УДК 621.391:519.2

А.Н. АЛЕКСЕЙЧУК, С.В. ГРИШАКОВ

СТОЙКИЕ И ПРАКТИЧНЫЕ РАНДОМИЗИРОВАННЫЕ ПОТОЧНЫЕ ШИФРЫ НА ОСНОВЕ КОДОВ РИДА–СОЛОМОНА

Аннотация. Рассмотрен класс рандомизированных поточных шифров, основанных на совместном применении шифрования, случайного кодирования и помехоустойчивого кодирования открытых сообщений двоичными линейными кодами. Показано, что в этом классе существуют шифры, имеющие сколь угодно высокую вычислительную стойкость относительно наиболее мощной из известных атак и обеспечивающие сколь угодно близкие к единице скорость передачи, достоверность приема, а также приемлемую сложность восстановления открытых сообщений законным получателем. Доказательство является конструктивным.

Ключевые слова: рандомизированный поточный шифр, случайное кодирование, корреляционная атака, обоснованная стойкость, код Рида–Соломона.

ВВЕДЕНИЕ

В работах М. Михалевича и Х. Имаи [1–4] предложен общий подход к построению рандомизированных поточных шифров (РПШ) на основе совместного применения шифрования, случайного (омофонного) кодирования, а также помехоустойчивого кодирования открытых сообщений двоичными линейными кодами. Основная цель создания таких шифров — повышение стойкости (при сохранении практичности) поточных шифров, используемых в настоящее время в системах беспроводной связи, в частности, в стандарте мобильной телефонии GSM. Другим побудительным мотивом является построение симметричных криптосистем, стойкость которых базируется на сложности решения известных вычислительно трудных математических задач, например, задачи о декодировании случайного двоичного линейного кода [5].

В работах [4, 6] исследована стойкость РПШ Михалевича–Имаи относительно атаки на основе подобранных открытых текстов. Более мощные атаки описаны в [7], где показано также, что стойкость этих шифров существенно зависит от строения их компонент и может быть значительно меньшей, чем утверждают их разработчики.

Исходные данные для построения РПШ Михалевича–Имаи — генератор гаммы и пара двоичных линейных кодов, используемых в конструкции рандомизатора для реализации случайного и помехоустойчивого кодирования соответственно. Исходя из условий стойкости и практичности РПШ, эти коды следует выбирать с учетом ряда жестких ограничений, что является нетривиальной задачей (отметим, что до появления настоящей статьи не предложено ни одного способа построения таких кодов).

Далее показано, как с помощью пары кодов Рида–Соломона можно обеспечить сколь угодно высокую вычислительную стойкость РПШ Михалевича–Имаи относительно наиболее мощной из известных атак [7] при сколь угодно близких к единице скорости передачи, достоверности приема, а также приемлемой сложности восстановления открытых сообщений законным получателем.

ОПРЕДЕЛЕНИЕ И ОСНОВНЫЕ ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ РПШ МИХАЛЕВИЧА–ИМАИ

Примем следующие обозначения: V_n — множество двоичных векторов длины n; $xy = x_1 y_1 \oplus \cdots \oplus x_n y_n$ — булево скалярное произведение векторов

$x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n) \in V_n$; $wt(x)$ — вес (Хемминга) вектора $x \in V_n$; $F_{m \times n}$ — множество $m \times n$-матриц над полем $F = \mathbf{GF}(2)$; $\overline{a, b} = \{x \in \mathbf{Z} : a \le x \le b\}$, $a, b \in \mathbf{Z}$.

Согласно [3, 4] исходными данными для построения рандомизированного поточного шифра $\mathcal{M}$ с параметрами $l, m, n \in \mathbf{N}$, $p \in (0, 1/2)$, где $l < m < n$, и множеством ключей K являются следующие объекты:

— порождающая матрица G_1 двоичного линейного $[n, m]$-кода C_1 с эффективным алгоритмом декодирования (декодером) $D: V_n \to C_1$, позволяющим надежно исправлять ошибки в двоичном симметричном канале (ДСК) с вероятностью искажения p;

— обратимая матрица $G_2 \in F_{m \times m}$;

— генератор гаммы, вырабатывающий по ключу $k \in K$ последовательность $f_0(k), f_1(k), \dots$ двоичных векторов длины n (при этом предполагается, что функции $f_i : K \to V_n$, $i = 0, 1, \dots$, могут зависеть от общедоступных параметров, например, векторов инициализации).

