УДК 004.052.2

РАЗРАБОТКА АЛГОРИТМА ОБНАРУЖЕНИЯ ОШИБОК В SPN-ШИФРСИСТЕМАХ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ИЗБЫТОЧНЫХ МОДУЛЯРНЫХ КОДОВ

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

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

Современные SPN-шифры широко применяются в самых различных областях. Это обусловлено тем, что такие шифры обладают лучшим сочетанием такими параметрами как: криптографическая стойкость, производительность, эффективность реализации и гибкость. Однако широкое применение SPN-криптосистем привело к увеличению числа атак на данные шифры. Среди таких атак особое место занимает атаки, использующие информацию, полученную по побочным каналам (side-channel-атакам), в частности на основе сбоев. Существующие методы противодействия атакам на основе сбоев не обладают достаточной эффективностью. Для обнаружения факта атаки на основе сбоев предлагается использовать избыточные коды, использующие алгебраическую систему конечных полей Галуа. К этим кодам относятся коды полиномиальной системы классов вычетов. Использование одного контрольного основания позволяет эффективно реализовать поиск и обнаружение ошибок, которые могут возникать из-за сбоев в работе SPN- криптосистем. Поэтому разработка алгоритма обнаружения ошибок в SPN-криптосистемахсистемах на основе избыточных полиномиальных кодов является актуальной задачей.

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

DEVELOPMENT OF ERROR DETECTION ALGORITHM IN SPN-CRIPTOSYSTEM BASED ON THE USE OF REDUNDANT MODULAR CODES

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

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

Modern SPN – ciphers are widely used in various fields. This is due to the fact that these ciphers have the best combination of parameters such as: strength, performance, effectiveness of implementation and flexibility. However, the wide use of SPN cryptographic system led to the increase in the number of attacks on these ciphers. Among such attacks, a special place is the attack using the information received in the side channels (side-channel attacks), in particular on the basis of failures. Existing methods for countering attacks based on failures are not sufficiently effective. For detection of attacks based on failures it is proposed to use redundant codes that use the algebraic system of finite Galois fields. These codes include codes of polynomial system classes deductions. Use one of the control base can effectively implement search and detection errors that can occur due to failures in the SPN cryptographic system. Therefore, the development of error detection algorithm in SPN – cryptographic system based on the excess of polynomial codes is an important task.

Keywords: cryptographic ciphers, SPN- cryptographic system, polynomial system classes deductions, detection error, positional characteristics

В настоящее время наблюдается повышенный интерес разработчиков к блочным симметричным шифрам, которые используют подстановочно-перестановочную сеть (Substitution-Permutation Network). Такие шифры относятся к SPN-шифрам. В отличие от *D*ES и ГОСТ 28147-89 эти шифры не используют сеть Фейстеля, а реализуют в одном раунде нелинейные и линейные преобразования, а также операцию наложения ключа. В результате этого в отличие от сети Фейстеля, при использовании SP-сети преобразуется весь входной блок, а не его половина. Однако в процессе работы шифратора SPN-шифров могут возникнуть сбои оборудования. Такие сбои могут быть результатом деструктивных воздействий как природного, так и антропогенного характера. Это приведет к искажению результата зашифрования.

Цель исследования

Повысить надежности работы SPN-шифрсистем можно за счет применения различных способов введения струтурной или временной избыточности. Однако известные способы противодействия последствиям сбоев в работе шифратора не учитывают особенности SPN-шифров, что приводит к значительным затратным схемным решениям. Решить данную проблему можно за счет использования избыточных

кодов, которые реализованы, как и SPN-шифры, в алгебраической системе, обладающей свойством кольца и поля. Поэтому целью работы является повышение надежности SPN-шифров за счет применения избыточных кодов полиномиальной системы классов вычетов (ПСКВ) с минимальной избыточностью, способных обнаруживать ошибки, вызванные сбоями.

