

10. Корченко А.Г., Рындюк В.А., Мелешко Е.А., Пацера Е.В. Исследование нечетких операций для применения в системах защиты информации // Матеріали V Міжнародн. науково-практичної конф. "Безпека інформації в інформаційно-телекомунікаційних системах". - К.: Видавництво "Інтерлінк", НДЦ "ТЕЗІС" НТУУ "КПІ", 2002. - С. 56.

11. Корченко А.Г. Методы и аппаратные средства реализации нечетких операций // Автоматизированные системы обработки информации: Сб. науч. трудов. – К.: КМУГА, 1996. – С. 17-25.

12. Корченко А.Г., Рындюк В.А., Пацера Е.В. Классификация нечетких чисел для рационального применения в методах и моделях систем защиты информации // Матеріали V Міжнародн. науково-практичної конф. "Безпека інформації в інформаційно-телекомунікаційних системах". - К.: Видавництво "Інтерлінк", НДЦ "ТЕЗІС" НТУУ "КПІ", 2002. - С. 57.

13. Алтунин А.Е., Семухин М.В. Модели и алгоритмы принятия решений в нечетких условиях: Монография. Тюмень: Издательство Тюменского государственного университета, 2000. 352 с.

14. Ротштейн А.П., Штовба С.Д. Нечеткая надежность алгоритмических процессов. – Винница: Континент – ПРИМ, 1997. – 142 с.

15. Борисов А.Н., Крумберг О.А., И.П. Федоров. Принятие решений на основе нечетких моделей. Примеры использования. Рига: Зинатне, 1990 г.

16. Борисов А.Н., Алексеев А.В., Меркурьева Г.В. и др. Обработка нечеткой информации в системах принятия решений.. - М.: Радио и связь, 1989. – 304 с.

Поступила 20.07.2002
После доработки 11.09.2002

УДК 621.391:519.2

Алексейчук А. Н.

ОПТИМАЛЬНОЕ СЛУЧАЙНОЕ КОДИРОВАНИЕ РАВНОВЕРОЯТНЫХ СООБЩЕНИЙ В Q-ИЧНОМ СИММЕТРИЧНОМ КАНАЛЕ СВЯЗИ

Настоящая статья является непосредственным продолжением работ автора [1, 2], посвященных исследованию вероятностных характеристик систем передачи дискретной информации со случайным кодированием в канале связи с аддитивным шумом, распределенным на конечной абелевой группе. Ранее теоретико-информационные свойства и способы построения таких систем для случая двоичного симметричного канала (ДСК) изучались в [3 – 11] и ряде других работ.

Далее в статье свободно используются терминология и обозначения, введенные в [2]. Рассматриваемая нами математическая модель системы передачи информации со случайным кодированием представляет собой вероятностно-криптографическую систему (ВКС) $\mathfrak{R} = (S, \sigma, W)$, состоящую из источника (S, P_S) , где S – конечное множество P_S – равномерное распределение вероятностей (РВ) на S , отображения $\sigma: Y \rightarrow S$ и стохастической матрицы

(канала) $W = \left\| W\left(\frac{y}{x}\right) \right\|_{x, y \in Y}$, удовлетворяющих следующим условиям:

- (а) S и Y – конечные абелевы группы;
- (б) σ – равновероятная функция из Y в S ,

$$|\sigma^{-1}(s)| = |Y| |S|^{-1}, s \in S; \quad (1)$$

(в) W – канал с аддитивным шумом, распределенным на группе Y ,

$$W(y/x) = \omega(y - x), \quad x, y \in Y, \quad (2)$$

где $\omega = (\omega(y): y \in Y)$ – распределение вероятностей на Y .

Отображению σ соответствует случайное кодирование источника, при котором сигнал $x \in Y$, используемый для передачи данного сообщения $s \in S$, выбирается случайно и равновероятно во множестве $\sigma^{-1}(s)$. При передаче по каналу связи W сообщение x искажается в канале и преобразуется с вероятностью $W(y/x)$ в выходное сообщение $y \in Y$.

Эффективность рассматриваемого способа случайного кодирования информации характеризуется вероятностью $\pi(\sigma, \delta) = \mathbf{P}\{\delta(y) = s\}$ правильного приема сообщений в канале W ВКС \mathfrak{R} с помощью данного декодера (отображения) $\delta: Y \rightarrow S$. Для вероятности $\pi(\sigma, \delta^*)$ правильного приема сообщений оптимальным декодером δ^* (таким, что $\pi(\sigma, \delta^*) \geq \pi(\sigma, \delta)$ для любого $\delta: Y \rightarrow S$ [10]) используется обозначение $\pi^*(\sigma)$. При $\delta = \sigma$ вероятность $\pi(\sigma, \sigma)$ обозначается через $\pi(\sigma)$.

