Математическое моделирование архитектуры и алгоритмов функционирования нейронной сети АРТ-2Д при распознавании различных режимов функционирования динамических объектов подтвердили работоспособность предложенной непрерывной сети адаптивной резонансной теории.

ЗАКЛЮЧЕНИЕ

Разработана новая непрерывная сеть адаптивной резонансной теории АРТ-2Д, позволяющая запоминать и распознавать режимы функционирования реальных динамических объектов. Новая сеть существенно расширяет возможности разработки эффективных систем распознавания на основе сетей адаптивной резонансной теории. В дальнейшем предполагается разработка непрерывных нейронных сетей АРТ с несколькими параллельно работающими полями входных нейронов в каждом из модулей сети. Такие нейронные сети необходимы для распознавания режимов функционирования динамических объектов с большим числом наблюдаемых переменных.

Библиографический список

1. Оссовский, С. Нейронные сети для обработки информации [Текст] / С. Оссовский. – М. : Финансы и статистика, 2002. – 344 с.
2. Руденко, О. Г. Основы теории искусственных нейронных сетей [Текст] / О. Г. Руденко, Е. В. Бодянский. – Харьков : ТЕЛЕТЕХ, 2002. – 317 с.
3. Круглов, В В. Искусственные нейронные сети : теория и практика [Текст] / В. В. Круглов, В. В. Борисов. –М. : Горячая линия – Телеком, 2001. – 382 с.
4. Carpenter, G. A. Massively parallel architecture for self-organizing neural pattern recognition machine [Text] / G. A. Carpenter, S. A. Grossberg // Computing, Vision, Graphics and Image Processing. – 1987. – Vol. 37. – P. 54-115.
5. Grossberg, S. Competitive learning : from interactive activation to adaptive resonance [Text] / S. Grossberg // Cognitive Science. – 1987. – Vol. 11. – P. 23-63.
6. Fausett, L. Fundamentals of Neural Networks: architectures, algorithms and applications [Text] / L. Fausett. – New Jersey : Prentice Hall Int., Inc., 1994. – 461 p.
7. Дмитриенко, В. Д. Специализированное вычислительное устройство для распознавания динамических режимов объектов управления [Текст] / В. Д. Дмитриенко, Р. Д. Расрас, А. М. Сырой // Інформаційно-керуючі системи на залізничному транспорті. – 2002. – № 1. – С. 15-22.
8. Дмитриенко, В. Д. Повышение точности и стабильности информационно-измерительных систем на основе нейронных сетей АРТ [Текст] / В. Д. Дмитриенко, Р. Д. Расрас // Вестник ХГПУ. – 2000. – Вып. 92. – С. 149-154.

УДК 621.391

СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ НА АЛГЕБРАИЧЕСКИХ БЛОКОВЫХ КОДАХ

А. А. Кузнецов

ВВЕДЕНИЕ

Симметричные криптосистемы на алгебраических блоковых кодах (теоретико-кодовые схемы) впервые предложены в работе Рао и Нама [1]. Основная идея, заложенная в эту конструкцию, состоит в использовании в качестве секретного ключа порождающей матрицы G линейного блокового (n, k, d) кода. Шифрованная информация (криптограмма) в виде вектора c^* длины n формируется по правилу

$$c^* = I \cdot G + e, \qquad (1)$$

где вектор $c = I \cdot G$ принадлежит (n, k, d) коду с порождающей матрицей G, I – k-разрядный информационный вектор, вектор e – секретный (случайный) вектор ошибок.

Формирование криптограммы осуществляется путем кодирования информационной последовательности I длиной k информационных символов в кодовое слово длиной n кодовых символов и добавления к нему случайного вектора ошибки e. Вес вектора ошибок $w(e) \le t$, где t – число ошибок, которое может исправить (n, k, d) блоковый код, $d = 2 \cdot t + 1$. На приемной стороне уполномоченный пользователь (знающий секретный ключ) дешифрует полученную криптограмму – декодирует кодовое слово с ошибками (n, k, d) алгебраического блокового кода. Для него задача декодирования – полиномиально разрешимая задача. Злоумышленник, не зная секретный ключ – матрицу G, вынужден применять методы декодирования случайного кода, функция сложности которых растет экспоненциально [2 – 3]. Это положение лежит в основе всех криптосистем на алгебраических блоковых кодах: код с быстрым алгоритмом декодирования (полиномиальной сложности) маскируется под произвольный (случайный) линейный код, декодирование которого представляется как вычислительно сложная задача.

Параметры симметричной криптосистемы Рао-Нама на алгебраических (n, k, d) блоковых кодах над $GF(2^m)$ определяются следующими выражениями:

– размерность секретного ключа (в битах)

$$l_{K+} = k \cdot n \cdot m; \tag{2}$$

– размерность информационного вектора (в битах):

$$l_I = k \cdot m; \tag{3}$$

– размерность криптограммы (в битах)

$$l_S = n \cdot m; \tag{4}$$

– относительная скорость передачи

$$R = l_I / l_S = k / n. \tag{5}$$

В работах [4 – 5] исследована возможность одновременного повышения безопасности и помехоустойчивости каналов передачи данных на основе использования симметричных криптосистем с алгебраическими блоковыми кодами. В то же время основным недостатком схемы Рао-Нама является большой объем ключа. Действительно, для хранения секретной порождающей матрицы (n, k, d) блокового кода над $GF(q)$ необходимо хранить, в общем случае, $n \times k$ q-ичных символов. В статье рассматриваются теоретико-кодовые схемы, построенные на обширных классах альтернантных и алгеброгеометрических кодов, теоретически обосновывается построение симметричных криптосистем с небольшим объемом ключевых данных.

1. ИССЛЕДОВАНИЕ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ НА АЛЬТЕРНАНТНЫХ КОДАХ

Воспользуемся определением обобщенных кодов Рида-Соломона и их подкодов – альтернантных кодов [6 – 7].

Определение 1 [6]. Пусть $X = (X_1, X_2, \ldots, X_n)$ вектор над $GF(q^m)$, причем все X_i – различные элементы $GF(q^m)$. Пусть также $h = (h_1, h_2, \ldots, h_n)$ – вектор над $GF(q^m)$ с необязательно различными h_i элементами $GF(q^m)$. Тогда (n, k, d) обобщенный код Рида-Соломона $\mathrm{ОРС}_k(X, h)$ состоит из всех векторов вида

$$(h_1 \cdot F(X_1), h_2 \cdot F(X_2), \ldots, h_n \cdot F(X_n)),$$

где $F(x)$ – любой многочлен с коэффициентами из $GF(q^m)$, степень которого не превосходит k. Код ОРС является кодом с максимально достижимым кодовым расстоянием, т.е. $d = r + 1$, $r = n - k$. Проверочная матрица $\mathrm{ОРС}_k(X, h)$ равна:

$$H=\begin{pmatrix} Y_1 & Y_2 & \dots & Y_n \\ X_1\cdot Y_1 & X_2\cdot Y_2 & \dots & X_n\cdot Y_n \\ X_1^2\cdot Y_1 & X_2^2\cdot Y_2 & \dots & X_n^2\cdot Y_n \\ \dots & \dots & \dots & \dots \\ X_1^{r-1}\cdot Y_1 & X_2^{r-1}\cdot Y_2 & \dots & X_1^{r-1}\cdot Y_n \end{pmatrix}=\begin{pmatrix} 1 & 1 & \dots & 1 \\ X_1 & X_2 & \dots & X_n \\ X_1^2 & X_2^2 & \dots & X_n^2 \\ \dots & \dots & \dots & \dots \\ X_1^{r-1} & X_2^{r-1} & \dots & X_1^{r-1} \end{pmatrix}\cdot\begin{pmatrix} Y_1 & 0 & \dots & 0 \\ 0 & Y_2 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & Y_n \end{pmatrix}, \quad (6)$$

где вектор $Y = (Y_1, Y_2, \dots, Y_n)$ такой, что $\forall Y_i \in GF(q^m)$, $Y_i \neq 0$ и $\text{ОРС}^{\perp}_k(X, h) = \text{ОРС}_r(X, Y)$.

Коды ОРС дают механизм построения обширного класса альтернантных кодов [6-7].