Материалы и методы исследования

Основу кодов ПСКВ составляет непозиционная система счисления, в которой в качестве оснований модулярного кода используются неприводимые полиномы $p_i(z)$. Произведение оснований кода ПСКВ позволяет определить рабочий диапазон

$$P(z) = \prod_{i=1}^{k} p_i(z). \quad (1)$$

Тогда полином $A(z)$, удовлетворяющий условию $\deg A(z) < \deg P(z)$, можно представить в виде кортежа остатков

$$A(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_k(z)), \quad (2)$$

где $\alpha_i(z) \equiv A(z) \bmod p_i(z)$; $i = 1, 2, \ldots, n$.

Так как операции сложения, вычитания и умножения по модулю можно свести к соответствующим операциям над остатками [4, 5, 8], то для кода ПСКВ имеет место равенство

$$\left|A(z) \circ B(z)\right|^{+}_{p(z)} = \left(\left|\alpha_1(z) \circ b_1(z)\right|^{+}_{p_1(z)}, \left|\alpha_1(z) \circ b_1(z)\right|^{+}_{p_2(z)}, ..., \left|\alpha_k(z) \circ b_k(z)\right|^{+}_{p_k(z)}\right), \quad (3)$$

где $A(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_k(z))$;
$B(z) = (b_1(z), b_2(z), ..., b_k(z))$; $\circ$ – модульная операция.

Для выполнения процедур обнаружения ошибки в код ПСКВ вводят минимальную избыточность – одно контрольное основание, которое удовлетворяет

$$\deg p_{k+1} \geq \deg p_k \geq \deg p_{k-1} ... \geq \deg p_1. \quad (4)$$

В результате происходит расширение рабочего диапазона до полного диапазона

$$P^*(x) = \prod_{i=1}^{k+1} p_i(x) = P(x) p_{k+1}(x). \quad (5)$$

Тогда условием отсутствия ошибки в кодовой комбинации кода ПСКВ является выполнение неравенства

$$\deg A(x) < \deg P_{\text{раб}}(x). \quad (6)$$

В противном случае получаем, что в коде ПСКВ произошла ошибка.

Для выполнения процедуры обнаружения ошибки в коде ПСКВ используют позиционные характеристики (ПХ) [2, 3, 6, 7]. В работе [1] приведен алгоритм вычисления данной позиционной характеристики – след полинома. Для получения конечного результата предлагается из исходного кода ПСКВ $A(x) = (\alpha_1(x), ...\alpha_2(x), ..., \alpha_{k+1}(x), ..., \alpha_{k+1}(x))$ последовательно вычитать константы нулевизации до тех пор, пока не получится код

$$L_{\text{след}}(x) = (0, 0, ..., L_{k+1}(x)). \quad (7)$$

При этом подбираются специальные константы нулевизации, так чтобы при выполнении данного итерационного алгоритма не было бы ни один выхода за пределы рабочего диапазона системы Полученное значение (7) называется следом числа.

Проведенный анализ позволил выявить основной недостаток метода вычисления данной позиционный характеристики, который был приведен в работе [1]. Он связан с последовательным характером вычислительного процесса. Для устранения данной проблемы был разработан алгоритм параллельного вычисления позиционной характеристики – след полинома. Для этого предлагается заменить константы нулевизации $M_i(z)$ на псевдоортогональные полиномы $B_i^*(x)$. Тогда получаем

$$\alpha_{k+1}(x) = \sum_{j=1}^{k} \alpha_{k+1}^{j}(x) \bmod p_{k+1}(x). \quad (8)$$

В этом случае нормированный след полинома можно получить путем вычитания из кода ПСКВ полинома $A(x)$ псевдоортогональных форм, то есть

$$L_{k+1}(x) = \alpha_{k+1}(x) - \sum_{j=1}^{k} \alpha_{k+1}^{j}(x) \bmod p_{k+1}(x). \quad (9)$$

Если значение нормированного следа полинома равно нулю, то исходный код ПСКВ является разрешенным. В противном случае произошло обнаружение ошибки.