В [2] получены следующие выражения вероятности правильного декодирования сообщений в произвольном канале W вида (2):

$$\pi(\sigma, \delta) = Q^{-1} \sum_{s \in S} \sum_{x, y \in Y} \omega(y - x) I_{\sigma, s}(x) I_{\delta, s}(y), \quad (3)$$

$$\pi(\sigma, \delta) = Q^{-2} \sum_{s \in S} \sum_{a \in Y} \hat{\omega}(a) I_{\sigma, s}^{\wedge}(a) \overline{I_{\delta, s}^{\wedge}(a)}, \quad (4)$$

где $Q = |Y|$, $I_{\sigma, s}, I_{\delta, s}$ – индикаторы множеств $\sigma^{-1}(s), \delta^{-1}(s)$ соответственно, $s \in S$, $\hat{\omega}, I_{\sigma, s}^{\wedge}, I_{\delta, s}^{\wedge}$ – преобразования Фурье указанных функций. В случае, когда ω является положительно определенным распределением вероятностей (удовлетворяет условию $\hat{\omega}(a) > 0, a \in Y$), установлены точные границы вероятности $\pi(\sigma)$ и показано, что оптимальный декодер δ^* ВКС $\mathfrak{R} = (S, \sigma, W)$ совпадает с отображением σ , если последнее является эпиморфизмом групп.

Настоящая статья посвящена более подробному исследованию вероятностных характеристик эффективности случайного кодирования в практически важном частном случае, когда W является q -ичным симметричным каналом связи с входным алфавитом F , где F – произвольная абелева группа порядка q и $Y = F^n$. Основным результатом состоит в получении нижней границы вероятности $\pi^*(\sigma)$, $\sigma: F^n \rightarrow S$ и обосновании условий, гарантирующих оптимальность (по критерию минимума $\pi^*(\sigma)$) случайного кодирования, определяемого отображением σ , в q -ичном симметричном канале с данным входным алфавитом F . В частности, с использованием полученной границы вероятности $\pi^*(\sigma)$ доказана оптимальность в классе всех равновероятных отображений $\sigma: \mathbf{GF}(q)^n \rightarrow \mathbf{GF}(q)^k, n = \frac{q^k - 1}{q - 1}, k = 2, 3, \dots$ систем с равномерным случайным кодированием, построенных на

основе q -ичных кодов Хэмминга. Ранее была установлена лишь оптимальность двоичных кодов Хэмминга в классе систем с линейным случайным кодированием в ДСК [4].

Представим выражения (3), (4) в более удобном для последующего анализа виде. Для любых $\sigma, \delta: Y \rightarrow S$ определим отображения $K_{\sigma,\delta}, D_{\sigma,\delta}: Y \rightarrow S$, полагая

$$K_{\sigma,\delta}(a) = Q^{-1} \sum_{s \in S} \#\{(x, y) \in Y^2 : \sigma(x) = \delta(y) = s, x - y = a\}, a \in Y, \quad (5)$$

$$D_{\sigma,\delta}(a) = Q^{-2} \sum_{s \in S} I_{\sigma,s}^{\wedge}(a) I_{\delta,s}^{\wedge}(a), a \in Y, \quad (6)$$

где символ $\#M$ обозначает мощность произвольного конечного множества M .

На основании (3) – (6) справедливы следующие равенства:

$$\pi(\sigma; \delta) = \sum_{a \in Y} \omega(-a) K_{\sigma,\delta}(a) = \sum_{a \in Y} \omega(a) D_{\sigma,\delta}(a). \quad (7)$$

При этом преобразование Фурье функции $K_{\sigma,\delta}$ имеет вид

$$\widehat{K}_{\sigma,\delta}(a) = Q D_{\sigma,\delta}(a), a \in Y, \quad (8)$$

На протяжении всего дальнейшего изложения предполагается, что W является q -ичным симметричным каналом связи,

$$\omega(a) = x(\Delta)^{n-\|a\|} y(\Delta)^{\|a\|}, a \in Y = F^n, \quad (9)$$

где $x(\Delta) = q^{-1}(1 + (q-1)\Delta)$, $y(\Delta) = q^{-1}(1 - \Delta)$, $\Delta \in [0, 1]$, F – абелева группа порядка $q > 1$, $\|a\|$ – вес Хэмминга вектора $a \in F^n$.

