УДК 004.052.2

ПРИМЕНЕНИЕ КОРРЕКТИРУЮЩИХ КОДОВ ПОЛИНОМИАЛЬНОЙ СИСТЕМЫ КЛАССОВ ВЫЧЕТОВ ДЛЯ УСТРАНЕНИЯ ПОСЛЕДСТВИЙ СБОЕВ ПРИ ШИФРОВАНИИ АЛГОРИТМОМ AES

Калмыков И.А., Степанова Е.П., Калмыков М.И., Топоркова Е.В.

ФГАОУ ВПО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

С момента разработки блочного шифра AES постоянно растет число атак, которые используют информацию, полученную по побочным каналам. Такую информацию можно получить на основе сбоев, которые принудительно создаются в процессе функционирования шифратора. Это приводит к нарушению нормальной работы шифратора, что способствует появлению ошибок в зашифрованном тексте. В результате данных действий нарушитель может получить значение секретного ключа. Для противодействия атаке на основе сбоев предлагается использовать полиномиальную систему классов вычетов, которая позволяет исправлять ошибки, вызванные сбоями в работе шифратора. В работе представлен алгоритм, применение которого позволяет осуществить коррекцию ошибки в процессе шифрования, возникшей из-за действий нарушителя.

Ключевые слова: алгоритм шифрования AES, атаки на основе сбоев, полиномиальная система классов вычетов, поле Галуа, алгоритмы обнаружения и коррекции ошибок, позиционные характеристики

APPLICATION CORRECTING CODES POLYNOMIAL RESIDUE NUMBER SYSTEM TO REMEDY THE FAILURES OF ENCRYPTION AES ALGORITHM

Kalmykov I.A., Stepanova E.P., Kalmykov M.I., Toporkova E.V.

Federal state Autonomous educational institution higher professional education «North-Caucasian Federal University, Stavropol, e-mail: kia762@yandex.ru

Since the development of the block cipher AES growing number of attacks that use the information provided on side channels. Such information can be obtained on the basis of failures that are forced in the operation of the encoder. This leads to malfunction of the encoder, which contributes to the appearance of errors in the ciphertext. As a result of these actions an attacker can get the value of the secret key. To counter the attack based on failures is proposed to use a polynomial system of residue classes, which can detect and correct errors caused by failures in the encoder. The paper presents the algorithm, which allows for the correction of an error in the encryption process, resulting from the actions of the offender

Keywords: encryption algorithm AES, an attack on the basis of failure, polynomial residue number system, Galois field, algorithms, error detection and correction, positional characteristics

Большинство современных систем на кристалле (СнК), которые нашли широкое применение в современных инфокоммуникационных системах, для защиты передаваемой информации от несанкционированного доступа используют криптографические алгоритмы шифрования. Наличие в современных системах на кристалле блока криптообработки позволяет эффективно их использовать при проектировании портативных радиостанций, систем управления и передачи высокоскоростной информации для больших и малых беспилотных летательных аппаратов, наземных роботов, интеллектуальных сенсорных сетей, а также широкополосных систем гражданского назначения (4–5) G стандарта [5, 8]. Особое место среди алгоритмов шифрования стандарт AES. При этом использование данного алгоритма шифрования в различных сферах привело к повышенному числу атак на AES [4, 7, 10].

Среди криптоатак особое место занимают атаки, которые используют информацию, полученную по побочным каналам. Как правило, такие криптоатаки строятся на основе сбоев, принудительно вызываемых в работе шифратора. Снизить эффективность реализации атак на основе сбоев можно за счет использования корректирующих кодов полиномиальной системы классов вычетов (ПСКВ). Поэтому разработка алгоритма поиска и коррекции ошибок, возникающих в процессе шифрования AES, является актуальной задачей.

Основная часть

Эффективность работы современных высокопроизводительных СнК во многом определяется наличием на кристалле не только процессорных ядер общего назначения, но и специализированных вычислительных модулей. При этом наряду с вычислительными ускорителями в состав СнК

стали чаще вводиться блоки криптографической защиты, что наглядно проявляется в в чипах линейки Marvell Armada, Sitara Am38x и TI OMAP [5, 8].

