состояний генератора, является величина λ_f^*, определяемая по формуле (6). Увеличение значений этой величины (при замене функции усложнения или блока управления движением ГГ) приводит к экспоненциальному уменьшению верхней границы средней вероятности ошибки оптимального критерия различения состояний ГГ в описанной вероятностной модели. Минимум значений λ_f^* по всей совокупности равновероятных булевых функций n переменных достигается на линейной функции $f_0(z_1, ..., z_n) = z_1 \oplus ... \oplus z_n$ и определяется по формуле (8).

Получена аналитическая граница надежности практически реализуемой корреляционной атаки на комбинирующий ГГ с неравномерным движением и линейной функцией усложнения, функционирующий в режиме реинициализации начального состояния (см. формулу (34)). Указанная атака аналогична первому этапу алгоритма корреляционного криптоанализа шифра A5/1 [7] и отличается от него лишь процедурой проверки соответствующих статистических гипотез. Получена также верхняя оценка объема материала, достаточного для успешного проведения описанной корреляционной атаки с заданной надежностью (см. формулу (35).

Моделирование на ЭВМ изложенных алгоритмов криптоанализа комбинирующих ГГ с неравномерным движением и проверка корректности применения полученных теоретических выводов к реальным ГГ составляют задачи дальнейших исследований авторов.

Литература: ***1.*** *Фомичев В. М. Дискретная математика и криптология. – М.: ДИАЛОГ-МИФИ, 2003. – 400 с.* ***2.*** *Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002.* ***3.*** *Meneses A., van Oorschot P., Vanderstone S. Handbook of applied cryptography. – CRC Press, 1997.* ***4.*** *Ekdahl P. On LFSR-based stream cipher: analysis and design. – Ph. D. Th., 2003.* ***5.*** *Kholosha A. A. Clock-controlled shift registers for key-stream generation. // http://eprint.iacr.org/2001/061.* ***6.*** *Gollman D., Chambers W. G. Clock-controlled shift registers: a review // IEEE J. on Selected Areas in Communication. – 1989. – V. 7. – № 4. – P. 525 – 533.* ***7.*** *Ekdahl P., Johansson T. Another attack on A5/1 // IEEE Trans. on Inform. Theory. – 2003. – Vol. 49. – P. 1 – 7.* ***8.*** *Armknecht F., Lano J., Preenel B. Extending the resynchronizating attack // http://eprint.iacr.org./2004/232.* ***9.*** *Боровков А. А. Математическая статистика. – М.: Наука., 1984. – 472 с.* ***10.*** *Сачков В. Н. Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982. – 384 с.* ***11.*** *Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. – 470 с.* ***12.*** *Ширяев А. Н. Вероятность. – М.: Наука, 1989. – 638 с.*

УДК 621.391:519.2

АЛГОРИТМЫ НЕЛИНЕЙНОГО СЛУЧАЙНОГО КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ СООБЩЕНИЙ Z_4-ЛИНЕЙНЫМИ КОДАМИ В МОДЕЛИ WIRE-TAP CHANNEL

Антон Алексейчук, Сергей Гришаков
СФ СБ Украины в составе ВИТИ НТУУ "КПИ"

Аннотация: **Рассматривается модель системы передачи информации по каналу связи с отводом, состоящая из бесшумного основного канала и двоичного симметричного отводного канала. Для данной модели предложены практически реализуемые алгоритмы случайного кодирования и декодирования сообщений двоичными нелинейными кодами, соответствующими линейным кодам над кольцом вычетов по модулю 4 при отображении Грея. Показано, что предложенные алгоритмы имеют не более чем квадратичные от длины используемого кода временную и емкостную сложности.**

Summary: **It is considering the model of information transmission system with the wiretap, which consists of the noiseless main channel and binary symmetrical wiretap channel. Practically realizable algorithms of the random messages coding and decoding by binary non-linear codes, which correspond to linear codes over the residue ring modulo 4 by Gray mapping are proposed for this model. It is shown that proposed algorithms have no more than quadratic time and space complexities from the length of using code.**

Ключевые слова: **Криптографическая защита информации, безусловно стойкий протокол согласования ключей, отводной канал, случайное кодирование, четверичный линейный код.**

I Введение

Одним из перспективных направлений современной криптографии, получивших заметное развитие за последние 10 – 15 лет, является синтез безусловно стойких криптографических протоколов согласования ключей по открытым каналам связи [1 – 5]. Для постановки, формализации и решения задач построения и анализа криптографических свойств таких протоколов традиционно используется математическая модель системы передачи информации по каналу связи с отводом (wire-tap channel) [6]. Известным общим методом повышения стойкости защиты информации в этой модели является случайное кодирование источника, при котором для передачи информационных сообщений по открытому каналу связи используются случайные сигналы, выбираемые в соответствии с заданным законом распределения из некоторых заранее определенных множеств таких сигналов [4 – 12].