Определение 2 [6]. Альтернантный (n, k, d) код $A(X, h)$ состоит из всех слов кода $\text{ОРС}^{\perp}_k(X, h)$ таких, что их компоненты лежат в поле $GF(q)$. Другими словами, $A(X, h)$ равен ограничению кода $\text{ОРС}_k(X, h)$ на подполе $GF(q)$. Таким образом, $A(X, h)$ состоит из всех векторов X над $GF(q)$, удовлетворяющих равенству

$$H \cdot X^T = 0,$$

где H – проверочная матрица $\text{ОРС}_k(X, h)$, задаваемая выражением (6).

Параметры альтернантного (n, k, d) кода $A(X, h)$ связаны соотношением:

$$n - mr \le k \le n - r;\ d \ge r + 1.$$

Порождающая матрица $A(X, h)$ может быть получена заменой каждого элемента матрицы H кода ОРС соответствующим вектором-столбцом длины m над $GF(q)$.

Альтернантные коды представляют собой обширный класс линейных блоковых кодов и обобщают (содержат как подкласс) все циклические коды, коды БЧХ и их обобщения, коды Гоппы, Сривэставы и др. [6 – 7].

Зададим симметричную теоретико-кодовую схему Рао-Нама на альтернантных кодах. Параметры криптосистемы определяются следующей леммой.

Лемма 1. Альтернантный (n, k, d) код над $GF(q)$ определяет симметричную теоретико-кодовую схему Рао-Нама с параметрами (в битах):

$$(n - (d-1)\cdot m)\cdot \log_2(q) \le l_{K+} \le (n - d + 1)\cdot n \cdot \log_2(q); \quad (7)$$

$$(n - (d-1)\cdot m)\cdot \log_2(q) \le l_I \le (n - d + 1)\cdot \log_2(q); \quad (8)$$

$$l_S = n \cdot \log_2(q); \quad (9)$$

$$(n - (d-1)\cdot m)/n \le R \le (n - d + 1)/n. \quad (10)$$

Доказательство Параметры криптосистемы на алгебраических блоковых кодах связаны соотношениями (2 – 5): $l_{K+} = k \cdot n \cdot m$; $l_I = k \cdot m$; $l_S = n \cdot m$; $R = k/n$. Параметры альтернантного (n, k, d) кода $A(X, h)$ связаны соотношением: $n - mr \le k \le n - r$; $d \ge r + 1$, где $A(X, h)$ задан через ограничение кода ОРС над $GF(q^m)$. После подстановки получим соотношения (7 – 10).

Результат леммы дает выражения по оценке параметров симметричных криптосистем на альтернантных кодах. В то же время из определения альтернантных кодов следует, что для однозначного построения проверочной матрицы кода необходимо и достаточно определить символы вектора-шаблона $Y = (Y_1, Y_2, \dots, Y_n)$. Практически это означает, что длина секретных ключевых данных в криптосистеме на альтернантных кодах будет определяться числом элементов вектора-шаблона Y, т.е. справедлива следующая теорема.

Теорема 1. Длина секретных ключевых данных в криптосистеме на альтернантных (n, k, d) кодах над $GF(q)$, заданных через ограничение ОРС кода над $GF(q^m)$, определяется выражением (в битах)

$$l_{K+} = n \cdot m \cdot \log_2(q). \quad (11)$$

Доказательство. Для определения всех коэффициентов проверочной матрицы альтернантного кода

$$H = \begin{pmatrix} Y_1 & Y_2 & \dots & Y_n \\ X_1 \cdot Y_1 & X_2 \cdot Y_2 & \dots & X_n \cdot Y_n \\ X_1^2 \cdot Y_1 & X_2^2 \cdot Y_2 & \dots & X_n^2 \cdot Y_n \\ \dots & \dots & \dots & \dots \\ X_1^{r-1} \cdot Y_1 & X_2^{r-1} \cdot Y_2 & \dots & X_1^{r-1} \cdot Y_n \end{pmatrix}$$

необходимо и достаточно определить все элементы вектора $Y = (Y_1, Y_2, \dots, Y_n)$. Размерность вектора $Y = (Y_1, Y_2, \dots, Y_n)$ – n символов из $GF(q^m)$. Следовательно, для того, чтобы определить секретный ключ – проверочную матрицу кода, потребуется n символов из $GF(q^m)$ или, что эквивалентно, $n \cdot m \cdot \log_2(q)$ бит.

Выражения (7 – 10) справедливы для криптосистем, построенных на всех кодах из обширного класса альтернантных кодов. Следующая лемма уточняет параметры криптосистем, построенных на альтернантных кодах Гоппы.

Лемма 2. Альтернантный (n, k, d) код Гоппы $\Gamma(L, G)$ над $GF(q)$ определяет симметричную теоретико-кодовую схему Рао-Нама с параметрами:

$$l_{K+} = n \cdot m \cdot \log_2(q); \quad (12)$$

$$l_I \geq (d-1) \cdot m \cdot \log_2(q); \quad (13)$$

$$l_S = n \cdot \log_2(q); \quad (14)$$

$$R \geq (n - (d-1) \cdot m)/n. \quad (15)$$

Доказательство. Альтернантный (n, k, d) код Гоппы $\Gamma(L, G)$ над $GF(q)$ состоит из всех векторов $c = (c_1, c_2, \dots, c_n)$ таких, что $R_c(x) \equiv 0 \bmod G(x)$, где $R_c(x) = \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i}$, $G(x)$ – многочлен с коэффициентами из $GF(q^m)$ (многочлен Гоппы), $L = (\alpha_1, \alpha_2, \dots, \alpha_n)$ – подмножество элементов из $GF(q^m)$ таких, что $G(\alpha_i) \neq 0 \ \forall \alpha_i \in L$ [6]. Параметры (n, k, d) кода Гоппы $\Gamma(L, G)$ связаны соотношениями: $n = |L|$, $k \geq n - mr$, $r = \deg G(x)$, $d \geq r + 1$. Подставим эти значения в выражения (2 – 5), с учетом (7-10) и (11) получим соотношения (12 – 15).

Последняя лемма определяет криптосистему на альтернантых кодах Гоппы, заданных матричным способом. В то же время, как показано в работах [4 – 5], выражение (12) можно существенно упростить. Для этого воспользуемся описанием кода Гоппы через многочлен Гоппы $G(x)$. Справедлива теорема.

Теорема 2. Альтернантный (n, k, d) код Гоппы $\Gamma(L, G)$ над $GF(q)$, заданный через многочлен Гоппы $G(x)$, определяет симметричную теоретико-кодовую схему Рао-Нама с длиной ключа:

$$l_{K+} \leq d \cdot \log_2(q); \quad (16)$$

Доказательство. Многочлен Гоппы $G(x)$ однозначно задает код Гоппы $\Gamma(L, G)$ над $GF(q)$. Действительно, как показано в [6 – 7], проверочную матрицу кода Гоппы можно записать в виде

$$H = \begin{pmatrix} G^{-1}(\alpha_1) & G^{-1}(\alpha_2) & \dots & G^{-1}(\alpha_n) \\ \alpha_1 G^{-1}(\alpha_1) & \alpha_2 G^{-1}(\alpha_2) & \dots & \alpha_n G^{-1}(\alpha_n) \\ \dots & \dots & \dots & \dots \\ \alpha_1^{r-1} G^{-1}(\alpha_1) & \alpha_2^{r-1} G^{-1}(\alpha_2) & \dots & \alpha_n^{r-1} G^{-1}(\alpha_n) \end{pmatrix},$$

т.е. все элементы матрицы однозначно задаются значениями многочлена $G(x)$ в элементах вектора $L = (\alpha_1, \alpha_2, \dots, \alpha_n)$ - подмножества элементов из $GF(q^m)$. Этого достаточно, чтобы задать симметричную криптосистему Рао-Нама. Секретным ключом в этом случае будет выступать многочлен $G(x)$, степень которого равна $\deg G(x) = r \leq d - 1$ [6]. Практически это означает, что секретный ключ полностью определяется $\deg G(x) + 1 = r + 1 \leq d$

значениями коэффициентов многочлена $G(x)$. Т.е. выражение (12) перепишется в виде $l_{K+} \le d \cdot log_2(q)$, что и завершает доказательство.