Для зашифрования на ключе $k \in K$ открытого текста $s_0, s_1, \dots, s_t$, где $s_i \in V_l$, $i \in \overline{0, t}$, отправитель генерирует последовательность независимых случайных векторов $u_0, v_0, u_1, v_1, \dots, u_t, v_t$, распределенных по законам

$$\mathbf{P}\{u_i = u\} = 2^{-(m-l)},\ u \in V_{m-l},\ \mathbf{P}\{v_i = v\} = p^{wt(v)}(1-p)^{n-wt(v)},\ v \in V_n,$$

и вычисляет шифрованный текст $z_0, z_1, \dots, z_t$ по формуле

$$z_i = (s_i, u_i)G_2G_1 \oplus f_i(k) \oplus v_i,\ i \in \overline{0, t}. \tag{1}$$

Отметим, что преобразование $s_i \mapsto (s_i, u_i)G_2$ в формуле (1) называется случайным кодированием сообщения $s_i \in V_l$, а преобразование $(s_i, u_i)G_2 \mapsto$ $\mapsto (s_i, u_i)G_2G_1$ представляет собой помехоустойчивое кодирование сообщения $(s_i, u_i)G_2$ кодом C_1. Законный получатель, зная вектор $f_i(k)$, может быстро восстановить сообщение $(s_i, u_i)G_2$ с помощью декодера D, а затем найти вектор s_i, используя обратимость матрицы G_2.

Основными показателями эффективности РПШ $\mathcal{M}$ являются следующие параметры:

– скорость передачи информации $\rho(\mathcal{M}) = l/n$;

– (максимальная) вероятность ошибочного декодирования сообщений законным получателем $p_e = \max\limits_{\substack{s \in V_l, \\ u \in V_{m-l}}} \mathbf{P}\{D((s, u)G_2G_1 \oplus v_1) \ne (s, u)G_2G_1\}$;

– вычислительная сложность декодера D.

Эффективность РПШ $\mathcal{M}$ зависит также от сложности процедур случайного и помехоустойчивого кодирования входных сообщений. Для уменьшения сложности кодирования в [6] предложено задавать матрицы G_1 и G_2 в виде

$$G_1 = \begin{pmatrix} I_{m-l} & 0 & A_1 \\ 0 & I_l & A_2 \end{pmatrix},$$

$$G_2 = \begin{pmatrix} 0 & I_l \\ I_{m-l} & B \end{pmatrix}, \tag{2}$$

где $A_1 \in F_{(m-l)\times(n-m)}$, $A_2 \in F_{l\times(n-m)}$, $B \in F_{(m-l)\times l}$, а I_l и I_{m-l} — единичные матрицы указанных порядков. Такой выбор матриц, по существу, не сужает класса рассматриваемых РПШ, однако не является обязательным.

Рассмотрим одну из наиболее мощных атак на РПШ $\mathcal{M}$, которая проводится с использованием подобранных открытых текстов и векторов инициализации [7].

Обозначим

$$C_0 = \{(0,u)G_2G_1\colon\ u \in V_{m-l}\},\ C_0^{\perp} = \{y \in V_n \mid \forall x \in C_0 : xy = 0\},$$

$$d_0^{\perp} = \min\{wt(x) : x \in C_0^{\perp} \setminus \{0\}\}. \tag{3}$$

Отметим, что множество C_0 является $[n, m-l]$-подкодом кода C_1, множество $C_0^{\perp}$ называется кодом, дуальным к C_0, а число $d_0^{\perp}$ — дуальным расстоянием кода C_0 (см., например, [8]).

При проведении атаки противник выполняет следующий алгоритм:

1) выбрать слово $h \in C_0^{\perp} \setminus \{0\}$;

2) подать T раз на вход алгоритма шифрования с неизвестным фиксированным ключом k сообщение $s_0 = 0$ и найти для выбранного $i = 0, 1, \ldots$ шифрованные сообщения

$$z^{(j)} = (0, u^{(j)})G_2G_1 \oplus f_i(k) \oplus v^{(j)},\ j \in \overline{1,T},$$

где $u^{(0)}$, $v^{(0)}$, $u^{(1)}$, $v^{(1)}$,… — независимые случайные векторы, распределенные по законам

$$\mathbf{P}\{u^{(j)} = u\} = 2^{-(m-l)},\ u \in V_{m-l},\ \mathbf{P}\{v^{(j)} = v\} = p^{wt(v)}(1-p)^{n-wt(v)},\ v \in V_n;$$

3) вычислить

$$z^{(j)}h = f_i(k)h \oplus v^{(j)}h,\ j \in \overline{1,T}, \tag{4}$$

и восстановить значение $f_i(k)h$ методом максимума правдоподобия.