Результаты исследования и их обсуждение

Рассмотрим применение разработанного метода для повышения надежности AES-шифрсистем. Шифр AES реализуется в $GF(2^8)$ с использованием $p(x) = x^8 + x^4 + x^3 + x + 1$. Предлагается вместо него использовать код ПСКВ с двумя рабочими основания $p_1(x) = x^4 + x + 1$ и $p_2(x) = x^4 + x^3 + 1$. В качестве контрольного основания применяем $p_3(x) = x^4 + x^3 + x^2 + x + 1$.

Для получения псевдоортогональных базисов вычислим ортогональные базисы для рабочих оснований. Тогда первый ортогональный базис $B_1(x) = m_1(x) P_1^*(x) = x^7 + x^5 + x^3 + x^2$.

Значение второго ортогонального базиса $B_2(x) = m_2(x) P_2^*(x) = x^7 + x^5 + x^3 + x^2 + 1$. Произведем расширение ПСКВ, добавляя в набор оснований контрольное основание.

Таблица 1

Значение $\alpha_1(x)B_1^*(x)\bmod P_{раб}(x)$

Остаток	Произведение $\alpha_1(x)B_1^*(x)\bmod P_{раб}(x)$
$\alpha_1(x) = 1$	$(1, 0, x^3 + 1)$
$\alpha_1(x) = x$	$(x, 0, x^2 + 1)$
$\alpha_1(x) = x^2$	$(x^2, 0, x + 1)$
$\alpha_1(x) = x^3$	$(x^3, 0, x^2 + x)$

Таблица 2

Значение $\alpha_2(x)B_2^*(x)\bmod P_{раб}(x)$

Остаток	Произведение $\alpha_2(x)B_2^*(x)\bmod P_{раб}(x)$
$\alpha_2(x) = 1$	$(0, 1, x^3)$
$\alpha_2(x) = x$	$(0, x, x^2 + x)$
$\alpha_3(x) = x^2$	$(0, x^2, x^2 + 1)$
$\alpha_2(x) = x^3$	$(0, x^3, x^3 + x)$

Таблица 3

Таблица замен S_1-блока по модулю $p_1(x) = x^4 + x + 1$

$s_2(x)$	Остаток $s_1(x)$ по модулю $p_1(x) = x^4 + x + 1$															
	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
…																
F	1	5	3	3	6	B	C	7	1	A	E	C	9	9	A	F

Таблица 4

Таблица замен S_2-блока по модулю $p_2(x) = x^4 + x^3 + 1$

$s_2(x)$	Остаток $s_1(x)$ по модулю $p_2(x) = x^4 + x^3 + 1$															
	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
…																
F	7	F	8	3	5	C	B	8	6	4	5	4	E	B	C	B

Затем произведем вычисление остатков ортогональных базисов по модулю контрольного основания. Получаем для первого ортогонального базиса

$$\beta_3(x) = B_1(x)\bmod p_3(x) = x^7 + x^5 + x^3 + x^2 \bmod x^4 + x^3 + x^2 + x + 1 = x^3 + 1.$$

Для второго ортогонального базиса получаем

$$\beta_3(x) = B_2(x)\bmod p_3(x) = x^7 + x^5 + x^3 + x^2 + 1 \bmod x^4 + x^3 + x^2 + x + 1 = x^3.$$

Тогда получаем два псевдоортогональных базиса

$$B_1^*(x) = (\beta_1(x), \beta_2(x), \beta_3(x)) = (1, 0, x^3 + 1);$$

$$B_2^*(x) = (\beta_1(x), \beta_2(x), \beta_3(x)) = (0, 1, x^3).$$

Вычислим значения, которые получаются при умножении псевдоортогональных базисов на остатки. Для первого модуля ПСКВ результаты приведены в табл. 1.

Для второго модуля ПСКВ результаты приведены в табл. 2.

Рассмотрим пример применения кода ПСКВ, обнаруживающего однократные ошибки. Пусть на входы S-блока поступает байт текущего состояния. При этом старшие 4 разряда байта определяют номер строки таблицы, а младшие 4 разряда – задают номер столбца. Так при подаче состояния $\{00011001\} = \{19_{16}\}$ на выходе S-блока будет результат $\{d4_{16}\} = \{11010100_2\}$, который находится на пересечении 1 строки и 9 столбца.

Рассмотрим применение избыточного кода ПСКВ, способного обнаружить ошибки, при работе S-блока. Пусть на вход

S-блока поступил двоичный входной вектор $S(x) = \{00011001_2\} = \{19_{16}\}$. Данное значение подается на вход прямого преобразователя ПСС-ПСКВ, на выходе которого будут

$$s_1(x) = \{19_{16}\} \bmod x^4 + x + 1 = x^4 + x^3 + 1 \bmod x^4 + x + 1 = x^3 + x = 1010_2 = A;$$

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

На входы таблиц замены S_1-блока по модулю $p_1(x) = x^4 + x + 1$ и S_2-блока по модулю $p_2(x) = x^4 + x^3 + 1$ поступают остатки $S(x) = (A, 0)$. Результат замены определяется из табл. 3 и 4. В табл. 3 показана таблица S_1-блока по рабочему модулю $p_1(x) = x^4 + x + 1$.

В табл. 4 показана таблица замен S_2-блока по рабочему модулю $p_2(x) = x^4 + x^3 + 1$.

Для обнаружения последствий сбоев в шифре AES вводим таблицу S_3. Табл. 5 содержит строки таблицы замен S_3-блока по модулю $p_3(x) = x^4 + x^3 + x^2 + x + 1$.

В табл. 3 на пересечении столбца A и строки **0** находится число 0. В табл. 4 на пересечении столбца A и строки **0** находится число 5. В результате воздействия байта состояния $S(x) = \{00011001_2\} = \{19_{16}\} = (A, 0)$ был получен байт подстановки, который в ПСКВ равен $S'(x) = (0, 5)$. Это соответствует подстановке $S'(x) = \{d4_{16}\} = \{11010100_2\}$, так как

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

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

Определим остаток полученного значения подстановки $S'(x) = \{d4_{16}\} = \{11010100_2\}$ по контрольному модулю. Тогда получаем

$$s_3'(x) = \{d4_{16}\} \bmod x^4 + x^3 + x^2 + x + 1 = x^3 + x^2 + 1 = \{D_{16}\}.$$

При подаче на вход табл. 3 значений остатков текущего блока $S(x) = (A, 0)$ с выхода третьей таблицы подстановки будет снято значение, равное $\{D_{16}\} = \{1101_2\} = \{x^3 + x^2 + 1\}$. Данное число находится на пересечении столбца A и строки **0** в табл. 3.

Полученные значения остатков нового блока $S'(x) = (0, 5) = (0, x^2 + 1)$ поступают на первый вход блока обнаружения ошибки. Блок обнаружения ошибок реализует вычисление остатка по контрольному основанию, используя значение остатков $S'(x) = (0, 5)$.

При использовании разработанного метода получили остатки:

$$x^2 B_2^*(x) \bmod p_3(x) = x^2 + 1;$$

$$1 \cdot B_2^*(x) \bmod p_3(x) = x^3.$$

Тогда, просуммировав остатки по контрольному основанию, получаем

$$(x^2 + 1) B_2^*(x) \bmod p_3(x) = x^3 + (x^2 + 1) = x^3 + x^2 + 1.$$

Одновременно с этим на второй вход блока обнаружения ошибки поступает значение $s_3'(x) = x^3 + x^2 + 1 = \{D_{16}\}$, которое было получено с выхода табл. 5. В результате этого получается, что след полинома равен нулю. Это означает, что ошибки в коде ПСКВ нет.