Выражения (7 – 16) устанавливают аналитическую зависимость между параметрами обширного класса альтернантных кодов и симметричных криптосистем на их основе по схеме Рао-Нама. В то же время в работе [2 – 3] показано, что криптосистемы на ОРС кодах могут быть взломаны алгоритмом полиномиальной сложности. Криптосистемы на альтернантных кодах (подкодах ОРС кодов) также считаются недостаточно стойкими. Там же отмечается, что перспективным направлением в развитии теоретико-кодовых схем являются криптосистемы на алгеброгеометрических кодах.

2. СИММЕТРИЧНЫЕ ТЕОРЕТИКО-КОДОВЫЕ СХЕМЫ НА АЛГЕБРОГЕОМЕТРИЧЕСКИХ КОДАХ

Перспективным направлением в развитии алгебраической теории блоковых кодов являются методы алгеброгеометрического кодирования [8 – 12]. Алгеброгеометрические коды как линейные системы, построенные по точкам гладкой проективной кривой, впервые были предложены в [8]. Асимптотически эти коды лежат выше границы Варшамова-Гилберта [9 – 10]. В [11 – 12] показано, что применение алгеброгеометрических кодов для кодирования передаваемой информации позволяет получить значительный энергетический выигрыш, который возрастает при переходе к кодам, построенным по кривым с бóльшим числом точек.

Рассмотрим алгеброгеометрический код над $GF(q)$, построенный по алгебраической кривой рода g. Кодовые параметры связаны соотношениями [8 – 10]: $k + d \ge n - g + 1$, длина кода n меньше либо равна числу точек на кривой X. При $2g < \alpha \le n$ алгеброгеометрический код имеет параметры $(n, \alpha - g + 1, d)$, $d \ge n - \alpha$, двойственный к нему код имеет параметры $(n, n - \alpha + g - 1, d^{\perp})$, $d^{\perp} \ge \alpha - 2g + 2$.

Параметры симметричной криптосистемы по схеме Рао-Нама на алгеброгеометрических кодах задаются следующей теоремой.

Теорема 3. Алгеброгеометрический (n, k, d) код над $GF(q)$, $q = 2^m$ определяет симметричную теоретико-кодовую схему с параметрами (в битах):

$$l_{K+} = (\alpha - g + 1) \cdot \left(2g\sqrt{q} + q + 1\right) \cdot m; \quad (17)$$

$$l_I = (\alpha - g + 1) \cdot m; \quad (18)$$

$$l_S = \left(2g\sqrt{q} + q + 1\right) \cdot m; \quad (19)$$

$$R = (\alpha - g + 1) / \left(2g\sqrt{q} + q + 1\right) \quad (20)$$

Доказательство. Симметричная теоретико-кодовая схема Рао-Нама, построенная с использованием порождающей матрицы алгебраического блокового (n, k, d) кода над $GF(2^m)$, обладает параметрами: $l_{K+} = k \cdot n \cdot m$, $l_I = k \cdot m$; $l_S = n \cdot m$; $R = k/n$. Параметры алгеброгеометрического кода, заданного через порождающую матрицу, определяются выражениями: $n \le N$, $k \ge \alpha - g + 1$, $d \ge n - \alpha$, где N – число точек алгебраической кривой, α – степень отображения, g - род кривой [8]. По теореме Хассе-Вейля $N \le 2g\sqrt{q} + q + 1$ [8-9]. Следовательно, длина алгеброгеометрического кода $n \le 2g\sqrt{q} + q + 1$. При выполнении равенства в последних выражениях параметры симметричной криптосистемы определяются следующими соотношениями:

$$l_{K+} = k \cdot n \cdot m = (\alpha - g + 1) \cdot \left(2g\sqrt{q} + q + 1\right) \cdot m;$$

$$l_I = k \cdot m = (\alpha - g + 1) \cdot m;$$

$$l_S = n \cdot m = \left(2g\sqrt{q} + q + 1\right) \cdot m;$$

$$R = l_I / l_S = k / n = (\alpha - g + 1) / \left(2g\sqrt{q} + q + 1\right),$$

что и завершает доказательство.

Пусть задан алгеброгеометрический код, построенный по эллиптической кривой (EC) через порождающую матрицу G^{EC}. Зададим симметричную теоретико-кодовую схему Рао-Нама, ее параметры определяются следующей теоремой.

Теорема 4. Алгеброгеометрический *(n, k, d)* код над $GF(2^m)$, построенный по эллиптической кривой через порождающую матрицу G^{EC}, определяет симметричную теоретико-кодовую схему Рао-Нама с параметрами:

$$l_{K+} = \alpha \cdot \left(2\sqrt{q} + q + 1\right) \cdot m;\ l_I = \alpha \cdot m;\ l_S = \left(2\sqrt{q} + q + 1\right) \cdot m;\ R = \alpha / \left(2\sqrt{q} + q + 1\right).$$

Доказательство. Действительно, симметричная теоретико-кодовая схема Рао-Нама, построенная с использованием порождающей матрицы алгебраического блокового *(n, k, d)* кода над $GF(2^m)$, обладает параметрами: $l_{K+} = k\ \ n \cdot m$; $l_I = k \cdot m$; $l_S = n \cdot m$; $R = k/n$. Эллиптической кривой в аффинном пространстве A^2 над полем $GF(q)$ называется гладкая кривая, заданная уравнением

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

или в P^2 заданная однородным уравнением

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3,$$

$a_i \in GF(q)$, род кривой $g = 1$ [13].

Алгеброгеометрический *(n, k, d)* код над $GF(q)$, построенный через отображение эллиптической вида $\varphi: EC \to P^{k-1}$, связан характеристиками $k + d \geq n$, причем: $n \leq 2\sqrt{q} + q + 1$, $k \geq \alpha$, $d \geq n - \alpha$. Подставим параметры эллиптического *(n, k, d)* кода над $GF(q)$ в выражения (2 – 5), получим искомые выражения.

В доказываемых ниже теоремах 5 – 8 устанавливается аналитическая зависимость между алгеброгеометрическими кодами, построенными по кривым Гурвица, Эрмита, Ферма, Сузуки, и параметрами соответствующих симметричных криптосистем по схеме Рао-Нама.

Теорема 5. Алгеброгеометрический *(n, k, d)* код над $GF(2^m)$, построенный по кривой Гурвица (*HurC*) через порождающую матрицу G^{HurC}, определяет симметричную теоретико-кодовую схему Рао-Нама с параметрами

$$l_{K+} = \left(\alpha - (q^{2/3} + q^{1/3})/2 + 1\right)\left(q + 2q^{2/3} + 2q^{1/3} + 1\right)m,\ l_I = \alpha \cdot m - (q^{2/3} + q^{1/3}) \cdot m/2 + m,$$

$$l_S = q \cdot m + 2q^{2/3} \cdot m + 2q^{1/3} \cdot m + m,\ R = \frac{\alpha + 1}{q + 2q^{2/3} + 2q^{1/3} + 1} - \frac{q^{2/3} + q^{1/3}}{2q + 4q^{2/3} + 4q^{1/3} + 2}.$$

Доказательство. Кривой Гурвица в проективном пространстве P^2 над полем $GF(q)$ называется гладкая кривая, заданная однородным уравнением

$$x^m y + y^m z + z^m x = 0,$$

причем $q = r^3$, r – положительное целое число, характеристика поля $GF(q)$ делится на $m^2 - m + 1$ [10].

