Современная наука и инновации.
2023. № 2(42). С. 59-70
Modern Science and Innovations.
2023; 2(42):59-70

ТЕХНИЧЕСКИЕ НАУКИ / TECHNICAL SCIENCE

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ / INFORMATICS, COMPUTER ENGINEERING AND MANAGEMENT

Научная статья / Original article

УДК 004.052.32
DOI: 10.37493/2307-910X.2023.2.6

Игорь Анатольевич Калмыков
[Igor A. Kalmykov],
Игорь Александрович Проворнов
[Igor A. Provornov]

Разработка математической модели отказоустойчивого преобразователя invsubbytes в полиномиальной системе классов вычетов

Development of a mathematical model of a fault-tolerant invsubbytes converter in a polynomial system of residue classes

Северо-Кавказский федеральный университет, г. Ставрополь, Россия / North-Caucasus Federal University, Stavropol, Russia, igorprovornov@yandex.ru

Аннотация. *Статья посвящена вопросу повышения отказоустойчивости процедуры InvSubBytes SPN-преобразователей. Описывается возможность применения корректирующего кода в полиномиальной системе классов вычетов в качестве инструмента детектирования и устранения последствий сбоев работы блоков замены.*

Ключевые слова: SPN-система, InvSubBytes, отказоустойчивость, полиномиальная система классов вычетов, корректирующие коды.

Для цитирования: Калмыков И. А., Проворнов И. А. Разработка математической модели отказоустойчивого преобразователя invsubbytes в полиномиальной системе классов вычетов // *Современная наука и инновации. 2023. №2 (42). С. 59-70. https://doi.org/10.37493/2307-910x.2023.2.6*

Abstract. *The article is devoted to the issue of improving the fault tolerance of the InvSubBytes procedure of SPN converters. Describes the possibility of applying a corrective code in a polynomial system of residue classes as a tool for detecting and eliminating the consequences of failures in the operation of replacement blocks.*

Key words: SPN system, InvSubBytes, fault tolerance, polynomial system of residue classes, corrective codes.

For citation: Kalmykov I. A., Skornov I. A. Development of a mathematical model of a fault-tolerant invsubbytes converter in a polynomial system of residue classes *Modern Science and Innovations. 2023;2(42):59-70. https://doi.org/10.37493/2307-910X.2023.2.6*

Введение. В настоящее время широкое распространение получает концепция «Интернета вещей» – сети передачи данных между физическими объектами и внешней средой. Подобные технологии активно используются в медицине, сельском хозяйстве, транспортных системах, управлении городской инфраструктурой и т.п. Вместе с тем, значительная часть передаваемой в таких системах информации является конфиденциальной и требует защиты от несанкционированного доступа.

Это достигается совокупностью применения различных мер, в том числе мер криптографической защиты информации. Одним из наиболее распространённых алгоритмов шифрования, применяемых в «Интернете вещей» является американский стандарт шифрования, представляющий собой реализацию технологии SPN-шифрования. Однако, американский стандарт шифрования может быть подвержен атакам на основе сбоев, заключающимся в активном внешнем воздействии на шифратор различных факторов,

нарушающих его нормальные условия эксплуатации. Возникающие в результате таких воздействий ошибки снижают криптостойкость шифрования.

Одним из вариантов противодействия атакам на основе сбоев считается внедрение механизмов обнаружения и исправления ошибок. Целью настоящего исследования является повышение отказоустойчивости дешифратора американского стандарта шифрования за счет применения корректирующих кодов в полиномиальной системе классов вычетов.

1. Проблематика обеспечения надежности систем, реализующих американский стандарт шифрования. Американский стандарт шифрования представляет собой симметричный криптоалгоритм, который в результате многократного применения к исходному набору данных размером 128 бит процедур сложения с ключевой информацией (AddRoundKey), подстановки (SubBytes), перемешения (MixColumns) и сдвига (ShiftRows) преобразует его в зашифрованный блок данных, пригодный для безопасной передачи по открытым каналам связи. Шифрование информации осуществляется за 10 последовательных шагов обработки данных (раундов), при этом в раундах с 1 по 9 включительно используются все 4 базовых процедуры, а в раунде 10 только 3 (за исключением перемешения). В свою очередь, на приёмной стороне происходит его расшифрование за счет повторного сложения с ключевой информацией (AddRoundKey) и последовательной реализации процедур, обратных к преобразованиям, выполненным в шифраторе: InvSubBytes, InvMixColumns, InvShiftRows. Дешифрование также осуществляется в течении 10 раундов, при этом в 1 раунде используются только процедуры AddRoundKey, InvSubBytes, InvShiftRows, а в раундах 2 по 10 включительно добавляется InvMixColumns. Таким образом, систему передачи данных с реализацией криптографической защиты информации на основе американского стандарта шифрования можно представить в виде совокупности отдельных операций, как показано на рисунке 1.