В настоящее время достаточно полно исследованы вероятностные характеристики эффективности систем передачи информации с линейным случайным кодированием в двоичном симметричном (отводном) канале связи [4 – 7, 10, 11]. В [12] авторами настоящей статьи предложен метод случайного кодирования на основе нелинейных систематических кодов над произвольной конечной абелевой группой и получены оценки стойкости защиты информации в системах передачи с нелинейным случайным кодированием. На примере двоичных кодов Препараты показано, что, используя нелинейные блоковые коды, можно добиться большей стойкости защиты информации в отводном канале при большей скорости передачи ее законному получателю, чем в аналогичных системах со случайным кодированием линейными кодами практически той же длины (кодами Хэмминга).

Очевидным недостатком систем с нелинейным случайным кодированием является, в общем случае, большая сложность процедур случайного кодирования сообщений при передаче и их декодирования при приеме законным получателем.

В настоящей статье предложены эффективные алгоритмы нелинейного случайного кодирования и декодирования сообщений двоичными нелинейными кодами, соответствующими линейным кодам над кольцом вычетов по модулю 4 при отображении Грея [13]. Показано, что предложенные алгоритмы имеют не более чем квадратичные (от длины кодового слова) временную и емкостную сложности и, следовательно, могут быть практически эффективно реализованы с использованием как программных, так и аппаратных вычислительных средств.

Дальнейшее изложение в статье построено следующим образом. В п. II приведены необходимые сведения о линейных кодах над кольцом вычетов по модулю 4. Более подробную информацию о них можно найти в [13]. В п. III описаны алгоритмы случайного кодирования и декодирования сообщений произвольными $\boldsymbol{Z}_4$-линейными кодами, а также важными, с практической точки зрения, кодами, соответствующими определенным расширенным циклическим кодам над кольцом вычетов по модулю 4. Последние включают в себя известные коды Кердока и Препараты [13 – 15]. Получены оценки временных и емкостных сложностей представленных алгоритмов. В п. IV изложены основные выводы статьи.

II Необходимые сведения о четверичных линейных кодах

Обозначим $\mathbf{Z}_2$ поле из двух элементов 0, 1; $\mathbf{Z}_4$ – кольцо наименьших неотрицательных вычетов по модулю 4. Двоичным (четверичным) кодом длины n называется произвольное множество $B \subseteq \mathbf{Z}_2^n$ ($C \subseteq \mathbf{Z}_4^n$). Четверичный код C называется линейным, если он является подмодулем свободного модуля $\mathbf{Z}_4^n$ (удовлетворяет условию $x + y \in C$ для любых $x, y \in C$).

Каждый линейный код $C \subseteq \mathbf{Z}_4^n$ после подходящей перестановки координат кодовых слов может быть задан единственной порождающей матрицей над кольцом $\boldsymbol{Z}_4$

$$G_C = \begin{pmatrix} E_{k_1}, & U, & V \\ 0, & 2E_{k_2}, & 2W \end{pmatrix}, \qquad (1)$$

где E_{k_1} (E_{k_2}) – единичная матрица порядка k_1 (k_2), $k_1, k_2 \geq 0$, U и W – $(0,1)$-матрицы размера $k_1 \times k_2$ и $k_2 \times (n - k_1 - k_2)$ соответственно, V – матрица размера $k_1 \times (n - k_1 - k_2)$. Строки матрицы (1) являются элементами минимальной системы образующих модуля C. При этом C изоморфен прямому произведению модулей $\mathbf{Z}_4^{k_1} \times (\mathbf{Z}_4 / 2\mathbf{Z}_4)^{k_2}$ (имеет тип $(4^{k_1}, 2^{k_2})$) и $|C| = 2^{2k_1 + k_2}$. Код C является свободным $\mathbf{Z}_4$-

модулем в том и только в том случае, когда $k_2 = 0$ [13].

Пусть $a = a_0 + 2a_1$ – двоичное разложение числа $a \in \mathbf{Z}_4$, $a_0, a_1 \in \{0, 1\}$. Стандартные отображения $\alpha, \beta, \gamma: \mathbf{Z}_4 \to \mathbf{Z}_2$ определяются по формулам

$$\alpha(a) = a_0,\ \beta(a) = a_1,\ \gamma(a) = a_0 \oplus a_1,\ a \in \mathbf{Z}_4.$$

Указанные отображения продолжаются на множество $\mathbf{Z}_4^n$ ($n = 2, 3, \ldots$), действуя покоординатно на четверичные векторы длины n. Отображение $\varphi: \mathbf{Z}_4^n \to \mathbf{Z}_2^{2n}$, определяемое по формуле

$$\varphi(c) = (\beta(c), \gamma(c)) = (\beta(c_1), \ldots, \beta(c_n), \gamma(c_1), \ldots, \gamma(c_n)),\ c = (c_1, \ldots, c_n) \in \mathbf{Z}_4^n, \quad (2)$$

называется отображением Грея. Как показано в [13], φ является изометрией пространства $\mathbf{Z}_4^n$ с метрикой Ли на пространство $\mathbf{Z}_2^{2n}$ с метрикой Хэмминга и позволяет строить двоичные нелинейные коды с большим числом кодовых слов и/или минимальным расстоянием, исходя из определенных четверичных линейных кодов (см также [14, 15]).

