

## ГРАНИЦЫ ДЛЯ СКОРОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В РАНДОМИЗИРОВАННЫХ ПОТОЧНЫХ ШИФРСИСТЕМАХ МИХАЛЕВИЧА – ИМАИ

### Введение

В работах М. Михалевича и Х. Имаи [1 – 5] предложен общий подход к построению рандомизированных поточных шифрсистем на основе совместного применения шифрования, случайного (омофонного) кодирования и помехоустойчивого кодирования открытых сообщений двоичными линейными кодами. Основная цель создания таких шифрсистем – повышение стойкости (при сохранении практичности) поточных шифров, используемых в системах беспроводной связи, в частности в стандарте мобильной телефонии GSM. Другим побудительным мотивом служит создание симметричных шифрсистем, стойкость которых базируется на сложности решения известных вычислительно трудных математических задач, например задачи о декодировании случайного двоичного линейного кода [6].

В [4, 5] исследована стойкость шифрсистем Михалевича – Имаи относительно атаки на основе подобранных открытых текстов. Ряд более мощных атак описан в [7], где показано, что стойкость этих шифрсистем существенно зависит от строения их компонент и может быть заметно меньше, чем утверждают их разработчики. Исходя из условий стойкости и практичности, выбирать компоненты для построения шифрсистем Михалевича – Имаи следует с учетом ряда жестких ограничений, что представляет собой нетривиальную задачу. В связи с этим важной промежуточной задачей является выяснение потенциальных возможностей указанных шифрсистем и нахождение общих ограничений, которым удовлетворяют отдельные показатели их эффективности при заданных значениях других показателей.

Цель статьи – нахождение границ для скорости передачи информации в шифрсистемах Михалевича – Имаи при заданных ограничениях относительно вероятности правильного приема сообщений законным получателем и стойкости шифрования. Полученные результаты аналогичны известным границам для скорости передачи (при заданной корректирующей способности) двоичных линейных кодов [8 – 10] и могут быть использованы при выборе отдельных параметров и компонент для построения шифрсистем Михалевича – Имаи.

Работа имеет следующую структуру. В п. 1 сформулированы определения основных понятий и введены показатели эффективности шифрсистем Михалевича – Имаи. В п. 2 описана корреляционная атака на шифрсистему и получена нижняя оценка сложности этой атаки. Указанный результат дополняет утверждение 4 в [7], устанавливающее верхнюю оценку сложности аналогичной атаки на шифрсистему Михалевича – Имаи. В п. 3 изложены основные результаты статьи, а в заключительной части – краткие выводы.

### 1. Определение и основные показатели эффективности шифрсистем Михалевича – Имаи

Ниже используются следующие обозначения:  $V_n$  – множество двоичных векторов длины  $n$ ;  $F_{m \times n}$  – множество  $m \times n$ -матриц над полем  $F = \mathbf{GF}(2)$ .

Согласно [3, 4], исходными данными для построения *рандомизированной поточной шифрсистемы Михалевича – Имаи* 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  $G_l$  двоичного линейного  $[n, m]$ -кода  $C_l$  с эффективным алгоритмом декодирования (декодером)  $D: V_n \rightarrow C_l$ , 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  $f_i : K \rightarrow V_n$ ,  $i = 0, 1, \dots$ , 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  $u_0, v_0, u_1, v_1, \dots, u_t, v_t$ , где вектор  $u_i$  распределен равномерно на множестве  $V_{m-l}$ , а вектор  $v_i$  – по закону Бернулли с параметрами  $n, p$ , и вычисляет шифрованный текст  $z_0, z_1, \dots, z_t$  по формуле

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

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  $(s_i, u_i)G_2 \mapsto (s_i, u_i)G_2G_1$  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  $G_2$  (рис. 1).

