УДК 681.3

НЕЛИНЕЙНЫЕ ПОМЕХОУСТОЙЧИВЫЕ КОДЫ НА ОСНОВЕ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Д.М. БИЛЬДЮК, С.Б. САЛОМАТИН

[1]*Белорусский государственный университет информатики и радиоэлектроники*
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
radno@bsuir.by

Рассматриваются криптографические помехоустойчивые коды на базе симметричных алгоритмов шифрования (DES, AES, ГОСТ 28147, СТБ 34.101.31). Произведен сравнительный анализ дистанционных свойств и характеристик декодирования данного класса кодов и двоичных кодов БЧХ.

Ключевые слова: криптографическое преобразование данных, помехоустойчивое кодирование, симметричные алгоритмы шифрования, границы помехоустойчивого кодирования, нелинейный код.

Двоичный помехоустойчивый криптографический код (R-код) с параметрами $(n, k, d_{\min})$ определяется как множество отображённых k-мерных векторов $\mathbf{a} = (a_0, a_1, \ldots, a_{k-1}) \in GF(2^k)$ в другое множество n-мерных векторов $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in GF(2^n)$, $k < n$, с минимальным расстоянием Хэмминга среди всех возможных пар кодовых слов – $d_{\min}$ [1]. Отображение реализуется на основе криптографического алгоритма $R_{m,n}$ с ключом шифрования $\mathbf{s} = (s_0, s_1, \ldots, s_{m-1}) \in GF(2^m)$, вектором избыточности $\mathbf{v} = (v_0, v_1, \ldots, v_{r-1}) \in GF(2^r)$, $r = n - k$, и задается функцией $\varphi(\mathbf{a}, \mathbf{s}, \mathbf{v}) : GF(2^k) \to GF(2^n)$ [1]:

$$\mathbf{c} \leftarrow \varphi(\mathbf{a}, \mathbf{s}, \mathbf{v}) : (\mathbf{a}, \mathbf{s}, \mathbf{v}) \to R_{m,n}(\mathbf{a} \mid \mathbf{v}, \mathbf{s}). \tag{1}$$

Параметры m и n (длина ключа шифрования и длина блока шифрования соответственно) в основном режиме (режиме электронной кодовой книги) криптографического преобразования могут принимать фиксированные значения [1]. Для формирования R-кода произвольной длины n необходимо использовать режимы криптографического преобразования с обратной связью длины в один бит, вектор инициализации $\mathbf{iv} = (iv_0, iv_1, \ldots, iv_{m-1}) \in GF(2^u)$, можно считать частью ключа. Тогда отображение задается функцией $\psi(\mathbf{a}, \mathbf{s}, \mathbf{v}, \mathbf{iv}) : GF(2^k) \to GF(2^n)$ [1]:

$$\begin{aligned}
&\mathbf{c} \leftarrow \psi(\mathbf{a}, \mathbf{s}, \mathbf{v}, \mathbf{iv}) : (\mathbf{a}, \mathbf{s}, \mathbf{v}, \mathbf{iv}) \to (\\
&\qquad \mathbf{o} \leftarrow \mathbf{iv};\ \mathbf{a'} \leftarrow \mathbf{a} \mid \mathbf{v};\\
&\qquad \mathbf{for}\ i\ \mathbf{from}\ 0\ \mathbf{to}\ n-1\ \mathbf{do}\\
&\qquad\qquad c_i \leftarrow \left(Rijndael_{m,u}(\mathbf{o}, \mathbf{s})\right)_{u-1} \oplus a'_i;\ \mathbf{o} \leftarrow (o_1, o_2, \ldots o_{u-1}, c_i);\\
&\qquad \mathbf{end\,do};\\
&\qquad \mathbf{return\,c};\ ).
\end{aligned} \tag{2}$$

Отображения при помощи функций (1) и (2) задают помехоустойчивый код с близкими дистанционными свойствами [2].

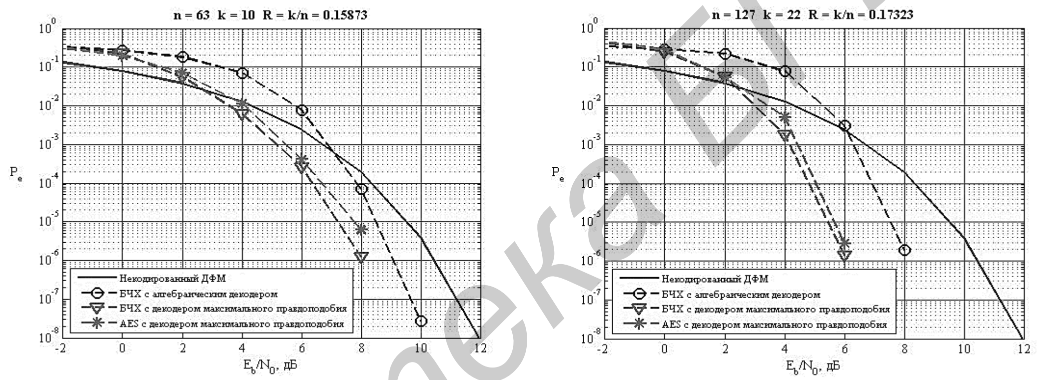
Сравнительный анализ эффективности корректирующих кодов R и БЧХ осуществляется с использованием вероятности ошибки на бит P_{eb} информационного слова **a** в зависимости от E_b / N_0 в канале с АБГШ [3] Параметры выбранных для сравнения кодов представлены в табл. 1.

Табл. 1. Параметры R и БЧХ кодов

n	7	15	15	15	31	31	31	31	63	63	63	63	63	127	127	127
k	4	5	7	11	6	11	16	21	7	10	16	18	24	8	15	22
$d_{\min}$ (БЧХ)	3	7	5	3	15	11	7	5	31	27	23	21	15	63	55	47
$d_{\min}$ (R)	2	4	2	1	8	3	1	1	19	15	9	7	2	44	32	20

Формирование R-кода осуществлялось с использованием функции (2), вектора избыточности **v** и инициализации **iv** использованы с координатами равными нулю. Вектор **s** – случайный.

Примеры результатов моделирования для табл. 1 представлены на рис. 1.



а *б*

Рис. 1. Примеры результатов моделирования с использованием R и БЧХ кодов с параметрами (63,10) (*а*) и (127,22) (*б*)

Представленные результаты показывают, что:

– ДМП осуществляет декодирование за границей корректирующей способности помехоустойчивого кода;

– существуют R-коды с зависимостью P_{eb} от отношения E_b / N_0 близкой к зависимости БЧХ-кодов при одинаковых параметрах (n,k), в случае использования ДМП (заметим, что $d_{\min}$ R-кода меньше чем у БЧХ-кода – см. табл. 1).

Список литературы

1. *Бильдюк Д.М., Саломатин С.Б.* // Декодирование нелинейного помехоустойчивого кода на базе криптографического алгоритма rijndael, Доклады БГУИР №8(70), 2012 – с.75-80.

2. *Фомичев В.М.* // Дискретная математика и криптология. Курс лекций / Под общ. ред. д-ра физ.-мат. н. Н. Д. Подуфалова. – М.: ДИАЛОГ-МИФИ, 2003.

3. *MacWilliams F.J., Sloane N.J.A.* // The Theory of Error- Correcting Codes. North-Holland, 1977.