Двоичные коды $B, B' \subseteq \mathbf{Z}_2^n$ называются эквивалентными, если они совпадают с точностью до перестановки координат кодовых слов. Код $B \subseteq \mathbf{Z}_2^n$ называется $\mathbf{Z}_4$-линейным, если существует линейный код $C \subseteq \mathbf{Z}_4^n$ такой, что коды $\varphi(C)$ и B эквивалентны. Примерами $\mathbf{Z}_4$-линейных кодов являются известные (нелинейные) коды Кердока, Дельсарта-Гетелса, модифицированные коды Препараты и ряд других [13 – 15].

Код $B \subseteq \mathbf{Z}_2^n$ называется систематическим, если в таблице, составленной из его слов, существует l столбцов, в которых каждый двоичный вектор длины l встречается ровно один раз. Номера указанных столбцов называются информационными координатами слов кода B. Ясно, что при этом $|B| = 2^l$.

Как показывает следующее утверждение, произвольный $\mathbf{Z}_4$-линейный код является систематическим.

Утверждение 1. Пусть $C \subseteq \mathbf{Z}_4^n$ – четверичный линейный код, порождающая матрица которого имеет вид (1). Тогда $\varphi(C)$ – систематический код с информационными координатами кодовых слов $1, 2, \ldots, k_1 + k_2,\ n + 1, \ldots, n + k_1$.

Доказательство. На основании формул (1), (2) произвольное слово x кода $\varphi(C)$ имеет вид

$$x = \varphi((x^{(1)}, x^{(2)})G_C) =$$

$$= (\beta(x^{(1)}), \beta(x^{(1)}U + 2x^{(2)}), \beta(x^{(1)}V + 2x^{(2)}W), \gamma(x^{(1)}), \gamma(x^{(1)}U + 2x^{(2)}), \gamma(x^{(1)}V + 2x^{(2)}W)), \quad (3)$$

где $x^{(1)} \in \mathbf{Z}_4^{k_1}$, $x^{(2)} \in \mathbf{Z}_2^{k_2}$. При этом, согласно равенствам

$$\beta(a + 2b) = \beta(a) \oplus b,\ \gamma(a + 2b) = \gamma(a) \oplus b,\ a \in \mathbf{Z}_4,\ b \in \mathbf{Z}_2,$$

подвектор x', состоящий из координат вектора (3) с номерами $1, 2, \ldots, k_1 + k_2, n + 1, \ldots, n + k_1$, равен

$$x' = (\beta(x^{(1)}), \beta(x^{(1)}U) \oplus x^{(2)}, \gamma(x^{(1)})),\ x^{(1)} \in \mathbf{Z}_4^{k_1},\ x^{(2)} \in \mathbf{Z}_2^{k_2}. \quad (4)$$

В силу биективности отображения $\varphi = (\beta, \gamma)$ все векторы (4) попарно различны и образуют в объединении совокупность всех двоичных векторов длины $2k_1 + k_2$. Отсюда непосредственно следует справедливость утверждения.

В качестве важного, с практической точки зрения, класса $\mathbf{Z}_4$-линейных кодов, рассмотрим коды, соответствующие при отображении Грея четверичным расширенным циклическим кодам длины n, порождающие многочлены которых являются делителями многочлена $z^{n-1} - 1$ [13, 16].

Пусть $g(z) = z^m + g_{m-1}z^{m-1} + \ldots + g_0 \in \mathbf{Z}_4[z]$ – унитарный многочлен степени m ($1 < m < n - 1$) такой, что $g(z) \mid z^{n-1} - 1$, $C_0 \subseteq \mathbf{Z}_4^{n-1}$ – циклический код, порожденный многочленом $g(z)$, $C \subseteq \mathbf{Z}_4^n$ – код, полученный добавлением к C_0 общей проверки на четность. Справедливо равенство

$$C = \{(c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \in \mathbf{Z}_4^n:\ c_0 + c_1 z + \ldots + c_{n-2}z^{n-2} = g(z)a(z),$$

$$a(z) \in \mathbf{Z}_4[z],\ \deg a(z) < n - 1 - m,\ c_{n-1} = -(c_0 + c_1 + \ldots + c_{n-2})\}. \quad (5)$$

На основании формулы (5) матрица

$$G(C)=\begin{pmatrix} g_0, g_1, \ldots, g_{m-1}, 1, 0, \ldots, 0, g_\infty \\ 0, g_0, g_1, \ldots, g_{m-1}, 1, 0, \ldots, 0, g_\infty \\ \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \\ 0, 0, \ldots, 0, g_0, g_1, \ldots, g_{m-1}, 1, g_\infty \end{pmatrix}, \quad (6)$$