Род кривой Гурвица $g = (q^{2/3} + q^{1/3})/2$. Число точек кривой Гурвица ниже границы Хассе-Вейля и определяется выражением вида $N = q + 2q^{2/3} + 2q^{1/3} + 1$. Параметры алгеброгеометрического кода по кривой Гурвица, заданного через порождающую матрицу, связаны соотношениями:

$$n \leq q + 2q^{2/3} + 2q^{1/3} + 1,\ k \geq \alpha - (q^{2/3} + q^{1/3})/2 + 1,\ d \geq n - \alpha$$

Подставим в соотношения для параметров схемы Рао-Нама, получим:

$$l_{K+} = \left(\alpha - (q^{2/3} + q^{1/3})/2 + 1\right)\left(q + 2q^{2/3} + 2q^{1/3} + 1\right)m,$$

$$l_I = \left(\alpha - (q^{2/3} + q^{1/3})/2 + 1\right)m = \alpha \cdot m - (q^{2/3} + q^{1/3}) \cdot m/2 + m,$$

$$l_S = \left(q + 2q^{2/3} + 2q^{1/3} + 1\right)m = q \cdot m + 2q^{2/3} \cdot m + 2q^{1/3} \cdot m + m,$$

$$R = \frac{\alpha - (q^{2/3} + q^{1/3})/2 + 1}{q + 2q^{2/3} + 2q^{1/3} + 1} = \frac{\alpha + 1}{q + 2q^{2/3} + 2q^{1/3} + 1} - \frac{q^{2/3} + q^{1/3}}{2q + 4q^{2/3} + 4q^{1/3} + 2}.$$

Теорема 6. Алгеброгеометрический *(n, k, d)* код над $GF(2^m)$, построенный по кривой Эрмита (HC) через порождающую матрицу G^{HC}, определяет симметричную теоретико-кодовую схему Рао-Нама с параметрами:

$$l_{K+} = \left(\alpha - (q - \sqrt{q})/2 + 1\right)\left(q\sqrt{q} + 1\right)m,\ l_I = \alpha m - (q - \sqrt{q}) \cdot m/2 + m,$$

$$l_S = q\sqrt{q}m + m,\ R = \frac{\alpha + 1}{q\sqrt{q} + 1} - \frac{q - \sqrt{q}}{2q\sqrt{q} + 2}.$$

Доказательство. Кривой Эрмита в P^2 над полем $GF(q)$ называется гладкая кривая, заданная однородным уравнением

$$x^{\sqrt{q}+1} + y^{\sqrt{q}+1} + z^{\sqrt{q}+1} = 0,$$

причем q = r^2, r – *положительное целое число [10].*

Род кривой Эрмита определяется выражением вида $g = (q - \sqrt{q})/2$. Число точек удовлетворяет верхней границе Хассе-Вейля и определяется выражением вида $N = q\sqrt{q} + 1$. Для алгеброгеометрического кода по кривой Эрмита, заданного через порождающую матрицу, справедливы кодовые соотношения:

$$n \le q\sqrt{q} + 1,\ k \ge \alpha - (q - \sqrt{q})/2 + 1,\ d \ge n - \alpha.$$

После подставки в (2 – 5) получим:

$$l_{K+} = \left(\alpha - (q - \sqrt{q})/2 + 1\right)\left(q\sqrt{q} + 1\right)m,$$

$$l_I = \left(\alpha - (q - \sqrt{q})/2 + 1\right)m = \alpha m - (q - \sqrt{q}) \cdot m/2 + m,$$

$$l_S = \left(q\sqrt{q} + 1\right)m = q\sqrt{q}m + m,$$

$$R = \frac{\alpha - (q - \sqrt{q})/2 + 1}{q\sqrt{q} + 1} = \frac{\alpha + 1}{q\sqrt{q} + 1} - \frac{q - \sqrt{q}}{2q\sqrt{q} + 2}.$$

Теорема 7. Алгеброгеометрический *(n, k, d)* код над $GF(2^m)$, построенный по кривой Ферма (FC) через порождающую матрицу G^{FC}, определяет симметричную теоретико-кодовую схему Рао-Нама с параметрами:

$$l_{K+} = \left(\alpha - \frac{q^{\frac{4}{3}} + 2q - q^{\frac{1}{3}}}{2} + 1\right)\left(q^{\frac{5}{3}} - q - q^{\frac{2}{3}} + 1\right)m,\ l_I = \alpha m - \left(q^{\frac{4}{3}} + 2q - q^{\frac{1}{3}}\right)\frac{m}{2} + m,$$

$$l_S = mq^{\frac{5}{3}} - mq - mq^{\frac{2}{3}} + m,\ R = \frac{\alpha + 1}{q^{\frac{5}{3}} - q - q^{\frac{2}{3}} + 1} - \frac{q^{\frac{4}{3}} + 2q - q^{\frac{1}{3}}}{2q^{\frac{5}{3}} - 2q - 2q^{\frac{2}{3}} + 2}.$$

Доказательство, как и прежде, состоит в подстановке конструктивных параметров алгеброгеометрического кода, построенного по кривой Ферма, в выражения (2-5).

Кривой Ферма в проективном пространстве P^2 над полем $GF(q)$ называется гладкая кривая, заданная однородным уравнением

$$x^{q^{2/3}+q^{1/3}+1} + x^{q^{2/3}+q^{1/3}+1} + x^{q^{2/3}+q^{1/3}+1} = 0,$$

причем q = r^3, r – *положительное целое число [10].*

Род кривой Ферма определяется выражением вида $g = (q^{4/3} + 2q - q^{1/3})/2$. Число точек кривой Ферма ниже границы Хассе-Вейля и определяется выражением вида $N = q^{5/3} - q - q^{2/3} + 1$. Тогда параметры алгеброгеометрического кода по кривой Ферма связаны соотношениями:

$$n \le q^{\frac{5}{3}} - q - q^{\frac{2}{3}} + 1,\ k \ge \alpha - \frac{q^{\frac{4}{3}} + 2q - q^{\frac{1}{3}}}{2} + 1,\ d \ge n - \alpha$$

После подстановки в (2-5) получим искомые соотношения.

Теорема 8. Алгеброгеометрический *(n, k, d)* код над $GF(2^m)$, построенный по кривой Сузуки через порождающую матрицу G^{SC}, определяет симметричную теоретико-кодовую схему Рао-Нама с параметрами:

$$l_{K+} = \left(\alpha - \frac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor} + 1\right)\left(q^2 + 1\right)m,\ l_1 = \alpha m - \frac{\left(q^2 - q\right)m}{\lfloor 2\sqrt{q} \rfloor} + m,$$

$$l_S = mq^2 + m,\ R = \frac{\alpha + 1}{q^2 + 1} - \frac{q^2 - q}{\left(q^2 + 1\right)\lfloor 2\sqrt{q} \rfloor}.$$

Доказательство. Кривой Сузуки в проективном пространстве P^2 над полем $GF(q)$ называется гладкая кривая, заданная однородным уравнением

$$x^{q_0}(z^q + zx^{q-1}) + y^{q_0}(y^q + yx^{q-1}) = 0,$$

$q = 2^{2f+1}$, $q_0 = 2^f$, f – положительное целое число [14].

Род такой кривой определяется выражением вида $g = q_0(q-1) = \frac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor}$. Число точек кривой Сузуки ниже границы Хассе-Вейля и определяется выражением вида $N = q^2 + 1$. Подставим параметры алгеброгеометрических кодов по кривой Сузуки: $n \le q^2 + 1$, $k \ge \alpha - \frac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor} + 1$, $d \ge n - \alpha$ в выражения (2 – 5), получим искомые соотношения.

Теоремы 4 – 8 задают симметричные криптосистемы на алгеброгеометрических кодах, построенных по эллиптическим кривым, кривым Гурвица, Эрмита, Ферма, Сузуки. Как следует из выражений (17 – 20), криптосистемы обладают высокими конструктивными показателями. Так, например, длина криптограммы для рассмотренных случаев превышает аналогичный показатель для кодов ОРС над тем же алфавитом символов. В то же время всем симметричным криптосистемам присущ существенный недостаток – большой объем секретных ключевых данных. Предлагается конструктивный способ устранения больших объемов ключа, состоящий в использовании в качестве секретных данных параметров алгебраической кривой. Длина ключа в заданных таким образом криптосистемах определяется следующей теоремой.

