31}$$

Доказательство. Обозначим I_A индикатор произвольного множества $A \subseteq Y$. Докажем соотношение

$$\hat{I}_{G+a}(x) = |G|\chi_a(x) I_{G^{\perp}}(x), \tag{32}$$

где $a \in Y$. В силу определения преобразования Фурье

$$\hat{I}_{G+a}(x) = \sum_{y \in Y} \chi_x(y) I_{G+a}(y) = \sum_{y \in G} \chi_x(a + y) = \chi_a(x)\hat{I}_G(x) = |G|\chi_a(x) I_{G^{\perp}}(x)$$

(последнее равенство следует из соотношений ортогональности (7)). Итак, равенство (32) доказано. Для доказательства (31) достаточно заметить, что в силу (9), (32) и (6) $\omega(G + a) = (\omega, I_{G+a}) = Q^{-1}(\hat{\omega}, \hat{I}_{G+a}) = Q^{-1}|G|\sum_{x \in Y} \hat{\omega}(x)\overline{\chi_a(x)} I_{G^{\perp}}(x) =$

$\left|G^{\perp}\right| \sum_{x \in G^{\perp}} \hat{\omega}(x)\overline{\chi_a(x)}$. Лемма доказана.

Непосредственно из равенств (28) – (31) вытекает следующая теорема, содержащая достаточное условие регулярности распределения вероятностей на конечной абелевой группе.

Теорема 3. Пусть ω является положительно полуопределенным РВ на группе Y, то есть удовлетворяет условию

$$\hat{\omega}(a) \geq 0, \; a \in Y. \tag{33}$$

Тогда ω есть регулярное распределение вероятностей, и вероятность правильного приема сообщений в канале W равна

$$\pi^*(\sigma) = \omega(G) = |S|^{-1} \sum_{x \in G^{\perp}} \hat{\omega}(x). \tag{34}$$

Рассмотрим в качестве применения теоремы 3 распределение ω вида (24) на группе $Y = F_1 \times \ldots \times F_n$, где $F_i = S$, $i \in \overline{1,n}$. Положим $\sigma(y_1, \ldots, y_n) = y_1 + \ldots + y_n$, $(y_1, \ldots, y_n) \in Y$.

Отображение σ является эпиморфизмом Y в S с ядром $G = \{(y_1, \ldots, y_n) \in S^n : y_1 + \ldots + y_n = 0\}$. Дуальная к G группа $G^\perp$ состоит векторов вида $(y, \ldots, y)$ длины n, где $y \in Y$ (указанные векторы аннулируют группу G и их число равно $|S| = |G^\perp|$). Таким образом, на основании (24), (25)

$$\hat{\omega}(a_1, \ldots, a_n) = \Delta_1 \ldots \Delta_n,\ (a_1, \ldots, a_n) \in Y \setminus 0$$

и по формуле (34)

$$\pi^*(\sigma) = |S|^{-1}(1 + \Delta_1 \ldots \Delta_n(|S| - 1)), \tag{35}$$

что совпадает с нижней границей (26). Итак, рассматриваемое отображение σ является оптимальным по критерию минимума вероятности правильного декодирования в классе ВКС с каналом W, определяемым соотношениями (24), (25).

В заключение приведем полное описание регулярных РВ на элементарной абелевой 2-группе. Докажем следующее вспомогательное утверждение.

Лемма 2. Пусть ω – РВ на абелевой группе Y, G – подгруппа группы Y, регулярная относительно РВ ω. Тогда имеет место неравенство

$$\sum_{a \in G^\perp \setminus 0} \hat{\omega}(a) \geq 0. \tag{36}$$

Доказательство. В силу регулярности группы G справедливы неравенства $\omega(G) \geq \omega(y + G)$, $y \in Y$, которые на основании утверждения леммы 1 могут быть записаны в виде

$$\sum_{a \in G^\perp} \hat{\omega}(a) \geq \sum_{a \in G^\perp} \hat{\omega}(a)\overline{\chi_y(a)},\ \ y \in Y. \tag{37}$$

