Инженерный вестник Дона, №10 (2024)
ivdon.ru/ru/magazine/archive/n10y2024/9541

Математическая модель отказоустойчивого блока нелинейного преобразования для беспроводных систем OFDM со скачкообразной сменой частоты

И.А. Калмыков, В.С. Сляднев, Т.А. Пелешенко, Д.В. Духовный

Северо-Кавказский федеральный университет, Ставрополь

По мере развития низкоорбитальных систем спутникового интернета (НССИ) на первый план выходят вопросы обеспечения эффективной работы в условиях преднамеренных помех. Одно из решений связано с применением систем, использующих одновременно методы OFDM и генераторы, реализующие скачкообразную смену частоты (ССЧ). Очевидно, что чем сложнее алгоритм выбора рабочих частот, тем эффективнее работы ССЧ. В статье в качестве генератора выбора рабочих частот предлагается применять SPN-шифр «Кузнечик». В результате этого система ССЧ будет обладать высокой стойкостью к вычислению номеров рабочей частоты системами радиоэлектронной борьбы. Однако в процессе функционирования ССЧ могут возникнуть сбои и отказы. Чтобы предотвратить их последствия предлагается реализовать SPN-шифр с использованием полиномиальных модулярных кодов классов вычетов (ПМККВ). Одним из преобразований в «Кузнечике» является нелинейное преобразование, которое выполняет операцию подстановка. Очевидно, что создание новой математической модели выполнения нелинейного преобразования с использованием МККВ позволит обеспечить работу генератора ССЧ на основе SPN-шифра в условиях сбоев и отказов.

Ключевые слова: низкоорбитальные системы спутникового интернета, SPN-шифр «Кузнечик», нелинейные преобразования, модулярные коды классов вычетов, математическая модель, отказоустойчивость, скачкообразная смена частоты, полиномиальный модулярный код классов вычетов, модулярный код классов вычетов, метод OFDM.

Введение

Появившийся в последние годы интерес к применению технологии OFDM в беспроводных системах, к которым также относятся низкоорбитальные системы спутникового интернета (далее НССИ), обусловлен возможностью обеспечения высокой скорости передачи за счет параллельного использования нескольких поднесущих [1]. Однако данную технологию предлагают применять и для противодействия средствам радиоэлектронной борьбы (далее РЭБ). Известно, что в беспородных системах из-за использования режима скачкообразной смены частоты (далее ССЧ) наблюдается снижение скорости передачи данных. В этом случае сигналы OFDM позволяют компенсировать этот недостаток [2].

В настоящее время разработано множество решений, позволяющих обеспечить более высокоскоростной обмен данными в OFDM. Особое место среди них занимают параллельная цифровая обработка сигналов на основе дискретных вейвлет преобразований модулярных кодах классов вычетов (далее МККВ) [3-5]. Однако МККВ также способны повысить отказоустойчивость систем OFDM, поддерживающих режим скачкообразной смены частот. Применение режима ССЧ связано с тем, что одним из способов деструктивного воздействия на НССИ является постановка заградительных помех. Благодаря блокам ССЧ, которые генерируют псевдослучайную последовательность номер радиочастот, у противника возникают сложности с реализацией данного воздействия. Очевидно, чем более случайным является закон изменения частот, тем эффективнее работают системы OFDM в условиях сложной помеховой обстановки. Поэтому для реализации блоков ССЧ целесообразно использовать SPN-преобразования «Кузнечик».

Для обеспечения высокой достоверности доведения информации системы OFDM НССИ должны обладать свойством устойчивости к отказам. В данной статье рассмотрены вопросы обеспечения отказоустойчивости блока ССЧ с помощью корректирующих МККВ. Так как в основе блока ССЧ лежит отечественное SPN-преобразование Кузнечик, то нелинейное S-преобразование является одним из наиболее аппаратно-затратных. Поэтому очевидно, что создание новой математической модели выполнения нелинейного преобразования с использованием МККВ позволит обеспечить работу генератора ССЧ на основе SPN-шифра в условиях сбоев и отказов. Цель статьи – обеспечение устойчивости к отказам блока ССЧ на основе использования корректирующих модулярных кодов и разработанной математической модели отказоустойчивого блока нелинейного преобразования SPN-сети Кузнечик.