размера $(n-1-m)\times n$, где $g_\infty = -(g_0 + g_1 + \ldots + g_{m-1} + 1)$, является порождающей матрицей кода C. При этом в силу обратимости в кольце $\mathbf{Z}_4$ элемента g_0 (вытекающей из условия $g(z) \mid z^{n-1} - 1$) код C является свободным подмодулем размерности $n-1-m$ модуля $\mathbf{Z}_4^n$. Отсюда на основании равенства (6) и утверждения 1 непосредственно вытекает, что двоичный код $B = \varphi(C)$ имеет длину $2n$, состоит из 4^{n-1-m} кодовых слов и является систематическим кодом с множеством информационных координат $\{1, \ldots, n-1-m, n+1, \ldots, 2n-1-m\}$. В частном случае, когда многочлен $g(z) \pmod 2$ является примитивным над полем из двух элементов, $n = 2^m$, $m \equiv 1 \pmod 2$, $m \geq 3$, двоичный код B имеет спектр расстояний, совпадающий со спектром расстояний кода Препараты длины 2^{m+1} и мощности $2^{2n-2(m+1)}$; в частности, дуальное расстояние кода B равно $2^m - 2^{(m-1)/2}$ [13].

III Случайное кодирование Z_4-линейными кодами в системе передачи информации по каналу связи с отводом

Напомним сущность метода случайного кодирования сообщений нелинейным систематическим кодом в системе передачи информации по каналу связи с отводом [12]. В простейшем частном случае указанная система передачи состоит из безызбыточного источника двоичных сообщений и двух статистически независимых каналов с общим входом: бесшумного основного канала от источника к законному получателю информации; двоичного симметричного отводного канала от источника к противнику [6]. Для передачи сообщений длины k, вырабатываемых источником, отправитель выбирает некоторый систематический код $B \subseteq \mathbf{Z}_2^n$ мощности 2^{n-k}.

Предположим, не ограничивая общности рассуждений, что информационные координаты слов кода B равны $1, 2, \ldots, n-k$. Тогда для передачи сообщения $s \in \mathbf{Z}_2^k$ используется двоичный вектор

$$u = x \oplus (0^{n-k}, s), \quad (7)$$

где x – случайное равновероятное слово кода B, 0^{n-k} – вектор длины $n-k$, все координаты которого равны 0.

Исходя из равенства (7), нетрудно убедиться в том, что законный получатель однозначно восстановит сообщение s по принятому вектору u. При этом вероятность $\pi^*(B)$ правильного восстановления s оптимальным декодером отводного канала удовлетворяет следующим неравенствам [12]:

$$2^{-k} \leq \pi^*(B) \leq 2^{-k} + (1-2p)^{d'},$$

где d' – дуальное расстояние кода B, p – вероятность искажения символа в отводном канале, $0 < p < 0{,}5$.

В [12] показано, что использование нелинейного систематического кода B позволяет в ряде случаев получить более эффективную (с точки зрения скорости передачи и стойкости защиты информации в отводном канале) систему со случайным кодированием по сравнению с аналогичными системами, построенными на основе двоичных линейных кодов практически той же длины. Вместе с тем, практическая реализация процедур нелинейного случайного кодирования и декодирования сообщений законным получателем требует, вообще говоря, большого объема памяти (порядка $n2^{n-k}$ бит) для хранения слов кода B либо больших временных затрат (порядка $k2^{n-k}$ двоичных операций), связанных с вычислением значений k нелинейных булевых функций от $n-k$ переменных (см. [12]).

Опишем алгоритмы случайного кодирования и декодирования сообщений $\mathbf{Z}_4$-линейными кодами, имеющие полиномиальные (не более чем квадратичные от длины кодового слова) временную и емкостную сложности.

Пусть задана порождающая матрица (1) линейного кода $C \subseteq \mathbf{Z}_4^n$ типа $(4^{k_1}, 2^{k_2})$, $k_1, k_2 \geq 0$.

Алгоритм случайного кодирования сообщений $\mathbf{Z}_4$*-линейным кодом* $B = \varphi(C)$ состоит из следующих шагов.

1. Сгенерировать независимые случайные и равновероятные векторы $x^{(1)} \in \mathbf{Z}_4^{k_1}$, $x^{(2)} \in \mathbf{Z}_2^{k_2}$.

2. Вычислить вектор x по формуле (3).

3. Для данного информационного сообщения $s = (s_1, s_2)$, где $s_1 \in \mathbf{Z}_2^{n-k_1-k_2}$, $s_2 \in \mathbf{Z}_2^{n-k_1}$, вычислить вектор $u = x \oplus (0^{k_1+k_2}, s_1, 0^{k_1}, s_2)$ и передать его по основному каналу связи.