Теорема 9. Алгеброгеометрический код над $GF(q)$ на алгебраической кривой X, заданной однородным многочленом степени $\deg X$, задает симметричную криптосистему Рао-Нама с длиной секретного ключа:

$$l_{K+} \le \frac{(\deg X + 1)(\deg X + 2)}{2} \cdot \log_2 q. \qquad (21)$$

Доказательство. Действительно, значения генераторных функций F_j в точках $P_i(X_i, Y_i, Z_i)$ алгебраической кривой X однозначно задают генераторную матрицу алгеброгеометрического кода [8 – 10]:

$$\begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \dots & F_{k-1}(P_{n-1}) \end{pmatrix}.$$

Значения точек кривой однозначно задаются видом однородного многочлена кривой, т.е. его коэффициентами. Однородный многочлен степени $\deg X$ состоит из суммы

одночленов степени deg$X$. Другими словами, число одночленов задает число коэффициентов, определяющих вид кривой. Всего в проективном пространстве P^n существует $C^n_{deg\,X+n}$ однородных одночленов, следовательно, в P^n однородный многочлен, задающий кривую, состоит из $\le C^2_{deg\,X+2}$ одночленов. Практически это означает, что для определения генераторной матрицы алгеброгеометрического кода над $GF(q)$ необходимо и достаточно задать

$$M \le C^2_{deg\,X+2} = \frac{(deg\,X+2)!}{(deg\,X)!\cdot 2!} = \frac{(deg\,X+1)(deg\,X+2)}{2}$$

символов из $GF(q)$, или, что эквивалентно, $M \cdot log_2 q$ бит.

Теорема 9 задает симметричные криптосистемы на алгеброгеометрических кодах с небольшим объемом ключа. Действительно, выражение (21) задает объем секретных ключевых данных, который растет как квадрат степени соответствующей кривой. В теоремах 5 – 8 размер ключа растет как произведение длины кода на число информационных символов, что значительно превышает аналогичный показатель для теоретико-кодовых схем из теоремы 9.

Приведем *пример*. Зафиксируем конечное поле $GF(2^6)$ и алгеброгеометрический код по кривой Эрмита с $R \approx 0{,}5$. По теореме 6 объем секретных ключевых данных составит:

$$l_{K+} \approx n\frac{R}{2}m = \frac{\left(q\sqrt{q}+1\right)^2}{2}\cdot m = 131584 \cdot 6 = 789504 \text{ бит.}$$

По выражению (21) объем секретных ключевых данных не превысит значения:

$$l_{K+} \le \frac{(deg\,X+1)(deg\,X+2)}{2}m = \frac{10\cdot 11}{2}6 = 330 \text{ бит.}$$

Очевидно, что в рассмотренном примере результат теоремы 9 позволяет уменьшить объем ключа более чем на три порядка.

3. ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ КРИПТОСИСТЕМ НА АЛГЕБРАИЧЕСКИХ БЛОКОВЫХ КОДАХ

Исследуем свойства симметричных теоретико-кодовых схем на алгебраических блоковых кодах. Введем следующие обозначения:

- I_{K+} – *сложность решения задачи криптоанализа (количество групповых операций);*
- I_K – *сложность формирования криптограммы (количество групповых операций);*
- I_{SK} – *сложность снятия криптограммы (количество групповых операций);*

Стойкость криптографического алгоритма, лежащего в основе криптосистем на алгебраических блоковых кодах базируется на решении трудноразрешимой задачи декодирования случайного кода. Следовательно, задача поиска хорошего (в смысле вычислительной сложности) алгоритма криптоанализа сводится к задаче поиска хорошего алгоритма декодирования случайного кода.

Декодирование произвольного линейного кода (кода общего положения) является весьма сложной вычислительной задачей, сложность ее решения растет экспоненциально. Так, для корреляционного декодирования произвольного (n, k, d) кода над $GF(q)$ необходимо, в общем случае, сравнить принятую последовательность со всеми разрешенными кодовыми словами и выбрать ближайшее (в метрике Хемминга), т.е. мощность множества слов кандидатов составит $N_K = q^k$. Даже для небольших n, k, d и q задача корреляционного декодирования весьма трудоемка и, очевидно, методы криптоанализа на его основе малоэффективны.

Одним из наиболее эффективных подходов к декодированию линейного блокового кода с произвольной внутренней структурой является перестановочный метод [6 – 7, 15]. Основная идея такого декодирования состоит в том, что набор информационных множеств

используется для образования соответствующего набора кандидатов в кодовые слова. Далее, согласно алгоритму, среди этих кандидатов выбирается ближайший. Если при этом в принятой последовательности нет ошибок в одной из информационных компонент, переданное кодовое слово будет находиться в перечне кандидатов. Таким образом, если фактическая комбинация ошибок может быть исправлена декодером максимального правдоподобия, то это кодовое слово будет иметь наименьшее расстояние к принятой последовательности и будет выбрано перестановочным декодером. При рассмотрении переставного декодирования комбинация ошибок будет найдена, если удастся найти такое информационное множество, которое целиком содержит эту комбинацию. Такое множество, являющееся кровельной комбинацией ошибок, и набор проверочных множеств, которые покрывают все наборы ошибок данного типа, называются покрытием. Задача декодера состоит в том, чтобы найти проверочное множество, которое покрывает неизвестную комбинацию ошибок. Рассмотрим границы для количества кровельных множеств.

Предположим, что с помощью *(n, k, d)* кода исправляются все комбинации из *t* или меньшего количества ошибок. Рассмотрим комбинацию только из *t* кратных ошибок, так как все ошибки меньшей кратности будут покрыты. Общее количество ошибок во всех *n* позициях равняется C_n^t. Поскольку объем кровельного множества равняется $n - k$, максимальное количество комбинаций ошибок, которые могут быть покрытые данным множеством равняется C_{n-k}^t. Поэтому наименьшее количество множеств, которые могут исправить все комбинации с *t* ошибок, ограничивается следующим выражением [15]:

$$N_{покр} \geq \frac{C_n^t}{C_{n-k}^t} = \frac{n(n-1)...(n-t-1)}{(n-k)(n-k-1)...(n-k-t-1)}$$

Для обработки каждого элемента кровельного множества и принятия решения по соответствующему слову-кандидату необходимо вычислить синдром и сравнить его с нулем. Для вычисления синдромной последовательности для каждого слова-кандидата необходимо выполнить $n \cdot r$ операций (при матричном умножении слова-кандидата на проверочную матрицу). Таким образом, сложность задачи криптоанализа как решение задачи декодирования случайного кода перестановочным декодером будет определяться выражением

$$I_{K+} = N_{покр} \cdot n \cdot r. \qquad (22)$$

Формирование криптограммы соответствует вычислению кодового слова замаскированного кода с последующим добавлением случайного вектора ошибок. Если замаскированный код задан порождающей матрицей G, то для формирования кодового слова достаточно умножить информационный вектор длины k символов на матрицу G. Сложность реализации этой процедуры составит $k \cdot n$ операций сложения и умножения над конечным полем [6 – 7, 15]. Сложность операции добавления случайного вектора ошибок к кодовому слову составит n операций сложения. Следовательно, запишем:

$$I_K = (k+1) \cdot n.$$

Сложность снятия криптограммы определяется сложностью алгебраического алгоритма декодирования алгебраического блокового кода. Для кодов БЧХ, кодов РС и их обобщений, альтернантных кодов и их подклассов, локализация ошибок сводится к решению системы линейных уравнений от *t* неизвестных, где *t* – исправляющая способность соответствующего кода [6 – 7, 15]. Для нахождения значений ошибок (для недвоичных кодов) необходимо дополнительно решить еще одну систему линейных уравнений от *t* неизвестных. Сложность декодирования, в этом случае, составит t^2 операций сложения и умножения в конечном поле для двоичных кодов и $2 \cdot t^2$ операций для недвоичных. Следовательно, для кодов ОРС запишем:

$$I_{SK} = 2 \cdot t^2.$$

Для алгеброгеометрических кодов сложность декодирования определяется следующим выражением [16]:

$$I_{SK} = 4t^2 + (t^2 - t)^2/4.$$

Проведем оценку отношения сложности взлома к сложности дешифрования I_{K+} / I_{SK} уполномоченным пользователем. Зафиксируем конечное поле $GF(2^m)$ и блоковый (n, k, d) код с относительной скоростью кодирования R. На рис. 1 – 4 приведены зависимости I_{K+} / I_{SK} для случаев: 1) коды по SC, 2) коды по FC, 3) коды по HC, 4) коды по $HurC$, 5) коды по EC, 6) коды ОРС.