Обозначим  $\mathcal{M} = \mathcal{M}(G_1, G_2, p, D)$  рандомизированную поточную шифрсистему Михале-вича – Имаи с параметрами  $l, m, n, p$  и декодером  $D$ , построенную по матрицам  $G_1, G_2$ , удовлетворяющим указанным выше условиям, и некоторому фиксированному генератору гаммы с множеством ключей  $K$  (здесь и далее предполагается, что источник открытых сообщений является безызбыточным, то есть вырабатывает последовательность  $s_0, s_1, \dots$  независимых случайных равновероятных векторов длины  $l$ ).

*Основные показатели эффективности шифрсистемы  $\mathcal{M}$ :*

- скорость передачи информации  $\rho(\mathcal{M}) = l/n$ ;
- вероятность  $p_e = \mathbf{P}\{D((s_i, u_i)G_2G_1 \oplus v_i) \neq (s_i, u_i)G_2G_1\}$  ошибочного декодирования сообщения  $z_i \oplus f_i(k)$  законным получателем,  $i = 0, 1, \dots$ ;
- вычислительная сложность декодера  $D$ .

Отметим, что в силу предположений о безызбыточности источника открытых сообщений и обратимости матрицы  $G_2$  вероятность  $p_e$  отлична от нуля и зависит только от кода  $C_1$ , декодера  $D$  и вероятности  $p$  искажения в ДСК. Кроме того, ясно, что  $\rho(\mathcal{M}) < 1$ .

Эффективность шифрсистемы  $\mathcal{M}$  зависит также от сложности процедур случайного и помехоустойчивого кодирования входных сообщений. Для уменьшения сложности кодирования в [5] предложено задавать матрицы  $G_1$  и  $G_2$  в виде

$$G_1 = \begin{pmatrix} I_{m-l} & 0 & A_1 \\ 0 & I_l & A_2 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 0 & I_l \\ I_{m-l} & B \end{pmatrix}, \quad (2)$$

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 не сужает класс рассматриваемых шифрсистем, однако не является обязательным.