Для обеспечения высокого уровня достоверности и конфиденциальности передаваемой и обрабатываемой информации в СнК широко применяется алгоритм шифрования AES (до проведения конкурсного отбора Rijndael). Выбор данного алгоритма криптозащиты, согласно [7], определяется хорошим сочетание криптографической стойкости, производительности, а также относительно низкими требованиями к аппаратурным затратам и платформам.

Однако, несмотря на отмеченные выше достоинства, блочный алгоритм шифрования AES, постоянно подвергается проверке на криптостойкость. Проводимые атаки на стандарт шифрования AES можно разделить на виды – атаки методом бумеранга; атаки на основе модификации методов криптоанализа на связанных ключах; алгебраические атаки; атаки, использующие информацию, полученную по побочным каналам (side-channel-атакам) [4].

В статье будут рассмотрены атаки последнего вида, которые относятся к активным атакам. В их основу положены различные воздействия на шифрующее устройство, которые осуществляются с целью внести искажения в информацию на различных этапах шифрования. В качестве основных мер воздействия на шифратор можно выделить – увеличение напряжения питания криптосистемы, изменение частоты шифрующего устройства, при котором частота значительно превышает максимально допустимую, помещение конструкции в электромагнитное поле, повышение температуры некоторой части шифратора. Для защиты от атаки используют добавление в шифрующий механизм датчиков воздействий, блокирующих шифратор при ненормальных параметрах системы, вычисление контрольной суммы, экранирование шифратора [4].

Однако представленные выше алгоритмы не учитывают особенности алгоритма шифрования, что приводит к значительным затратным решениям. Повысить эффективность противодействия этим криптоатакам можно за счет корректирующих кодов ПСКВ.

Алгоритм AES относится к симметричным системам шифрования, в основу которого положен математический аппарат поля Галуа $GF(2^8)$ с порождающий полиномом $m(x) = x^8 + x^4 + x^3 + x + 1$. Выбор такого порождающего полинома позволяет выполнять криптографические операции над байтами, которые рассматриваются как элементы конечного поля $GF(2^8)$. Использование ПСКВ позволяет перейти к аналогичным операциям, которые эффективно можно реализовать в полях меньшей размерности $GF(2^4)$. В этом случае неприводимые полиномы $m_1(x) = x^4 + x + 1$ и $m_2(x) = x^4 + x^3 + 1$, которые являются порождающими многочленами, можно использовать в качестве рабочих оснований ПСКВ. Согласно [1, 2, 9] использование двух оснований $m_1(x) = x^4 + x + 1$ и $m_2(x) = x^4 + x^3 + 1$ позволяет осуществлять в ПСКВ операции модульные проводить параллельно, помодульно и независимо

$$\begin{cases} \left| A(x) \otimes B(x) \right|^{+}_{x^4+x+1} = \left| \alpha_i(x) \otimes b_i(x) \right|^{+}_{x^4+x+1}; \\ \left| A(x) \otimes B(x) \right|^{+}_{x^4+x^3+1} = \left| \alpha_i(x) \otimes b_i(x) \right|^{+}_{x^4+x^3+1}, \end{cases} \quad (1)$$

где $\otimes$ – операции сложения, вычитания и умножения в $GF(p)$; $A(x) = (\alpha_1(x), \alpha_2(x), ..., \alpha_k(x))$ и $B(x) = (b_1(x), b_2(x), ..., b_n(x))$; $\alpha_1(x) \equiv A(x) \bmod m_1(x)$; $b_1(x) \equiv B(x) \bmod m_1(x)$; $l = 1, \ldots, k$.

Наряду с высокой скоростью выполнения вычислений коды ПСКВ способны обнаруживать и исправлять ошибки, которые возникают из-за отказа и сбоев оборудования [6]. Для обеспечения коррекции ошибок при работе алгоритма шифрования AES предлагается использовать многочлен $m_3(x) = x^4 + x^3 + x^2 + x + 1$. В работе [1] показан алгоритм вычисления синдрома ошибки для кода ПСКВ, использующего одно контрольное основание, который позволяет обнаруживать факт наличия ошибок, вызванных сбоями в работе устройства. Для обнаружения и исправления однократной ошибки в коде ПСКВ $A(z) = (\alpha_1(x), \alpha_2(x), ..., \alpha_k(x))$ вводят избыточное основание $\deg m_{k+1}(x) \geq \deg m_k(x)$. Для коррекции однократной ошибки в коде ПСКВ вычисляют два контрольных остатка

$$\alpha_{k+1}(x) = \sum_{i+1}^{k} \alpha_i(x);$$

$$\alpha_{k+2}(x) = \sum_{i+1}^{k} (i(x)\alpha_i(x)) \bmod m_{k+1}(x), \quad (2)$$

где $i(x)$ – полиномиальная форма i-го номера; Σ – суммирование по модулю два.

Чтобы обнаружить однократную ошибку в комбинации ПСКВ вычисляются значения

$$\alpha^{*}_{k+1}(x) = \sum_{i+1}^{k} \alpha_i(x);$$

$$\alpha^{*}_{k+2}(x) = \sum_{i+1}^{k} (i(x)\alpha_i(x)) \bmod m_{k+1}(x). \quad (3)$$

Значения $\alpha^{*}_{k+1}(x)$ и $\alpha^{*}_{k+2}(x)$, используются для вычисления синдрома ошибки

$$\delta_1(x) = \alpha_{k+1}(x) + \alpha^{*}_{k+1}(x);$$

$$\delta_2(x) = \alpha_{k+2}(x) + \alpha^{*}_{k+2}(x), \qquad (4)$$

Если синдром ошибки равен нулю, то есть $\delta_1(x) = 0$ и $\delta_2(x) = 0$, то комбинация ПСКВ не содержит ошибки. В противном случае – комбинация ПСКВ содержит ошибку. При этом по величине синдрома ошибки $\delta_1(x)$ и $\delta_2(x)$ можно однозначно определить местоположение и глубину ошибки в модулярном коде ПСКВ.

Анализ, представленного в работе [1], алгоритма поиска и коррекции ошибок в модулярном коде ПСКВ показывает, что данный алгоритм можно эффективно применить для противодействия атакам на основе, проводимых на алгоритм шифрования AES. Известно, что каждый раунд алгоритма AES состоит из четырех преобразований – замены байтов SubBytes, побайтового сдвига строк Shift Rows, перемешивания столбцов MixColums, сложение с раундовым ключом AddRoundKey.

Применение избыточного кода ПСКВ потребует внесения определенных аппаратных изменений в структуру шифратора AES. В работе [3], приведен алгоритм применения корректирующего кода ПСКВ при реализации базовой процедуры замены блоков в алгоритме шифрования AES. Суть его состоит в том, что для получения кода ПСКВ байт открытого текста S поступает на вход преобразователя из позиционного кода в код ПСКВ, с выхода которого снимаются значения двух остатков $s_1(x) \equiv S(x) \bmod m_1(x)$, $s_2(x) \equiv S(x) \bmod m_2(x)$.

Затем два четырехразрядных блока данных, определяемые текущим байтом $S(x)$, поступают на входы преобразователя SubBytes, который представляется в виде двух таблиц размером 256×4 бит. После выполнения операции подстановки проводится проверка на наличие ошибок в коде ПСКВ. Для этого согласно (3) вычисляются значения проверочных остатков по модулю $m_3(x) = x^4 + x^3 + x^2 + x + 1$. Затем происходит вычисление синдрома ошибки согласно (4). При необходимости, ошибка будет исправлена.

После этого результат операции подстановки, представленный по двум информационным основаниям $m_1(x) = x^4 + x + 1$ и $m_2(x) = x^4 + x^3 + 1$, подвергается следующим раундовым преобразованиям – побайтовом сдвиге строк Shift Rows, перемешивании столбцов MixColums; сложение с раундовым ключом AddRoundKey. Рассмотрим применение корректирующего кода ПСКВ при проведении операции перемешивания столбцов MixColums. В этом преобразовании столбцы состояния рассматриваются как многочлены над расширением поля Галуа $GF(2^8)$ и умножаются по модулю двучлена $x^4 + 1$ на многочлен

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

Данную операцию в матричном виде можно представить как

$$s'_{0c} = (\{02\} \bullet s_{0c}) \oplus (\{03\} \bullet s_{1c}) \oplus s_{2c} \oplus s_{3c};$$

$$s'_{1c} = s_{0c} \oplus (\{02\} \bullet s_{1c}) \oplus (\{03\} \bullet s_{2c}) \oplus s_{3c}; \qquad (5)$$

$$s'_{0c} = s_{0c} \oplus s_{1c} \oplus (\{02\} \bullet s_{2c}) \oplus (\{03\} \bullet s_{s3});$$

$$s'_{0c} = (\{03\} \bullet s_{0c}) \oplus s_{1c} \oplus s_{2c} \oplus (\{02\} \bullet s_{3c}).$$

где c – номер столбца массива State; {02} – соответствует умножению на x; {03} – соответствует умножению на $x + 1$.

При этом умножение байтов массива State на {02} и на {03} выполняются по модулю $m(x) = x^8 + x^4 + x^3 + x + 1$. Пусть на вход преобразователя MixColums поступил 32-битовый столбец $s_{0C} = CA$; $s_{1C} = D1$; $s_{2C} = E2$; $s_{3C} = 4F$. В избыточном коде ПСКВ эти байты, представленные в 16-ричной системе счисления, имеют вид $CA = (D, 2, F, 9)$, $D1 = (5, 0, 5, 5)$, $E2 = (3, 1, 2, 1)$, $4F = (3, 0, 3, 3)$. Рассмотрим получение нового значения байта

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

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

Информационные остатки первого байта $CA = (D, 2)$ поступают на входы табл. 1 и 2. Представленная часть табл. 1 содержит остатки результата умножения, приведенной по модулям $m_1(x) = x^4 + x + 1$. На пересечении второй строки и столбца D располагается остаток $4 = 0100 = x^2$.

Табл. 2 содержит результат умножения $x \cdot s_j(x)$ по модулю $m_2(x) = x^4 + x^3 + 1$. На пересечении второй строки и столбца D располагается остаток $8 = 0100 = x^3$.

Кроме того, информационные остатки первого байта $CA = (D, 2)$ поступают на входы табл. 3 и 4. Табл. 3 содержит данные о сумме остатков информационных оснований ПСКВ. На пересечении 2 строки и столбца D находится остаток $C = 1100 = x^3 + x^2$.

В табл. 4 представлены данные о втором контрольном остатке. На пересечении 2 строки и столбца D находится остаток $B = 1011 + x^3 + x + 1$.

Таким образом, после выполнения операции умножения имеем

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

Таблица 2

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

	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

Таблица 3

Первый контрольный остаток $\alpha_3(x)$

	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

Таблица 4

Второй контрольный остаток $\alpha_4(x)$

	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

Рассмотрим умножение второго состояния $D1 = (5, 0, 5, 5)$ на коэффициент на $\{03\}$. Данную операцию можно представить в виде

$$\left(\{03\} \bullet D1\right) = \left(\{02\} \bullet D1\right) \oplus D1 = B9 \oplus D1.$$

Чтобы получить первое слагаемое воспользуемся табл. 1–4. На пересечении 0 строки и 5 столбца находится остаток:

– в табл. 1 (первый информационный остаток) – $7_{16} = 0111 = x^2 + x + 1$;
– в табл. 2 (второй информационный остаток) – $C_{16} = 1100 = x^3 + x^2$;
– в табл. 3 (первый контрольный остаток) – $B_{16} = 1011 = x^3 + x + 1$;
– в табл. 4 (второй контрольный остаток) – $0_{16} = 0000$.

Полученный результат складываем по модулю два с $D1 = (5, 0, 5, 5)$. Тогда

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

$$\alpha_3(x) = \left(x^3 + x + 1\right) + \left(x^2 + 1\right) = x^3 + x^2 + x = E_{16};$$

$$\alpha_4(x) = 0 + \left(x^2 + 1\right) = x^2 + 1 = 5_{16}.$$

Тогда имеем результат умножения на $\{03\}$

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

В табл. 5 показано суммирование полученных результатов.

Таблица 5

Результат вычисления нового состояния $s'_{0C}(x)$

	$\alpha_1(x)$	$\alpha_2(x)$	$\alpha_3(x)$	$\alpha_4(x)$
$8F =$	x^2	x^3	$x^3 + x^2$	$x^3 + x + 1$
$68 =$	x	$x^3 + x^2$	$x^3 + x^2 + x$	$x^2 + 1$
$E2 =$	$x + 1$	1	x	1
$4F =$	$x + 1$	0	$x + 1$	$x + 1$
$s'_{0C}(x) =$	$x^2 + x$	$x^2 + 1$	$x + 1$	$x^3 + x^2$

В результате получили новое состояние

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

Проведем проверку контрольных оснований согласно (3). Получаем

$$\alpha_3^*(x) = \sum_{i+1}^{2} \alpha_i(x) = \left(x^2 + x\right) + \left(x^2 + 1\right) = x + 1 = 3_{16};$$

$$\alpha_4^*(x) = \sum_{i+1}^{2} (i(x)\alpha_i(x)) \bmod m_3(x) = \left(x^2 + x\right) + x\left(x^2 + 1\right) = x^3 + x^2 = C_{16}.$$

Воспользуемся равенством (4), чтобы вычислить синдром ошибки

$$\delta_1(x) = \alpha_3(x) + \alpha_2^*(x) = \left(x + 1\right) + \left(x + 1\right) = 0;$$

$$\delta_2(x) = \alpha_4(x) + \alpha_4^*(x) = \left(x^3 + x^2\right) + \left(x^3 + x^2\right) = 0.$$

Значит, ошибка отсутствует – сбоя в процессе работы шифратора AES не было.

Пусть в результате сбоя произошло искажение первого слагаемого и ошибка произошла по первому остатку, а глубина ошибки равна $\Delta\alpha_1(x) = 1$. Тогда с выхода табл. 1 будет снят остаток $\alpha_1^*(x) = \alpha_1(x) + \Delta\alpha_1(x) = x^2 + 1$. Тогда имеем комбинацию

$$L_{\text{сбой}}\left(\{02\} \bullet CA\right) = \left(x^2 + 1, x^3, x^3 + x^2, x^3 + x + 1\right).$$

В табл. 6 показано суммирование полученных результатов.

Таблица 6

Результат вычисления нового состояния $s'_{0C}(x)$

	$\alpha_1(x)$	$\alpha_2(x)$	$\alpha_3(x)$	$\alpha_4(x)$
8F =	$\boldsymbol{x^2 + 1}$	x^3	$x^3 + x^2$	$x^3 + x + 1$
68 =	x	$x^3 + x^2$	$x^3 + x^2 + x$	$x^2 + 1$
E2 =	x + 1	1	x	1
4F =	x + 1	0	$x + 1$	$x + 1$
$s'_{0C}(x) =$	$\boldsymbol{x^2 + x + 1}$	$x^2 + 1$	$x + 1$	$x^3 + x^2$