Таким образом, цель атаки — получить «один бит информации» о ключе k, исходя из набора сообщений (4).

В [7] показано, что трудоемкость атаки ограничена сверху величиной $O((1-2p)^{-2wt(h)})$. Для решения задачи обоснования стойкости РПШ относительно этой атаки получим нижнюю границу объема материала, необходимого для ее успешного выполнения.

Обозначим

$$p_0 = 1/2 \cdot (1-(1-2p)^{wt(h)}),\ p_1 = 1-p_0,$$

$$a = f_i(k)h,\ \xi_j = z^{(j)}h = a \oplus v^{(j)}h,\ j \in \overline{1,T}.$$

Из определения случайных векторов $u^{(0)}, v^{(0)}, u^{(1)}, v^{(1)}, \ldots$ следует, что последовательность $\xi = \xi_1, \xi_2, \ldots, \xi_T$ является схемой Бернулли с параметрами (T, p_a). При этом задача восстановления числа a по набору его искаженных значений (4) равносильна проверке следующих двух гипотез: H_0: $\mathbf{P}\{\xi_1 = 1\} = p_0$; H_1: $\mathbf{P}\{\xi_1 = 1\} = p_1$.

Для любого $v \in V_T$ обозначим $\mathbf{P}_0(v) = \mathbf{P}\{\xi = v \mid H_0\}$, $\mathbf{P}_1(v) = \mathbf{P}\{\xi = v \mid H_1\}$ и рассмотрим произвольный критерий для проверки гипотез H_0 и H_1, основанный на критическом множестве M. Вероятности ошибок первого и второго рода указанного критерия определяются по формулам $\alpha = \sum\limits_{v \in M} \mathbf{P}_0(v)$ и $\beta = 1 - \sum\limits_{v \in M} \mathbf{P}_1(v)$ соответственно.

Лемма 1. Для любого $\delta \in (0, 1/2)$ справедливо следующее утверждение:

$$1/2 \cdot (\alpha + \beta) \le \delta \Rightarrow T \ge 1/16 \cdot (1-2\delta)^2 (1-2p)^{-2wt(h)}.$$

Доказательство. Воспользуемся леммой 15 из [9], согласно которой

$$\max_{M\subseteq V_T}\left|\sum_{v\in M}(x^{wt(v)}(1-x)^{T-wt(v)}-2^{-T})\right|\le 2\sqrt{T}|2x-1|,\ x\in[0,1]. \qquad (5)$$

Справедливы соотношения

$$1-2\delta\le 1-(\alpha+\beta)=\sum_{v\in M}(\mathbf{P}_1(v)-\mathbf{P}_0(v))\le\left|\sum_{v\in M}(\mathbf{P}_0(v)-2^{-T})\right|+\left|\sum_{v\in M}(\mathbf{P}_1(v)-2^{-T})\right|,$$

$$\mathbf{P}_0(v)=p_0^{wt(v)}(1-p_0)^{T-wt(v)},\ \mathbf{P}_1(v)=p_1^{wt(v)}(1-p_1)^{T-wt(v)},$$

из которых на основании формулы (5) и равенства $p_1=1-p_0$ следует, что

$$1-2\delta\le 2\sqrt{T}|2p_0-1|+2\sqrt{T}|2p_1-1|=4\sqrt{T}(1-2p_0).$$

Итак, $T\ge 1/16\cdot(1-2\delta)^2(1-2p_0)^{-2}$, что и требовалось доказать.

Следствие. Для выполнения описанной атаки на РПШ $\mathcal{M}$ со средней вероятностью ошибки, не превышающей δ, $\delta\in(0,1/2)$, необходимо не менее $T_\delta(\mathcal{M})=1/16\cdot(1-2\delta)^2(1-2p)^{-2d_0^\perp}$ значений (4), где $d_0^\perp$ определяется по формуле (3).

