УДК 004.052.2

ПОВЫШЕНИЕ УСТОЙЧИВОСТИ К СБОЯМ АЛГОРИТМА ШИФРОВАНИЯ AES НА ОСНОВЕ ИЗБЫТОЧНОЙ ПОЛИНОМИАЛЬНОЙ СИСТЕМЫ КЛАССОВ ВЫЧЕТОВ

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 принятия и по настоящее время блочный шифр AES постоянно подвергается различным криптоатакам, в том числе атакам, использующим информацию, полученную по побочным каналам. Особое место среди последних занимают атаки на основе сбоев в работе шифратора. Такая атака позволяет злоумышленнику нарушить нормальную работу шифратора, вызвать ошибки в зашифрованном тексте, а затем на основе криптоанализа получить значение секретного ключа. Для противодействия атаке на основе сбоев предлагается использовать полиномиальную систему классов вычетов, которая позволяет обнаруживать и 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

IMPROVING ROBUST AES ENCRYPTION ALGORITHM BASED ON REDUNDANT POLYNOMIAL POLYNOMIAL RESIDUE NUMBER SYSTEM

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 adoption and the present block cipher AES is constantly exposed to various cryptotoken, including attacks using information obtained through side-channels. A special place among the last attack is based on the malfunction of the encoder. This attack allows evil to Myslenice disrupt the normal operation of the encoder, cause errors in the encrypted text, and then on the basis of cryptanalysis to obtain the value of the secret key. To counter the attack on the basis of failures is proposed to use a polynomial system classes deductions, which can detect and correct errors caused by malfunction of 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 system of residue classes, Galois field, algorithms, error detection and correction, positional characteristics

В современных инфокоммуникационных системах все большее применение находят параллельные вычислительные системы, расположенные на едином кристалле. Для обеспечения защиты информации от НСД в них, как правило, используют стандарт шифрования AES. Проведенный анализ работ [1–4] показал, что данный алгоритм шифрования подвергается различным криптоатакам, с целью его взлома и получения секретного ключа. Среди них особое место занимают криптоатаки, которые используют информацию, полученную по побочным каналам, в том числе на основе сбоев в работе шифратора. В результате проведения такой атаки злоумышленник, нарушая нормальную работу шифратора, вызывает ошибки в зашифрованном тексте, а затем на основе криптоанализа получает значение секретного ключа. Противостоять такому деструктивному воздействию можно за счет кодов, которые позволят обнаружить и исправить ошибки, вызванные сбоем в работе шифратора. Поэтому разработка алгоритма поиска и исправления ошибок с использованием полиномиальной системы классов вычетов (ПСКВ), которая полностью соответствует математической основе алгоритма шифрования AES, является актуальной задачей.

Современные системы на кристалле (СнК) объединяют на кристалле помимо нескольких процессорных ядер общего назначения еще и специализированные вычислительные модули. Так, в чипах Marvell Armada и TI OMAP [5] на одном чипе объединяются процессорные модули и криптографический ускорители. Так, для обеспечения конфиденциальности передаваемой информации в микропроцессорах Sitara Am38x, которые предназначены для использования в приборах и системах управления промышленной, введен криптопроцессор [6].

Одним из наиболее часто используемых алгоритмов криптозащиты является алгоритм шифрования AES. Это связано с тем, что данный алгоритм имеет лучшее сочетание криптографической стойкости, производительности, эффективности реализации

и гибкости. В качестве достоинств алгоритма шифрования AES можно выделить высокий уровень защищенности, реализацию в smart-картах благодаря низким требованиям к объемам памяти, высокую эффективность на любых платформах [7].

Широкое применение стандарта шифрования AES стимулировало большое число атак на данный алгоритм, которые делятся на следующие группы. Основу первой группы составляют «классические атаки» на алгоритм шифрования. В работе [1] показано проведение атаки методом бумеранга на 6-раундовую версию алгоритма со 128-битным ключом.

Вторая группа криптоатак базируется на модификации различных методов криптоанализа на связанных ключах. Так комбинация метода бумеранга и связанных ключей способствовала проведению атаки на 10 из 12 раундов алгоритма AES-192 [2].

Третья группа криптоатак на алгоритм шифрования AES·связаны с попытки использования алгебраических свойств алгоритма для его вскрытия. Такие атаки относятся к «алгебраическим атакам» [3].

В четвертую группу можно отнести исследования, которые посвящены атакам, использующим информацию, полученную по побочным каналам (side-channel-атакам). Особое место среди криптоатак по побочным каналам занимает атака на основе сбоев [4]. Эта атака относится к активным атакам. Эти атаки возможны в условиях, когда на шифрующее устройство осуществляются различные воздействия с целью внести искажения в информацию на различных этапах шифрования. В качестве защиты от атаки используют добавление в шифрующий механизм датчиков воздействий, блокирующих шифратор при ненормальных параметрах системы, вычисление контрольной суммы, экранирование шифратора.

Однако данные способы не учитывают особенности алгоритма шифрования, что приводит к значительным затратным решениям, в том числе и для блочного шифра AES. Поэтому разработка алгоритма, позволяющего противодействовать такой атаке путем обнаружения и коррекции возникшей ошибки в процессе шифрования, является актуальной задачей. Для противодействия атакам на основе сбоев в алгоритме AES предлагается использовать полиномиальную систему классов вычетов.

Известно, что алгоритм шифрования AES использует математический аппарат поля Галуа $GF(2^8)$ с порождающим полиномом $m(x) = x^8 + x^4 + x^3 + x + 1$. При этом алгоритм оперирует байтами, которые рассматриваются как элементы конечного поля $GF(2^8)$. Если в качестве информационных оснований ПСКВ использовать неприводимые полиномы 4 степени, то есть $m_1(x) = x^4 + x + 1$ и $m_2(x) = x^4 + x^3 + 1$, то операции в поле $GF(2^8)$ можно заменить аналогичным операциями в полях меньшей размерности $GF(2^4)$. Следовательно, при реализации алгоритма шифрования AES можно эффективно использовать полиномиальную систему классов вычетов с двумя основаниями $m_1(x) = x^4 + x + 1$ и $m_2(x) = x^4 + x^3 + 1$.

Как показано в работах [8–10], ПСКВ позволяет организовать вычисления параллельно, помодульно и независимо друг от друга, так как операции сложения, вычитания и умножения сводятся к соответствующим операциям над остатками по модулям $p_l(z)$ над полем:

$$\left|A(x) \otimes B(x)\right|^{+}_{p_j(x)} = \left|\alpha_i(x) \otimes b_i(x)\right|^{+}_{p_j(x)}, \quad (1)$$

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

Известно, что операции, которые реализуются в блоке замены байтов – преобразователе SubBytes алгоритма AES, представляют собой совокупность операций умножения и сложения по модулю. Значит, данные операции можно эффективно реализовать в полиномиальной системе классов вычетов.

Кроме того, коды ПСКВ позволяют обнаруживать и корректировать ошибки, которые возникают в процессе работы вычислительного устройства из-за отказа и сбоев оборудования [9, 10]. Для решения данной задачи в набор информационных оснований ПСКВ вводятся дополнительные контрольные основания. При реализации алгоритма шифрования на основе ПСКВ предлагается использовать в качестве рабочих оснований следующие полиномы $m_1(x) = x^4 + x + 1$ и $m_2(x) = x^4 + x^3 + 1$. Использование данных полиномов позволяет обеспечить рабочий диапазон, степень которого будет равна восьми. В качестве контрольного основания выбираем полином $m_3(x) = x^4 + x^3 + x^2 + x + 1$. Применение одного контрольного основания ПСКВ позволяет обнаруживать факт наличия ошибок, вызванных сбоями в работе устройства.

Повысить эффективность противодействия сбоям в работе алгоритма AES можно за счет алгоритма коррекции, который приведен в работе [9]. В работе [10] приведена схемная реализация этого алгоритма. Для реализации процесса обнаружения и исправления ошибок в модулярном коде полинома $A(z) = (\alpha_1(x), \alpha_2(x), ..., \alpha_k(x))$ вводят избыточность. С этой целью выбирается

одно контрольное основание $m_{k+1}(x)$, удовлетворяющее условию

$$\deg m_{k+1}(x) \geq \deg m_k(x). \quad (2)$$

При этом использовании данного контрольного модуля можно однозначно исправить однократную ошибку. Под однократной ошибкой понимается искажение одного разряда в кодовой комбинации, представленной в ПСКВ. Для этого необходимо провести вычисления:

$$\alpha_{k+1}(x) = \sum_{i+1}^{k} \alpha_i(x), \quad (3)$$

$$\alpha_{k+2}(x) = \sum_{i+1}^{k} (i(x)\alpha_i(x)) \bmod m_{k+1}(x), \quad (4)$$

где $i(x)$ – полиномиальная форма i-го порядкового номера, Σ – слоение по модулю два.

Для обнаружения ошибки в переданной кодовой комбинации вычисляются значения

$$\alpha^*_{k+1}(x) = \sum_{i+1}^{k} \alpha_i(x), \quad (5)$$

$$\alpha^*_{k+2}(x) = \sum_{i+1}^{k} (i(x)\alpha_i(x)) \bmod m_{k+1}(x). \quad (6)$$

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

$$\delta_1(x) = \alpha_{k+1}(x) + \alpha^*_{k+1}(x), \quad (7)$$

$$\delta_2(x) = \alpha_{k+2}(x) + \alpha^*_{k+2}(x), \quad (8)$$

Если синдром ошибки $\delta_1(x) = 0$ и $\delta_2(x) = 0$, то комбинация не содержит ошибки. В противном случае, когда $\delta_1(x) \neq 0$ и $\delta_2(x) \neq 0$, комбинация является запрещенной, т.е. ошибочной. По величине $\delta_1(x)$ и $\delta_2(x)$ можно провести коррекцию однократной ошибки.

Рассмотрим применение избыточной ПСКВ при реализации базовой процедуры замены блоков в алгоритме шифрования AES. Байт открытого текста S поступает на вход преобразователя из позиционного кода в код ПСКВ, с выхода которого снимаются значения двух остатков $s_1(x)$ и $s_2(x)$, где $s_1(x) \equiv S(x) \bmod m_1(x)$ и $s_2(x) \equiv S(x) \bmod m_2(x)$. Таким образом, текущий байт представляет $S(x)$ собой два четырехразрядных блока данных. В таком виде данные поступают на входы преобразователя SubBytes. При этом первый остаток $s_1(x)$ определяет номер столбца, а номер строки задается остатком по второму модулю $s_2(x)$. В этом случае таблица замен SubBytes, которая требовала блок памяти 256×8 бит, теперь представляется в виде двух таблиц размером 256×4 бит. Каждая из таблиц представляет собой остаток числа результата подстановки $S'(x)$, приведенной по модулям $m_1(x) = x^4 + x + 1$ и $m_2(x) = x^4 + x^3 + 1$ соответственно. В табл. 1 приведены первые три строки таблицы замен S_1-блока по рабочему модулю $m_1(x) = x^4 + x + 1$.

В табл. 2 приведены первые три строки таблицы замен S_2-блока по модулю $m_2(x) = x^4 + x^3 + 1$ соответственно.

Пусть байт открытого текста равен $S(x) = \{00011001_2\} = \{19_{16}\}$. Данное значение поступает на вход преобразователя из позиционного кода в ПСКВ, с выхода которого будут сниматься два остатка:

$$s_1(x) = S(x) \bmod x^4 + x + 1 = \{19_{16}\} \bmod x^4 + x + 1 = x^4 + x^3 + 1 \bmod x^4 + x + 1 = x^3 + x = A$$

$$s_2(x) = S(x) \bmod x^4 + x^3 + 1 = \{19_{16}\} \bmod x^4 + x^3 + 1 = x^4 + x^3 + 1 \bmod x^4 + x^3 + 1 = 0.$$

Таблица 1

Таблица замен S_1-блока по модулю $m_1(x) = x^4 + x + 1$

$s_2(x)$	Остаток $s_1(x)$ по модулю $m_1(x) = x^4 + x + 1$															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	9	9	2	F	D	B	B	5	B	F	0	1	4	3	F	9
1	D	5	9	0	9	3	4	A	4	F	6	0	4	8	9	1
2	A	2	E	5	A	4	6	C	2	4	D	6	6	D	F	8

Таблица 2

Таблица замен S_2-блока по модулю $m_1(x) = x^4 + x + 1$

$s_2(x)$	Остаток $s_1(x)$ по модулю $m_1(x) = x^4 + x + 1$															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7	F	8	3	5	C	B	8	6	4	5	4	E	B	C	B
1	B	1	4	6	D	9	B	F	D	F	A	1	6	B	C	2
2	2	0	A	7	F	4	3	2	3	5	E	B	1	9	9	9

Таким образом, на входы каждой из таблиц замен S_1-блока по модулю $m_1(x) = x^4 + x + 1$ и S_2-блока по модулю $m_1(x) = x^4 + x^3 + 1$ поступают остатки S(x) = (A, 0). Результат замены определяется из табл. 1 и 2. В табл. 1 на пересечении столбца А и строки 0 находится число 0. В табл. 2 на пересечении столбца А и строки 0 находится число 5. В результате воздействия на байт состояния S(x) = $\{00011001_2\}$=$\{19_{16}\}$=(A, 0) был получен байт подстановки, который в ПСКВ по этим двум основаниям представляется в виде двух остатков S'(x) = (0, 5). Полученный результат соответствует подстановке S'(x) = ={$d4_{16}$}={11010100_2}. Это подтверждается следующими сравнениями:

$$s_1'(x) = \{d4_{16}\} \bmod x^4 + x + 1 = x^7 + x^6 + x^4 + x^2 \bmod x^4 + x + 1 = 0;$$

$$s_2'(x) = \{d4_{16}\} \bmod x^4 + x^3 + 1 = x^7 + x^6 + x^4 + x^2 \bmod x^4 + x^3 + 1 = x^2 + 1 = 5.$$

Для реализации противодействия атакам, построенных на сбоях работы шифратора, используются дополнительно табл. 3 и 4. Табл. 3 содержит данные о сумме остатков информационных оснований ПСКВ $m_1(x) = x^4 + x + 1$ и $m_2(x) = x^4 + x^3 + 1$. Результат был получен на основе равенства (3).

В табл. 4 представлены данные о взвешенной сумме остатков рабочих оснований $m_1(x) = x^4 + x + 1$ и $m_2(x) = x^4 + x^3 + 1$. Результат был получен на основе равенства (4).

Таким образом, при подаче на вход табл. 3 и 4 значений остатков $S(x)$ = (A, 0) с выхода табл. 3 будет снято значение $\{5_{16}\} = \{0101_2\} = \{x^2 + 1\}$. Данное число находится на пересечении столбца А и строки 0 в табл. 3. С выхода табл. 4 будет снято значение $\{A_{16}\} = \{1010_2\} = \{x^3 + x\}$.

Пусть в процессе работы шифратора AES атак не проводилось. Тогда после выполнения операции подстановки проводится проверка на наличие ошибок в комбинации ПСКВ:

$$s_3^*(x) = \sum_{i+1}^{2} s_i'(x) = 0 + x^2 + 1 = x^2 + 1 = \{5_{16}\}.$$

$$s_4^*(x) = \sum_{i+1}^{2} (i(x)s_i'(x)) \bmod m_3(x) = \left(0 + x(x+1)\right) \bmod x^4 + x^3 + x^2 + x + 1 = x^3 + x = \{A_{16}\}.$$

Затем, согласно (7) и (8), производится вычисление синдрома ошибки. Так как синдром равен нулю, то сбоя в процессе работы шифратора не произошло. Полученные значения остатков $s_1'(x) = 0000_2$ и $s_2'(x) = 1010_2$ по рабочим основаниям ПСКВ дальше будут участвовать в последующих раундовых преобразованиях, побайтовом сдвиге строк Shift Rows, перемешивании столбцов MixColums сложении с раундовым ключом AddRoundKey.

Пусть в процессе работы шифратора произошла атака на основе сбоев. Сбой вызвал изменение остатка по основанию $m_1(x) = x^4 + x + 1$, а его глубина равна $\Delta s_1(x) = 1$. Тогда

$$s_1^{\text{ош}}(x) = s_1'(x) + \Delta s(x) = 0 + 1 = 0001_2.$$

В результате на вход блока, реализующего алгоритм коррекции ошибок, подается

$$S'(x) = (s_1^{\text{ош}}(x), s_2'(x), s_3'(x), s_4'(x)) = (0001_2, 0101_2, 0101_2, 1010_2) = (1, x^2 + 1, x^2 + 1, x^3 + x).$$

Таблица 3

Остатки $\alpha_3(x)$ по модулю $m_3(x) = x^4 + x^3 + x^2 + x + 1$

$s_2(x)$	Остаток $s_1(x)$ по модулю $m_1(x) = x^4 + x + 1$															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	E	6	A	C	8	7	0	D	D	B	5	5	A	8	3	2
1	6	4	D	6	4	A	F	5	9	0	C	1	2	3	5	3
2	8	2	4	2	5	0	5	E	1	1	3	D	7	4	6	1

Таблица 4

Остатки $\alpha_4(x)$ по модулю $m_3(x) = x^4 + x^3 + x^2 + x + 1$

$s_2(x)$	Остаток $s_1(x)$ по модулю $m_1(x) = x^4 + x + 1$															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7	E	B	9	7	A	4	C	7	7	A	9	1	C	E	6
1	2	7	1	C	A	8	B	D	7	8	B	2	8	7	8	5
2	E	2	3	B	D	C	0	8	4	E	8	9	4	6	4	3

Тогда вычисленные новые значения проверочных остатков, согласно (5) и (6), равны

$$s_3^*(x) = \sum_{i+1}^{2} s_i^{'}(x) = 1 + x^2 + 1 = x^2 = \{4_{16}\}.$$

$$s_4^*(x) = \sum_{i+1}^{2} (i(x)s_i^{'}(x)) \bmod m_3(x) = \left(1 + x\left(x+1\right)\right) \bmod x^4 + x^3 + x^2 + x + 1 = x^3 + x + 1 = \{B_{16}\}.$$

Затем производится вычисление синдрома ошибки

$$\delta_1(x) = s_3^{'}(x) + s_3^*(x) = \left(x^2 + 1\right) + \left(x^2\right) = 1.$$

$$\delta_2(x) = s_4^{'}(x) + s_4^*(x) = \left(x^3 + x\right) + \left(x^3 + x + 1\right) = 1.$$

Так как синдром ошибки не равен нулю, то это свидетельствует о том, что в ходе выполнения раундового преобразования произошел сбой. Тогда, зная местоположение ошибки и ее глубину, можно провести коррекцию

$$s_1^{'}(x) = s_1^{\text{ош}}(x) + \Delta s(x) = 0001 + 0011 = 0000_2.$$

Таким образом, благодаря разработанному алгоритму коррекции ошибок с использованием ПСКВ можно устранять последствия сбоев в работе шифратора алгоритма AES.

Выводы

Для противодействия атакам на основе сбоев был разработан алгоритм коррекции ошибок с использованием кодов ПСКВ. При этом переход от работы в поле Галуа $GF(2^8)$ к полям Галуа $GF(2^4)$ позволяет корректировать ошибки при меньших схемных затратах. Использование алгоритма обеспечивает исправление всех однократных ошибок и до 80 процентов двукратных ошибок, возникающих из-за сбоев в работе шифратора. При этом требуется в 1,22 раза меньше схемных затрат по сравнению с классической системой маскирования отказов «2 из 3». Полученные результаты свидетельствуют об эффективности применения кодов ПСКВ для противодействия последствиям атак на основе сбоев.

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., Щелкунова Ю.О., Барильская А.В. Устройство для коррекции ошибок в полиномиальной системе классов вычетов // Патент РФ № 2453902. Бюл. № 17 от 20.06.2012.

3. 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).

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

5. Стандарт криптографической защиты – AES. Конечные поля /Зензин О.С., Иванов М.А. Под ред. М.А. Иванова. – М.: КУДИЦ-ОБРАЗ, 2002. – 176 с.

6. Biham E., Dunkelman O., Keller N. Related-Key Boomerang and Rectangle Attacks. 2005. URL: http://vipe.technion.ac.il – (дата обращения: 15.06.2015).

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

8. Ferguson N., Schroeppel R., Whiting D. A simple algebraic representation of Rijndael/ Draft 2001/05/16.URL: http://citeseer.ist.psu.edu. (дата обращения: 15.06.2015).

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.