Алгоритм восстановления сообщения s *по принятому вектору* u состоит в следующем.

1. Выделить вектор $x' = (x_1', x_2', x_3')$ вида (4), $x_1', x_3' \in \mathbf{Z}_2^{k_1}, x_2' \in \mathbf{Z}_2^{k_2}$, состоящий из координат с номерами $1, 2, \ldots, k_1 + k_2, n + 1, \ldots, n + k_1$ вектора u.

2. Вычислить вектор $x^{(1)}$ по формуле $x^{(1)} = \varphi^{-1}(x_1', x_3')$, где φ^{-1} – отображение, обратное к отображению (2).

3. Вычислить вектор $x^{(2)}$ по формуле $x^{(2)} = \beta(x^{(1)}U) \oplus x_2'$.

4. Вычислить информационное сообщение $s = (s_1, s_2)$, полагая

$s_1 = u^{(1)} \oplus \beta(x^{(1)}V) \oplus x^{(2)}W$, $s_2 = u^{(2)} \oplus (\gamma(x^{(1)}U) \oplus x^{(2)}, \gamma(x^{(1)}V) \oplus x^{(2)}W)$,

где $u^{(1)} \in \mathbf{Z}_2^{n-k_1-k_2}$ и $u^{(2)} \in \mathbf{Z}_2^{n-k_1}$ – подвекторы вектора u, состоящие из его координат с номерами $k_1 + k_2 + 1, \ldots, n$ и $n + k_1 + 1, \ldots, 2n$ соответственно.

Корректность приведенных алгоритмов следует непосредственно из равенств (3), (4).

В случае, когда $C \subseteq \mathbf{Z}_4^n$ является расширенным циклическим кодом, порожденным унитарным многочленом $g(z) \in \mathbf{Z}_4[z]$ степени m, где $1 < m < n - 1$ и $g(z) \mid z^{n-1} - 1$ (см. п. II), описанные выше алгоритмы могут быть модифицированы следующим образом.

Алгоритм случайного кодирования сообщений $\mathbf{Z}_4$*-линейным кодом* $B = \varphi(C)$, *соответствующим расширенному циклическому коду* C *вида* (5).

- Сгенерировать случайный равновероятный вектор $a = (a_0, a_1, \ldots, a_{n-m-2}) \in \mathbf{Z}_4^{n-m-1}$.
- Вычислить коэффициенты многочлена $c_0 + c_1 z + \ldots + c_{n-2} z^{n-2} = g(z)a(z)$, где $a(z) = a_0 + a_1 z + \ldots + a_{n-m-2} z^{n-m-2}$; положить $c_{n-1} = -(c_0 + c_1 + \ldots + c_{n-2})$.
- Для данного информационного сообщения $s = (s_1, s_2)$, где $s_1, s_2 \in \mathbf{Z}_2^{m+1}$, вычислить вектор

$$u = \varphi((c_0, c_1, \ldots, c_{n-1})) \oplus (0^{n-m-1}, s_1, 0^{n-m-1}, s_2), \quad (8)$$

и передать его по основному каналу связи.

Алгоритм восстановления сообщения s *по принятому вектору* u *вида* (8) имеет сдедующий вид.

1. Выделить вектор $c' \in \mathbf{Z}_2^{2(n-m-1)}$, состоящий из координат с номерами $1, \ldots, n - m - 1, n + 1, \ldots, 2n - m - 1$ вектора u.

2. Вычислить вектор $(c_0, c_1, \ldots, c_{n-m-2}) = \varphi^{-1}(c')$.

3. Вычислить коэффициенты многочлена $a(z) = a_0 + a_1 z + \ldots + a_{n-m-2} z^{n-m-2}$ по формулам

$$a_i = c_i - \sum_{j=0}^{i-1} a_j g_{i-j}, \; i \in \overline{0, n-m-2}, \text{ если } g_0 = 1;$$

$$a_i = \sum_{j=0}^{i-1} a_j g_{i-j} - c_i, \; i \in \overline{0, n-m-2}, \text{ если } g_0 = -1;$$

вычислить вектор $(c_{n-m-1}, c_{n-m}, \ldots, c_{n-1})$, полагая

$$c_i = \sum_{j=0}^{i} a_j g_{i-j}, \; i \in \overline{n-m-1, n-2}, \; c_{n-1} = -(c_0 + c_1 + \ldots + c_{n-2}).$$

4. Вычислить информационное сообщение $s = \varphi((c_{n-m-1}, c_{n-m}, \ldots, c_{n-1})) \oplus (u^{(1)}, u^{(2)})$, где $u^{(1)}$ и $u^{(2)}$ – подвекторы вектора u, состоящие из его координат с номерами $n - m, \ldots, n$ и $2n - m, \ldots, 2n$ соответственно.