Материал и методы исследования

1. Основные преобразования в SPN-сети «Кузнечик»

В основу отечественного стандарта шифрования SPN-типа Кузнечик положены преобразования в конечном поле Галуа GF (2^8). В качестве полинома, порождающего 8-разрядные элементы поля GF (2^8), выбран $p(x) = x^8 + x^7 + x^6 + x + 1$. Данный шифр в качестве блока открытого текста использует двоичный код длиной 128 бит. Размер блока зашифрованного текста совпадает с размером отрытого текста и составляет 128 бит. Процесс преобразования открытого текста в закрытый включает [6,7]:

- девять полноценных раундов шифрования;

- десятый сокращенный раунд, который содержит только операцию суммирования с десятым 128-битным раундовым ключом.

Каждый раунд включает в себя следующие криптографические функции:

- операцию суммирования по модулю входного 128-битового вектора и 128-битовогораундового ключа (обозначается X);

- операцию нелинейного преобразования 128-битового двоичного вектора (обозначается S);

- операцию линейного преобразования 128-битового двоичного вектора (обозначается L).

Рассмотрим более подробно нелинейное преобразование, которое реализуется в SPN-сети Кузнечик. Данное преобразование реализуется с помощью блока подстановки S. Использование операции подстановки направлено на нарушение статистических зависимостей открытого и закрытого текстов. Данный результат можно добиться, если операция замены будет обладать набор следующих свойств [8,9]. Во-первых, S-преобразование должно обеспечивать лавинный эффект, при котором изменение одного бит входного вектора должно привести к изменению сразу нескольких бит в

выходном векторе. Во-вторых, S-преобразование должно обеспечивать эффективное противодействие атакам на основе линейного криптоанализа. В этом случае даже наличие большого числа пар открытых и закрытых блоков текстов не должно нарушителю выявить секретный ключ. В-третьих, при разработке S-преобразования были учтены и атаки, в основу которых положен дифференциальный криптоанализ. Особенностью данных атак является то, что они реализуются при наличии у нарушителя возможности зашифрования, подобранные ими тексты. Для реализации данной атаки злоумышленник сначала вычисляет дифференциал, используя суммирование по модулю два:

$$\Delta\tilde{p} = \tilde{p}_1 + \tilde{p}_2, \qquad (1)$$

где $\tilde{p}_1$, $\tilde{p}_2$ – два блока открытого текста, известные злоумышленнику.

Затем он их зашифровывает и вычисляет дифференциал шифротекстов:

$$\Delta\tilde{c} = \tilde{c}_1 + \tilde{c}_2 . \qquad (2)$$

После этого он находит частоту возвращения различных $\Delta\tilde{c}$ при заданном дифференциале открытых тестов (1). Это позволяет злоумышленнику получить дополнительную информацию о секретном ключе.

В-четвертых, S-преобразование должно обеспечивать эффективное противодействие алгебраическим атакам, которые учитывают алгебраические свойства шифра.

Отмеченные свойства были учтены при разработке S-преобразователя для SPN-сети Кузнечик. Структура S-преобразователя показана на рисунке 1. Согласно [6] на вход S-преобразователя поступает 128-битовый вектор, который представляет собой 16 байтов $(a(0), a(1), \ldots, a(15))$. Данный преобразователь осуществляет замену входного байта $a(j)$ на соответствующий выходной байт $a^*(j)$, где $j = 0, 1, \ldots, 15$.

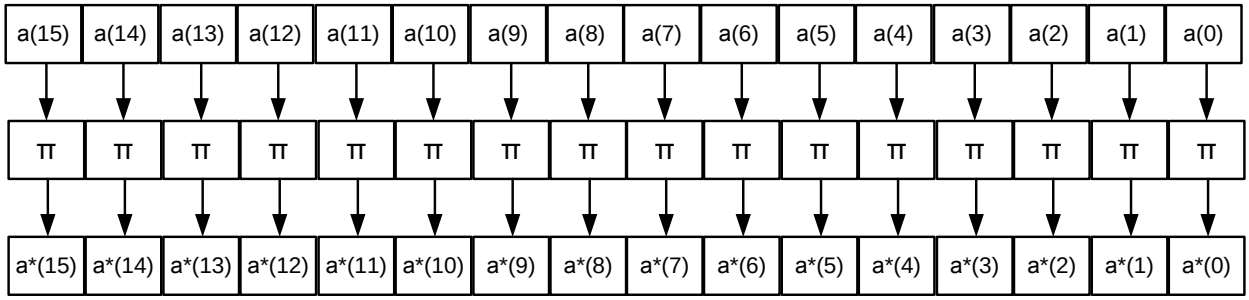

Рис. 1. – Структура S-преобразователя

Правило замены в S-преобразователе определяется

$$S(a)=\pi(a)=\pi(a(15))||...||\pi(a(0))=(a^*(15)||...||a^*(0)), \quad (3)$$

где $a=(a(15)||...||a(0))$ – входной вектор; $a^*=(a^*(15)||...||a^*(0))$ – выходной вектор; $\pi(a)=\pi(a(15))||...||\pi(a(0))$ – процедура замены байтов.