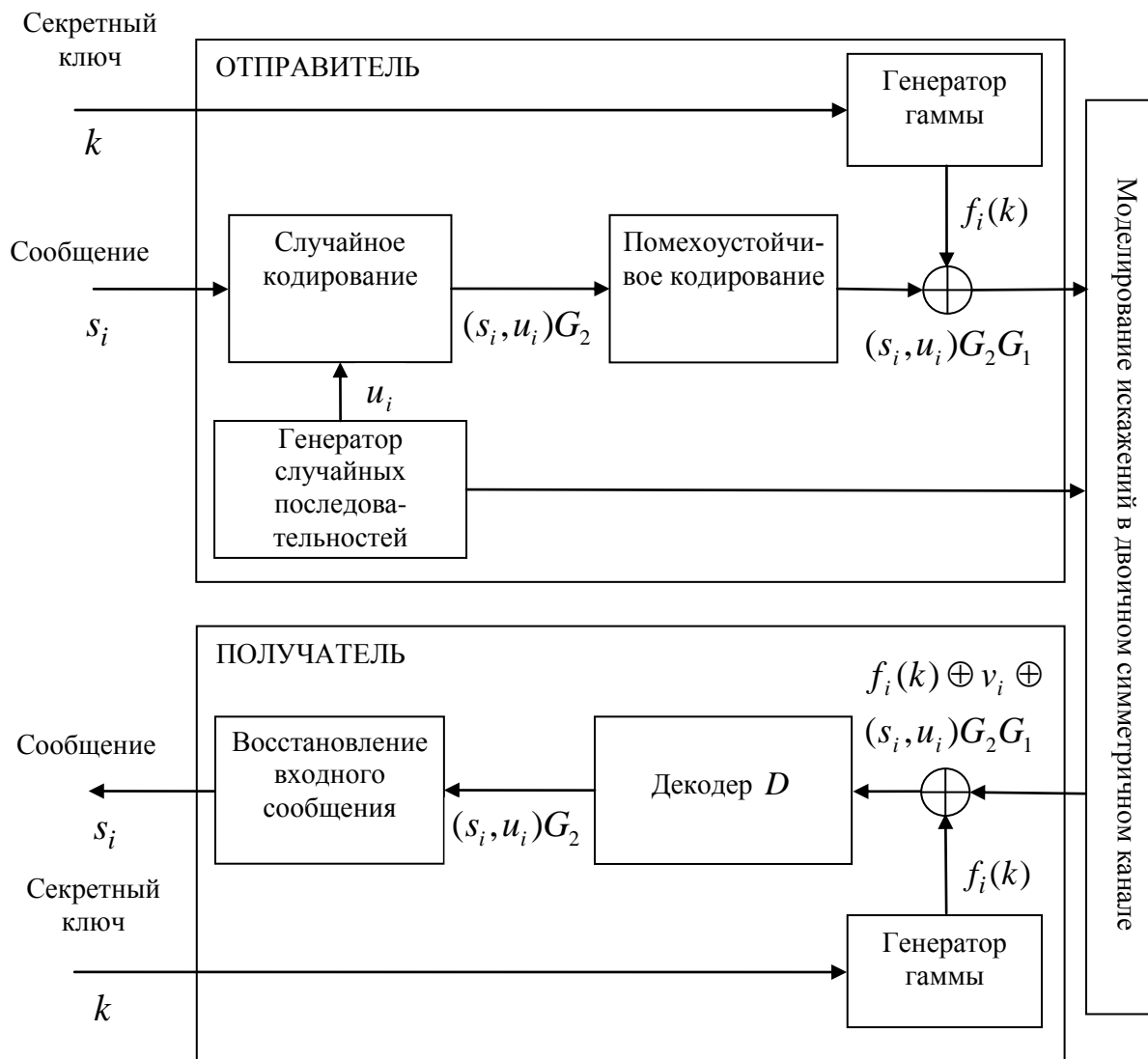


Рис. 1. Схема рандомизированной поточной шифрсистемы  $\mathcal{M}(G_1, G_2, p, D)$

### 1. Корреляционная атака на шифрсистему Михалевича – Имаи

Рассмотрим одну из наиболее мощных атак на шифрсистему  $\mathcal{M} = \mathcal{M}(G_1, G_2, p, D)$ , которая проводится с использованием подобранных векторов инициализации [7].

Обозначим

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

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

где  $wt(x)$  – вес Хемминга вектора  $x$ . 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) выбирает слово  $h \in C_0^\perp \setminus \{0\}$  веса  $d_0^\perp$ ;

2) подает  $T$  раз на вход шифрсистемы с неизвестным фиксированным ключом  $k$  сообщение  $s = 0$  и находит (для выбранного  $i = 0, 1, \dots$ ) зашифрованные сообщения

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

где  $u^{(0)}, v^{(0)}, u^{(1)}, v^{(1)}, \dots$  – независимые случайные векторы, распределенные по законам;

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

3) вычисляет

$$z^{(j)}h^T = f_i(k)h^T \oplus v^{(j)}h^T, \quad j \in \overline{1, T} \quad (3)$$

и восстанавливает значение  $f_i(k)h^T$  методом максимума правдоподобия.

Следующее утверждение устанавливает нижнюю оценку сложности описанной атаки.

**Утверждение 1.** Для успешного выполнения атаки с вероятностью  $1/2 + \theta$ ,  $\theta \in (0, 1/2)$ , необходимо не менее

$$T_\theta(\mathcal{M}) = 1/4 \cdot \theta^2 (1-2p)^{-2d_0^\perp} \quad (4)$$

уравнений системы (3).