Используя (9), находим

$$\widehat{\omega}(a) = \Delta^{\|a\|}, a \in F^n; \quad (10)$$

таким образом, равенство (7) может быть записано в следующем виде:

$$\pi(\sigma; \delta) = \sum_{i=0}^n A_i(K_{\sigma,\delta}) x(\Delta)^{n-i} y(\Delta)^i = \sum_{i=0}^n A_i(D_{\sigma,\delta}) \Delta^i, \quad (11)$$

где

$$A_i(K_{\sigma,\delta}) = \sum_{\substack{a \in F^n \\ \|a\|=i}} K_{\sigma,\delta}(a), A_i(D_{\sigma,\delta}) = \sum_{\substack{a \in F^n \\ \|a\|=i}} D_{\sigma,\delta}(a), i \in \overline{0, n}. \quad (12)$$

Отметим, что упорядоченные наборы чисел $(A_i(K_{\sigma,\delta}): i \in \overline{0,n})$ и $(A_i(D_{\sigma,\delta}): i \in \overline{0,n})$ представляют собой весовые спектры отображений $K_{\sigma,\delta}$ и $D_{\sigma,\delta}$ соответственно, а равенство (11) является классическим тождеством Мак-Вильямс для весовых функций Хэмминга отображения $K_{\sigma,\delta}$ и его преобразования Фурье (см. (8)) [12, 13].

Установим ряд простейших свойств чисел (12). В дальнейшем будем писать K_σ, D_σ вместо $K_{\sigma,\sigma}, D_{\sigma,\sigma}$ соответственно.

Лемма 1. Для любой равновероятной функции $\sigma: Y \rightarrow S$ и произвольного декодера $\delta: Y \rightarrow S$ справедливы следующие соотношения:

(а) $A_i(K_{\sigma,\delta}) \geq 0, i \in \overline{0,n};$

(б) $A_i(D_\sigma) \geq 0, i \in \overline{0,n};$

(в) $K_{\sigma,\delta}(0) = \sum_{i=0}^n A_i(D_{\sigma,\delta}) \leq 1,$

причем равенство имеет место в том и только том случае, когда $\delta = \sigma;$

(г) $D_{\sigma,\delta}(0) = Q^{-1} \sum_{i=0}^n A_i(K_{\sigma,\delta}) = |S|^{-1}.$

Доказательство. Утверждение (а) непосредственно следует из (5) и (12). Для доказательства (б) достаточно заметить, что в силу (6)

$$D_\sigma(a) = Q^{-2} \sum_{s \in S} \left| I_{\sigma,s}^\wedge(a) \right|^2 \geq 0, a \in Y. \tag{13}$$

Докажем неравенство (в). На основании (8) имеем

$$K_{\sigma,\delta}(0) = Q^{-1} \sum_{a \in Y} K_{\sigma,\delta}^\wedge(a) = \sum_{a \in Y} D_{\sigma,\delta}(a) = \sum_{i=0}^n A_i(D_{\sigma,\delta}).$$

Далее, в силу (5)

$$K_{\sigma,\delta}(0) = Q^{-1} \sum_{s \in S} \# \{x \in Y : \sigma(x) = \delta(x) = s\} \leq Q^{-1} \sum_{s \in S} |\sigma^{-1}(s)| = 1,$$

причем последнее неравенство обращается в равенство тогда и только тогда, когда $\delta = \sigma.$

Докажем соотношения (г). В силу (8)

$$Q^{-1} \sum_{i=0}^n A_i(K_{\sigma,\delta}) = Q^{-1} \sum_{a \in Y} K_{\sigma,\delta}(a) = Q^{-1} K_{\sigma,\delta}^\wedge(0) = D_{\sigma,\delta}(0).$$

Таким образом, остается убедиться в справедливости равенства

$$D_{\sigma,\delta}(0) = |S|^{-1}. \quad (14)$$

Заметим, что поскольку для любого $s \in S$

$$I_{\sigma,s}^{\wedge}(0) = \sum_{x \in Y} I_{\sigma,s}(x) = |\sigma^{-1}(s)|, \quad I_{\delta,s}^{\wedge}(0) = \sum_{x \in Y} I_{\delta,s}(x) = |\delta^{-1}(s)|,$$

то на основании (6) и равновероятности функции σ

$$D_{\sigma,\delta}(0) = Q^{-2} \sum_{s \in S} |\sigma^{-1}(s)| |\delta^{-1}(s)| = Q^{-2} \frac{Q}{|S|} \sum_{s \in S} |\delta^{-1}(s)| = |S|^{-1},$$

что и требовалось доказать.