Поскольку множество сужений $\overline{\chi_y}\big|_{G^\perp}$ характеров $\overline{\chi_y}$, $y \in Y$ на подгруппу $G^\perp$ совпадает с группой $\hat{G}^\perp$, то соотношения (37) равносильны следующей системе неравенств:

$$\sum_{a \in G^\perp \setminus 0} \hat{\omega}(a) \geq \sum_{a \in G^\perp \setminus 0} \hat{\omega}(a)\chi(a),\ \chi \in \hat{G}^\perp \tag{38}$$

(слагаемые в обеих частях (37), соответствующие значению $a = 0$, равны 1). Суммируя (38) по всем $\chi \in \hat{G}^\perp$, $\chi \neq 1$, на основании (7) получим неравенство

$$(|G^\perp| - 1) \sum_{a \in G^\perp \setminus 0} \hat{\omega}(a) \geq -\sum_{a \in G^\perp \setminus 0} \hat{\omega}(a),$$

равносильное (36). Лемма доказана.

Предположим теперь, что Y является элементарной абелевой 2-группой. В этом случае для любого $a \in Y$ множество $G^{\perp} \stackrel{\text{def}}{=} \{0, a\}$ является двоичным групповым кодом. Применяя к этому коду неравенство (36), получим, что каждое регулярное РВ ω на группе Y удовлетворяет условию (33). Таким образом, справедлива следующая теорема.

Теорема 4. Пусть Y – элементарная абелева 2-группа. Тогда классы регулярных и положительно полуопределенных распределений вероятностей на группе Y совпадают.

Список литературы:

1. *Wyner A.D.* The Wire-Tap Channel // Bell System Techn. J. – 1975. – V. 54. – № 8. – P. 1355-1388.
2. *Massey J.L.* An Introduction to Contemporary Cryptology // Proc. IEEE. – 1988. – V. 76. - № 5. – P. 533-549.
3. *Штарьков Ю.М.* Некоторые теоретико-информационные задачи защиты дискретных данных // Проблемы передачи информации. – 1994. – Т. 30. – В. 2. – С. 49-60.
4. *Goldwasser S., Micali S.* Probabilistic encryption // J. of Computer and System Sciences.– 1984. – V. 28. – P. 270-299.
5. *Алексейчук А.Н.* Математическая модель и задачи анализа стойкости вероятностно-криптографических систем в системах защиты информации // Захист інформації. – 2001. – № 3. – С. 5-12.
6. *Maurer U. M.* Provable Security in Cryptography: Diss. ETH № 9260. – 1990. – 120 p.
7. *Иванов В.А.* Автоматные преобразования случайных последовательностей // Труды по дискретной математике (под ред. В. Я. Козлова и др.). – М.: ТВП, 1998. – Т. 2. – С. 151-168.
8. *Иванов В.А.* О методе случайного кодирования // Дискретная математика. – 1999. – Т. 11. – В. 3. – С. 99-108.
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. *Алексейчук А.Н., Кривоножко Г.Е.* Оптимальная схема декодирования сообщений безызбыточного источника в групповых вероятностно-криптографических системах // Збірник наукових праць ІПМЕ НАН України. – К.: 2001. – В. 14. – С. 26-33.
11. *Коржик В.И., Яковлев В.А.* Неасимптотические оценки кодового зашумления одного канала // Проблемы передачи информации. – 1981.– Т. 17. – В. 4. – С. 11-18.
12. *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.
13. *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2 т. / Пер. с англ. – М.: Мир, 1988. – 818 с.
14. *Дельсарт Ф.* Алгебраический подход к схемам отношений теории кодирования. – М.: Мир, 1976. – 134 с.
15. *Логачев А.О., Сальников А.А., Ященко В.В.* Бент-функции на конечной абелевой группе // Дискретная математика. – 1997. – Т. 9. – В. 4. – С. 3-20.
16. *Гантмахер Ф.Р.* Теория матриц. – М.: Наука, 1966. – 576 с.
17. *Ошкин И.Б., Проскурин Г.В.* Нижние оценки различения подмножеств единичного куба // Проблемы передачи информации. – 1994. – Т. 30. – В. 3. – С. 15-22.