УДК 511+519.719.2

КРИПТОГРАФИЧЕСКАЯ СИСТЕМА В ПОЛИНОМИАЛЬНЫХ КЛАССАХ ВЫЧЕТОВ ДЛЯ КАНАЛОВ С ШУМОМ И ИМИТИРУЮЩИМ ЗЛОУМЫШЛЕННИКОМ

Д.В. Самойленко, адъюнкт, e-mail: sam-0019@yandex.ru
О.А. Финько, профессор, e-mail: ofinko@yandex.ru
Краснодарское высшее военное училище (ВИ)

Рассматривается помехоустойчивая модулярная криптографическая система, функционирующая в полиномиальных классах вычетов. Предложен алгоритм расширения системы оснований криптографической системы. Представлена оценка помехоустойчивости предложенной криптографической системы по отношению к традиционной.

Ключевые слова: *Китайская теорема об остатках, криптоаналитик, криптография, криптосистема, модулярная арифметика, полиномиальные классы вычетов, поля Галуа, помехоустойчивое кодирование.*

CRYPTOGRAPHIC SYSTEM IN POLYNOMIAL CLASS DEDUCTION FOR CHANNEL WITH NOISE AND IMITATING VIOLATOR

D.V. Samoylenko, adjunct, e-mail: sam-0019@yandex.ru
O.A. Finko, professor, e-mail: ofinko@yandex.ru
Krasnodar High Military School (VI)

Antinoise modular cryptographic system, functioning in polynomial class deduction, is discussed. The Offered algorithm of the expansion of the system of the bases of the cryptographic system. The estimation to noise-immunity offered cryptographic system to traditional is presented.

Key words: *Chinese remainder theorem, cryptanalyst, cryptography, cryptosystem, modular arithmetic, polynomial residues, Galois fields, antinoise coding.*

Задача любой криптографической системы (КС) заключается в защите данных от неконтролируемых изменений при передаче их по общедоступным каналам связи или другим видам использования. Способность КС обеспечить эту защиту делает ее чувствительной к влиянию искажений различного происхождения (случайные помехи, имитирующие действия криптоаналитика) при передаче по каналам связи. Изменение одного бита зашифрованных данных (криптограмм) может привести к частичной или полной потере расшифрованных данных, что в свою очередь приведет к потере управления и контроля при выполнении различных задач. Поэтому для достоверной передачи криптограмм возникает необходимость в использовании КС, адаптированных для работы в таких условиях.

В то же время известны подходы к созданию таких КС [1, 2]. Так, в работах [3–7] рассматривалась блочная КС, функционирующая в кольце Z_p неотрицательных целых чисел по модулю p. Однако известно, что системы, функционирующие в поле Галуа с характеристикой 2, обладают рядом преимуществ, а именно высоким быстродействием, простотой реализации и эффективностью.

Цель статьи – разработка помехоустойчивой модулярной КС в кольце многочленов $GF(2)$, способной противостоять различного рода деструктивным воздействиям, как преднамеренным, так и непреднамеренным.

В [3–7] предложена КС в кольце Z_p, которая способна противостоять деструктивным воздействиям различного происхождения.

Правила зашифрования и расшифрования определены в общем виде:

$$C \to E_{k_1}{:}M, \tag{1}$$

$$M \to D_{k_2}{:}C, \tag{2}$$

где C – криптограмма, M – открытый текст, k_1 и k_2 – ключи, соответственно зашифрования и расшифрования. При $k_1 \neq k_2$ КС называется асимметрической, а при $k_1 = k_2$ – симметрической [8].

Открытый текст M разбивается на блоки $M_1, M_2, \ldots, M_n$, где M_i – m-битовый блок от-

крытого текста. Соответственно для получения последовательности криптограмм $C_1, C_2,\ldots, C_n$ потребуется n операций зашифрования и n операций расшифрования. Поэтому преобразования (1) и (2) можно переписать в виде

$$\begin{cases} C_1 \to E_{k_{1,1}}{:}M_1, \\ C_2 \to E_{k_{1,2}}{:}M_2, \\ \ldots\ldots\ldots\ldots \\ C_n \to E_{k_{1,n}}{:}M_n, \end{cases} \tag{3}$$

$$\begin{cases} M_1 \to D_{k_{2,1}}{:}C_1, \\ M_2 \to D_{k_{2,2}}{:}C_2, \\ \ldots\ldots\ldots\ldots \\ M_n \to D_{k_{2,n}}{:}C_n, \end{cases} \tag{4}$$

где $k_{1,i} \neq k_{2,i}$ или $k_{1,i} = k_{2,i}$ $(i = 1, 2, \ldots, n)$ в соответствующих случаях.

Рассмотрим систему блоков криптограмм (3) в виде системы двоичных векторов:

$$\begin{cases} \vec{C}_1 = \left\{c_{m-1}^{(1)} c_{m-2}^{(1)} \ldots c_0^{(1)}\right\}, \\ \vec{C}_2 = \left\{c_{m-1}^{(2)} c_{m-2}^{(2)} \ldots c_0^{(2)}\right\}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \vec{C}_n = \left\{c_{m-1}^{(n)} c_{m-2}^{(n)} \ldots c_0^{(n)}\right\}, \end{cases} \tag{5}$$

где $c_j^{(i)} \in \{0,1\}\left(i = 1, 2, \ldots, n,\ j = m-1,\ m-2, \ldots, 0\right)$.

Представим коэффициенты $c_j^{(i)}$ системы (5) как коэффициенты алгебраических полиномов полей Галуа $GF(p)$ характеристики $p = 2$. Тогда (5) примет вид

$$\begin{aligned} C_1(x) &= c_{m-1}^{(1)} x_1^{m-1} + c_{m-2}^{(1)} x_1^{m-2} + \ldots + c_0^{(1)}, \\ C_2(x) &= c_{m-1}^{(2)} x_2^{m-1} + c_{m-2}^{(2)} x_2^{m-2} + \ldots + c_0^{(2)}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ C_n(x) &= c_{m-1}^{(n)} x_n^{m-1} + c_{m-2}^{(n)} x_n^{m-2} + \ldots + c_0^{(n)}. \end{aligned}$$

При передаче последовательности криптограмм $C_1(x), C_2(x),\ldots, C_n(x)$ влияние искажений проявляется в том, что вместо одних переданных криптограмм принимаются другие $C_1^*(x), C_2^*(x),\ldots, C_n^*(x)$. Соответственно в результате расшифрования принятых криптограмм адресат получит блоки открытых текстов $M_1^*, M_2^*,\ldots, M_n^*$, отличающиеся от исходных $M_1, M_2,\ldots, M_n$.

Будем представлять $C_i(x)$ как наименьшие неотрицательные полиномиальные вычеты по основаниям-полиномам $m_i(x)$, таким что $\gcd\left(m_i(x), m_j(x)\right) = 1$, где $i \neq j$; $i, j = 1, 2, \ldots, n$, причем $0 \le \deg C_i(x) < \deg m_i(x)$, где $\deg C_i(x)$ – степень полинома $(i = 1, 2, \ldots, n)$. Тогда множество криптограмм $\left\{C_1(x), C_2(x),\ldots, C_n(x)\right\}$ можно рассматривать как единый информационный блок модулярного полиномиального кода (МПК) по системе оснований-полиномов $m_1(x), m_2(x),\ldots, m_n(x)$. В соответствии с Китайской теоремой об остатках для многочленов [9, 10] для заданного множества попарно взаимно простых многочленов $m_1(x), m_2(x),\ldots, m_n(x)$ и множества многочленов $C_1(x), C_2(x),\ldots, C_n(x)$, таких что $\deg C_i(x) < \deg m_i(x)$, система сравнений

$$\begin{cases} C(x) \equiv C_1(x) \bmod m_1(x), \\ C(x) \equiv C_2(x) \bmod m_2(x), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ C(x) \equiv C_n(x) \bmod m_n(x) \end{cases} \tag{6}$$

имеет единственное решение $C(x)$.