Оценим сложность предложенных алгоритмов. Будем считать, что четверичные числа представлены двухмерными двоичными векторами (числу $a \in \mathbf{Z}_4$ соответствует вектор $(\alpha(a), \beta(a))$ его двоичных разрядов). Далее под элементарной операцией (ЭО) будем понимать любую из арифметических операций (сложения, умножения) в поле $\mathbf{Z}_2$. Временную (емкостную) сложность алгоритма определим стандартным образом как максимальное число элементарных операций (максимальный объем памяти ЭВМ в битах), необходимых для выполнения данного алгоритма на любом допустимом наборе входных данных [17].

Для удобства ссылок, сформулируем в виде отдельного утверждения следующий простой результат.

Лемма. Сумму (произведение) двух четверичных чисел можно вычислить, используя 4 элементарные операции. Для вычисления каждого значения $\varphi(c)$, $\varphi^{-1}(b)$, где $c \in \mathbf{Z}_4^n$, $b \in \mathbf{Z}_2^{2n}$, достаточно ровно n ЭО.

Доказательство. Пусть $a, b \in \mathbf{Z}_4$, $a = a_0 + 2a_1$, $b = b_0 + 2b_1$, где $a_0, a_1, b_0, b_1 \in \mathbf{Z}_2$,

$$a + b = s_0 + 2s_1,\ ab = p_0 + 2p_1,\ s_0, s_1, p_0, p_1 \in \mathbf{Z}_2.$$

Первое утверждение леммы следует из равенств $s_0 = a_0 \oplus b_0$, $s_1 = a_1 \oplus b_1 \oplus a_0 b_0$, $p_0 = a_0 b_0$, $p_1 = a_0 b_1 \oplus a_1 b_0$. Справедливость второго утверждения вытекает непосредственно из формулы (2).

Лемма доказана.

Обозначим $T_К(n, k_1, k_2)$ и $T_{ДК}(n, k_1, k_2)$ ($Q_К(n, k_1, k_2)$ и $Q_{ДК}(n, k_1, k_2)$) временные (емкостные) сложности алгоритмов случайного кодирования и, соответственно, восстановления сообщений в системе передачи со случайным кодированием кодом $B = \varphi(C)$, где $C \subseteq \mathbf{Z}_4^n$ – линейный код типа $(4^{k_1}, 2^{k_2})$.

Утверждение 2. Пусть $n \in \mathbf{N}$, $k_1, k_2 \in \mathbf{N}_0$, $k_1 + k_2 \le n$. Тогда

$$T_К(n, k_1, k_2) = 4(n - k_1 - k_2)(2k_1 + 2k_2 - 1) + 8k_1k_2 + n - k_2 \le 4n^2 + n, \quad (9)$$

$$T_{ДК}(n, k_1, k_2) = 2(n - k_1 - k_2)(4k_1 + 4k_2 - 3) + 8k_1k_2 + 3n - 2k_1 - 3k_2 \le 4n^2 + 3n, \quad (10)$$

$$Q_К(n, k_1, k_2) \le 2n^2 + 8n, \quad (11)$$

$$Q_{ДК}(n, k_1, k_2) \le 2n^2 + 8n. \quad (12)$$

Доказательство. Убедимся в справедливости соотношения (9). Заметим, что для вычисления вектора x по формуле (3) достаточно найти векторы

1. $\beta(x^{(1)}U) \oplus x^{(2)}$ (требуется $4k_2(2k_1 - 1) + k_2$ элементарных операций; см. первое утверждение леммы);
2. $\beta(x^{(1)}V) \oplus x^{(2)}W$ (требуется $4(n - k_1 - k_2)(2k_1 - 1) + 4(n - k_1 - k_2)(2k_2 - 1) + n - k_1 - k_2$ ЭО);
3. $\gamma(x^{(1)})$ (k_1 ЭО; см. формулу (2));
4. $\gamma(x^{(1)}U) \oplus x^{(2)}$ (достаточно $2k_2$ ЭО, поскольку значение $x^{(1)}U$ найдено на шаге 1));
5. $\gamma(x^{(1)}V) \oplus x^{(2)}W$ (достаточно $2(n - k_1 - k_2)$ ЭО).

Далее, для вычисления вектора u по сообщениям x и $s = (s_1, s_2)$ на шаге 3 описанного выше алгоритма случайного кодирования потребуется выполнить $(n - k_1 - k_2) + (n - k_1)$ ЭО.

Складывая приведенные выражения трудоемкостей и принимая во внимание неравенства

$$k_1k_2 \le \frac{n^2}{4},\ (n - k_1 - k_2)(k_1 + k_2) \le \frac{n^2}{4},$$

вытекающие из условия $k_1 + k_2 \le n$, после простых арифметических преобразований получим формулу (9).

Соотношения (10) – (12) доказываются аналогично. Отметим лишь, что как при случайном кодировании, так и при декодировании сообщений память ЭВМ используется для хранения векторов $(x^{(1)}, x^{(2)})G_C$, x, s, u и матриц U, V, W.

Утверждение доказано.