Лемма 2. Для любой равновероятной функции σ справедливо неравенство

$$\sum_{i=1}^n i A_i(D_{\sigma}) \leq \frac{q-1}{q} n. \quad (15)$$

Доказательство. Дифференцируя обе части равенства (11) по Δ и полагая в полученном выражении $\Delta = 1$, получим следующую цепочку соотношений:

$$\begin{aligned} \sum_{i=1}^n i A_i(D_{\sigma}) \Delta^{i-1} \Big|_{\Delta=1} &= \sum_{i=0}^n A_i(K_{\sigma}) ((n-i) \frac{q-1}{q} x(\Delta)^{n-i-1} y(\Delta)^i - \\ & q^{-1} i x(\Delta)^{n-i} y(\Delta)^{i-1}) \Big|_{\Delta=1} = A_0(K_{\sigma}) \frac{q-1}{q} n - q^{-1} A_1(K_{\sigma}) \leq \frac{q-1}{q} n \end{aligned}$$

(последнее неравенство вытекает из утверждений (а) и (в) леммы 1). Итак, имеет место (15), что и требовалось доказать.

Получим оценки вероятности $\pi(\sigma)$ правильного приема сообщений (с помощью декодера $\delta = \sigma$) в канале W вида (9). Предварительно определим понятие коэффициента защищенности информации в вероятностно-криптографической системе с q -ичным симметричным каналом, обобщающее аналогичное понятие, введенное в [10] для случайного кодирования в ДСК. А именно, назовем коэффициентом защищенности информации в ВКС $\mathfrak{R} = (S, \sigma, W)$ с каналом W вида (9) число

$$d(\sigma) = \min\{i \in \overline{1, n} : A_i(D_{\sigma}) > 0\}. \quad (16)$$

Отметим, что в силу (11), (13) параметр $d(\sigma)$ корректно определен выражением (16).

Следующая теорема, обобщающая один из результатов, полученных в [11] для систем с линейным случайным кодированием в двоичном симметричном канале, устанавливает границы вероятности $\pi(\sigma)$, зависящие явным образом от характеристик отображения $\sigma: F^n \rightarrow S$.

Теорема 1. Для любой равновероятной функции σ имеют место неравенства

$$|S|^{-1} (1 + (|S| - 1)\Delta^f) \leq \pi(\sigma) \leq |S|^{-1} (1 + (|S| - 1)\Delta^{d(\sigma)}), \quad (17)$$

где

$$f = \frac{q-1}{q} n \frac{|S|}{|S|-1}. \quad (18)$$

Доказательство. В силу равенства (11) и утверждений (б) – (г) леммы 1 справедливы соотношения

$$\pi(\sigma) = \frac{1}{|S|} + \sum_{i=d(\sigma)}^n A_i(D_\sigma) \Delta^i \leq \frac{1}{|S|} + \Delta^{d(\sigma)} \sum_{i=1}^n A_i(D_\sigma) = \frac{1}{|S|} + \Delta^{d(\sigma)} \left(1 - \frac{1}{|S|}\right),$$

из которых вытекает верхняя оценка (17). Далее, в силу выпуклости вниз функции $\exp_{\Delta}(x) = \Delta^x$, $x \in (-\infty, \infty)$, утверждений (б), (в) леммы 1 и неравенства (15) имеют место следующие соотношения:

$$\pi(\sigma) \geq \frac{1}{|S|} + \frac{|S|-1}{|S|} \exp_{\Delta} \left(\sum_{i=1}^n i A_i(D_\sigma) \frac{|S|}{|S|-1} \right) \geq \frac{1}{|S|} + \frac{|S|-1}{|S|} \exp_{\Delta} \left(\frac{q-1}{q} n \frac{|S|}{|S|-1} \right) = |S|^{-1} (1 + (|S| - 1)\Delta^f). \quad (19)$$

Итак, неравенства (17) полностью доказаны.