Выполняется операция расширения МПК $\left\{C_1(x), C_2(x),\ldots, C_n(x)\right\}$ путем введения r избыточных оснований-полиномов $m_{n+1}(x)$, $m_{n+2}(x),\ldots, m_{n+r}(x)$ и получение r избыточных вычетов $C_{n+1}(x), C_{n+2}(x),\ldots, C_{n+r}(x)$:

$$\begin{cases} C_{n+1}(x) \equiv C(x) \mod m_{n+1}(x), \\ C_{n+2}(x) \equiv C(x) \mod m_{n+2}(x), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ C_{n+r}(x) \equiv C(x) \mod m_{n+r}(x). \end{cases}$$

Причем $\gcd\left(m_i(x), m_j(x)\right) = 1$, где $i \neq j$; $i, j = 1, 2, \ldots, n+r$ и $\deg m_1(x),\ldots, \deg m_n(x) < \deg m_{n+1}(x) < \ldots < \deg m_{n+r}(x)$.

В совокупности элементы информационного блока $\left\{C_1(x), C_2(x),\ldots, C_n(x)\right\}$ и полученная последовательность избыточных криптограмм $\left\{C_{n+1}(x), C_{n+2}(x),\ldots, C_{n+r}(x)\right\}$ обра-

зуют расширенный МПК в кольце многочленов $F[x]$ над $GF(2)$.

Введем метрику МПК и линейного двоичного кода (ЛДК).

Метрика МПК: *весом кодового вектора* $\{C(x)\}$ в МПК является количество ненулевых криптограмм (вычетов) и обозначается $w(\{C(x)\})$.

Кодовое расстояние между $\{C(x)\}$ и $\{D(x)\}$ определяется как вес их разности $w(\{C(x)-D(x)\})$.

Минимальное кодовое расстояние МПК – наименьшее расстояние между двумя любыми кодовыми векторами по Хэммингу с учетом данного определения веса.

Под одиночной ошибкой в кодовом слове МПК будем понимать произвольное искажение одной из криптограмм кодового слова МПК. Соответственно q-кратная ошибка определяется как произвольное искажение q криптограмм кодового слова МПК.

Полученный код обнаруживает все одиночные ошибки, если количество избыточных криптограмм $r \ge 1$, и исправляет q или менее ошибок, если $2q \le r$.

Обнаружение ошибок в принятой последовательности криптограмм $C_1^*(x),\ldots,C_n^*(x),\ldots,C_{n+r}^*(x)$ осуществляется путем сравнения $C^*(x)$ с $M(x)=\prod_{i=1}^{n} m_i(x)$, где $C^*(x)$ – решение системы сравнений (6) для принятой последовательности криптограмм $C_i^*(x)$ $(i=1, 2, \ldots, n+r)$; * указывает на возможные искажения.

Если $0 \le C^*(x) < M(x)$, то принимается решение о том, что принятая последовательность криптограмм $C_1^*(x),\ldots,C_n^*(x),\ldots,C_{n+r}^*(x)$ не содержит обнаруживаемых ошибок. В противном случае фиксируется ошибка, предельная кратность которой определяется обнаруживающими способностями кода [11, 12].

Метрика ЛДК соответствует метрике Хэмминга. *Нормой (или весом)* кодового слова $x=(x_1, x_2, \ldots, x_n)$ называется число ненулевых символов.

Кодовое расстояние между словами $x=(x_1, x_2, \ldots, x_n)$ и $y=(y_1, y_2, \ldots, y_n)$ линейного двоичного кода над $GF(q)$ равно весу их разности.

Минимальное кодовое расстояние ЛДК – минимальное из всевозможных попарных расстояний между его кодовыми словами и равно $d_{\min}$.

Под одиночной ошибкой в метрике ЛДК понимается искажение одного бита криптограммы $C_i(x)$. Соответственно t-кратная ошибка определяется как произвольное искажение t бит криптограммы $C_i(x)$.

Пример n-канальной КС с одним избыточным каналом представлен на рис. 1.

Таким образом, вводимая в виде избыточных криптограмм избыточность, обеспечивает свойства КС контролировать ошибки кодового слова МПК (количество искаженных криптограмм) и корректировать ошибки в отдельно взятой криптограмме (количество искаженных бит).

Расширение МПК является одной из основных операций, выполняемых в указанной КС. В [13] предложен алгоритм расширения модулярного кода, функционирующего в кольце Z_p. Рассмотрим данный алгоритм применительно к рассматриваемой КС. Суть его состоит в решении системы сравнений (6). В соответствии с Китайской теоремой об остатках для многочленов [9, 10], решению системы сравнений (6) будет соответствовать выражение

$$C(x)=\sum_{i=1}^{n} C_i(x)B_i(x) - r_C(x)M(x), \qquad (7)$$

где $B_i(x)=k_i(x)M_i(x)$ – полиномиальные ортогональные базисы, $k_i(x)=M_i^{-1}(x) \bmod m_i(x)$, $M_i(x)=\dfrac{M(x)}{m_i(x)}$, $M(x)=\prod_{i=1}^{n} m_i(x)$, $r_C(x)$ – ранг $C(x)$ для $i=1, 2, \ldots, n$.

Естественно полагать, что определение $r_C(x)$ будет производиться непосредственно в процессе выполнения операции расширения. Тогда

$$r_C(x)=\text{Quotient}\left(\frac{C_i(x)k_i(x)}{m_i(x)}\right), \qquad (8)$$

где $\text{Quotient}\left(\dfrac{C_i(x)k_i(x)}{m_i(x)}\right)$ – наименьшее целое от деления $C_i(x)k_i(x)$ на основание $m_i(x)$, для $i=1, 2, \ldots, n$.

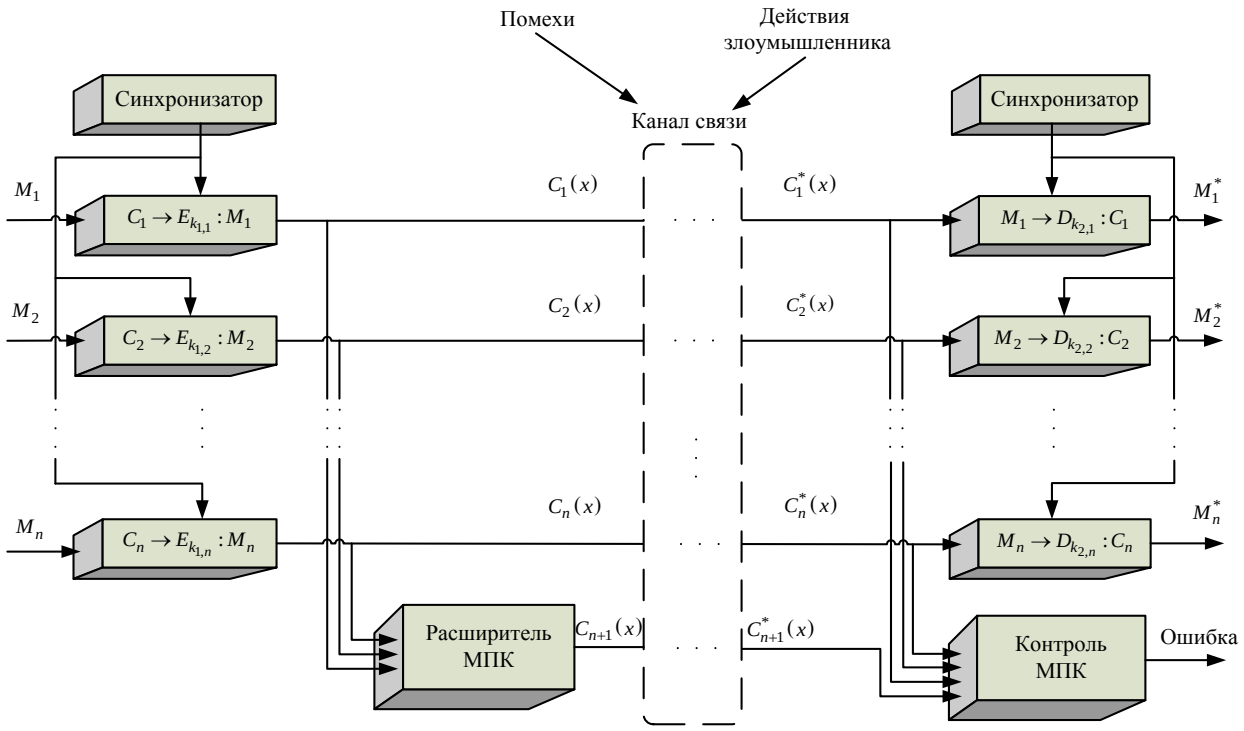

Рис. 1. КС с обнаружением однократных ошибок

Для получения $C_{n+1}(x)$ выражение (7) с учетом (8) примет вид

$$C_{n+1}(x) = C_1(x)\beta_1(x) \bmod m_{n+1}(x) + \\ + C_2(x)\beta_2(x) \bmod m_{n+1}(x) + \ldots \\ \ldots + C_n(x)\beta_n(x) \bmod m_{n+1}(x) - \\ - r_C(x)\mu(x) \bmod m_{n+1}(x),$$

где

$\beta_i(x) = B_i(x) \bmod m_{n+1}(x)$, $\mu(x) = M(x) \bmod m_{n+1}(x)$, для $i = 1, 2, \ldots, n$.

Выполним

$$G_1(x) = C_1(x)\beta_1(x) \bmod m_{n+1}(x) = \\ = g_{m-1}^{(1)} x^{m-1} + g_{m-2}^{(1)} x^{m-2} + g_{m-3}^{(1)} x^{m-3} + \ldots + g_0^{(1)},$$

$$G_2(x) = C_2(x)\beta_2(x) \bmod m_{n+1}(x) = \\ = g_{m-1}^{(2)} x^{m-1} + g_{m-2}^{(2)} x^{m-2} + g_{m-3}^{(2)} x^{m-3} + \ldots + g_0^{(2)},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$G_n(x) = C_n(x)\beta_n(x) \bmod m_{n+1}(x) = \\ = g_{m-1}^{(n)} x^{m-1} + g_{m-2}^{(n)} x^{m-2} + g_{m-3}^{(n)} x^{m-3} + \ldots + g_0^{(n)},$$

$$A(x) = r_C(x)\mu(x) \bmod m_{n+1}(x) = \\ = a_{m-1} x^{m-1} + a_{m-2} x^{m-2} + a_{m-3} x^{m-3} + \ldots + a_0.$$

Представим полиномы $G_i(x)(i = 1, 2, \ldots, n)$ и $A(x)$ в форме последовательности двоичных коэффициентов:

$$G_1(x) = \left(g_{m-1}^{(1)}\ g_{m-2}^{(1)}\ g_{m-3}^{(1)} \ldots g_0^{(1)}\right),$$
$$G_2(x) = \left(g_{m-1}^{(2)}\ g_{m-2}^{(2)}\ g_{m-3}^{(2)} \ldots g_0^{(2)}\right),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$G_n(x) = \left(g_{m-1}^{(n)}\ g_{m-2}^{(n)}\ g_{m-3}^{(n)} \ldots g_0^{(n)}\right),$$
$$A(x) = \left(a_{m-1}\ a_{m-2}\ a_{m-3} \ldots a_0\right).$$

Получим

$$C_{n+1}(x) = x^{m-1}\left(a_{m-1} \oplus \bigoplus_{i=1}^{n} g_{m-1}^{(i)}\right) + \\ + x^{m-2}\left(a_{m-2} \oplus \bigoplus_{i=1}^{n} g_{m-2}^{(i)}\right) + \\ + x^{m-3}\left(a_{m-3} \oplus \bigoplus_{i=1}^{n} g_{m-3}^{(i)}\right) + \ldots \\ \ldots + \left(a_0 \oplus \bigoplus_{i=1}^{n} g_0^{(i)}\right) \bmod m_{n+1}(x) = \\ = \sum_{j=0}^{m-1} x^j \bigoplus_{i=1}^{n}\left(a_j \oplus g_j^{(i)}\right) \bmod m_{n+1}(x).$$

Приведенные выше преобразования позволяют без прямого определения $C(x)$, в соответствии с Китайской теоремой об остатках для многочленов, окончательно получить итоговое выражение для вычисления $C_{n+1}(x)$.

Ввиду способности КС обнаруживать и исправлять ошибки, возникает необходимость в оценке достоверности передачи данных. Для этого выполним расчет достоверности при передаче данных по каналу связи для предложенной многоканальной КС и КС-прототипа, использующей линейные коды.

Под достоверностью будем понимать степень соответствия принятых криптограмм переданным. Численно достоверность передачи информации будем характеризовать вероятностью гарантированно обнаруживаемой ошибки в криптограммах на приемной стороне КС [10, 14].

Введем допущение: ошибки кратности q в передаваемой последовательности криптограмм $C_1(x),\ldots,C_n(x),\ldots,C_{n+r}(x)$ происходят независимо друг от друга и их распределение подчиняется биномиальному закону:

$$P(q)=\sum_{q=1}^{n}\binom{n}{q}p^q(1-p)^{n-q}.$$

Для того чтобы оценить степень деструктивных воздействий на передаваемую последовательность криптограмм $C_1(x),\ldots,C_n(x),\ldots,C_{n+r}(x)$, необходимо знать величину p вероятности ошибочного приема криптограммы $C_i(x)$. Вероятность p ошибочного приема криптограммы $C_i(x)$ является величиной постоянной и вычисляется, если известна закономерность возникновения искажений, вызванных действиями криптоаналитика. Действия криптоаналитика на криптограмму $C_i(x)$ носят аналитический характер, поэтому последствия таких воздействий для приемной стороны являются *непредсказуемыми и случайными* [15]. Примем допущение: искажения вызванные действиями криптоаналитика на криптограмму $C_i(x)$ носят равновероятный характер.

Пусть p_{cr} – вероятность искажения бита криптограммы $C_i(x)$, вызванного действиями криптоаналитика. На основании принятых допущений, а также с учетом $d_{\min}$ определим для КС-прототипа вероятность искажения криптограммы $C_i(x)$, вызванного действиями криптоаналитика:

$$p_{cr_1}=p_{cr}\sum_{t=i+1}^{h}\binom{h}{t}2^{-h},$$

где $\sum_{t=i+1}^{h}\binom{h}{t}$ – общее количество искажений в криптограмме $C_i(x)$, не обнаруживаемых данным методом контроля; $i+1\le t\le h$ – кратность ошибок, которые не будут обнаружены данным методом контроля; h – длина блока криптограммы; 2^h – общее количество возможных искажений.

Для многоканальной КС вероятность искажения криптограммы $C_i(x)$, вызванного действиями криптоаналитика, равна:

$$p_{cr_2}=\frac{p_{cr}\left(\binom{h}{1}+\binom{h}{2}+\cdots+\binom{h}{t}\right)}{2^h}=\frac{p_{cr}2^h}{2^h}=p_{cr},$$

так как КС контролирует ошибки любой кратности в масштабе одной криптограммы $C_i(x)$.

Тогда для КС-прототипа, использующей линейные коды, вероятность гарантированно обнаруживаемых ошибок равна:

$$P_{er_1}=\sum_{q=1}^{n}\binom{n}{q}p_{cr_1}^{q}\left(1-p_{cr_1}\right)^{n-q}.$$

Для предложенной КС вероятность гарантированно обнаруживаемых ошибок равна:

$$P_{er_2}=1-\sum_{q=0}^{d_{\min}-1}\binom{l}{q}p_{cr\,2}^{q}\left(1-p_{cr_2}\right)^{l-q},$$

где $l=n+r$.

Зависимости P_{er_1}, P_{er_2} и выигрыша $P_{er_2}-P_{er_1}$ от коэффициента избыточности применяемого (линейного – в первом случае, модулярного – во втором) кода при ограничениях $p_{cr}=1{,}5\times10^{-1}$, $l=12$ представлены на рис. 2. Здесь $K_r=1-n/l$ – коэффициент избыточности.

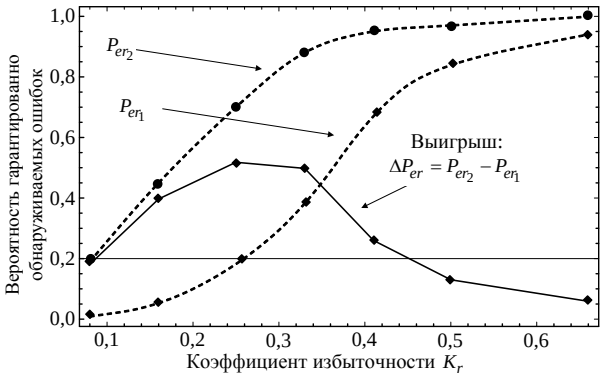

Рис. 2. Зависимость вероятности гарантированно обнаруживаемых ошибок от коэффициента избыточности