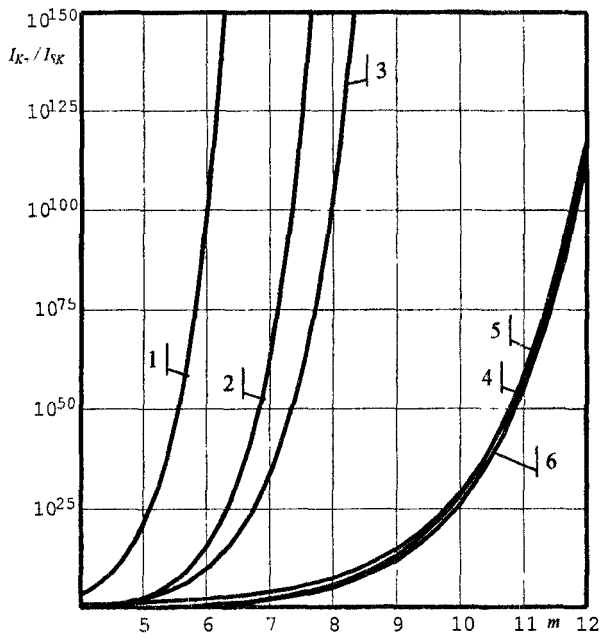

Рис. 1. Отношение I_{K+} / I_{SK} в криптосистеме на кодах с $R = 0,1$

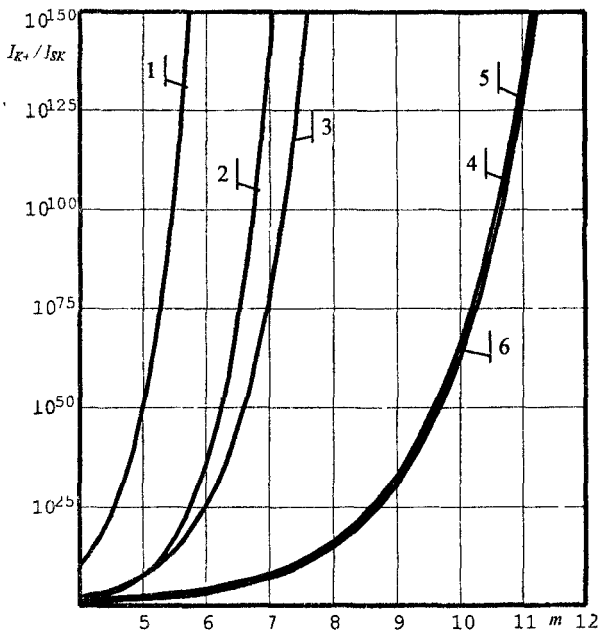

Рис. 2. Отношение I_{K-} / I_{SK} в криптосистеме на кодах с $R = 0,25$

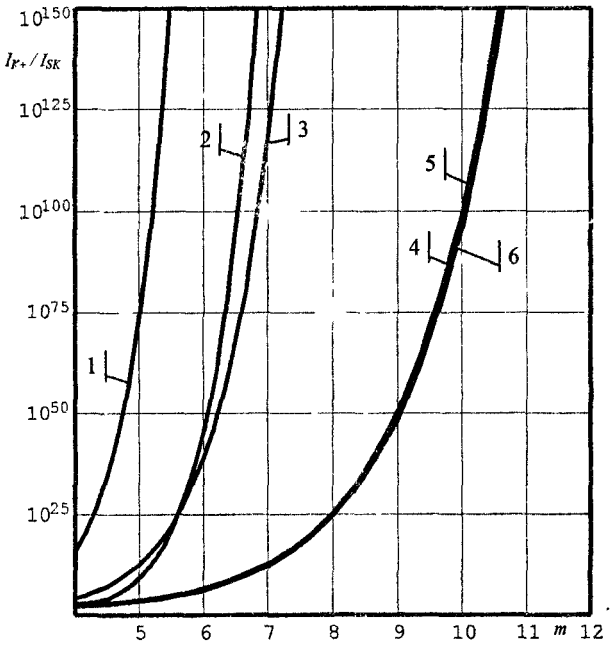

Рис. 3. Отношение I_{K-} / I_{SK} в криптосистеме на кодах с $R = 0,5$

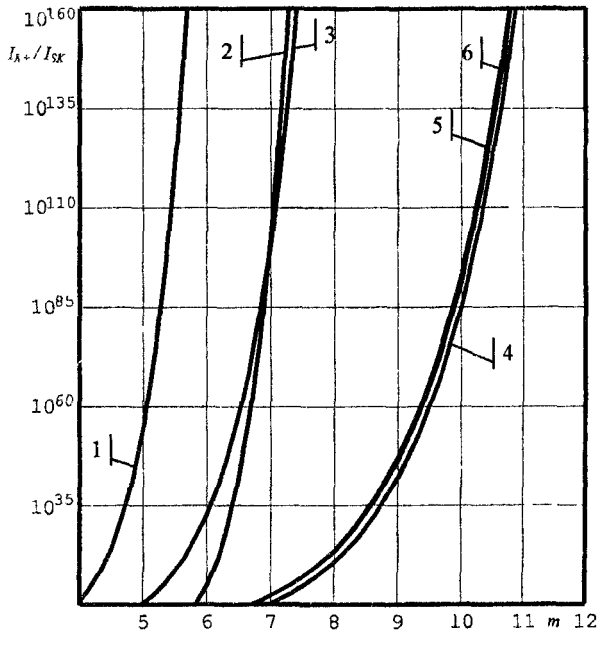

Рис. 4. Отношение I_{K+} / I_{SK} в криптосистеме на кодах с $R = 0,75$

Проведем исследования помехоустойчивости теоретико-кодовых схем и криптостойкости, которую они могут обеспечить при интегрированном повышении безопасности и достоверности информации. Зафиксируем алгебраический (n, k, d) код над $GF(q)$. Пусть e – вектор ошибок, который добавляется к кодовому слову при формировании криптограммы (см. выражение (1)). Пусть $w(e) \leq t$, $t = (d - 1)/2$. Обозначим

долю веса вектора ошибок вектора e, приходящегося на искусственное внесение теоретико-кодовой схемой, символом $\rho = w(e)/t$. Тогда потенциальная стойкость криптосистемы, построенная на алгебраических кодах, будет определяться величиной $\rho\ t$, а помехоустойчивость передаваемых криптограмм определяться величиной $(1-\rho)\ t$

Помехоустойчивость определяется минимальным соотношением сигнал/шум, необходимым для обеспечения требуемой достоверности Зафиксируем соотношение сигнал/шум и вид модуляции. Предположим, что передача цифровых сообщений осуществляется по дискретному каналу без памяти, т.е. ошибки в последовательно передаваемых кодовых символах происходят независимо с вероятностью P_o. Тогда вероятность ошибки кратности i на длине блока n будет равна $P_i = C_n^i P_o^i (1-P_o)^{n-i}$. Если процедура декодирования позволяет исправить t ошибок, то вероятность ошибочного декодирования равна:

$$P_{ош} = \sum_{i=t+1}^{n} P_i = \sum_{i=t+1}^{n} C_n^i P_o^i (1-P_o)^{n-i}.$$

При интегрированном решении задач безопасности и помехоустойчивости теоретико-кодовая схема будет исправлять $(1-\rho)\ t$ возникших ошибок, следовательно.

$$P_{ош} = \sum_{i=(1-\rho)t+1}^{n} P_i = \sum_{i=(1-\rho)t+1}^{n} C_n^i P_o^i (1-P_o)^{n-i}.$$

Аналогичные изменения внесем и в выражение (22) для расчета I_{K+}. На рис. 3 – 8 приведены зависимости $I_{K+}(\rho)$ и $P_{ош}(\rho)$ для кодов ОРС, алгеброгеометрических кодов по эллиптическим кривым, кривым Гурвица, Эрмита, Ферма, Сузуки с $R = 0{,}5$, $P_o = 10^{-3}$. Цифрами на рисунках обозначены зависимости, которые соответствуют использованию кодов над $GF(2^m)$: 1) $m = 3$; 2) $m = 4$; 3) $m = 5$, 4) $m = 6$, 5) $m = 7$, 6) $m = 8$, 7) $m = 9$, 8) $m = 10$, 9) $m = 11$; 10) $m = 12$.