*Доказательство.* Положим  $a = f_i(k)h^T$ ,  $\xi_j = z^{(j)}h^T = a \oplus v^{(j)}h^T$ ,  $j \in \overline{1, T}$ . В силу выбора вектора  $h$  и определения случайных векторов  $u^{(0)}, v^{(0)}, u^{(1)}, v^{(1)}, \dots$  последовательность  $\xi = \xi_1, \xi_2, \dots, \xi_T$  является схемой Бернулли с параметрами  $(T, p_a)$ , где  $p_0 = 1/2 \cdot \left(1 - (1-2p)^{d_0^\perp}\right)$ ,  $p_1 = 1 - p_0$ . При этом задача восстановления числа  $a$  по набору его искаженных значений (3) равносильна проверке следующих двух гипотез:

$$H_0: \mathbf{P}\{\xi_1 = 1\} = p_0; \quad H_1: \mathbf{P}\{\xi_1 = 1\} = p_1.$$

Для любого  $v \in V_T$  обозначим  $\mathbf{P}_0(v) = \mathbf{P}\{\xi = v | H_0\}$ ,  $\mathbf{P}_1(v) = \mathbf{P}\{\xi = v | H_1\}$ . Рассмотрим произвольный критерий для проверки гипотез  $H_0$  и  $H_1$ , основанный на критическом множестве  $A$ . Напомним, что вероятности ошибок первого и второго рода указанного критерия определяются по формулам  $\alpha = \sum_{v \in A} \mathbf{P}_0(v)$  и  $\beta = 1 - \sum_{v \in A} \mathbf{P}_1(v)$  соответственно. Для доказательства утверждения требуется убедиться в справедливости следующего соотношения:

$$1/2 \cdot (\alpha + \beta) \leq 1/2 - \theta \Rightarrow T \geq T_\theta(\mathcal{M}).$$

Воспользуемся леммой 15 в [11], согласно которой

$$\max_{A \subseteq V_T} \left| \sum_{v \in A} (q^{wt(v)}(1-q)^{T-wt(v)} - 2^{-T}) \right| \leq 2\sqrt{T} |2q-1|, \quad q \in [0, 1]. \quad (5)$$

Справедливы соотношения

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

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

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

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

Итак,  $T \geq 1/4 \cdot \theta^2 (1 - 2p_0)^{-2} = T_\theta(\mathcal{M})$ , что и требовалось доказать.

## 2. Границы для скорости передачи информации в шифрсистемах Михалевича – Имаи при заданных ограничениях относительно стойкости и вероятности правильного приема сообщений законным получателем

Напомним, что скоростью передачи двоичного линейного  $[n, k]$ -кода называется число  $k/n$ . Для любого натурального  $n > 1$  и  $\delta \in (0, 1)$  обозначим  $R_n(\delta)$  наибольшую скорость передачи двоичных линейных кодов длины  $n$  с минимальным расстоянием  $d \geq \delta n$ . В теории кодирования известен ряд верхних границ параметра  $R_n(\delta)$  (как точных, так и асимптотических при  $n \rightarrow \infty$ ,  $\delta = \text{const}$ ) [8 – 10]. Приведем здесь две границы, необходимые для дальнейшего.

*Лемма 1.* Для любого натурального  $n > 1$  справедливы неравенства

$$R_n(\delta) \leq -1/n \cdot \log(1 - (2\delta)^{-1}), \text{ если } 1/2 < \delta < 1, \quad (6)$$

$$R_n(\delta) \leq 1 - H_2(1/2 \cdot (1 - \sqrt{1 - 2\delta + 2/n}) - 1/n) + \log(n\sqrt{n})/n, \text{ если } 1/n < \delta \leq 1/2, \quad (7)$$

где  $H_2(x) = -x \log x - (1-x) \log(1-x)$ ,  $x \in (0, 1)$ .

*Доказательство.* Формула (6) следует из известной границы Плоткина для минимального расстояния  $d$  двоичного линейного  $[n, k]$ -кода (см., например, [10], с. 40):

$$d \leq n/2 \cdot \frac{2^k}{2^k - 1},$$

а формула (7) – из границы Бассалыго-Элайеса [9], с. 270: если  $2(d-1) \leq n$ , то

$$k/n \leq 1/n \cdot \log \left( d 2^n \left( \sum_{i=0}^t \binom{n}{i} \right)^{-1} \right),$$

где

$$t = \left\lfloor n/2 \cdot \left( 1 - \sqrt{1 - \frac{2(d-1)}{n}} \right) \right\rfloor,$$

и оценок для суммы биномиальных коэффициентов [8], с.302:

$$\sum_{i=0}^t \binom{n}{i} \geq \binom{n}{t} \geq \frac{2^{nH_2(t/n)}}{\sqrt{8n(1-t/n)t/n}} \geq \frac{2^{nH_2(t/n)}}{2\sqrt{n}}.$$

Лемма доказана.