В результате получили новое состояние

$$s'_{0C}(x) = \left(x^2 + x + 1, x^2 + 1, x + 1, x^3 + x^2\right).$$

Проведем проверку контрольных оснований согласно (3). Получаем

$$\alpha_3^*(x) = \sum_{i+1}^{2} \alpha_i(x) = \left(x^2 + x + 1\right) + \left(x^2 + 1\right) = x;$$

$$\alpha_4^*(x) = \sum_{i+1}^{2} (i(x)\alpha_i(x)) \bmod m_3(x) = \left(x^2 + x + 1\right) + x\left(x^2 + 1\right) = x^3 + x^2 + 1.$$

Воспользуемся равенством (4), чтобы вычислить синдром ошибки

$$\delta_1(x) = \alpha_3(x) + \alpha_2^*(x) = (x) + (x+1) = 1;$$

$$\delta_2(x) = \alpha_4(x) + \alpha_4^*(x) = (x^3 + x^2 + 1) + (x^3 + x^2) = 1.$$

В результате получили, что синдром ошибки отличен от нуля. Это свидетельствует о том, что код содержит ошибку, вызванную сбоем в работе шифратора. По значению синдрома ошибки $\delta_1(x) = 1$ и $\delta_2(x) = 1$ из памяти берется вектор ошибки, который равен $\overline{e} = (1,0,0,0)$. Данный вектор ошибки складываем с ошибочно комбинацией

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

Таким образом, ошибка, вызванная из-за атаки на основе сбоев, была устранена.

Выводы

Обобщая полученные результаты, можно сделать вывод о том, что разработанный алгоритм поиска и коррекции ошибок с помощью избыточного кода ПСКВ позволяет не только обнаруживать, но и исправлять ошибки. То есть данный алгоритм способен устранять последствия атаки на основе сбоев на алгоритм шифрования AES.

Список литературы

1. Калмыков И.А., Калмыков М.И. Новая технология, повышающая корректирующие способности модулярных кодов // Теория и техника радиосвязи. – Воронеж. ОАО «Концерн «Созвездие». – 2014. – № 3. – С. 5–13.

2. Калмыков И.А., Саркисов А.Б., Яковлева Е.М., Калмыков М.И. Модулярный систолический процессор цифровой обработки сигналов с реконфигурируемой структурой // Вестник Северо-Кавказского федерального университета. – 2013. – № 2 (35). – С. 30–35.

3. Калмыков И.А., Степанова Е.П., Калмыков М.И., Топоркова Е.В. Повышение помехоустойчивости к сбоям алгоритма шифрования AES на основе избыточной полиномиальной системы классов вычетов // Современные наукоемкие технологии. – 2015. – № 7. – С. 38–42.

4. Компьютеры – Атака по сторонним каналам – Типы side-channel атак. – URL: http://chinapads.ru/c/s/ataka_po_storonnim_kanalam_-_tipyi_side-channel_atak. (дата обращения: 15.06.2015).

5. Самарин А.А. Sitara AM335x – новая линейка макропроцессоров для промышленных применений с ядром Cortex-A8 // Компоненты и технологии. – 2012. – № 3. – С. 57–64.

6. Червяков Н.И. Калмыков И.А., Щелкунова Ю.О., Бережной В.В. Математическая модель нейронной сети для коррекции ошибок в непозиционном коде расширенного поля Галуа // Нейрокомпьютеры: разработка, применение. – 2003. – № 8–9. – С. 10–16.

7. Biham E., Dunkelman O., Keller N. Related-Key Boomerang and Rectangle Attacks. 2005. – URL: http://vipe.technion.ac.il – (дата обращения: 12.11.2015).

8. Cwennap L. Marvel lands a quad – Microprocessor Report, 2010, December.

9. Kalmykov I.A., Katkov K.A., Naumenko D.O, Sarkisov A.B., Makarova A.V. Parallel modular technologies in digital signal processing // Life Science Journal. – 2014. – № 11(11s). – P. 435–438.

10. Park J.H., Moon S.J., Choi D.H., Kang Y.S., Ha J.C. Differential fault analysis for round-reduced AES by fault injection // ETRI Journal. – 2011. – Vol. 33, № 3. – P. 434–442.