Следствие 1. Для любой равновероятной функции σ коэффициент $d(\sigma)$ защищенности информации в ВКС $\mathfrak{R} = (S, \sigma, W)$ удовлетворяет неравенству

$$d(\sigma) \leq f, \quad (20)$$

которое обращается в равенство в том и только том случае, когда достигается нижняя граница (17).

Доказательство. Если $d(\sigma) = f$, то равенство

$$\pi(\sigma) = |S|^{-1} (1 + (|S| - 1)\Delta^f) \quad (21)$$

имеет место в силу (17). Пусть теперь выполняется (21). Тогда на основании (19) достигается верхняя граница (15)

$$\sum_{i=1}^n i A_i(D_\sigma) = \frac{q-1}{q} n. \quad (22)$$

Далее, в силу строгой выпуклости функции $\exp_{\Delta}(x)$, $x \in (-\infty, \infty)$, все числа $A_i(D_{\sigma})$, $i \in \overline{1, n}$ равны нулю, за исключением $A_{d(\sigma)}(D_{\sigma}) = \frac{|S| - 1}{|S|}$ (см. (16), утверждения (в) и (г) леммы 1).

Итак, имеют место соотношения

$$A_{d(\sigma)}(D_{\sigma}) = \frac{|S| - 1}{|S|}, A_i(D_{\sigma}) = 0, i \neq d(\sigma). \quad (23)$$

На основании (22), (23) получаем

$$d(\sigma) A_{d(\sigma)}(D_{\sigma}) = \frac{q - 1}{q} n, d(\sigma) = f,$$

что и требовалось доказать.

Следуя [10], назовем случайное кодирование, определяемое равновероятной функцией $\sigma^*: F^n \rightarrow S$, оптимальным случайным кодированием q -ичного симметричного канала (9), если для любой равновероятной функции $\sigma: F^n \rightarrow S$ выполняется неравенство

$$\pi^*(\sigma^*) \leq \pi^*(\sigma). \quad (24)$$

Достаточное условие оптимальности случайного кодирования в классе всех равновероятных отображений группы F^n в группу S содержит следующая теорема.

Теорема 2. Пусть $\sigma^*: F^n \rightarrow S$ – равновероятная функция, удовлетворяющая условию $d(\sigma^*) = f$. Тогда случайное кодирование, определяемое этой функцией, является оптимальным. При этом оптимальный декодер δ^* ВКС $\mathfrak{R}^* = (S, \sigma^*, W)$ совпадает с σ^* .

Доказательство. Пусть $\sigma: F^n \rightarrow S$ – произвольная равновероятная функция. На основании утверждений теоремы 1, следствия 1 и определения оптимального декодера имеют место неравенства

$$\pi(\sigma^*) = |S|^{-1} (1 + (|S| - 1)\Delta^f) \leq \pi(\sigma) \leq \pi^*(\sigma). \quad (25)$$

Покажем, что декодер δ^* ВКС \mathfrak{R}^* совпадает с функцией σ^* (и, следовательно, $\pi(\sigma^*) = \pi^*(\sigma^*)$). Тогда неравенство (24) непосредственно следует из соотношений (25).

Заметим, что в силу соотношений (6) и (13) для любой равновероятной функции $\theta: F^n \rightarrow S$ справедливо следующее утверждение: если $D_{\theta}(a) = 0$, где $a \in Y$, то для любого $\delta: F^n \rightarrow S$ $D_{\theta, \delta}(a) = 0$. Полагая $\theta = \sigma^*$, $\delta = \delta^*$, на основании (23) получаем

$$A_i(D_{\sigma^*, \delta^*}) = 0, i \neq f. \quad (26)$$

Отсюда, используя равенство (11) и утверждения (в), (г) леммы 1, находим

$$\pi^*(\sigma^*) = \sum_{i=0}^n A_i(D_{\sigma^*, \delta^*}) \Delta^i = \frac{1}{|S|} + \Delta^f \sum_{i=1}^n A_i(D_{\sigma^*, \delta^*}) \leq \frac{1}{|S|} + \Delta^f (1 - \frac{1}{|S|}) = \pi(\sigma^*).$$

Итак, $\pi^*(\sigma^*) = \pi(\sigma^*)$, что и требовалось доказать.

Получим более подробное описание групповых вероятностно-криптографических систем [2], удовлетворяющих условиям теоремы 2.