Очевидно, что при возникновении сбоев или отказов в работе S-преобразователя благодаря лавинному эффекту на выходе на выходе шифратора будут искажены многие биты. В результате этого блоки ССЧ на передающей и приемной сторонах будут выдавать разные номера частот для перестроения. А это в свою очередь приведет к нарушению функционирования системы OFDM НССИ. Устранить данную ситуацию можно за счет применения корректирующих полиномиальных модулярных кодов классов вычетов (далее ПМККВ).

2. Корректирующие полиномиальные модулярные коды классов вычетов

Полиномиальные модулярные коды классов вычетов являются арифметическими кодами в кольце неприводимых полиномов [10-12] Для получения кодовой комбинации в полиномиальных модулярных кодах необходимо выбрать неприводимые многочлены $p_1(x), p_2(x), ..., p_k(x)$. При этом должно выполняться условие

$$\deg p_1(x) \le ... \le \deg p_{k-1}(x) \le \deg p_k(x), \quad (4)$$

где $\deg p_i(x)$ – степень i-го основания ПМК; $i=1,...,k$.

Затем целое число C необходимо перевести в двоичный код, а затем этот код представить в виде полинома. Тогда ПМК представляет собой набор остатков при делении $C(x)$ на $p_1(x), p_2(x), \ldots, p_k(x)$, которые являются основаниями кода:

$$C(x) = (C_1(x), C_2(x), \ldots, C_k(x)), \quad (5)$$

где $C_i(x) \equiv C(x) \bmod p_i(x)$; $i = 1, \ldots, k$.

Выбранные многочлены задают рабочий диапазон ПМК:

$$P_k(x) = \prod_{i=1}^{k} p_i(x). \quad (6)$$

В полиноминальных модулярных кодах можно выполнять параллельно следующие модульные операции:

$$\left|C(x) \circ Z(x)\right|^{+}_{p(z)} = \left(\left|C_1(x) \circ Z_1(x)\right|^{+}_{p_1(x)}, \ldots, \left|C_k(x) \circ Z_k(x)\right|^{+}_{p_k(x)}\right), \quad (7)$$

где $Z_i(x) \equiv Z(x) \bmod p_i(x)$; $i = 1, \ldots, k$; $\circ$ – операции сложения и умножения по модулю.

Коды ПМККВ способны параллельно выполнять модульные операции по основаниям, используя при этом остатки в качестве операндов. Это позволяет повысить производительность специализированных вычислительных систем [13,14]. Так как в процессе выполнения модульных операций промежуточные результаты не переходят от одного основания к другому, то ПМККВ способны обнаруживать и корректировать ошибки вычислений. Для этого необходимо в ПМККВ ввести избыточность, то есть добавить дополнительные контрольные основания.

Анализ работ [11, 13, 14] показывает, что для выполнения операций обнаружения и коррекции искаженных остатков в ПМККВ необходимо ввести избыточность в виде контрольных оснований. Если в процессе вычислений будет искажен только один остаток, то в ПМККВ достаточно добавить два контрольных основания $p_{k+1}(x), p_{k+2}(x)$. Выбор этих оснований

осуществляет согласно условию:

$$\deg p_1(x) \le \ldots \le \deg p_k(x) \le \deg p_{k+1}(x) \le \deg p_{k+2}(x). \quad (8)$$

В результате этого, во-первых, будет увеличена на два остатка кодовая комбинация:

$$C(x) = (C_1(x), \ldots, C_k(x), C_{k+1}(x), C_{k+2}(x)), \quad (9)$$

Во-вторых, это приведет к увеличению диапазона возможных комбинаций избыточного ПМККВ:

$$P_{k+2}(x) = \prod_{i=1}^{k+2} p_i(x). \quad (10)$$

Количество разрешенных кодовых комбинаций ПМККВ определяется k информационными основаниями. То есть:

$$\deg C(x) < \deg P_k(x). \quad (11)$$

Известно, что все модульные коды относятся к непозиционным кодам, в которых достаточно сложно выполняются операции сравнения. В результате этого были разработаны алгоритмы, которые без обратного преобразования из ПМККВ в позиционный код позволяют проверить условие (11). Так в работе [11] предлагается провести коррекцию ошибок с использованием интервального полинома:

$$L(x) = \left[\frac{C(x)}{P_k(x)}\right] = \left|\sum_{i=1}^{k+r} C_i(x) R_i(x) + K^*(x)\right|^+_{P_r(x)}, \quad (12)$$

где $B_1(x) = R_i(x) P_k(x) + B_i^*(x)$ – ортогональные базисы ПМККВ; $P_r(x) = \prod_{i=k+1}^{k+r} p_i(x)$; $K^*(x)$ – ранг полинома.