Следующее вспомогательное утверждение является частным случаем известного результата о связи между скоростью передачи, пропускной способностью канала и вероятностью ошибочного декодирования [12], с. 223.

*Лемма 2.* Пусть  $C_1$  – двоичный линейный  $[n, m]$ -код, используемый для передачи случайных равновероятных сообщений в ДСК с вероятностью искажения  $p \in (0, 1/2)$ ,  $D$  – произвольный декодер кода  $C_1$  с вероятностью ошибочного декодирования  $p_e$  такой, что

$$p_e + H_2(p_e) < 1. \text{ Тогда } m/n \leq \frac{1 - H_2(p)}{1 - p_e - H_2(p_e)}.$$

Получим верхние границы скорости передачи информации в шифрсистемах Михалеви-ча – Имаи.

**Утверждение 2.** Пусть  $\mathcal{M} = \mathcal{M}(G_1, G_2, p, D)$  – шифрсистема Михалеви-ча – Имаи с параметрами  $l, m, n, p$  такая, что  $T_\theta(\mathcal{M}) \geq T \geq 1$ , где  $\theta \in (0, 1/2)$  и  $T_\theta(\mathcal{M})$  определяется по формуле (4). Тогда

$$\lambda_\theta(T, p) \stackrel{\text{def}}{=} -\frac{\log(4\theta^{-2}T)}{2n \log(1-2p)} \in (0, 1) \quad (8)$$

и

$$\rho(\mathcal{M}) \leq m/n - (1 - R_n(\lambda_\theta(T, p))). \quad (9)$$

В частности, если вероятность  $p_e$  ошибочного декодирования сообщений декодером  $D$  такова, что  $p_e + H_2(p_e) < 1$ , то

$$\rho(\mathcal{M}) \leq \frac{1 - H_2(p)}{1 - p_e - H_2(p_e)} - 1 - 1/n \cdot \log(1 - (2\lambda_\theta(T, p))^{-1}), \quad (10)$$

если  $\lambda_\theta(T, p) > 1/2$ ;

$$\rho(\mathcal{M}) \leq \frac{1 - H_2(p)}{1 - p_e - H_2(p_e)} - H_2\left(\frac{1}{2} \cdot (1 - \sqrt{1 - 2\lambda_\theta(T, p) + 2/n}) - 1/n\right) + \log(n\sqrt{n})/n, \quad (11)$$

если  $1/n < \lambda_\theta(T, p) \leq 1/2$ .

*Доказательство.* Рассмотрим код  $C_0 = \{(0, u)G_2G_1 : u \in V_{m-l}\}$ , скорость передачи которого равна  $1 - (m-l)/n$ . Из условия  $T_\theta(\mathcal{M}) \geq T$  и формулы (4) следует, что минимальное расстояние этого кода удовлетворяет неравенству  $d_0^\perp \geq n\lambda_\theta(T, p)$ . Поскольку при этом  $T \geq 1$  и  $d_0^\perp < n$  (в противном случае выполняется равенство  $n - (m-l) = 1$ , которое противоречит условию  $m < n$ ), то справедливо соотношение (8).

Далее, согласно определению функции  $R_n$ , скорость передачи кода  $C_0$  не превосходит числа  $R_n(\lambda_\theta(T, p))$ , откуда следует неравенство (9). Наконец, формулы (10), (11) вытекают из формул (6), (7) и леммы 2.

Утверждение доказано.