Пусть ошибка из-за сбоя произошла по второму основанию ПСКВ $p_2(x) = x^4 + x^3 + 1$ и ее глубина $\Delta s_2(x) = 1$. Тогда

$$s_2^{\text{ош}}(x) = s_2'(x) + \Delta s_2(x) = (x^2 + 1) + 1 = x^2 = 0100_2.$$

Тогда на вход блока обнаружения ошибок, буде подан код из двух остатков ПСКВ

$$S'(x) = (s_1'(x), s_2^{\text{ош}}(x)) = (0000_2, 0100_2) = (0, x^2 + 1).$$

Проведем расчет остатка по контрольному основанию $s_3^*(x)$ с помощью псевдоортогональных базисов. В вычисление данного остатка принимает участие полином

$$x^2 B_2^*(x) \bmod p_3(x) = x^2 + 1.$$

Тогда, просуммировав остатки по контрольному основанию, получаем

$$x^2 B_2^*(x) \bmod p_3(x) = x^3.$$

Одновременно с этим на второй вход блока обнаружения ошибки поступает значение $s_3'(x) = x^3 + x^2 + 1 = \{D_{16}\}$, которое было получено с выхода табл. 5. Тогда нормированный след полинома будет равен

$$L_3(x) = \alpha_3(x) - \sum_{j=1}^{2} \alpha_3^j(x) \bmod p_3(x) = (x^3 + x^2 + 1) + x^3 = x^2 + 1.$$

Таблица 5

Остатки $a_3(x)$ по модулю $p_3(x) = x^4 + x^3 + x^2 + x + 1$

$s_2(x)$	Остаток $s_1(x)$ по модулю $p_1(x) = x^4 + x + 1$															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	A	E	0	7	0	B	2	C	B	D	C	8	9	1	F
1	E	0	E	3	C	F	5	7	6	F	9	8	2	6	4	F
…																
F	0	F	8	2	C	5	D	1	6	5	2	2	9	8	A	A

Полученный результат свидетельствует о том, что избыточный код ПСКВ содержит ошибку. Однако по величине данной позиционной характеристики определить местоположение ошибки нельзя.

Заключение

В работе проведена разработка и исследование новых принципов построения избыточных кодов полиномиальной системы классов вычетов, позволяющих обнаруживать ошибки на основе вычисления позиционной характеристики нормированный след. Показана возможность использования разработанного алгоритма вычисления данной ПХ для обнаружения ошибок, возникающих в процессе работы криптосистемы AES. Проведенные исследования показали, что применение разработанного алгоритма позволяет вычислить ПХ за одну итерацию по сравнению *k* итерациями вычисления следа числа, приведенных в работе [1], что значительно снижает временные затраты на обнаружение ошибки.

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

Список литературы

1. Акушский И.Я., Юдицкий Д.М. Машинная арифметика в остаточных классах. – М.: Сов. радио. 1968. – 440 с.

2. Барсагаев А.А., Калмыков М.И., Алгоритмы обнаружения и коррекции ошибок в модулярных полиномиальных кодах // Международный журнал экспериментального образования. РАЕ – 2014. – № 3. – С. 131–134.

3. Горденко Д.В., Калмыков И.А., Резеньков Д.Н., Саркисов А.Б. Методы и алгоритмы реконфигурации непозиционных вычислительных структур для обеспечения отказоустойчивости спецпроцессоров. – Ставрополь: Издательско-информационный центр «Фабула». – 2014. – 180 с.

4. Калмыков М.И., Гончаров П.С., Степанова Е.П. Непозиционный код класса вычетов в параллельных технологиях цифровой обработки сигналов // Успехи современного естествознания. РАЕ – 2014. – № 3. – С. 102–107.

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

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

7. Резеньков Д.Н. Определение местоположения и глубины ошибок при постепенной деградации структуры спецпроцессора полиномиальной системы классов вычетов // Актуальные проблемы и инновации в экономике, управлении, образовании, информационных технологиях – Ставрополь, 2009. – Т. 4, № 5. – С. 94–95.

8. 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. http://www.lifesciencesite.com.