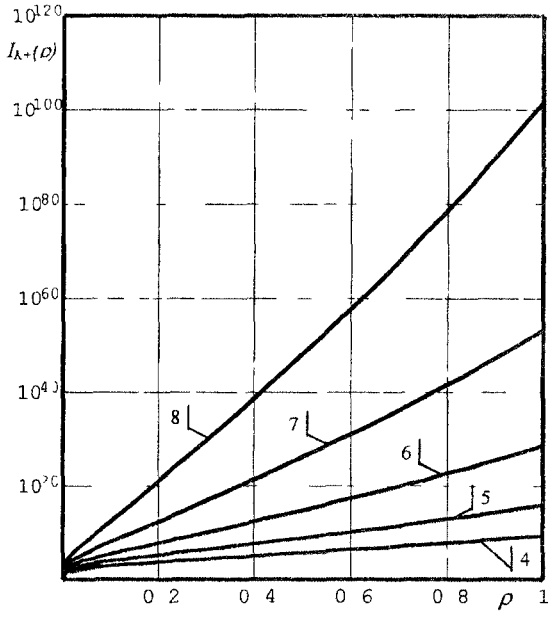

Рис 5 Зависимость $I_{K+}(\rho)$ для криптосистем на кодах ОРС

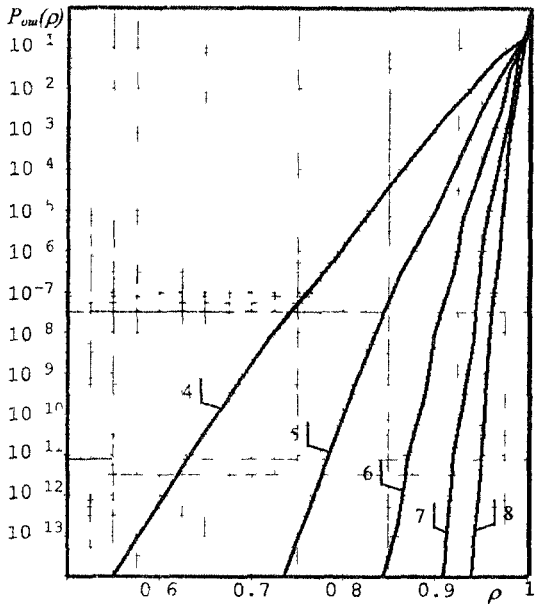

Рис 6 Зависимость $P_{ош}(\rho)$ для криптосистем на кодах ОРС

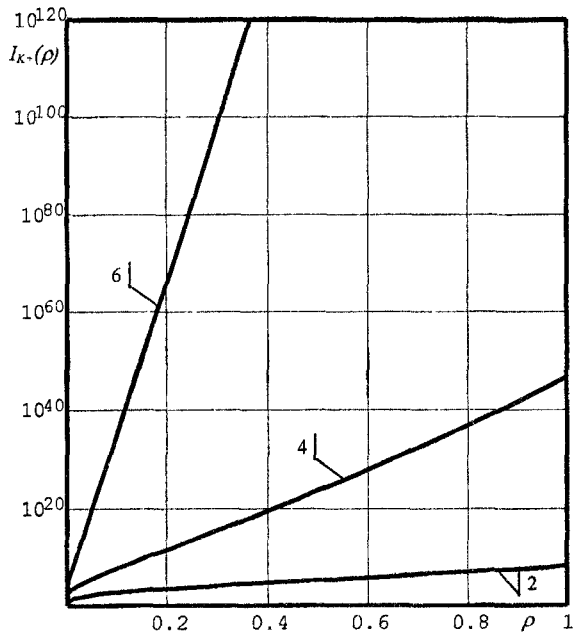

Рис. 7. Зависимость $I_{K+}(\rho)$ для криптосистем на кодах по *НС*

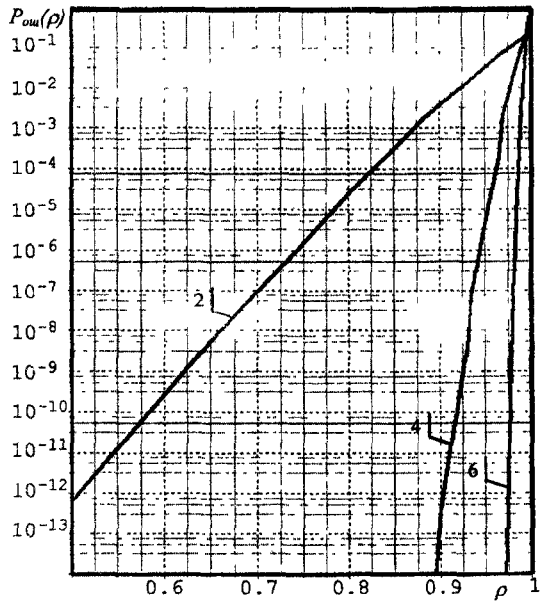

Рис. 8. Зависимость $P_{ош}(\rho)$ для криптосистем на по *НС*

Проведенные исследования показали, что использование алгебраических блоковых кодов позволяет построить криптографически стойкие теоретико-кодовые схемы. Сложность взлома возрастает при переходе к алгебраическим кодам с большей длиной, что достигается либо увеличением мощности конечного поля, либо переходом к алгеброгеометрическим кодам, построенным по кривым бóльшего порядка (см. рис. 1 – 4). Приведенные зависимости показывают, что наибольшую стойкость к взлому криптосистемы методом перестановочного декодирования обладают алгеброгеометрические коды, построенные по кривым Сузуки, Ферма, Эрмита. Их применение позволяет эффективно использовать теоретико-сложностную задачу декодирования случайного кода и получать большие значения I_{K+}/I_{SK}. Отношение I_{K+}/I_{SK} возрастает при переходе к кодам, построенным над полями бóльшей мощности. Для получения больших значений I_{K+}/I_{SK} наиболее предпочтительно использовать коды с $R \approx 0.5$.

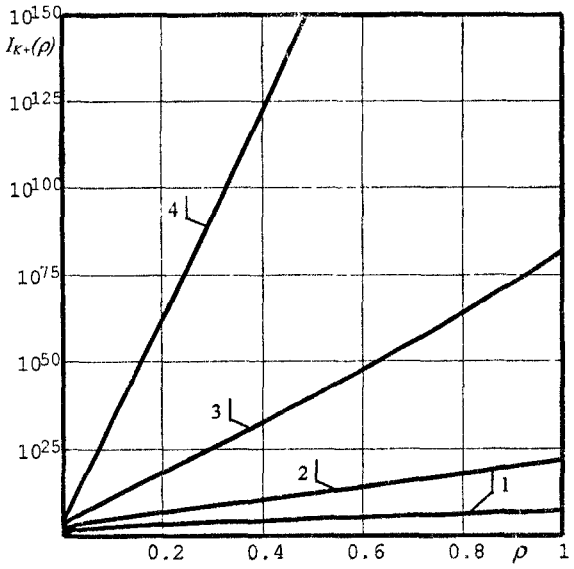

Рис. 9. Зависимость $I_{K+}(\rho)$ для криптосистем на кодах по *SC*

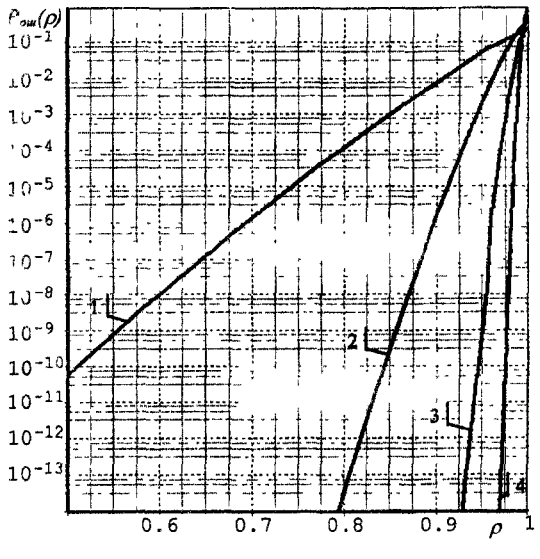

Рис. 10. Зависимость $P_{ош}(\rho)$ для криптосистем на кодах по *SC*

Проведенные исследования показали, что криптосистемы на алгебраических блоковых кодах позволяют эффективно обеспечивать безопасность и помехоустойчивость (достоверность) информации. Действительно, как показано на рис. 5 – 10, применение теоретико-кодовых схем позволяет интегрировано (в один прием) защищать информацию от воздействия злоумышленника и бороться с возникающими ошибками. Так, при $\rho \approx 0.8 \sim 0.9$ теоретико-кодовые схемы, построенные на большинстве алгебраических кодах над $GF(2^m)$, $m \approx 6 \sim 10$ позволяют обеспечить криптостойкость $I_{K+}(\rho) > 10^{30}$ и вероятность ошибочного декодирования $P_{ош}(\rho) < 10^{-9}$.