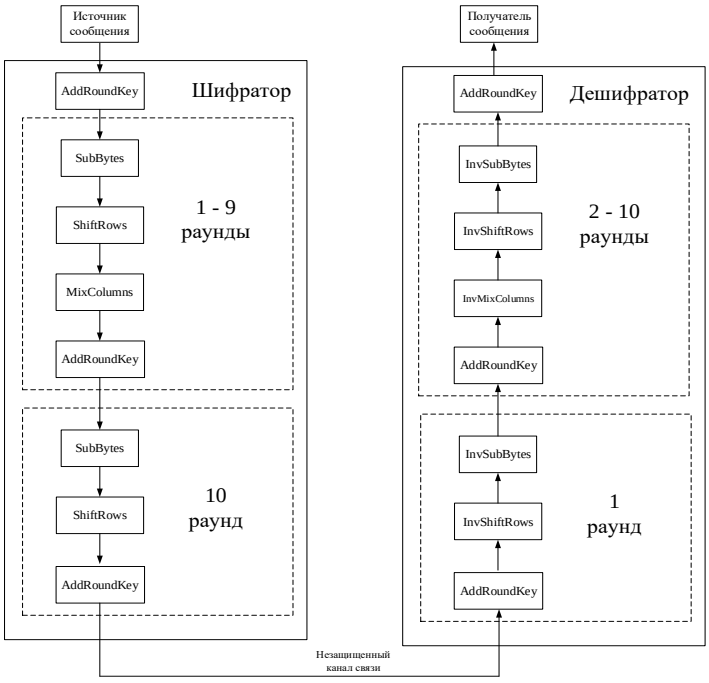

Рисунок 1. Система передачи данных с криптографической защитой
Figure 1. Data transmission system with cryptographic protection

С точки зрения отказоустойчивости рассматриваемой системы, наиболее уязвимыми являются блоки выполнения процедур SubBytes, MixColumns, InvSubBytes и InvMixColumns так они требуют более сложной аппаратной реализации, что приводит к увеличению вероятности возникновения сбоев в процессе функционирования.

В работе [1] предложен способ повышения отказоустойчивости процедуры SubBytes за счет применения корректирующих кодов полиномиальной системы классов вычетов. Вместе с тем, на текущий момент нерешенной является научная задача реализации обратного преобразования InvSubBytes, что приводит к необходимости дополнительных

преобразований обрабатываемой информации из позиционной системы счисления в полиномиальную систему классов вычетов.

Преобразование InvSubBytes предназначено для замены входного блока данных, который в американском стандарте шифрования представлен 8 битами, на другой блок данных в соответствии с таблицей замены, представленной на рисунке 2.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1d
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3d	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Рисунок 2. Таблица замены процедуры InvSubBytes
Figure 2. InvSubBytes procedure replacement table

В классической реализации InvSubBytes байт интерпретируется как два шестнадцатеричных символа, при этом первый символ является идентификатором строки в таблице перестановки, а второй – столбца. На пересечении строки и столбца, обозначенных этими шестнадцатеричными символами, находится новый байт. Однако, при такой реализации система не является отказоустойчивой и любой сбой в ее работе приведет к получению ошибочного значения на выходе блока замены и, как следствие, к сбою работы всего алгоритма.

Одним из методов выявления и устранения ошибок, возникающих в системах обработки и передачи информации, является применение корректирующего кодирования. Основным принципом корректирующего кодирования является добавление в передаваемую (полезную) информацию избыточных (служебных) данных, которые на приемной стороне используются для обнаружения и исправления ошибок. Корректирующая способность кода зависит от отношения служебной информации к полезной: повышение избыточности кода увеличивает его корректирующие свойства. Однако, избыточность снижает эффективность использования системы передачи. С учетом этих взаимно противоречивых требований, перспективным способом повышения отказоустойчивости является применение кодов, обеспечивающих коррекцию ошибок при минимальной относительной избыточности.

2. Математические основы полиномиальной системы классов вычетов. В полиномиальной системе классов вычетов число представляется в виде набора остатков от его деления на полиномы-основания p_i:

$$A = (\alpha_1(x), \alpha_2(x) \ldots \alpha_i(x) \ldots \alpha_k(x)) \quad (1)$$

где $\alpha_i(x) = A \bmod p_i$.