Пусть отображение $\sigma: F^n \rightarrow S$ является эпиморфизмом группы F^n в группу S . Обозначим $G = \{y \in Y: \sigma(y) = 0\}$ ядро гомоморфизма σ , G^\perp – группу, дуальную к G [13]. В силу изоморфизма $S \cong F^n/G$ соответствующее σ случайное кодирование вполне определяется подгруппой G группы F^n (групповым кодом длины n над абелевой группой F [13]). Следуя терминологии [5], назовем указанное кодирование случайным кодированием источника (S, P_S) групповым кодом G (в q -ичном симметричном канале W).

Согласно [2], вероятность правильного приема сообщений в канале W равна

$$\pi^*(\sigma) = \sum_{a \in G} \omega(\hat{a}) = |S|^{-1} \sum_{a \in G^\perp} \hat{\omega}(a). \quad (27)$$

Сравнивая (27) и (7), с учетом (9), (10) получаем

$$A_i(D_\sigma) = \#\{a \in G^\perp : \|a\| = i\}, \quad i \in \overline{0, n}.$$

В частности, коэффициент защищенности информации в системе со случайным кодированием групповым кодом G совпадает с минимальным расстоянием дуального кода G^\perp (для двоичных линейных кодов это утверждение доказано в [10])

$$d(\sigma) = \min\{\|a\| : a \in G^\perp \setminus 0\}. \quad (28)$$

Неравенство (20) в данном случае устанавливает верхнюю границу минимального расстояния (в метрике Хэмминга) группового кода $G^\perp \subseteq F^n$ мощности $|G^\perp| = |S|$, известную (при $F = (\mathbf{GF}(q), +)$) как граница Плоткина [14].

На основании полученных выше результатов справедливо следующее утверждение.

Следствие 2. Если для данных абелевых групп F, S и натурального n существует групповой код $K \subseteq F^n$ мощности $|S|$ с минимальным расстоянием

$$d_K = f = \frac{q-1}{q} n \frac{|S|}{|S|-1}, \quad (29)$$

то оптимальным случайным кодированием, определяемым эпиморфизмом групп $\sigma: F^n \rightarrow S$, является случайное кодирование групповым кодом $G = K^\perp$ и только оно.

Итак, для построения оптимального случайного кодирования сообщений в q -ичном симметричном канале (9) достаточно найти групповой код $K \subseteq F^n$, удовлетворяющий условию (29), и положить отображение σ , определяющее способ случайного кодирования, равным каноническому эпиморфизму группы F^n в факторгруппу $F^n/K^\perp \cong S$.

Отметим, что в силу (28) групповой код $K \subseteq F^n$, достигающий границы (29), является эквидистантным, то есть содержит ненулевые кодовые слова одинакового веса d_K . Хорошо известным примером такого кода служит q -ичный симплексный код \mathfrak{Q}_k , дуальный к коду

Хэмминга с параметрами $n = \frac{q^k - 1}{q - 1}$, $n - k$ ($k = 2, 3, \dots$) над полем $\mathbf{GF}(q)$ [12]. (Поскольку

столбцами порождающей матрицы кода \mathfrak{Q}_k являются все ненулевые векторы $x \in \mathbf{GF}(q)^k$, первая отличная от нуля координата которых равна 1 [12], то вес ненулевых слов кода \mathfrak{Q}_k

равен q^{k-1} , и этот код достигает верхней границы Плоткина (29)). Таким образом, при указанных значениях k и n случайное кодирование q -ичным кодом Хэмминга является оптимальным в классе всех равновероятных отображений группы $F^n = (\mathbf{GF}(q)^n, +)$ группу $S = (\mathbf{GF}(q)^k, +)$. Отметим, что в [4] фактически доказана оптимальность двоичных кодов Хэмминга (по критерию минимума вероятности правильного приема сообщений) в классе линейных кодов с параметрами $(2^k - 1, 2^k - k - 1)$.

Приведем еще один пример группового кода K , удовлетворяющего условиям следствия 2. Пусть F – произвольная абелева группа порядка q , $\alpha_1, \dots, \alpha_n$ – произвольные автоморфизмы группы F . Рассмотрим множество

$$K = \{(\alpha_1(r), \dots, \alpha_n(r)) : r \in F\}. \quad (30)$$

Очевидно, что $K \subseteq F^n$ есть групповой код мощности q , и для любого ненулевого вектора $x \in K$ выполняется равенство $\|x\| = n$. Следовательно, K имеет минимальное расстояние $d_K = n$, и равенство (29) выполняется при $S = F$.