Ранг вычисляется согласно:

$$K^*(x) = \left[\sum_{j=1}^{k} C_j(x) B_j^*(x) \Big/ P_k(x)\right] \quad (13)$$

Если $L(x)=0$, то комбинация ПМККВ считается разрешенной. В работе [13] для коррекции ошибок было предложено использовать смешанную систему, для которой имеет место следующее равенство

$$C(x)=a_1(x)+\ldots+a_k(x)\prod_{i=1}^{k-1}p_i(x)+a_{k+1}(x)P_k(x)+a_{k+2}(x)P_k(x)p_{k+1}(x). \qquad (14)$$

При этом коэффициенты смешанной системы определяются:

$$a_i(x)=\left|\sum_{j=1}^{i}C_j(x)b_i^j(x)\right|_{p_i(x)}^{+}\Bigg|_{p_i(x)}^{+}, \qquad (15)$$

где $b_i^j(x)$ – коэффициенты смешанной системы, для которых имеет место $B_j(x)=\left(0,\ldots,0,b_i^j(x),b_{i+1}^j(x),\ldots,b_{i+2}^j(x)\right);\ i=1,\ldots,k+2$.

Если $a_{k+1}(x)=a_{k+2}(x)=0$, то комбинация ПМККВ считается разрешенной.

В работе [14] предлагается использовать синдром ошибки:

$$\begin{cases}\delta_{k+1}(x)=\left|C_{k+1}(x)-C_{k+1}^{'}(x)\right|_{p_{k+1}(x)}^{+}\\ \delta_{k+2}(x)=\left|C_{k+2}(x)-C_{k+2}^{'}(x)\right|_{p_{k+2}(x)}^{+},\end{cases} \qquad (16)$$

где $C_j^{'}(x)=f(C_1(x),\ldots,C_k(k));\ j=k+1,k+2$; f – алгоритм вычисления контрольных остатков ПМККВ.

Однако данные методы нельзя использовать для повышения отказоустойчивости блоков ССЧ. Это связано с тем, что при реализации SPN-сети Кузнечик в ПМККВ в качестве контрольного основания можно взять только один неприводимый полином, а в рассмотренных примерах – необходимо минимум два. В работе [15] показана возможность использования ПМККВ с одним контрольным основанием для повышения надежности SPN-шифратора. Однако предложенный в данной статье метод позволяет только обнаруживать ошибочные остатки, а не корректировать их. Поэтому для разработки математической модели отказоустойчивого блока

нелинейного преобразования SPN-сети Кузнечик воспользуемся алгоритмом вычисления невязки [16]:

$$\begin{cases} \delta_1(x) = C_3(x) + C_3'''(x), \\ \delta_2(x) = C_4(x) + C_4'''(x), \end{cases} \quad (17)$$

где $C_3(x), C_4(x)$ – контрольные остатки ПМККВ.

При этом вторые слагаемые $C_3'''(x), C_4'''(x)$ выражения (17) вычисляются:

$$C_3''' = C_1(x) + C_2(x). \quad (18)$$

$$C_4''' = \left(C_1(x) + xC_2(x)\right) \bmod p_3(x). \quad (19)$$

3. Математическая модель отказоустойчивого S-преобразователя, реализованного в полиномиальном модулярном коде

Математическая модель отказоустойчивого S-преобразователя, реализованного в ПМККВ, состоит из:

1. Преобразования из позиционного кода в ПМККВ

$$a(15) \| a(14) \| \ldots \| a(0) = \begin{cases} a_1(15) \| a_1(14) \| \ldots \| a_1(0), \\ a_2(15) \| a_2(14) \| \ldots \| a_2(0), \end{cases} \quad (20)$$

где $a_i(j) \equiv a(j) \bmod p_i(x)$; $i = 1, 2$; $j = 0, 1, \ldots, 15$.

2. S-преобразования в ПМККВ:

$$\pi(a_1(j) \| a_2(j)) = (a_1^*(j) \| a_2^*(j) \| a_3^*(j) \| a_4^*(j)), \quad (21)$$

где $a_1^*(j), a_2^*(j)$ – информационные остатки комбинации ИПМККВ; $a_3^*(j), a_4^*(j)$ – вычисленные ранее избыточные остатки комбинации ИПМККВ; $j = 0, 1, \ldots, 15$.