Пусть теперь $C \subseteq \mathbf{Z}_4^n$ – расширенный циклический код, порожденный унитарным многочленом $g(z)$ степени m, имеющим ровно d ненулевых коэффициентов, где $1 < d \le m + 1 < n$, $g(z) \mid z^{n-1} - 1$. Обозначим $\widetilde{T}_{\text{К}}(n,m,d)$ и $\widetilde{T}_{\text{ДК}}(n,m,d)$ ($\widetilde{Q}_{\text{К}}(n,m,d)$ и $\widetilde{Q}_{\text{ДК}}(n,m,d)$) соответственно временные (емкостные) сложности алгоритмов случайного кодирования и декодирования сообщений кодом $B = \varphi(C)$.

Утверждение 3. Справедливы следующие соотношения:

$$\widetilde{T}_{\text{К}}(n,m,d) \le 8(n-1)d + n + 2(m+1) \le 8(n-1)d + 3n, \tag{13}$$

$$\widetilde{T}_{\text{ДК}}(n,m,d) \le 8(n-1)d + n + m + 1 \le 8(n-1)d + 2n, \tag{14}$$

$$\widetilde{Q}_{\text{К}}(n,m,d) = 6n + 2m + 2 \le 8n, \tag{15}$$

$$\widetilde{Q}_{\text{ДК}}(n,m,d) = 6n + 2m + 2 \le 8n. \tag{16}$$

Доказательство. Убедимся в справедливости неравенств (14) (соотношения (13), (15), (16) доказываются аналогично). Заметим, что, согласно лемме, вычисление вектора $\varphi^{-1}(c')$ на шаге 2 описанного выше алгоритма восстановления сообщения s по вектору (8) потребует $n - m - 1$ ЭО. Далее, трудоемкость шага 3 составляет не более $8(n-1)d$ ЭО, поскольку каждое значение a_i ($i \in \overline{0, n-m-2}$), c_i ($i \in \overline{n-m-1, n-2}$) можно вычислить, используя не более d умножений и $d-1$ сложений в $\mathbf{Z}_4$, то есть $4(2d-1)$ ЭО, а для нахождения значения c_{n-1} потребуется $4(n-1)$ ЭО (см. первое утверждение леммы). Наконец, трудоемкость шага 4 алгоритма составляет $2(m+1)$ ЭО. Складывая приведенные выражения трудоемкостей, получим формулу (14).

Утверждение доказано.

IV Выводы

Предложенные на основании соотношений (9) – (16) алгоритмы нелинейного случайного кодирования и декодирования сообщений $\mathbf{Z}_4$-линейными кодами имеют не более чем квадратичные от длины кодового слова временную и емкостную сложности. Таким образом, указанные алгоритмы могут быть практически эффективно реализованы с использованием программных или аппаратных вычислительных средств.

В случае, когда число ненулевых коэффициентов многочлена $g(z) \in \mathbf{Z}_4[z]$ ограничено сверху постоянной, не зависящей от длины n кода C, временные сложности (13), (14) алгоритмов случайного кодирования и, соответственно, декодирования сообщений кодом $B = \varphi(C)$ зависят от n линейно. Аналогичный порядок роста имеют емкостные сложности указанных алгоритмов (см. формулы (15), (16)).

Отметим, что в случае, когда над полем $\mathbf{Z}_2$ существует примитивный трехчен $h(z) = z^m + z^l + 1$ степени $m \ge 3$, $m \equiv 1 \pmod 2$, унитарный многочлен $g(z) \in \mathbf{Z}_4[z]$ можно выбрать таким образом, чтобы при выполнении условий

$$h(z) \equiv g(z) \pmod 2,\ g(z) \mid z^{n-1} - 1,\ n = 2^m \tag{17}$$

число его ненулевых коэффициентов было равно наименьшему возможному значению d = 4. Действительно, согласно [13], стр. 15, искомый многочлен g(z) однозначно определяется условиями (17) и имеет следующий вид:

$$g(z) = z^m + z^l + 2z^{\frac{m+l}{2}} - 1, \text{ если } l \equiv 1 \pmod 2;$$

$$g(z) = z^m - z^l + 2z^{\frac{l}{2}} - 1, \text{ если } l \equiv 0 \pmod 2.$$

При выполнении соотношений (17) $B = \varphi(C)$ является $\mathbf{Z}_4$-линейным кодом Препараты длины $N = 2n$ и мощности $2^{2n-2(m+1)}$, где C – расширенный циклический код, порожденный многочленом $g(z)$ (см. п.

II). Таким образом, на основании формул (13) – (16) случайное кодирование (декодирование) сообщений кодом Препараты B может быть реализовано с линейными временной и емкостной сложностями, составляющими порядка $16N$ элементарных операций и $4N$ бит соответственно.