ЗАКЛЮЧЕНИЕ

В ходе проведенных исследований получили дальнейшее развитие симметричные криптосистемы, основанные на использовании теоретико-сложностной проблемы декодирования случайного кода, отличающиеся от известных применением комплексных механизмов обеспечения безопасности и достоверности информационных ресурсов, что позволяет эффективно защищать информацию от несанкционированного доступа, случайного или преднамеренного ее искажения. Впервые получено теоретическое обоснование симметричных криптосистем на алгеброгеометрических кодах, отличающееся от известных использованием в качестве секретного ключа параметров алгебраической кривой, что позволяет задавать теоретико-кодовые схемы с требуемыми параметрами и небольшим объемом служебных данных. Проведенные исследования показали, что криптосистемы на алгебраических блоковых кодах позволяют эффективно обеспечивать безопасность и помехоустойчивость (достоверность) информации. Их применение позволяет интегрировано (в один прием) защищать информацию от воздействия злоумышленника и бороться с возникающими ошибками. Криптосистемы, построенные на алгебраических блоковых кодах, обеспечивают криптостойкость (число операций, необходимых для взлома системы) более 10^{30} групповых операций. Потеря достоверности информации (вероятность ошибки) не превосходит $10^{-9} - 10^{-12}$.

Библиографический список

1. Rao, T. R. N. Private-key algebraic-coded cryptosystem [Text] / T. R. N. Rao, K. H. Nam // Advances in Cryptology : Proc. conf., New York, 1986. – 1986. – P. 35-48.

2. Сидельников, В. М. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона [Текст] / В. М. Сидельников, С. О. Шестаков // Дискретная математика. – 1992. – Т. 4, № 3. – С. 57-63.

3. Сидельников, В. М. Криптография и теория кодирования [Текст] / В. М. Сидельников // Московский университет и развитие криптографии в России : материалы конф МГУ. – 2002. – 22 с.

4. Халимов, Г. З. Применение помехоустойчивого кодирования для обеспечения безопасности каналов передачи данных [Текст] / Г. З. Халимов, А. Д. Буханцов // Передача, обработка и отображение информации : тр. междунар. науч.-техн. конф. / под ред. А. В. Королева ; НАНУ, ПАНИ. – Харьков, 1994. – С. 28.

5. Халимов, Г. З. Обеспечение безопасности каналов передачи данных на основе помехоустойчивых кодов [Текст] / Г. З. Халимов, А. В. Северинов // Системы управления и связь / ХВУ. – Харьков, 1996. – С. 116-119.

6. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки [Текст] / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М. : Связь, 1979. – 744 с.

7. Блейхут, Р. Теория и практика кодов, контролирующих ошибки [Текст] / Р. Блейхут. – М. : Мир, 1986. – 576 с.

8. Гоппа, В. Д. Коды на алгебраических кривых [Текст] / В. Д. Гоппа // Доклады АН СССР. – 1981. – Т. 259, № 6. – С. 1289-1290.

9. Цфасман, М. А. Коды Гоппы, лежащие выше границы Варшамова-Гилберта [Текст] / М. А. Цфасман // Проблемы передачи информации. – 1982. – № 3. – С. 3-6.

10. Pellikaan, Ruud Asymptotically good sequences of curves and codes [Text] / Pellikaan Ruud // Proc. 34th Allerton conf. on communication, control, and computing, Urbana-Champaign, October 2-4, 1996. – 1996. – P. 276-285.

11. Кузнецов, А. А. Энергетический выигрыш алгеброгеометрического кодирования [Текст] / А. А. Кузнецов // Радиотехника : всеукр. межвед. научн.-техн. сб. – 2003. – Вып. 133. – С. 76-82.

12. Кузнецов, А. А. Энергетическая эффективность алгеброгеометрических кодов [Текст] / А. А. Кузнецов // Электронное моделирование : междунар. науч.-теорет. журн. / НАНУ, РАН. – 2004. – № 2. – С. 27-38.

13. Болотов, А. А Алгоритмические основы эллиптической криптографии [Текст] / А. А. Болотов. - М. : Изд-во МЭИ, 2000. – 100 с.

14. Bierbrauer, J. Universal hashing and geometric codes, to appear in Designs [Electronic resource] / J. Bierbrauer // Codes and Cryptography. – 1994. – Access mode: http://www.math.mtu.edu/~jbierbra/hashco1.ps

15. Кларк, Дж.-мл. Кодирование с исправлением ошибок в системах цифровой связи [Текст] : пер. с англ. / Дж.-мл. Кларк, Дж. Кейн ; под ред. Б. С. Цыбакова. – М. : Радио и связь, 1987. – 392 с.

16. Кузнецов, А. А. Алгебраическое декодирование кодов по кривым Эрмита [Текст] / А. А Кузнецов, А. В. Северинов, Д. А. Задворный, В. Н. Лысенко // Вісник ХПІ. – 2003. – № 26. – С 95-102.

УДК 621.395

ОБ УМЕНЬШЕНИИ ОБЪЕМА ТРАФИКА ПРИ ПАКЕТНОЙ ПЕРЕДАЧЕ РЕЧЕВЫХ СООБЩЕНИЙ ЗА СЧЕТ КОДИРОВАНИЯ ПАУЗ*

С. П. Белов, Е. И. Прохоренко

ВВЕДЕНИЕ

Речевые сообщения передаются посредством речевых сигналов, под которыми, в контексте данной работы, понимается результат кодирования звуков речи с помощью некоторых устройств. В ряде случаев, как, например, в традиционной телефонии, передаются электрические сигналы, возникающие на выходе микрофона при воздействии колебаний воздушного потока. В современных цифровых системах речевые сигналы представляют в дискретном виде и передают, в соответствии с некоторыми правилами, значения дискретных отсчетов, что приводит к необходимости кодирования сигнала.

Некоторые системы связи не могут работать непрерывно, например спутниковые системы передают сообщения в определенные моменты времени, находясь в определенных точках пространства, метеорные каналы связи работают при наличии определенных условий передачи. В этих случаях предварительно формируются пакеты битовых представлений сигналов, которые затем посылаются в канал связи, а на приемной стороне декодируются по известным правилам – такой принцип передачи информации принято называть пакетным режимом.

В процессе формирования пакетов исходные данные могут быть преобразованы таким образом, чтобы сократить объем их битового представления, что позволяет уменьшить трафик. Это можно считать основным преимуществом пакетной передачи. Во многом благодаря этому в настоящее время режим пакетной передачи получил широкое распространение в телекоммуникационных сетях, например в мобильных системах, IP-телефонии и др.

При передаче речевых сообщений сокращение трафика может быть достигнуто за счет кодирования пауз, так как при диалоге каждый из участников говорит, в среднем, только 35 процентов времени [1]. Кодирование пауз заключается в определении интервала, на котором отсутствуют звуки речи, фиксации начала этого интервала и его длительности. Кроме того, для воспроизведения речи с комфортным звучанием необходимо определить некоторые параметры этого интервала, например значения математического ожидания и наименьшего среднеквадратичного отклонения.

Известны различные методы обнаружения пауз в речевых сообщениях, среди которых достаточно широкое распространение получила технология VAD (детектор речевой активности) [3]. Технология VAD используется совместно с большим числом речевых кодеков. Обнаружение паузы основано на поиске сигнала продолжительностью в несколько сотен миллисекунд, со значениями отсчетов ниже заданного уровня (обычно –

* Работа финансировалась в рамках гранта Белгородского государственного университета.