Отметим, что неравенства (9) – (11) справедливы для любых шифрсистем Михалеви-ча – Имаи, стойкость которых относительно описанной выше атаки составляет не менее  $T$  операций (зашифрования открытого сообщения  $s_i = 0$ ), а вероятность правильного приема сообщений законным получателем ограничена снизу числом  $1 - p_e$ , где  $p_e + H_2(p_e) < 1$ .

На рис. 2 показаны графики верхних границ параметра  $\rho(\mathcal{M})$  (как функций параметра  $p$ ), построенные с использованием соотношений (10), (11) при  $n = 512$ ,  $p_e = 10^{-8}$ ,  $\theta = 0,45$  и  $T \in \{2^{20}, 2^{30}, 2^{40}\}$ . Как видно из зависимостей на рисунке, при  $T = 2^{20}$  максимальная скорость передачи информации не превосходит 0,3 а при  $T = 2^{40}$  – меньше, чем 0,15. Таким образом, для обеспечения стойкости порядка  $2^{40}$  операций необходимо выбирать длину открытых сообщений  $l \leq \lfloor 0,15n \rfloor = 76$  бит (какими бы ни были остальные компоненты шифрсистемы).

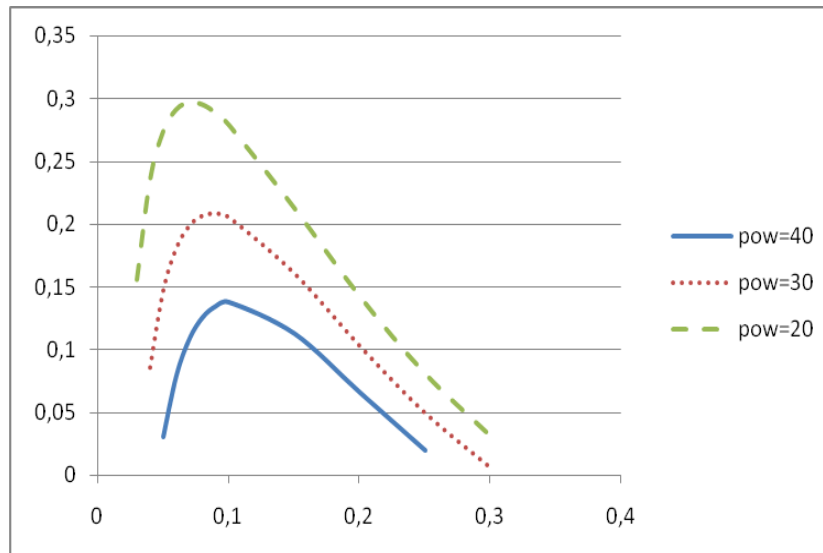


Рис. 2. Зависимости верхних оценок скорости передачи информации в шифрсистемах Михалевича – Имаи от вероятности искажения в ДСК

Отметим также, что при  $T > 2^{65}$  и указанных выше значениях  $n$ ,  $p_e$ ,  $\theta$  выражения в правых частях неравенств (10), (11) отрицательны для всех  $p$ , удовлетворяющих условию (8), что свидетельствует об отсутствии шифрсистем Михалевича – Имаи, обладающих указанной стойкостью. Кроме того, при передаче сообщений со скоростью 0,5 (или выше) максимальное значение стойкости шифрсистемы не превосходит  $T = 2^{4,88}$  операций, что свидетельствует о ее уязвимости к рассмотренной выше атаке.

В заключение докажем утверждение, устанавливающее нижнюю границу для скорости передачи, при которой существуют шифрсистемы Михалевича – Имаи с заданной стойкостью. Этот результат аналогичен известной границе Варшавова – Гилберта (см., например, [10], с. 44).