Литература: ***1.*** *Maurer U.M. Secret key agreement by public discussion from common information // IEEE Trans. on Inform. Theory. – 1993. – Vol. 39. – № 3. – P. 733-742.* ***2.*** *Ahlswede R., Csiszar I. Common randomness in information theory and cryptography – Part 1: Secret sharing // IEEE Trans. Inform. Theory. – 1993. – V. 39. – № 4. – P. 1121-1132.* ***3.*** *Bennet C. H.,Brassard G., Maurer U. M.Generalized privacy amplifications // IEEE Trans. Inform. Theory. – 1995. – V. 41. – № 6. – P. 1915-1923.* ***4.*** *Decatur S.,Goldreich O., Ron D. A probabilistic error-correcting scheme //* http://eprint.iacr.org./1997/005. ***5.*** *Thangarai A., Dihidar S., Calderbank A. R., McLaughlin S., Merolla J.-M.Capacity achiving codes for the wire-tap channel with applications to quantum key distribution //* http://eprint.arXiv.IT/0411003v1.– 2 Nov.2004. ***6.*** *Wyner A. D. The Wire-Tap Channel // Bell System Techn. J. – 1975. – V. 54. – № 8. – P. 1355-1388.* ***7.*** *Коржик В. И., Яковлев В. А. Неасимптотические оценки кодового зашумления одного канала // Проблемы передачи информации. – 1981.– Т. 17.– В. 4.– С. 11-18.* ***8.*** *Алексейчук А. Н. Случайное кодирование в канале связи с аддитивным шумом, распределенным на конечной абелевой группе // Захист інформації. – 2002.– № 3.– С. 7-16.* ***9.*** *Алексейчук А. Н. Оптимальное случайное кодирование равновероятных сообщений в q-ичном симметричном канале // Захист інформації. – 2002. – № 4. – С. 49-58.* ***10.*** *Иванов В. А. О методе случайного кодирования // Дискретная математика.– 1999. – Т. 11. – В. 3. – С. 99-108.* ***11****.Алексейчук А. Н., Сергиенко Ю. В. Оценки стойкости и способ реализации кодовой защиты дискретных сообщений с использованием каскадных кодов // Электронное моделирование. – 2003. – Т. 25. – № 5. – С. 33-44.* ***12.*** *Алексейчук А. Н., Гришаков С.В. Нелинейное случайное кодирование в системах передачи информации по каналу связи с отводом // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – В. 8. – К.: 2004. – С. 133-140.* ***13.*** *Hammous A. R., Kumar P. V., Calderbank A. R., Sloane N.J.A., Sole P. The Z_4-linearity of Kerdock,Preparata,Goethals and related codes // Bull. Amer. Math. Soc. – 1993. – V. 29. – № 2.– P. 218-222.* ***14****. Нечаев А. А. Код Кердока в циклической форме // Дискретная математика. – 1989. – Т. 1. – Вып. 4. – С. 123-139.* ***15.*** *Кузьмин А. С., Нечаев А. А. Построение помехоустойчивых кодов с использованием линейных рекуррент над кольцами Галуа // Успехи матем. наук – 1992. – Т. 47. – № 5. – С. 183-184.* ***16.*** *Calderbank A. R., Sloane N.J.A. Modular and p-adic ciclic codes // Design, Codes and Cryptography. – 1995. – V. 6. – P. 21-35.* ***17.*** *Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов: Пер. с англ. – М.: Мир, 1979. – 535 с.*

УДК 681.3.06

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ПРИ РОЗПІЗНАВАННІ МАКРОВІРУСІВ

Ігор Терейковський
Державний університет інформаційно-комунікаційних технологій

Анотація: **Розглянута можливість використання нейронної мережі типу багатошаровий перспетрон в системах розпізнавання комп'ютерних макровірусів. Сформована архітектура такого перспетрона та показані принципи визначення переліку вхідних параметрів.**
Summary: **The opportunity of use neuronet such as many layers perspetron in systems of recognition computer macroviruses is considered. The architecture such perspetron is generated and the principles of definition of the list of entrance parameters are shown.**
Ключові слова: **Вірус, антивірус, нейронні мережі, перспетрон.**

Значний обсяг успішних вірусних атак на інформаційні ресурси сучасних автоматизованих інформаційних систем визначає важливість розробки ефективних технологій антивірусного захисту. Не зважаючи, на те, що розробці антивірусних систем присвячено достатньо багато досліджень, практичний досвід та висновки [1] вказують на їх відносно низьку ефективність. При цьому потенційно висока небезпека комп'ютерних вірусів зафіксована як у вітчизняних, так і в закордонних нормативних документах в галузі захисту інформації [2, 3].

Багато в чому необхідність вдосконалення антивірусного захисту зумовлена недосконалістю системи діагностики, яка не здатна адекватно реагувати на появу нових вірусів, створених за допомогою сучасних технологій. Завдання ускладнюється тим, що для кожної операційної системи та програмного середовища потрібно використовувати власну методику розпізнавання вірусів. Разом з цим, для більшості