Вопрос о полном описании равновероятных отображений $\sigma: F^n \rightarrow S$, удовлетворяющих условию $d(\sigma) = f$, остается в настоящее время открытым.

1. *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.
2. *Алексейчук А.Н.* Случайное кодирование в канале связи с аддитивным шумом, распределенным на конечной абелевой группе // Захист інформації. – 2002. – № 3. – С. - .
3. *Wyner A.D.* The Wire-Tap Channel // Bell System Techn. J. – 1975. – V. 54. – № 8. – P. 1355-1388.
4. *Коржик В.И., Яковлев В.А.* Неасимптотические оценки кодового зашумления одного канала // Проблемы передачи информации. – 1981. – Т. 17. – В. 4. – С. 11-18.
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. *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. – С. 61-66.
7. *Горицкий В.М.* Вероятностная криптография в системах защиты информации: кодовая защита // Электроника и связь. – 1998. – В. 5. – С. 140-145.
8. *Горицкий В.М.* К оценке эффективности концепции WTC кодами Хэмминга для решения задач защиты заранее известных последовательностей // Защита информации: сборник научных трудов Национального авиационного ун-та. – К.: КМУГА, 1999. – С. 73-75.
9. *Яковлев В.А.* Границы для оценки неопределенности в системе передачи со случайным кодированием // Радиотехника. – 1996. – № 12. – С. 58-63.
10. *Иванов В.А.* О методе случайного кодирования // Дискретная математика. – 1999. – Т. 11. – В. 3. – С. 99-108.
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. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки: Пер. с англ. – М.: Связь, 1979. – 743 с.
13. *Дельсарт Ф.* Алгебраический подход к схемам отношений теории кодирования. – М.: Мир, 1976. – 134 с.

14. Лидл Р., Нидеррайтер Г. Конечные поля: В 2 т. / Пер. с англ. – М.: Мир, 1988. – 818 с.

Поступила 20.03.2002

УДК 519.6:519.712.3:510.52:511.12

Богданов А.М., Зинченко Я.В.

УМНОЖЕНИЕ СВЕРХБОЛЬШИХ ЧИСЕЛ И БЫСТРОЕ ПРЕОБРАЗОВАНИЕ ХААРА

В настоящее время в некоторых алгоритмах, которые применяются в асимметричных криптографических системах, при зашифровании, расшифровании и выполнении вспомогательной задачи по формированию ключей используется операция возведения в степень по модулю простого числа или произведения простых чисел, т.е. вычисление выражений вида:

$$a = b^z \pmod{k}. \quad (1)$$

Например, в системе RSA зашифрование сводится к вычислению:

$$c = m^e \pmod{n}, \quad (2)$$

где c – зашифрованное сообщение, m – открытое сообщение, e – ключ зашифрования и $n = p \cdot q$ – модуль. Расшифрование, соответственно, сводится к вычислению:

$$m = c^d \pmod{n}, \quad (3)$$

где d – ключ расшифрования.

В системе экспоненциального ключевого обмена открытый ключ формируется по правилу:

$$Y = \alpha^x \pmod{q}, \quad (4)$$

где Y – открытый ключ, α – фиксированный примитивный элемент поля $GF(q)$, x – ключ зашифрования и q – модуль.

При выполнении операции модулярного возведения в степень на универсальных ЭВМ требуется большое количество вычислений (в соотношениях (1)-(4) параметры представляют собой целые многоразрядные числа размерностью 512-4096 бит), поэтому асимметричные криптосистемы, в которых используется операция модулярного возведения в степень, несмотря на все свои достоинства, не являются эффективными с точки зрения скоростных характеристик при зашифровании и расшифровании сообщений большой длины. Так, например, быстродействие программной реализации RSA примерно в 100 раз ниже, чем быстродействие программной реализации DES. Кроме того, последние достижения в теории криптоанализа асимметричных алгоритмов (дискретное логарифмирование в конечных полях и факторизация больших чисел) заставляют разработчиков увеличивать размерности параметров систем, что еще больше снижает скорость их работы [1].

Учитывая вышесказанное, существует необходимость в выделении ряда методов и приемов, которые позволили бы минимизировать количество вычислений при выполнении модулярного возведения в степень и тем самым увеличить скорость работы асимметричных криптосистем.

Рассмотрим пример вычисления модулярной экспоненты Y в соотношении (4).

Пусть $x = 9$, тогда: