УДК 004.052.2

РАЗРАБОТКА НОВОГО ПРИНЦИПА ПОСТРОЕНИЯ ИЗБЫТОЧНЫХ МОДУЛЯРНЫХ КОДОВ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ SPN-КРИПТОСИСТЕМ

[1]Калмыков И.А., [1]Топоркова Е.В., [1]Калмыков М.И., [2]Бабенко Л.К.

[1]ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru;
[2]ФГАОУ ВО «Южный федеральный университет», Ростов-на-Дону

Целью исследований является повышение надежности работы шифраторов SPN-криптосистем в условиях воздействия сбоев природного и антропогенного характеров. Достижение данной цели возможно за счет реализации SPN-криптосистем с использованием полиномиальной системы классов вычетов (ПСКВ). Применение кодов ПСКВ позволяет перенести выполнение криптографических преобразований из поля Галуа $GF(2^8)$ в поля меньшей размерности $GF(2^4)$. Такой переход обеспечивает возможность применения кода ПСКВ с двумя многочленами, порождающими элементы полей $GF(2^4)$. Известно, что использование избыточного многочлена в модулярном коде позволяет только обнаруживать ошибки. Чтобы обеспечить надежную работу SPN-шифр-систем в условиях сбоев, необходимо разработать новые принципы построения избыточных модулярных кодов. Данные принципы позволят исправлять ошибку, возникающую из-за сбоев в SPN-криптосистеме, при использовании одного контрольного основания. Поэтому разработка алгоритма коррекции ошибок кодом полиномиальной системы классов вычетов, обладающим минимальной избыточностью, является актуальной задачей.

Ключевые слова: криптографические шифры, SPN-криптосистемы, полиномиальная система классов вычетов, обнаружение ошибки, коррекция ошибки, позиционные характеристики

DEVELOPMENT OF A NEW PRINCIPLE THE CODING REDUNDANCY CODE MODULAR TO IMPROVE RELIABILITY SPN-CRYPTOSYSTEM

[1]Kalmykov I.A., [1]Toporkova E.V., [1]Kalmykov M.I., [2]Babenko L.K.

[1]Federal state Autonomous educational institution higher education
«North-Caucasian Federal University, Stavropol, e-mail:kia762@yandex.ru;
[2]Federal State Autonomous Educational Institution of Higher Education
«Southern Federal University», Rostov-on-Don

The aim of the research is to increase the reliability of the encoders SPN cryptosystem in terms of the impact of failures of natural and anthropogenic character. The achievement of this goal is possible through the implementation of the SPN cryptosystem using polynomial residue number system (PRNS). The use of codes PRNS allows to defer the implementation of cryptographic transformations from the Galois field $GF(2^8)$ field in the lower-dimensional $GF(2^4)$. This transition enables application code PRNS with two polynomials, a generating elements of the fields $GF(2^4)$. It is known that the use of excess of a polynomial in modular code only allows detecting errors. To ensure reliable operation of the SPN- cryptosystem in terms of failures it is necessary to develop new principles of a redundant modular code. These guidelines will allow you to correct the error resulting from failures in SPN-cryptosystem, using one of the control bases. Therefore, the development of error correction code polynomial residue number system, with minimal redundancy, is an urgent task.

Keywords: cryptographic ciphers, SPN- cryptographic system, polynomial residue number system, detection error, error correction, positional characteristics

В настоящее время сфера применения криптографических методов защиты информации постоянно увеличивается. Это связано с тем, что системы шифрования играют важную роль в сохранении и передаче конфиденциальных данных. Симметричные алгоритмы по сравнению с асимметричными алгоритмами шифрования обладают целым рядом достоинств, таких как более простая аппаратная и программная реализации, а также высокая скорость зашифрования и расшифрования [1]. Среди симметричных шифров особое место занимают SPN-шифры, в которых используют подстановочно-перестановочную сеть. Однако в процессе работы шифраторы SPN-шифров могут быть подвергнуты атакам типа сбоев. Это приводит к нарушению работы шифратора и снижению степени защиты данных. Поэтому разработка алгоритмов, позволяющих устранить эти последствия, является актуальной задачей.

Цель исследования

В настоящее время для повышения надежности работы SPN-шифр-систем предлагается использовать дублирование, маскирование ошибок методом «2 из 3», а также использовать многократный просчет. Однако данные методы устранения последствий сбоев в работе шифратора характеризуются значительными схемными затратами. Это

связано с тем, что они не в полной степени используют математическую основу SPN-шифров, реализованных в полях GF(2^8). В качестве перспективного направления решения данной проблемы можно отметить использование корректирующих кодов, реализованных в полях Галуа. Поэтому целью работы является повышение надежности SPN-криптосистем за счет применения новых принципов кодирования модулярных кодов полиномиальной системы классов вычетов (ПСКВ).

Материалы и методы исследования

Одним из наиболее известных их представителей является шифр AES. Это итерационный блочный шифр, который реализует схему «квадрат». Блочный шифр AES нашел широкое применение благодаря хорошему сочетанию таких показателей, как криптографическая стойкость, производительность и относительно низкие схемные затраты.

С целью повышения надежности работы его шифратора в [10] предлагается свести шифрование из поля GF(2^8) к шифрованию в конечных полях меньшего порядка. В этом случае элементы поля Галуа GF(2^8) представляются в виде элементов полей GF(2^4). Такой переход позволяет использовать код ПСКВ с двумя информационными основаниями.

В полиномиальной системе классов вычетов двоичный код $A = 10\ldots11$ представляется в полиномиальной форме $A(z) = z^m + \ldots + z + 1$, а затем этому полиному в соответствие ставится набор остатков, полученных при делении этого кода на полиномы-основания [8, 9]:

$$A(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_k(z)), \quad (1)$$

где $\alpha_i(z) \equiv A(z) \bmod p_i(z)$; $i = 1, ..., k$.

Данный набор оснований кода ПСКВ образует рабочий диапазон

$$P_{\text{раб}}(z) = \prod_{i=1}^{k} p_i(z).$$

Так как сравнения по одному и тому же модулю можно почленно складывать, вычитать и умножать, то для двух полиномов $A(z)$ и $B(z)$, имеющих соответственно коды $(\alpha_1(z), \alpha_2(z), ..., \alpha_k(z))$ и $(\beta_1(z), \beta_2(z), ..., \beta_k(z))$, справедливо соотношение:

$$\left|A(z) \circ B(z)\right|^{+}_{p(z)} = \left(\left|\alpha_1(z) + \beta_1(z)\right|^{+}_{p_1(z)}, ..., \left|\alpha_k(z) + \beta_k(z)\right|^{+}_{p_k(z)}\right). \quad (2)$$

Параллельность обработки данных по основаниям ПСКВ позволяет обеспечить высокую скорость выполнения модульных операций. Благодаря этому свойству коды ПСКВ нашли широкое применение в системах реального масштаба времени [3–5]. При этом параллельная и независимая обработка остатков служат идеальной основой для построения процедур обнаружения и коррекции ошибок, возникающих из-за сбоев в работе системы [2, 6, 7].

Для коррекции ошибок с помощью модулярных кодов необходимо расширить рабочий диапазон до величины полного диапазона:

$$P(z) = \prod_{i=1}^{k+r} p_i(z) = P_{\text{раб}}(z) \prod_{i=n+1}^{k+r} p_i(z). \quad (3)$$

Для этого вводят избыточные основания $p_{k+1}(z), ..., p_{k+r}(z)$, выбираемые из условия

$$\deg p_{k-1}(z) \le \deg p_k(z) \le \deg p_{k+1}(z) \le ... \le \deg p_{k+r}(z), \quad (4)$$

где $\deg p_i(z)$ – степень неприводимого полинома $p_i(z)$; k – количество рабочих оснований.

Чтобы провести такую процедуру в модулярных кодах, применяют различные позиционные характеристики. Если основания ПСКВ являются основаниями обобщенной полиадической системы (ОПС), то имеем, что

$$A(z) = \left[\alpha_1(z), \alpha_2(z), ..., \alpha_{k+2}(z)\right] = \left[a_1(z), a_2(z), ..., a_{k+2}(z)\right].$$

Тогда, используя коэффициенты ОПС, можно представить

$$A(z) = a_1(z) + a_2(z)p_1(z) + ... + a_{k+1}(z)P_{\text{раб}}(z) + a_{k+2}(z)P_{\text{раб}}(z)p_{k+1}(z). \quad (5)$$

Из равенства (5) видно, что если код ПСКВ принадлежит рабочему диапазону, то старшие коэффициенты ОПС, соответствующие контрольным основаниям, должны равняться нулю $a_{k+1}(z) = 0, a_{k+2}(z) = 0$. В работе [7] представлен алгоритм вычисления данной ПХ.

В работе [2] предлагается обнаруживать и корректировать ошибки на основе ПХ-интервала. В этом случае данная позиционная характеристика определяется

$$L_{\text{инт}}(z) = \left|\sum_{i=1}^{k+2} \alpha_i(z) K_i(z) + R_a(z)\left|P_{\text{раб}}(z)\right|^{+}_{P_{\text{конт}}(z)}\right|^{+}_{P_{\text{конт}}(z)}, \quad (6)$$

где $K_i(z) = \left[\frac{B_i(z)}{P_{\text{раб}}(z)}\right]$; $B_i^*(z) \equiv B_i(z) \bmod P_{\text{раб}}(z)$; $P_{\text{конт}}(z) = \prod_{i=k+1}^{k+2} p_i(z)$; $R_a(z) = \left[\frac{\sum_{i=1}^{k} \alpha_i(z) B_i^*(z)}{P_{\text{раб}}(z)}\right]$.

В работе [6] представлен алгоритм вычисления ПХ – невязки контрольных остатков. Для получения данной ПХ вычисляют разность между значениями остатков $\alpha_{k+1}(z)$, $\alpha_{k+2}(z)$ по контрольным основаниям кода ПСКВ $A(z)=(\alpha_1(z),\alpha_2(z),...,\alpha_{k+2}(z))$ и результатам вычисления остатков $\alpha'_{k+1}(z),\alpha'_{k+2}(z)$ с использованием рабочих оснований:

$$\begin{cases}\delta_{k+1}(z)=\left|\alpha_{k+1}(z)-\alpha'_{k+1}(z)\right|^{+}_{p_{k+1}(z)}\\ \delta_{k+2}(z)=\left|\alpha_{k+2}(z)-\alpha'_{k+2}(z)\right|^{+}_{p_{k+2}(z)}\end{cases}, \quad (7)$$

где $\alpha'_j(z)=\left|C_j(z)\left|p_j(z)-\sum_{i=1}^{k}\alpha_i(z)K_i(z)+R_a(z)\right|^{+}_{p_j(z)}\right|^{+}_{p_j(z)}$; $C_j(z)=\left|K_j^{-1}(z)\right|^{+}_{p_j(z)}$; $R_a(z)$ – ранг $A(z)$ в безызбыточной ПСКВ; $K_i(z)=\left[B_i(z)/P_{\text{раб}}(z)\right]$; $j=k+1,\ k+2$.

Анализ рассмотренных алгоритмов показал, что классические принципы построения корректирующих модулярных кодов невозможно использовать для повышения надежности SPN-криптосистем. Это связано с тем, что для коррекции однократной ошибки в кодах ПСКВ используют два контрольных модуля. А в SPN-криптосистеме контрольным модулем может быть только полином $p_3(z)=z^4+z^3+z^2+z+1$. Значит, для проведения коррекции ошибок необходимо разработать новые принципы построения избыточных кодов ПСКВ.

Очевидно, что для коррекции однократной ошибки в модулярном коде необходимо наличие как минимум двух контрольных остатков $\alpha_{k+1}(z)$ и $\alpha_{k+2}(z)$. Первый остаток $\alpha_{k+1}(z)$ должен указывать глубину ошибки, т.е. $\alpha_{k+1}(z)=\alpha_1(z)+\alpha_2(z)+...+\alpha_k(z)$. Если ошибка произошла по i-му основанию кода ПСКВ, то получаем

$$A^{*}(z)=(\alpha_1(z),,...,,\alpha_{i-1}(z),\alpha_i(z)+\Delta\alpha_i(z),\alpha_{i+1}(z),...,\alpha_{k+2}(z)), \quad (8)$$

где $\Delta\alpha_i(z)$ – глубина ошибки по i-му основанию кода ПСКВ.

Тогда получаем, что

$$\alpha^{*}_{k+1}(z)=\alpha_1(z)+...+\alpha_{i-1}(z)+(\alpha_i(z)+\Delta\alpha_i(z))+\alpha_{i+1}(z)+...+\alpha_k(z).$$

Чтобы определить глубину ошибки, необходимо сложить эти остатки. Получаем

$$\delta_1(z)=\alpha_{k+1}(z)+\alpha^{*}_{k+1}(z)=\Delta\alpha_i(z). \quad (9)$$

Второй остаток $\alpha_{k+2}(z)$ должен указать номер отказавшего основания. Тогда

$$\alpha_{k+2}(z)=\left(1\cdot\alpha_1(z)+2(z)\alpha_2(z)+...+k(z)\alpha_k(z)\right)\bmod p_{k+1}(z), \quad (10)$$

где $i(z)$ – полиномиальная форма двоичного представления числа i.

Если ошибка произошла по i-му основанию кода ПСКВ, то остаток $\alpha_{k+2}(z)$ равен

$$\alpha_{k+2}(z)=\left(1\cdot\alpha_1(z)+...+i(z)(\alpha_i(z)+\Delta\alpha_i(z))+...+k(z)\alpha_k(z)\right)\bmod p_{k+1}(z). \quad (11)$$

Чтобы определить номер отказавшего основания необходимо сложить эти остатки.

$$\delta_2(z)=(\alpha_{k+2}(z)+\alpha^{*}_{k+2}(z))\bmod p_{k+1}(z)=i(z)\Delta\alpha_i(z). \quad (12)$$

Очевидно, что если разделить значение $\delta_{k+2}(z)$ на $\delta_{k+1}(z)$, то результат дает $i(z)$ – полиномиальную форму двоичного представления отказавшего канала. Таким образом, разработанный новый принцип построения избыточного кода ПСКВ с одним контрольным модулем позволяет корректировать ошибки, возникающие в процессе работы SPN-криптосистем.

Результаты исследования и их обсуждение

Шифр AES реализуется в GF(2^8) с использованием $p(z)=z^8+z^4+z^3+z+1$. Предлагается вместо него использовать код ПСКВ с двумя основаниями $p_1(z)=z^4+z+1$ и $p_2(z)=z^4+z^3+1$. В качестве контрольного основания – $p_3(z)=z^4+z^3+z^2+z+1$. Рассмотрим применение разработанного принципа при проведении операции MixColums. В этом преобразовании столбцы состояния рассматриваются как многочлены над GF(2^8) и умножаются по модулю двучлена z^4+1 на многочлен

$$g(z)=\{03\}z^3+\{01\}z^2+\{01\}z+\{02\}.$$

При этом умножение байтов массива State на {02} и на {03} выполняются по модулю $p(z)$. Пусть на вход преобразователя MixColums поступил 32-битовый столбец $s_{0C}=\{CA_{16}\}$, $s_{3C}=\{4F_{16}\}$ $s_{2C}=\{E2_{16}\}$, $s_{1C}=\{D1_{16}\}$. В избыточном коде ПСКВ эти байты, представленные в 16-ричной системе счисления, имеют вид $\{CA_{16}\}$ = (D, 2, F, 9), $\{D1_{16}\}$=(5,0,5,5), $\{E2_{16}\}$ = (3, 1, 2,1), $\{4F_{16}\}$ = (3, 0, 3, 3). Рассмотрим получение нового значения байта:

$$s'_{0c}=(\{02\}\bullet CA)+(\{03\}\bullet D1)+E2+4F=8F+68+E2+4F=4A.$$

При умножении первого байта CA на значение константы {02} получается байт $(\{02\}CA) \bmod z^8 + z^4 + z^3 + z + 1 = 8F$. Представим данное произведение в коде ПСКВ с двумя информационными основаниями $p_1(z) = z^4 + z + 1$ и $p_2(z) = z^4 + z^3 + 1$. Получаем $\{02\} \bullet CA = 8F = (z^2, z^3) = (\{4_{16}\}, \{8_{16}\})$. Вычислим значения двух контрольных остатков:

$$\alpha_3 = \{02_{16}\} \bullet \{CA_{16}\} = z^3 + z^2 = \{C_{16}\},$$

$$\alpha_4 = (\{02_{16}\} \bullet \{CA_{16}\}) \bmod p_3(z) = z^3 + z + 1 = \{B_{16}\}.$$

Тогда произведение можно записать в виде кода ПСКВ в следующем виде:

$$\{02\} \bullet CA = 8F = (z^2, z^3, z^3 + z^2, z^3 + z + 1) = (4, 8, C, B).$$

Рассмотрим, как будет получен аналогичный результат с использованием соответствующих таблиц. Информационные остатки первого байта CA = (D, 2) поступают на входы табл. 1 и табл. 2. Представленная часть табл. 1 содержит остатки результата умножения $z \cdot s_j(z)$, приведенной по модулям $p_1(z) = z^4 + z + 1$. На пересечении второй строки и столбца D располагается $\{4_{16}\} = 0100 = z^2$.

Табл. 2 содержит результат умножения $z \cdot s_j(z)$ по модулю $p_2(z) = z^4 + z^3 + 1$. На пересечении второй строки и столбца D располагается остаток $\{8_{16}\} = 0100 = z^3$.

Кроме того, информационные остатки первого байта CA = (D, 2) поступают на входы табл. 3 и табл. 4. Табл. 3 содержит данные о сумме остатков информационных оснований ПСКВ. На пересечении 2-й строки и столбца D находится $\{C_{16}\} = 1100 = z^3 + z^2$.

В табл. 4 представлены данные о втором контрольном остатке. На пересечении второй строки и столбца D таблицы находится остаток $\{B_{16}\} = 1011 = z^3 + z + 1$.

Таким образом, после выполнения операции умножения первого байта имеем

$$\{02\} \bullet CA = 8F = (z^2, z^3, z^3 + z^2, z^3 + z + 1) = (4, 8, C, B).$$

Рассмотрим умножение второго байта состояния $\{D1_{16}\} = (5, 0, 5, 5)$ на коэффициент на {03}. Получаем $(\{03\} \bullet \{D1_{16}\}) = (\{02\} \bullet \{D1_{16}\}) + \{D1_{16}\} = \{B9_{16}\} + \{D1_{16}\} = \{68_{16}\}$. Тогда

$$\alpha_1(x) = (z^2 + z + 1) + (z^2 + 1) = z = 2_{16};\ \alpha_2(z) = (z^3 + z^2) + 0 = z^3 + z^2 = C_{16}.$$

$$\alpha_3(x) = (z^3 + z + 1) + (z^2 + 1) = z^3 + z^2 + z = E_{16};\ \alpha_4(z) = 0 + (z^2 + 1) = z^2 + 1 = 5_{16}.$$

Тогда результат умножения на константу {03} имеет вид

$$(\{03\} \bullet D1) = B9 + D1 = 68_{16} = (z, z^3 + z^2, z^3 + z^2 + z, z^2 + 1) = (2, C, E, 5).$$

При перемешивании столбцов MixColums получили новое состояние

$$s'_{0C}(z) = (z^2 + z, z^2 + 1, z + 1, z^3 + z^2) = (6, 5, 3, C) = 4A.$$

Проведем проверку контрольных оснований. Получаем

$$\alpha_3^*(z) = \sum_{i+1}^{2} \alpha_i(x) = x + 1 = 3_{16};\ \alpha_4^*(z) = \sum_{i+1}^{2} (i(z)\alpha_i(z)) \bmod p_3(z) = z^3 + z^2 = C_{16}.$$

Тогда синдром ошибки $\delta_1(z) = \alpha_3(z) + \alpha_2^*(z) = 0$; $\delta_2(z) = \alpha_4(z) + \alpha_4^*(z) = 0$.

Пусть из-за сбоя произошло искажение первого слагаемого на величину $\Delta\alpha_1(z) = 1$. Тогда с выхода табл. 1 снимается $\alpha_1^*(z) = \alpha_1(z) + \Delta\alpha_1(z) = z^2 + 1$, то есть комбинация

$$M_{\text{сбой}}(\{02\} \bullet CA) = (z^2 + 1, z^3, z^3 + z^2, z^3 + z + 1).$$

В результате получили новое состояние:

$$s'_{0C}(z) = (z^2 + z + 1, z^2 + 1, z + 1, z^3 + z^2).$$

Тогда остатки равны

$$\alpha_3^*(z) = (z^2 + z + 1) + (z^2 + 1) = z;\ \alpha_4^*(x) = (z^2 + z + 1) + z(z^2 + z) = z^3 + z^2 + 1.$$

Синдром ошибки $\delta_1(z) = \alpha_3(z) + \alpha_2^*(z) = (z) + (z + 1) = 1$; $\delta_2(z) = \alpha_4(z) + \alpha_4^*(z) = 1$. По значению синдрома ошибки $\delta_1(x) = 1$ и $\delta_2(x) = 1$ из памяти берется вектор ошибки, который равен $\bar{e} = (1, 0, 0, 0)$, с помощью которого ошибка исправляется:

$$s'_{0C}(z) = (z^2 + z + 1, z^2 + 1, z + 1, z^3 + z^2) + (1, 0, 0, 0) = (z^2 + z, z^2 + 1, z + 1, z^3 + z^2).$$

Таблица 1

Остатки результата умножения $x \cdot s_j(x) \bmod x^4 + x + 1$

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	F	9	6	8	7	1	E	E	1	7	8	6	9	F	0
1	D	2	4	B	5	A	C	3	3	C	A	5	B	4	2	D
2	D	2	4	B	5	A	C	3	3	C	A	5	B	4	2	D
3	…							…								…
F	D	2	4	B	5	A	C	3	3	C	A	5	B	4	2	D

Таблица 2

Остатки результата умножения $x \cdot s_j(z) \bmod z^4 + z^3 + 1$

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	C	C	0	0	C	C	0	C	0	0	C	C	0	0	C
1	E	2	2	E	E	2	2	E	2	E	E	2	2	E	E	2
2	8	4	4	8	8	4	4	8	4	8	8	4	4	8	8	4
3	…							…								…
F	B	7	7	B	B	7	7	5	7	B	B	7	7	B	B	7

Таблица 3

Первый контрольный остаток $\alpha_3(z)$

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	3	5	6	8	B	D	E	2	1	7	4	A	9	F	C
1	3	0	6	5	B	8	E	D	1	2	4	7	9	A	C	F
2	5	6	0	3	D	E	8	B	7	4	2	1	F	C	A	9
3	…							…								…
F	6	5	3	0	E	D	B	6	4	7	1	2	C	F	9	A

Таблица 4

Второй контрольный остаток $\alpha_4(z)$

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	8	E	6	8	0	6	E	9	1	7	F	1	9	F	7
1	E	6	0	8	6	E	8	0	7	F	9	1	F	7	1	9
2	2	A	C	4	A	2	4	C	B	3	5	D	3	B	D	5
3	…							…								…
F	4	C	A	2	C	4	2	9	D	5	3	B	5	D	B	3

Обобщая полученные результаты, можно сделать вывод о том, что разработанный алгоритм поиска и коррекции ошибок с помощью избыточного кода ПСКВ требует меньших схемных затрат на реализацию. Так, троированная мажоритарная система требует использования трех пар табл. 1 и 2 для маскирования ошибок, вызванных сбоями в шифраторе AES. А разработанные принципы построения избыточных кодов ПСКВ позволяет корректировать однократную ошибку с использованием четырех таблиц, приведенных в статье.

Заключение

Проведенный анализ известных алгоритмов обнаружения и исправления ошибок в модулярных кодах показал, что они не могут быть применены для повышения надежности работы SPN-криптосистем, так используют два контрольных основания. Исходя из особенностей реализации SPN-криптосистем в полях GF(2^4), в работе осуществлена разработка и исследование новых принципов построения избыточных кодов полиномиальной системы классов вычетов, позволяющих корректировать ошибки на основе использования одного контрольного основания. Показана возможность применения данных принципов при разработке новых модулярных кодов ПСКВ, способных корректировать ошибки, возникающие в процессе работы криптосистемы AES. Проведенные исследования

показали, что применение разработанного алгоритма позволяет вычислять местоположение и глубину ошибки при меньших схемных затратах по сравнению с методом маскирования ошибок «2 из 3».

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-37-50081.

Список литературы

1. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М.: Гелиос АРВ. 2006. – 376 с.

2. Гапочкин А.В., Калмыков М.И., Васильев П.С. Обнаружение и коррекция ошибки на основе вычисления интервального номера кода классов вычетов // Современные наукоёмкие технологии. – 2014. – № 6. – С. 9–14.

3. Калмыков И.А., Воронкин Р.А., Резеньков Д.Н., Емарлукова Я.В., Фалько А.А. Генетические алгоритмы в системах цифровой обработки сигналов // Нейрокомпьютеры: разработка, применение – 2011. – № 5. – С. 20–27.

4. Калмыков И.А., Зиновьев А.В., Резеньков Д.Н., Гахов В.Р. Применение систолических ортогональных преобразований в полиномиальной системе классов вычетов для повышения эффективности цифровой обработки сигналов // Инфокоммуникационные технологии. – 2010. – Том 8, № 3, – С. 4–11.

5. Калмыков И.А., Дагаева О.И. Разработка псевдослучайной функции повышенной эффективности // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 160–169.

6. Калмыков И.А., Резеньков Д.Н. Локализация ошибок в модулярных кодах полиномиальной системы классов вычетов с минимальной избыточностью // Фундаментальные исследования. – 2008. – № 3. – С. 75–76.

7. Стрижков Н.С., Калмыков М.И. Алгоритм преобразования из модулярного кода в полиадическую систему основания для систем обнаружения и коррекции ошибок // Международный журнал экспериментального образования. – 2014. – № 3. – С. 127–131.

8. Червяков Н.И., Калмыков И.А., Щелкунова Ю.О., Шилов А.А., Бережной В.В. Нейросетевая реализация в ПСКВ операций ЦОС повышенной разрядности // Нейрокомпьютеры: разработка, применение. – 2004. – № 5–6. – С. 94–100.

9. Kalmykov I.A., Katkov K.A., Olegovich N.D., Sarkisov A.B., Makarova A.V. Parallel Modular Technologies in Digital Signal Processing // Life Science Journal. – 2014. – T. 11. № 11s. P. 435–438.

10. Stefan Mangard, Manfred Aigner, Sandra Dominikus. A Highly Regular and Scalable AES Hardware Architecture. // IEEE Transactions on Computers. – 2003. – Volume 52, Issue 4. – P. 483–491.

References

1. Babenko L.K., Ishhukova E.A. Sovremennye algoritmy blochnogo shifrovanija i metody ih analiza. M.: Gelios ARV. 2006. 376 p.

2. Gapochkin A.V., Kalmykov M.I., Vasilev P.S. Obnaruzhenie i korrekcija oshibki na osnove vychislenija intervalnogo nomera koda klassov vychetov // Sovremennye naukojomkie tehnologii. 2014. no. 6. pp. 9–14.

3. Kalmykov I.A., Voronkin R.A., Rezenkov D.N., Emarlukova Ja.V., Falko A.A. Gene-ticheskie algoritmy v sistemah cifrovoj obrabotki signalov // Nejrokompjutery: razra-botka, primenenie 2011. no. 5. pp. 20–27.

4. Kalmykov I.A., Zinovev A.V., Rezenkov D.N., Gahov V.R. Primenenie sistoliche-skih ortogonalnyh preobrazovanij v polinomialnoj sisteme klassov vychetov dlja povy-shenija jeffektivnosti cifrovoj obrabotki signalov // Infokommunikacionnye tehnologii. 2010. Tom 8, no. 3, pp. 4–11.

5. Kalmykov I.A., Dagaeva O.I. Razrabotka psevdosluchajnoj funkcii povyshennoj jef-fektivnosti // Izvestija JuFU. Tehnicheskie nauki. 2011. no. 12 (125). pp. 160–169.

6. Kalmykov I.A., Rezenkov D.N. Lokalizacija oshibok v moduljarnyh kodah polinomi-alnoj sistemy klassov vychetov s minimalnoj izbytochnostju // Fundamentalnye issle-dovanija. 2008. no. 3. pp. 75–76.

7. Strizhkov N.S., Kalmykov M.I. Algoritm preobrazovanija iz moduljarnogo koda v poliadicheskuju sistemu osnovanija dlja sistem obnaruzhenija i korrekcii oshibok // Mezhdunarodnyj zhurnal jeksperimentalnogo obrazovanija. 2014. no. 3. pp. 127–131.

8. Chervjakov N.I., Kalmykov I.A., Shhelkunova Ju.O., Shilov A.A., Berezhnoj V.V. Nejrosetevaja realizacija v PSKV operacij COS povyshennoj razrjadnosti // Nejrokompjutery: razrabotka, primenenie. 2004. no. 5–6. pp. 94–100.

9. Kalmykov I.A., Katkov K.A., Olegovich N.D., Sarkisov A.B., Makarova A.V. Parallel Modular Technologies in Digital Signal Processing // Life Science Journal. 2014. T. 11. no. 11s. pp. 435–438.

10. Stefan Mangard, Manfred Aigner, Sandra Dominikus. A Highly Regular and Scalable AES Hardware Architecture. // IEEE Transactions on Computers. 2003. Volume 52, Issue 4. pp. 483–491.