**Утверждение 3.** Пусть  $C_1$  – двоичный линейный  $[n, m]$ -код с порождающей матрицей  $G_1$  и дуальным расстоянием  $d_1^\perp \leq n/2$ ;  $p \in (0, 1/2)$ ,  $T \geq 1$ ,  $\theta \in (0, 1/2)$  и  $l \in \mathbf{N}$  таковы, что

$$l/n < m/n - H_2(\lambda_\theta(T, p)), \quad (12)$$

где

$$\lambda_\theta(T, p) = -\frac{\log(4\theta^{-2}T)}{2n \log(1-2p)} < d_1^\perp n^{-1}. \quad (13)$$

Тогда существует матрица  $G_2$  вида (1) такая, что  $\rho(\mathcal{M}(G_1, G_2, p, D)) \geq l/n$  и  $T_\theta(\mathcal{M}(G_1, G_2, p, D)) \geq T$  (каким бы ни был декодер  $D: V_n \rightarrow C_1$ ).

*Доказательство.* Достаточно убедиться в том, что при случайном равновероятном выборе матрицы  $B$  дуальное расстояние кода  $C_0 = \{(0, u)G_2G_1 : u \in V_{m-l}\}$ , соответствующего случайной матрице  $G_2$  вида (1), удовлетворяет условию  $d_0^\perp \geq n\lambda_\theta(T, p)$  с положительной вероятностью.

Запишем матрицу  $G_1$  в виде  $G_1 = \begin{pmatrix} G_1' \\ G_1'' \end{pmatrix}$ , где  $G_1' \in F_{(m-l) \times n}$ ,  $G_1'' \in F_{l \times n}$ . По определению

код  $C_0$  состоит из всех слов вида  $(0, u)G_2G_1 = (u, uB) \begin{pmatrix} G_1' \\ G_1'' \end{pmatrix} = uG_1' \oplus uBG_1''$ , где  $u \in V_{m-l}$ .

Предположим, что  $d_0^\perp < n\lambda_\theta(T, p)$ ; тогда существует ненулевой вектор  $x \in V_n$  веса  $wt(x) \leq \lfloor n\lambda_\theta(T, p) \rfloor$ , ортогональный коду  $C_0$ , то есть удовлетворяющий условию

$$B(G_1''x) = G_1'x. \quad (14)$$

Заметим, что  $G_1''x \neq 0$ , поскольку в противном случае  $G_1''x = 0$ ,  $G_1'x = 0$  и, значит,  $x \in C_1^\perp \setminus \{0\}$ , откуда на основании формулы (13) вытекает, что  $wt(x) \geq d_1^\perp > n\lambda_\theta(T, p)$ . Следовательно, для любого фиксированного  $x \in V_n \setminus \{0\}$  вероятность события (14) равна  $2^{-(m-l)}$ . Отсюда, используя неравенство Чернова (см., например, [9], с. 300) и формулу (12), получим, что

$$\begin{aligned} \mathbf{P}\{d_0^\perp < n\lambda_\theta(T, p)\} &\leq \sum_{x \in V_n: 1 \leq wt(x) \leq \lfloor n\lambda_\theta(T, p) \rfloor} 2^{-(m-l)} = \\ &= 2^{-(m-l)} \sum_{i=1}^{\lfloor n\lambda_\theta(T, p) \rfloor} \binom{n}{i} \leq 2^{-(m-l)} 2^{nH_2(n\lambda_\theta(T, p))} < 1. \end{aligned}$$

Итак, справедливо неравенство  $\mathbf{P}\{d_0^\perp \geq n\lambda_\theta(T, p)\} > 0$ , что и требовалось доказать.

Отметим, что утверждение 3, как и граница Варшавова – Гилберта, содержит лишь достаточные условия существования искомых объектов (шифрсистем Михалевича – Имаи с заданными стойкостью и скоростью передачи) без указания эффективного способа их построения. Разработка эффективных алгоритмов построения шифрсистем Михалевича – Имаи, обладающих необходимыми для приложений свойствами, является задачей дальнейших исследований.