ПОСТРОЕНИЕ РПШ НА ОСНОВЕ ДВОИЧНЫХ ЛИНЕЙНЫХ КОДОВ

Покажем, что для построения РПШ вместо матриц G_1 и G_2 можно использовать пару двоичных линейных кодов, один из которых содержится в другом.

Лемма 2. Пусть C_0, C_1 — двоичные линейные коды с параметрами $[n, m-l]$ и $[n, m]$ соответственно, $C_0\subseteq C_1$, $l<m<n$. Тогда для любой порождающей матрицы $\widetilde{G}_1$ кода C_1 найдутся обратимая $m\times m$-матрица G_2 вида (2) и подстановочная матрица $P\in F_{m\times m}$ такие, что $C_0=\{(0,u)G_2G_1\colon u\in V_{m-l}\}$, где $G_1=P\widetilde{G}_1$.

Доказательство. Пусть $G_0=A\widetilde{G}_1$ — порождающая матрица кода C_0, где $A\in F_{(m-l)\times m}$. Поскольку $m-l=\operatorname{rank}(G_0)\le\operatorname{rank}(A)\le m-l$, то $\operatorname{rank}(A)=m-l$. Следовательно, существуют обратимая матрица $U\in F_{(m-l)\times(m-l)}$ и подстановочная матрица $P\in F_{m\times m}$ такие, что $A=U(I_{m-l},B)P$, где $B\in F_{(m-l)\times l}$. Из равенства $G_0=A\widetilde{G}_1=U(I_{m-l},B)P\widetilde{G}_1$ и обратимости матрицы U следует, что $(I_{m-l},B)P\widetilde{G}_1$ — порождающая матрица кода C_0. Наконец, зададим матрицу G_2 по формуле (2) и получим

$$C_0=\{u(I_{m-l},B)P\widetilde{G}_1\colon u\in V_{m-l}\}=\{(0,u)G_2(P\widetilde{G}_1)\colon u\in V_{m-l}\}.$$

Лемма доказана.

Отметим, что способ построения матриц G_1 и G_2, описанный в доказательстве леммы 2, является алгоритмически эффективным. При этом стойкость РПШ $\mathcal{M}$, соответствующего кодам C_0 и C_1, зависит от дуального расстояния кода C_0.

РАНДОМИЗИРОВАННЫЕ ПОТОЧНЫЕ ШИФРЫ, ОСНОВАННЫЕ НА КОДАХ РИДА–СОЛОМОНА

На основании изложенного ранее сформулируем задачу построения стойких (относительно описанной атаки) и практичных РПШ следующим образом. Пусть заданы генератор гаммы и числа $\rho,\varepsilon\in(0,1)$, $\delta\in(0,1/2)$, $T_0\in\mathbf{N}$. Требуется построить двоичный линейный $[n,m]$-код C_1, его $[n,m-l]$-подкод C_0 и задать число $p\in(0,1/2)$ так, чтобы выполнялись следующие условия:

— практичность РПШ $\mathcal{M}$, соответствующего кодам C_0, C_1: скорость передачи информации в системе удовлетворяет неравенству $\rho(\mathcal{M}) \geq \rho$, вероятность p_e ошибочного декодирования сообщений законным получателем не превышает ε, алгоритм декодирования кода C_1 имеет приемлемую (полиномиально зависящую от n) временную сложность;

— стойкость РПШ $\mathcal{M}$: объем материала, необходимый для успешного (со средней вероятностью ошибки не более δ) проведения корреляционной атаки на шифр, удовлетворяет неравенству $T_\delta(\mathcal{M}) \geq T_0$.

Покажем, что поставленная задача имеет конструктивное решение.

Для любого натурального $r \geq 2$ обозначим $R_{N,K}$ код Рида–Соломона длины $N = 2^r - 1$ и размерности $K \in \overline{1, N-1}$ над полем $F_{2^r} = \mathbf{GF}(2^r)$. Зафиксируем базис $\alpha = (\alpha_1, \ldots, \alpha_r)$ поля F_{2^r} над полем F и рассмотрим двоичный $[Nr, Kr]$-код

$$\overline{R}_{N,K} = \{(\alpha(x_0), \ldots, \alpha(x_{N-1})) : (x_0, \ldots, x_{N-1}) \in R_{N,K}\}, \tag{6}$$

где $\alpha(x)$ — набор координат элемента $x \in F_{2^r}$ в базисе α.

Лемма 3. Минимальные расстояния кодов $\overline{R}_{N,K}$ и $\overline{R}_{N,K}^{\perp}$ удовлетворяют неравенствам

$$d(\overline{R}_{N,K}) \geq N - K + 1, \; d(\overline{R}_{N,K}^{\perp}) \geq K + 1. \tag{7}$$

При этом существует алгоритм декодирования кода (6), позволяющий исправлять любую комбинацию из $s \leq \lfloor 1/2 \cdot (N-K) \rfloor$ (двоичных аддитивных) ошибок со сложностью $O(2^r r^2)$ операций в поле F_{2^r}.

Доказательство. Пусть $\beta = (\beta_1, \ldots, \beta_r)$ — базис поля F_{2^r}, дуальный к базису α (см., например, [10], с. 78). Для любого $y \in F_{2^r}$ обозначим $\beta(y)$ набор координат элемента y в базисе β и заметим, что

$$\overline{R}_{N,K}^{\perp} = \{(\beta(y_0), \ldots, \beta(y_{N-1})) : (y_0, \ldots, y_{N-1}) \in R_{N,K}^{\perp}\}. \tag{8}$$

Действительно, коды в обеих частях равенства (8) имеют одинаковую размерность над полем F, причем код в правой части этого равенства содержится в $\overline{R}_{N,K}^{\perp}$ в силу дуальности базисов α и β.

Неравенства (7) следуют непосредственно из формул (6), (8) и известных выражений для минимальных расстояний кодов $R_{N,K}$ и $R_{N,K}^{\perp}$ (см., например, [8], с. 289): $d(R_{N,K}) = N - K + 1$, $d(R_{N,K}^{\perp}) = K + 1$.

Наконец, известны алгоритмы декодирования кода $R_{N,K}$, позволяющие исправлять любые комбинации из $s \leq \lfloor 1/2 \cdot (N-K) \rfloor$ (аддитивных над F_{2^r}) ошибок со сложностью $O(2^r r^2)$ операций [11]. Каждый такой алгоритм очевидным образом преобразуется в алгоритм декодирования кода $\overline{R}_{N,K}$, позволяющий исправлять такое же количество (аддитивных над F) ошибок с той же временной сложностью.

Лемма доказана.

Сформулируем и докажем теорему, содержащую основной результат настоящей статьи.

Теорема 1. Пусть $\rho \in (0,1)$, $\delta \in (0, 1/2)$, $r \in \mathbf{N}$, $r > \log_2(1 + 5(1-\rho)^{-1})$,

$$N = 2^r - 1, \; K_1 = \lfloor N/2 \cdot (1 + \rho + N^{-1}) \rfloor, \; K_0 = \lceil N/2 \cdot (1 - \rho - N^{-1}) \rceil - 1.$$

Рассмотрим РПШ $\mathcal{M}$ с параметрами

$$l = (K_1 - K_0)r,\ m = K_1 r,\ n = Nr,\ p = \frac{1-\rho}{6r}, \tag{9}$$

соответствующий двоичным линейным кодам $C_0 = \overline{R}_{N,K_0}$, $C_1 = \overline{R}_{N,K_1}$.

Тогда справедливы следующие утверждения:

а) имеет место неравенство $\rho(\mathcal{M}) \geq \rho$;

б) вероятность ошибочного декодирования сообщений законным получателем удовлетворяет неравенству

$$p_e \leq \exp\left\{-\frac{2N}{9r}(1-\rho-3/2\cdot N^{-1})^2\right\}; \tag{10}$$

в) сложность декодирования сообщений законным получателем составляет $O(2^r r^2)$ операций в поле F_{2^r};

г) объем материала, необходимый для успешного (со средней вероятностью ошибки не более δ) проведения атаки на шифр, удовлетворяет неравенству

$$T_\delta(\mathcal{M}) \geq 1/16\cdot(1-2\delta)^2 \exp\left\{\frac{N}{3r}(1-\rho-N^{-1})^2\right\}. \tag{11}$$

Доказательство. Используя неравенство $r > \log_2(1+5(1-\rho)^{-1})$, нетрудно убедиться в том, что $1 \leq l < m < n$. Отсюда следует, в частности, что $R_{N,K_0} \subseteq R_{N,K_1}$ и, значит, $C_0 \subseteq C_1$.

Утверждение а) следует из соотношений

$$\rho(\mathcal{M}) = l/n = N^{-1}(K_1 - K_0) >$$

$$> N^{-1}(N/2\cdot(1+\rho+N^{-1})-1-N/2\cdot(1-\rho-N^{-1})) = \rho,$$

а утверждение г) — из соотношений (см. следствие леммы 1 и лемму 3)

$$T_\delta(\mathcal{M}) = 1/16\cdot(1-2\delta)^2(1-2p)^{-2d_0^\perp},\ d_0^\perp = d(\overline{R}_{N,K_0}^{\perp}) \geq K_0 + 1$$

и неравенств

$$(1-2p)^{2d_0^\perp} \leq \exp\{-4pd_0^\perp\} \leq \exp\{-4p(K_0+1)\} \leq \exp\{-2pN(1-\rho-N^{-1})\} =$$

$$= \exp\left\{-\frac{N}{3r}(1-\rho-N^{-1})(1-\rho)\right\} \leq \exp\left\{-\frac{N}{3r}(1-\rho-N^{-1})^2\right\}.$$

Далее, используя в качестве декодера D кода C_1 алгоритм декодирования, указанный в формулировке леммы 3, получим утверждение в). Кроме того, в этом случае вероятность ошибочного декодирования сообщений законным получателем не превышает вероятности события $\{wt(v_1) > \lfloor 1/2\cdot(N-K_1)\rfloor\}$, где v_1 — случайный вектор, распределенный по закону $\mathbf{P}\{v_1 = v\} = p^{wt(v)}(1-p)^{n-wt(v)}$, $v \in V_n$. Используя неравенство Чернова, получим, что

$$p_e \leq \mathbf{P}\{wt(v_1) > \lfloor 1/2\cdot(N-K_1)\rfloor\} \leq \mathbf{P}\{wt(v_1) > N/2\cdot(1-\rho-N^{-1})\} =$$

$$= \mathbf{P}\left\{n^{-1}wt(v_1) - p > \frac{1}{3r}(1-\rho-3/2\cdot N^{-1})\right\} \leq$$

$$\leq \exp\left\{-2n\left(\frac{1}{3r}(1-\rho-3/2\cdot N^{-1})\right)^2\right\} = \exp\left\{-\frac{2N}{9r}(1-\rho-3/2\cdot N^{-1})^2\right\}.$$

Итак, справедливо утверждение б).

Теорема доказана.

Таблица 1. Результаты расчетов по формулам (9)–(11)

$\rho = 0.5,\ \delta = 0.05$						
r	l	m	n	p	p_e	$\log T_\delta(\mathcal{M})$
10	5120	7670	10230	0.008333	0.003517	7.948
11	11264	16885	22517	0.007556	0.000033	18.025
12	24576	36852	49140	0.006944	$6\cdot10^{-9}$	36.683
$\rho = 0.9,\ \delta = 0.05$						
r	l	m	n	p	p_e	$\log T_\delta(\mathcal{M})$
15	442380	466935	491505	0.001111	0.007829	6.209
16	943712	996128	1048560	0.001042	0.000112	15.387
17	2005388	2116789	2228207	0.000980	$3.6\cdot10^{-8}$	32.768

В табл. 1 приведены численные значения параметров, характеризующих стойкость и практичность некоторых РПШ из теоремы 1.

Как видно из табл. 1, при $\rho = 0.5$, $r = 12$ можно гарантировать приемлемую вероятность правильного приема сообщений законным получателем при умеренной длине кодовых слов и стойкости шифрования порядка $2^{36.683}$ (операций зашифрования одного открытого сообщения длины l бит). При $\rho = 0.9$ для достижения аналогичной стойкости следует увеличить длину кодовых слов до двух с лишним миллионов бит, что не очень практично. В этом случае в качестве альтернативного варианта можно использовать рандомизированные поточные шифры с нелинейным случайным кодированием, обеспечивающие требуемую стойкость при стопроцентной достоверности приема открытых сообщений законным получателем и умеренной длине передаваемых сообщений [12].

ЗАКЛЮЧЕНИЕ

Согласно полученной теореме, выбирая достаточно большое значение r, можно обеспечить сколь угодно высокую стойкость соответствующего РПШ при сколь угодно близких к единице скорости передачи, достоверности приема, а также приемлемой сложности восстановления открытых сообщений законным получателем.