Количество чисел, которые можно представить в конкретной полиномиальной системе классов вычетов определяется выражением:

$$A < P_{раб}, \quad (2)$$

где $P_{раб} = \prod_{i=1}^{k} p_i$ – рабочий диапазон.

Операции сложения, вычитания и умножения чисел сводятся к соответствующим операциям с их остатками:

$$A+B=(\alpha_1(x)+\beta_1(x),\alpha_2(x)+\beta_2(x)\ldots\alpha_i(x)+\beta_i(x)\ldots\alpha_k(x)+\beta_k(x)), \quad (3)$$

$$A-B=(\alpha_1(x)-\beta_1(x),\alpha_2(x)-\beta_2(x)\ldots\alpha_i(x)-\beta_i(x)\ldots\alpha_k(x)-\beta_k(x)), \quad (4)$$

$$A\cdot B=(\alpha_1(x)\cdot\beta_1(x),\alpha_2(x)\cdot\beta_2(x)\ldots\alpha_i(x)\cdot\beta_i(x)\ldots\alpha_k(x)\cdot\beta_k(x)). \quad (5)$$

Уменьшение разрядности обрабатываемых операндов и параллельное выполнение операций позволяет увеличить быстродействие системы. Кроме того, независимость выполнения операций над остатками и отсутствие взаимосвязи между вычислительными трактами позволяют не допустить распространения возникающих ошибок, что является предпосылкой создания на базе полиномиальной системы классов вычетов эффективных корректирующих кодов [2].

Для реализации корректирующих свойств кода остатки разделяются на информационные и контрольные:

$$A=(\alpha_1(x),\alpha_2(x)\ldots\alpha_k(x),\alpha_{k+1}(x),\alpha_{k+2}(x)\ldots\alpha_n(x)), \quad (6)$$

где k – количество информационных остатков,

n – общее количество остатков.

Остатки в количестве $r=n-k$ используются для обнаружения и коррекции возникающих ошибок [3].

При реализации корректирующих алгоритмов также используются значения контрольного и полного диапазонов:

$$P_{контр}=\prod_{i=n-k+1}^{n}p_i, \quad (7)$$

$$P_{полн}=P_{раб}\cdot P_{контр}. \quad (8)$$

3. Разработка математической модели отказоустойчивого преобразователя InvSubBytes в полиномиальной системе классов вычетов.

Под математической моделью понимается система математических элементов и отношений между ними, адекватно отражающая некоторые свойства объекта, существенные с точки зрения решаемой задачи.

В свою очередь с точки зрения описания преобразования InvSubBytes значимыми свойствами являются:

- входной бит данных, поступающий на вход преобразователя InvSubBytes;
- выходной бит данных, являющийся результатом работы преобразователя InvSubBytes;
- функциональные зависимости, связывающие входные и выходные данные.

Так как взаимосвязь входных и выходных параметров американского стандарта шифрования определена его спецификацией, то задача разработки математической модели отказоустойчивого преобразователя InvSubBytes сводится к разработке такого вычислительного алгоритма, результаты работы которого должны повторять результаты классического алгоритма, но его принципы дополнительно должны обеспечивать возможность устранения возникающих ошибок.

В качестве прототипа подобного алгоритма, целесообразно использовать алгоритм, описанный в [4], в котором устранение ошибок производится за счет использования контрольных остатков, вычисляемых следующим образом:

$$\alpha_{k+1}=\lambda_1^{k+1}\cdot\alpha_1+\ldots\lambda_i^{k+1}\cdot\alpha_i+\ldots\lambda_k^{k+1}\cdot\alpha_k \bmod p_{k+1}, \quad (9)$$

$$\alpha_{k+2} = \lambda_1^{k+2} \cdot \alpha_1 + ... \lambda_i^{k+2} \cdot \alpha_i + ... \lambda_k^{k+2} \cdot \alpha_k \bmod p_{k+2}, \quad (10)$$

где λ_i^{k+1}, λ_i^{k+2} – константы системы счисления,

p_{k+1}, p_{k+2} – контрольные основания.

Предлагается использовать следующую модификацию алгоритма:

- информационные основания: $p_1(x) = x^4 + x + 1$, $p_2(x) = x^4 + x^3 + 1$;
- контрольное основание $p_3(x) = p_1(x) = x^4 + x^3 + x^2 + x + 1$;
- $\lambda_1^{k+1} = 1$, $\lambda_2^{k+1} = 1$, $\lambda_1^{k+2} = 1$, $\lambda_2^{k+2} = x$;
- при определении первого контрольного остатка не выполнять деление по модулю p_{k+1};
- при определении второго контрольного остатка выполнять деление по модулю p_{k+1}.

Для реализации процедуры InvSubBytes в рассматриваемой полиномиальной системе классов вычетов предлагается:

1) Входной байт $S_{вх}$, рассматриваемый как элемент конечного поля GF(2^8), представлять в полиномиальной системе классов вычетов, т.е. в виде набора остатков от его деления на полиномы-основания $p_1(x)$, $p_2(x)$:

$$p_1(x) = x^4 + x + 1, \quad (11)$$

$$p_2(x) = x^4 + x^3 + 1. \quad (12)$$

Тогда представление входного байта $S_{вх}$ будет иметь вид:

$$S_{вх} = (s_1(x), s_2(x)), \quad (13)$$

где: $s_1(x) = S_{вх} \bmod p_1$,

$s_2(x) = S_{вх} \bmod p_2$.

2) Набор выходных значений S-блока (т.е. все множество GF(2^8) хранить и представлять в полиномиальной системе классов вычетов в виде совокупности информационных ($\alpha_1(x)$, $\alpha_2(x)$) и контрольных ($\alpha_3(x)$, $\alpha_4(x)$) остатков, рассчитываемых по формулам:

$$\alpha_1(x) = S_{вых} \bmod p_1, \quad (14)$$

$$\alpha_2(x) = S_{вых} \bmod p_2, \quad (15)$$

$$\alpha_3(x) = \alpha_1(x) + \alpha_2(x), \quad (16)$$

$$\alpha_4(x) = (\alpha_1 + x \cdot \alpha_2(x)) \bmod p_3(x), \quad (17)$$

где $p_3(x) = x^4 + x^3 + x^2 + x + 1$ – контрольное основание.

3) Представление входного байта в полиномиальной системе классов вычетов использовать как идентификаторы строк и столбцов в таблицах, содержащих информацию о значении выходного байта $S_{вых}$, при этом s_1 использовать как идентификатор строки, а s_2 – как идентификатор столбца. На пересечении s_1 и s_2 в первой таблице следует разместить $\alpha_1(x)$, во второй – $\alpha_2(x)$, в третьей – $\alpha_3(x)$, в четвертой – $\alpha_4(x)$. При построении таблиц необходимо сохранить соответствие пар входного и выходного

байтов стандартной реализации InvSubBytes для возможности интеграции предлагаемого варианта процедуры и классического.

Таким образом, выходное значение $S_{вых}$ будет определяться в результате работы четырех таблиц замены, представленных на рисунках 3 – 6.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	d	7	1	a	0	e	b	c	7	7	5	6	b	b	7	f
1	b	9	8	e	a	1	c	4	e	9	1	1	d	8	1	2
2	1	f	0	0	f	8	1	4	8	6	0	f	7	3	d	0
3	2	d	8	1	8	c	6	1	0	f	c	3	6	a	f	3
4	2	b	2	2	5	5	e	b	d	2	8	1	c	4	a	9
5	a	6	c	9	9	3	3	7	4	2	b	c	f	4	e	3
6	3	e	3	d	c	9	8	8	6	d	9	8	c	7	a	6
7	d	b	6	3	0	3	e	d	0	0	e	f	b	8	9	7
8	4	5	2	a	a	7	6	c	1	e	9	5	a	4	0	f
9	f	7	1	5	c	7	9	d	f	c	0	5	b	d	5	e
a	9	6	4	a	9	5	a	2	a	2	e	2	6	f	2	7
b	5	c	6	d	6	6	b	2	d	f	2	6	4	0	3	f
c	9	8	5	3	2	a	9	f	a	e	d	5	a	b	b	e
d	5	8	7	5	8	0	2	3	b	4	3	4	3	1	4	1
e	7	0	0	5	c	c	4	1	e	7	4	e	c	a	3	9
f	4	5	b	f	7	d	6	e	0	1	4	d	b	8	8	9

Рисунок 3. Таблица определения $\alpha_1(x)$.

Figure 3. Definition table.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	4	6	2	c	a	7	e	d	d	c	9	3	9	b	b	4
1	1	9	3	9	4	1	2	a	b	7	e	6	b	d	b	9
2	3	1	e	b	5	8	f	5	b	b	2	7	2	9	3	3
3	b	c	2	4	5	8	2	d	4	c	e	d	f	a	d	0
4	3	0	5	f	2	b	5	4	e	1	e	c	c	7	f	0
5	0	9	7	b	2	4	a	f	b	8	7	9	6	0	6	c
6	1	3	3	d	1	8	9	6	7	f	f	0	3	4	3	8
7	8	3	5	8	5	2	e	a	9	0	d	8	c	a	d	a
8	4	3	0	5	e	0	d	6	a	4	e	f	d	6	7	e
9	3	3	5	1	a	5	c	6	2	f	6	e	6	2	6	2
a	5	e	e	b	a	4	1	6	8	c	f	d	4	b	2	1
b	c	b	a	0	1	6	2	a	1	0	e	0	d	1	7	f
c	6	f	d	f	7	9	4	a	7	1	9	0	6	8	5	0
d	8	7	7	7	1	d	4	5	d	1	e	9	d	9	c	7
e	e	f	8	a	0	4	f	8	8	9	8	c	5	2	6	3
f	3	5	a	9	8	5	c	a	c	0	2	7	f	4	c	1

Рисунок 4. Таблица определения $\alpha_2(x)$.

Figure 4. Definition table.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	9	1	3	6	a	9	5	1	a	b	c	5	2	0	c	b
1	a	0	b	7	e	0	e	e	5	e	f	7	6	5	a	b
2	2	e	e	b	a	0	e	1	3	d	2	8	5	a	e	3
3	9	1	a	5	d	4	4	c	4	3	2	e	9	0	2	3
4	1	b	7	d	7	e	b	f	3	3	6	d	0	3	5	9
5	a	f	b	2	b	7	9	8	f	a	c	5	9	4	8	f
6	2	d	0	0	d	1	1	e	1	2	6	8	f	3	9	e
7	5	8	3	b	5	1	0	7	9	0	3	7	7	2	4	d
8	0	6	2	f	4	7	b	a	b	a	7	a	7	2	7	1
9	c	4	4	4	6	2	5	b	d	3	6	b	d	f	3	c
a	c	8	a	1	3	1	b	4	2	e	1	f	2	4	0	6
b	9	7	c	d	7	0	9	8	c	f	c	6	9	1	4	0
c	f	7	8	c	5	3	d	5	d	f	4	5	c	3	e	e
d	d	f	0	2	9	d	6	6	6	5	d	d	8	8	8	6
e	9	f	8	f	c	8	b	9	6	e	c	2	9	8	5	a
f	7	0	1	6	f	8	a	4	c	1	6	a	4	c	4	8

Рисунок 5. Таблица определения $\alpha_3(x)$.

Figure 5. Definition table.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	5	b	5	1	7	0	4	5	e	c	4	0	a	e	2	7
1	9	8	e	f	2	3	8	3	b	7	e	d	8	1	4	3
2	7	d	f	5	5	b	c	e	d	3	4	1	3	2	b	6
3	7	6	c	9	2	f	2	8	8	4	3	a	b	d	6	3
4	4	b	8	f	1	0	4	3	2	0	7	a	7	a	7	9
5	a	7	2	c	d	b	4	a	1	1	5	d	3	4	2	8
6	1	8	5	4	e	a	9	4	8	0	4	8	a	f	c	5
7	e	d	c	0	a	7	1	a	1	0	7	c	0	f	0	0
8	c	3	2	0	5	7	f	0	6	6	6	8	3	8	e	0
9	9	1	b	7	b	d	2	1	b	1	c	a	7	9	9	a
a	3	9	b	f	e	d	8	e	9	9	3	b	e	a	6	5
b	e	9	1	d	4	a	f	5	f	f	d	6	d	2	d	2
c	5	5	c	e	c	b	1	8	4	c	c	5	6	8	1	e
d	6	6	9	b	a	9	a	9	2	6	c	5	6	0	f	f
e	8	d	3	2	c	4	9	2	d	6	7	5	6	e	f	f
f	2	f	c	e	4	7	d	9	b	1	0	3	6	0	3	b

Рисунок 6. Таблица определения $\alpha_4(x)$.

Figure 6. Definition table.

В предлагаемой реализации процедуры InvSubBytes благодаря наличию контрольных остатков существует возможность устранения сбоев в работе блоков вычисления информационных остатков за счет работы следующего корректирующего алгоритма:

1) На основе значений $\alpha_1(x)$ и $\alpha_2(x)$, полученных в результате работы блоков замены, функционирующих в соответствии с таблицами, предоставленными на рисунках 3 и 4, вычисляются контрольные значения $\alpha_{3_к}(x)$ и $\alpha_{4_к}(x)$:

$$\alpha_{3_к}(x) = \alpha_1(x) + \alpha_2(x), \quad (18)$$

$$\alpha_{4_к}(x) = (\alpha_1 + x \cdot \alpha_2(x)) \bmod p_3(x). \quad (19)$$

В случае корректной работы этих блоков замены рассчитанные значения $\alpha_{3_к}(x)$ и $\alpha_{4_к}(x)$ совпадают со значениями $\alpha_3(x)$ и $\alpha_4(x)$, полученными в результате работы блоков замены, функционирующих в соответствии с таблицами, предоставленными на рисунках 5 и 6.

2) Вычисляются синдромы ошибки, которые являются показателем степени искажения информационных остатков:

$$\delta_1(x) = \alpha_3(x) \oplus \alpha_{3_к}(x), \quad (20)$$

$$\delta_2(x) = \alpha_4(x) \oplus \alpha_{4_к}(x). \quad (21)$$

3) На основе полученных значений $\delta_1(x)$, $\delta_2(x)$ и априорной информации о распределении ошибок, фрагмент которой представлен в таблице 1, проводится локализация и исправление ошибок:

$$S_{вых_{корр}} = S_{вых} + \Delta S_{вых}, \quad (22)$$

где $\Delta S_{вых}$ – вектор ошибки.

Таблица 1 – Соответствие значений $\delta_1(x)$ и $\delta_2(x)$ локализации ошибок.
Table 1 – Correspondence of values and localization of errors.

Местоположение ошибки		δ_1	δ_2
α_1(3 *разряд*)		x^3	x^3
α_1(2 *разряд*)		x^2	x^3
α_1(1 *разряд*)		x	x
α_1(0 *разряд*)		1	1
α_2(3 *разряд*)		x^3	$x+1$
α_2(2 *разряд*)		x^2	x^2
α_2(1 *разряд*)		x	x^2
α_2(0 *разряд*)		1	x^3+x^2+1
Местоположение ошибок		δ_1	δ_2
α_1(0 *разряд*)	α_2(0 *разряд*)	0	$x+1$
α_1(0 *разряд*)	α_2(1 *разряд*)	$x+1$	x^2+1
…	…	…	…
α_1(3 *разряд*)1	α_2(3 *разряд*)	0	x^2+x+1

Рассмотрим пример работы предлагаемой модели.

Пусть на вход устройства реализации процедуры InvSubBytes поступает число 44_{16}, тогда в полиномиальной системе классов вычетов оно будет иметь вид:

$$44_{16} = \left(44_{16} \bmod x^4 + x + 1, 44_{16} \bmod x^4 + x^3 + 1\right) = \left(8_{16,} B_{16}\right).$$

Используя значения 8_{16} и B_{16} из первой таблицы замены извлекается значение $\alpha_1(x) = D_{16}$, из второй – $\alpha_2(x) = 1_{16}$, из третьей – $\alpha_3(x) = C_{16}$, из четвертой – $\alpha_4(x) = F_{16}$.

В полиномиальной форме эти значения будут иметь вид:

$$D_{16} = x^3 + x^2 + 1,$$
$$1_{16} = 1,$$
$$C_{16} = x^3 + x^2,$$
$$F_{16} = x^3 + x^2 + x + 1.$$

Для проверки корректности значений $\alpha_1(x)$ и $\alpha_2(x)$ вычисляются значения $\alpha_{3_к}(x)$ и $\alpha_{4_к}(x)$ в соответствии с выражениями (10) и (11):

$$\alpha_{3_к}(x) = \alpha_1(x) + \alpha_2(x) = x^3 + x^2 + 1 + 1 = x^3 + x^2 = C_{16},$$
$$\alpha_{4_к}(x) = (x^3 + x^2 + 1 + (x \cdot 1) \bmod x^4 + x^3 + x^2 + x + 1 = x^3 + x^2 + x + 1 = D_{16}.$$

В соответствии с выражениями (12) и (13) вычисляются синдромы ошибок:

$$\delta_1 = C_{16} + C_{16} = 0,$$
$$\delta_2 = F_{16} + F_{16} = 0.$$

Равенство коэффициентов $\delta_1(x)$ и $\delta_2(x)$ указывает на равенства $\alpha_3(x) = \alpha_{3_к}(x)$ и $\alpha_4(x) = \alpha_{4_к}(x)$. Таким образом, проведенные вычисления подтвердили отсутствие сбоев в блоках замены, результатом работы которых является получение информационных остатков выходного значения InvSubBytes.

Допустим, в ходе работы блока замены, содержащего первые информационные остатки выходного значения InvSubBytes произошел сбой, и результатом его работы стало значение $\alpha_1 = F$, тогда:

$$\alpha_{3_к}(x) = x^3 + x^2 + x,$$
$$\alpha_{4_к}(x) = x^3 + x^2 + 1,$$
$$\delta_1(x) = \alpha_3(x) + \alpha_{3_к}(x) = (x^3 + x^2) + (x^3 + x^2 + x) = x,$$
$$\delta_2(x) = \alpha_4(x) + \alpha_{4_к}(x) = (x^3 + x^2 + x + 1) + (x^3 + x^2 + 1) = x.$$

С учетом информации о связи коэффициентов δ_1 и δ_2 с локализацией и глубиной ошибки (таблица 1) можно сделать вывод, что ошибка произошла в первом разряде первого информационного остатка. Факт сбоя в работе блока замены можно использовать как условие повторного выполнения алгоритма или как условие запуска механизмов коррекции.

Для устранения коррекции ошибки необходимо выполнить вычисления в соответствии с выражением (14). С учетом известной информации о местоположении ошибки:

$$\Delta S_{вых} = (x, 0).$$

Тогда выходное значение блока коррекции ошибок:

$$S_{вых_{корр.}} = S_{вых} + \Delta S_{вых} = (x^3 + x^2 + x + 1, 1) + (x, 0) = (x^3 + x^2 + 1, 1) = (D_{16}, 1_{16}).$$

Таким образом, ошибка, являющаяся последствием сбоя в работе преобразователя InvSubBytes, устранена.

4. Сравнительный анализ существующих корректирующих кодов в полиномиальной системе классов вычетов. В настоящий момент при построении отказоустойчивых систем в полиномиальной системе классов вычетов преимущественно

используются методы на основе вычисления позиционных характеристик, одной из которых является интервал числа [5].

Для реализации данного метода необходимо:

1) Для каждого основания p_i вычислить ортогональный базис B_i:

$$P_i = \frac{P_{полн}}{p_i}, \tag{23}$$

$$\delta_i = P_i \bmod p_i, \tag{24}$$

$$\delta_i m_i \equiv 1 \bmod p_i, \tag{25}$$

$$B_i = m_i P_i. \tag{26}$$

2) Для каждого основания p_i вычислить значение S_i:

$$S_i = \frac{B_i}{P_{раб}}. \tag{27}$$

3) Для каждого информационного основания вычислить значение B_i^*:

$$B_i^* = B_i \bmod P_{раб}. \tag{28}$$

4) Перевести обрабатываемое число из позиционной системы счисления в полиномиальную систему классов вычетов в соответствии с выражением (1).

5) Вычислить ранг безибыточной системы:

$$r^* = \left[\frac{\sum_{i=1}^{k} \alpha_i \cdot B_i^*}{P_{раб}} \right]. \tag{29}$$

6) Вычислить значение интервала, указывающего на местоположение ошибки:

$$G = \left[\sum_{i=1}^{n} \alpha_i \cdot S_i + r^* \right]_{P_{контр}} \tag{30}$$

7) На основе значения интервала G определить вектор ошибки $\Delta S_{вых}$, выполнить исправление возникшей ошибки в соответствии с выражением (22).

Для полиномиальной системы классов вычетов с информационными основаниями $p_1 = x^4 + x + 1,\ p_2 = x^4 + x^3 + 1$ и контрольными основаниями $p_3 = x^5 + x^2 + 1,\ p_4 = x^5 + x^3 + 1$:

$$P_{раб} = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1,$$

$$P_{контр} = x^{10} + x^8 + x^7 + x^5 + x^3 + x^2 + 1,$$

$$S_1 = x^{11} + x^9 + x^7 + x^5 + x^2,$$

$$S_2 = x^9 + x^7 + x^3 + x,$$

$$S_3 = x^5 + x^3 + 1,$$

$$S_4 = x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + 1,$$

$$B_1^* = x^7 + x^5 + x^3 + x^2,$$

$$B_2^* = x^7 + x^5 + x^3 + x^2 + 1.$$

Таким образом, для рассматриваемой системы выражение (30) будет иметь вид:

$$G = \left[\alpha_1 \cdot S_1 + \alpha_2 \cdot S_2 + \alpha_3 \cdot S_3 + \alpha_4 \cdot S_4 + r^*\right]_{P_{контр}} =$$

$$= \left[\begin{array}{c} \alpha_1 \cdot (x^{11} + x^9 + x^7 + x^5 + x^2) + \alpha_2 \cdot (x^9 + x^7 + x^3 + x) + \alpha_3 \cdot (x^5 + x^3 + 1) + \\ + \alpha_4 \cdot (x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + 1) + \dfrac{\alpha_1 \cdot (x^7 + x^5 + x^3 + x^2) + \alpha_2 \cdot (x^7 + x^5 + x^3 + x^2 + 1)}{P_{раб}} \end{array}\right]_{P_{контр}}.$$

По результатам сравнения предлагаемого алгоритма и известного можно сделать вывод, что вычислительная сложность последнего значительно выше за счет:

- большего количества операций (в известном алгоритме – 11, в предлагаемом – 5);
- большей разрядности обрабатываемых чисел.

Заключение. Предлагаемый вариант процедуры InvSubBytes позволяет обеспечить реализацию процедуры InvSubBytes, несмотря на возникший в процессе функционирования сбой, за счет применения корректирующих модулярных кодов.

Данную математическую модель целесообразно использовать при построении дешифратора американского стандарта шифрования, способного сохранять работоспособное состояние в условиях сбоев SPN-преобразователя.

Перспективным направлением исследования является разработка математических и структурных моделей:

- процедуры InvMixColumns;
- шифратора/дешифратора американского стандарта шифрования;
- системы передачи данных с реализацией криптографической защиты информации на основе американского стандарта шифрования.

ЛИТЕРАТУРА

1. Проворнов И. А. Исследование корректирующей способности модулярных кодов, применяемых в AES-системах // Проблемы разработки перспективных микро- и наноэлектронных систем (МЭС). 2022. № 4. С. 136–141.

2. Червяков Н. И., Сахнюк П. А., Шапошников А. В., Ряднов С. А. Модулярные параллельные вычислительные структуры нейропроцессорных систем. М.: ФИЗМАТЛИТ, 2003. 288 с.

3. Калмыков И. А., Гахов В. Р. и др. Применение корректирующих кодов полиномиальной системы классов вычетов для построения спецпроцессоров цифровой обработки сигналов / Труды международного Форума по проблемам науки, техники и образования. Том 1. / Под ред.: В. П. Савиных, В. В. Вишневского. М.: Академия наук, 2004. С. 133-135.

4. Устройство для обнаружения и исправления ошибок в системе остаточных классов: а. с. 714399 СССР: МКИ С С6 F 11/08 / Г. Г. Смолко, И. Я. Акушинский, В.М. Бурцев, Л.В. Каплан (СССР). – № 2439703/18–24; заявл. 26.01.77; опубл. 05.02.80, Бюл. № 5.

5. Калмыков И.А. Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов / Под ред. Н.И. Червякова. М.: ФИЗМАТЛИТ, 2005. 276 с.

REFERENCES

1. Promornov I.A. Investigation of the correcting ability of modular codes used in AES systems // Problems of development of promising micro- and nanoelectronic systems (MES). 2022. No. 4. P. 136-141.

2. Chervyakov N.I., Sakhnyuk P.A., Shaposhnikov A.V., Ryadnov S.A. Modular parallel computing structures of neuroprocessor systems. M.: FIZMATLIT, 2003. 288 p.

3. Kalmykov I.A., Gakhov V.R., etc. Application of correcting codes of the polynomial system of deduction classes for the construction of special processors of digital signal processing /

Proceedings of the International Forum on Science, Technology and Education. Volume 1./ Edited by: V.P. Savinykh, V.V. Vishnevsky. – M.: Academy of Sciences, 2004. P. 133-135.

4. Device for detecting and correcting errors in the system of residual classes: a. c. 714399 USSR: MKI C C6 F 11/08 / G. G. Smolko, I. Ya. Akushinsky, V. M. Burtsev, L.V. Kaplan (USSR). – No. 2439703/18–24; dec. 01/26/77; publ. 05.02.80, Bull. No. 5.

5. Kalmykov I.A., Mathematical models of neural network fault-tolerant computing tools operating in a polynomial system of deduction classes / Edited by N.I. Chervyakova. – M.: FIZMAT-LIT, 2005. – 276 p.

ОБ АВТОРАХ / ABOUT THE AUTHORS

Калмыков Игорь Анатольевич, профессор, доктор технических наук, профессор кафедры информационной безопасности автоматизированных систем Института цифрового развития ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, Российская Федерация, e-mail: kia762@yandex.ru.

Kalmykov Igor Anatolyevich, Professor, Doctor of Technical Sciences, Professor of the Department of Information Security of Automated Systems of the Institute of Digital Development of the North-Caucasus Federal University, Stavropol, Russian Federation, e-mail: kia762@yandex.ru.

Проворнов Игорь Александрович, аспирант Института цифрового развития ФГАОУ ВО «Северо-Кавказский федеральный университет, Ставрополь, Российская Федерация. e-mail: igorprovornov@yandex.ru

Provornov Igor Aleksandrovich, postgraduate student, Institute for Digital Development of North-Caucasian Federal University, Stavropol, Russian Federation, e-mail: igorprovornov@yandex.ru

Дата поступления в редакцию: 03.04.2023
После рецензирования:13.05.2023
Дата принятия к публикации:07.06.2023