Таким образом, в данной статье предложена помехоустойчивая КС, функционирующая в кольце многочленов $GF(2)$, ориентированная на применение в современных и перспективных многопользовательских шифрованных каналах связи. Отличительной чертой предложенной КС является полная инвариантность к кратности ошибок сообщений в шифрованных каналах связи ограниченного числа отдельных пользователей. При этом помимо повышения уровня помехоустойчивости достигается увеличение имитостойкости КС. Для дальнейшего существенного увеличения имитостойкости КС избыточный канал связи должен быть зашифрован. Существенным достоинством является также и то, что данная КС строится на основе существующих одноканальных КС. Если при этом исходная КС является сертифицированной, то при ряде ограничений, накладываемых на порядок получения ключей и соблюдении условий эксплуатации, проблема сертификации предложенной КС может быть снята.

Литература

1. *Godoy W.* A proposal of a cryptography algorithm with techniques of error correction / W. Godoy, D. Periera // Computer Communications 20(15), 1997. – Pp. 1374–1380.

2. *Сидельников В.М.* Криптография и теория кодирования / В.М. Сидельников. – М. : Изд-во МГУ им. М.В. Ломоносова, 2002. – 128 с.

3. *Финько О.А.* Групповой контроль ассиметричных криптосистем методами модулярной арифметики / О.А. Финько // XIV Междунар. школа-семинар «Синтез и сложность управляющих систем» : сб. науч. тр. / Нижегород. пед. ун-т ; под ред. акад. РАН О.Б. Лупанова. – Н. Новгород : Изд-во Нижегород. пед. ун-та, 2003. – С. 85–86.

4. *Финько О.А.* Многоканальные модулярные системы, устойчивые к искажениям криптограмм / О.А. Финько // 50 лет Модулярной арифметике : сб. науч. тр. Междунар. науч. конф. – М. : Ангстрем, МИЭТ, 2006. – С. 552–558.
http://www.computer-museum.ru/books/archiv/sokcon18.pdf

5. *Финько О.А.* Конструкции, контролирующие ошибки, на основе действующих криптографических стандартов / О.А. Финько, Д.В. Самойленко // Дискретные модели в теории управляющих систем : VIII Междунар. конф. – М. : Изд-во МГУ им. М.В. Ломоносова, 2009. – С. 318–320.

6. *Финько О.А.* Многоканальные системы, устойчивые к искажению криптограмм. В коллект. монограф. «Криптографические методы защиты информации / под ред. Е.А. Сухарева. Кн. 4. – М. : Радиотехника, 2007. – С. 91–96.

7. *Самойленко Д.В.* Оценка помехоустойчивости криптосистемы, основанной на Китайской теореме об остатках, для N каналов с шумом и имитирующим злоумышленником / Д.В. Самойленко, О.А. Финько // Информационная безопасность : XI Междунар. конф. Ч. 3. – Таганрог : Изд-во ТТИ ЮФУ, 2010. – С. 154–159.

8. *Алферов А.П.* Основы криптографии : учеб. пособие, 2-е изд., испр. и доп. / А.П. Алферов, А.Ю. Зубов. – М. : Гелиос АРВ, 2002. – 480 с.

9. *Габидулин Э.М.* Кодирование в радиоэлектронике / Э.М. Габидулин, В.Б. Афанасьев. – М. : Радио и связь, 1986. – 176 с.

10. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки / Р. Блейхут. – М. : Мир, 1986. – 576 с.

11. *Амербаев В.М.* Теоретические основы машинной арифметики. – Алма-Ата : Наука, 1976. – 324 с.

12. *Торгашев В.А.* Система остаточных классов и надежность ЦВМ / В.А. Торгашев. – М. : Сов. радио, 1973. – 120 с.

13. *Самойленко Д.В.* Алгоритм расширения системы больших оснований модулярной арифметики / Д.В. Самойленко, О.А. Финько // Информационная безопасность : XI Междунар. конф. Ч. 3. – Таганрог : Изд-во ТТИ ЮФУ, 2010. – С. 151–154.

14. *Питерсон У.* Коды, исправляющие ошибки / У. Питерсон. – М. : Мир, 1976. – 575 с.

15. *Бабаш А.В.* Криптография / А.В. Бабаш, Г.П. Шанкин. – М. : Солон-Р, 2002. – 512 с.

Статья поступила в редакцию 02.09.2010 г.