### Выводы

Получены верхние границы для скорости передачи информации в рандомизированных поточных шифрсистемах Михалевича – Имаи при заданных ограничениях относительно вероятности правильного приема сообщений законным получателем и стойкости шифрования. Установлена нижняя граница для максимальной скорости передачи, при которой существуют шифрсистемы Михалевича – Имаи с заданной стойкостью.

Полученные результаты аналогичны известным границам для скорости передачи (при заданной корректирующей способности) двоичных линейных кодов. Они позволяют оценивать эффективность шифрсистем Михалевича – Имаи при заданных требованиях к их стойкости, а также максимальную стойкость при заданных требованиях к эффективности (скорости передачи информации и вероятности правильного приема сообщений законным получателем).

Применение полученных границ к шифрсистемам Михалевича – Имаи с параметром  $n = 512$  показывает, что их стойкость не превосходит  $2^{65}$  операций (какими бы ни были их компоненты). При передаче сообщений со скоростью 0,3 максимальное значение стойкости шифрсистемы не превосходит  $2^{20}$  операций, а увеличение скорости до 0,5 приводит к потере стойкости.

**Список литературы:** 1. *Mihaljević M.J.* A stream ciphering approach based on wiretap channel coding / M.J. Mihaljević, H. Imai // 8<sup>th</sup> Central European Conference of Cryptography 2008, Graz, Austria, July 2-4, E-Proc. (3 p.), 2008. 2. *Mihaljević M.J.* An approach for stream cipher design based on joint computing over random and secret data / M.J. Mihaljević, H. Imai // Computing. – 2009. – Vol. 85. – № 1-2. – P. 153 – 168. 3. *Mihaljević M.J.* An information-theoretic and computational complexity security analysis of a randomized stream cipher model / M.J. Mihaljević, H. Imai // 4<sup>th</sup> Western European Workshop on Research in Cryptology – WeWoRC 2011, Weimar, Germany, July 20-22, Conf. Record. – 2011. – P. 21 – 25. 4. *Mihaljević M.J.*



Employment of homophonic coding for improvement of certain encryption approaches based on the LPN problem / M.J. Mihaljević, H. Imai // Symmetric Key Encryption Workshop – SKEW 2011, Copenhagen, Denmark, Feb. 16-17, E-Proc. (17 p.), 2011. 5. *Mihaljević M.J.* Homophonic coding design for communication systems employing the encoding-encryption paradigm / M.J. Mihaljević, F. Oggier, H. Imai // arXiv:1012.5895v1 [cs.CR], 29 Dec, 2010. 6. *Berlekamp E.R.* On the inherent intractability of certain coding problems / E.R. Berlekamp, R.J. McEliece, H. van Tilborg // IEEE Trans. Inform. Theory. – 1978. – Vol. 24. – № 3. – P. 384 – 386. 7. *Alekseychuk A.N.* On the computational security of randomized stream ciphers proposed by Mihaljević and Imai / A.N. Alekseychuk, S.V. Gryshakov // Захист інформації. – 2014. – Т. 16. – № 4. – С. 328 – 334. 8. *Мак-Вильямс Ф.Дж.* Теория кодов, исправляющих ошибки / Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн ; пер. с англ. – М. : Связь, 1979. – 743 с. 9. *Дискретная математика и математические вопросы кибернетики* / Васильев Ю.Л., Ветухновский Ф.Я., Глаголев В.В. и др. – Т. 1. – М. : Наука, 1974. – 311 с. 10. *Влэдуц С.Г.* Алгеброгеометрические коды. Основные понятия / С.Г. Влэдуц, Д.Ю. Ногин, М.А. Цфасман. – М. : МЦНМО, 2003. – 504 с. 11. *Vaudenay S.* Decorrelation: a theory for block cipher security / S. Vaudenay // J. of Cryptology. – 2003. – Vol. 16. – № 4. – P. 249 – 286. 12. *Фано Р.* Передача информации. Статистическая теория связи / Р. Фано ; пер. с англ. – М. : Мир, 1966. – 438 с.

*Национальний технічний  
університет України «КПІ»*

*Поступила в редколлегию 11.04.2015*