СПИСОК ЛИТЕРАТУРЫ:

1. Mihaljević M.J., Imai H. A stream ciphering approach based on wiretap channel coding. *8th Central European Conference of Cryptography 2008*. Graz, Austria (2–4 July, 2008). E-Proc. 3 p.
2. Mihaljević M.J., Imai H. An approach for stream cipher design based on joint computing over random and secret data. *Computing.* 2009. Vol. 85, N 1–2, P. 153–168.
3. Mihaljević M.J., Imai H. An information-theoretic and computational complexity security analysis of a randomized stream cipher model. *4th Western European Workshop on Research in Cryptology WeWoRC 2011*. Weimar, Germany, 20–22 July, 2011). P. 21–25.
4. Mihaljević M.J., Imai H. Employment of homophonic coding for improvement of certain encryption approaches based on the LPN problem. *Symmetric Key Encryption Workshop SKEW 2011*. Copenhagen, Denmark (16–17 Feb. 2011). E-Proc. 17 p.
5. Berlekamp E.R., McElice R.J., van Tilborg H. On the inherent intractability of certain coding problems. *IEEE Trans. Inform. Theory*. 1978. Vol. 24, N 3. P. 384–386.
6. Mihaljević M.J., Oggier F., Imai H. Homophonic coding design for communication systems employing the encoding-encryption paradigm. arXiv:1012.5895v1 [cs.CR]. 2010. 29 Dec.
7. Alekseychuk A.N., Gryshakov S.V. On the computational security of randomized stream ciphers proposed by Mihaljevic and Imai. *Захист інформації.* 2014. Т. 16, № 4. С. 328–334.

8. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. Москва: Связь, 1979. 743 с.
9. Vaudenay S. Decorrelation: a theory for block cipher security. *J. of Cryptology.* 2003. Vol. 16, N 4. P. 249–286.
10. Лидл Р., Нидеррайтер Г. Конечные поля: в 2-х т. Москва: Мир, 1988. Т. 1.
11. Федоренко С.В. Методы быстрого декодирования линейных блоковых кодов: монография. С.-Петербург: ГУАПб 2008. 199 с.
12. Alekseychuk A.N., Gryshakov S.V. Randomized stream ciphers with enhanced security based on nonlinear random coding. *Journal of Mathematic and System Science*. 2015. Vol. 5, N 12. P. 516–522.

Надійшла до редакції 06.10.2016

А.М. Олексійчук, С.В. Гришаков

СТІЙКІ ТА ПРАКТИЧНІ РАНДОМІЗОВАНІ ПОТОКОВІ ШИФРИ НА БАЗІ КОДІВ РІДА–СОЛОМОНА

Анотація. Розглянуто клас рандомізованих потокових шифрів, що базуються на сумісному застосуванні шифрування, випадкового кодування та завадостійкого кодування відкритих повідомлень двійковими лінійними кодами. Показано, що в цьому класі існують шифри, що мають як завгодно високу обчислювальну стійкість відносно найбільш потужної з відомих атак та забезпечують як завгодно близькі до одиниці швидкість передачі, достовірність прийому, а також прийнятну складність відновлення відкритих повідомлень законним одержувачем. Доведення є конструктивним.

Ключові слова: рандомізований потоковий шифр, випадкове кодування, кореляційна атака, обґрунтована стійкість, код Ріда–Соломона.

A.N. Alekseychuk, S.V. Gryshakov

SECURE AND PRACTICAL RANDOMIZED STREAM CIPHERS BASED ON REED–SOLOMON CODES

Abstract. In this paper we consider a class of randomized stream ciphers based on joint employment of encryption, random coding, and error-correction coding by binary linear codes. It is shown that in this class there exist ciphers that have arbitrarily high computational security against the most powerful from all known attacks providing that both the transmission rate and the receiving accuracy have the value arbitrarily close to 1. The complexity of recovering plain messages by the legitimate receiver is acceptable as well. The proof is constructive.

Keywords: randomized stream cipher, random coding, correlation attack, provable security, Reed-Solomon code.

Алексейчук Антон Николаевич,
доктор техн. наук, доцент, заведующий кафедрой Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского», e-mail: alex-dtn@ukr.net.

Гришаков Сергей Владимирович,
соискатель, Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского», e-mail: gsv-crypto@mail.ru.