3. Вычисления избыточных остатков:

$$\begin{aligned} a_3'''(j) &= a_1^*(j) + a_2^*(j), \\ a_4'''(j) &= \left| a_1^*(j) + x \cdot a_2^*(j) \right|_{p_3(x)}. \end{aligned} \quad (22)$$

4. Коррекции ошибки:

$$\begin{aligned}\delta_3(x) &= a_3^*(j) + a_3'''(j),\\ \delta_4(x) &= a_4^*(j) + a_4'''(j).\end{aligned} \qquad (23)$$

Если $\delta_3(x) = \delta_4(x) = 0$, то при выполнении S-преобразования ошибки не было. Если $\delta_3(x) = \delta_4(x) \neq 0$, то коррекция первого остатка комбинации:

$$a_1(j) = \tilde{a}_1(j) + \delta_3(x). \qquad (24)$$

Если невязка не является нулевой и при этом выполняется условие $\delta_3(x) \neq \delta_4(x)$, то исправлению подвергается второй остаток:

$$a_2(j) = \tilde{a}_2(j) + \delta_3(x). \qquad (25)$$

Результаты исследования и их обсуждение

Для избыточного ПМККВ кода берем $p_1(x) = x^4 + x + 1$, $p_2(x) = x^4 + x^3 + 1$. Это информационные основания. Контрольное – $p_3(x) = x^4 + x^3 + x^2 + x + 1$.

Пусть входной байт a(0) = 81_{10} = 0101 0001_2. Данный байт подается на вход S-преобразователя. С выхода снимается $a^*(0) = \pi(a(0)) = 112_{10} = 10011101_2$.

Воспользуемся разработанной математической моделью S-преобразователя.

1. Выполним преобразование из позиционного кода в ПМККВ:

$$a(0) = x^6 + x^4 + 1 = (x^3 + x^2 + x \,||\, x^2 + x + 1).$$

2. Для выполнения S-преобразования в ПМККВ остатки $a_1(0), a_2(0)$ передаются на входы четырех таблиц. В первой и второй таблицах происходит их замена на информационные остатки комбинации ИПМККВ $a_1^*(0), a_2^*(0)$. В третьей и четвертой таблицах происходит выбор соответствующих контрольных $a_3^*(0), a_4^*(0)$. Получаем:

$$\pi(a(0)) = a^*(0) = x^6 + x^5 + x^4 = (x^3 + 1 || x^3 + x^2 + 1).$$

В таблицах 3 и 4 хранятся избыточные остатки:

$$a_3^*(0) = a_1^*(0) + a_2^*(0) = x^2,\ a_4^*(0) = \left|a_1^*(0) + x \cdot a_2^*(0)\right|_{p_3(x)} = x^3 + x^2.$$

3. Выполним вычисление избыточных остатков, используя (22):

$$a_3'''(0) = (x^3 + 1) + (x^3 + x^2 + 1) = x^2,$$
$$a_4'''(0) = \left|(x^3 + 1) + x \cdot (x^3 + x^2 + 1)\right|_{x^4+x^3+x^2+x+1} = x^3 + x^2.$$

4. Произведем проверку полученного результата, используя (23):

$$\delta_3(x) = a_3^*(0) + a_3'''(0) = x^2 + x^2 = 0,$$
$$\delta_4(x) = a_4^*(0) + a_4'''(0) = (x^3 + x^2) + (x^3 + x^2) = 0.$$

Так как $\delta_3(x) = \delta_4(x) = 0$, то при выполнении S-преобразования ошибки не было. После этого комбинация $a^*(0) = (x^3 + 1 || x^3 + x^2 + 1)$ поступает на блок, выполняющий линейное преобразование.

Пусть при выполнении S-преобразования на выходе первой таблицы получится ошибочный остаток $\tilde{a}_1^*(0) = x^3 + x + 1$. Тогда ошибочная комбинация имеет вид $\tilde{a}^*(0) = (x^3 + x + 1 || x^3 + x^2 + 1 || x^2 || x^3 + x^2)$. Используя (22) вычислим избыточные остатки:

$$a_3'''(0) = (x^3 + x + 1) + (x^3 + x^2 + 1) = x^2 + x,$$
$$a_4'''(0) = \left|(x^3 + x + 1) + x \cdot (x^3 + x^2 + 1)\right|_{x^4+x^3+x^2+x+1} = x^3 + x^2 + x.$$

Произведем проверку полученного результата, используя (23):

$$\delta_3(x) = a_3^*(0) + a_3'''(0) = x^2 + (x^2 + x) = x,$$
$$\delta_4(x) = a_4^*(0) + a_4'''(0) = (x^3 + x^2) + (x^3 + x^2 + x) = x.$$

Так как $\delta_3(x) = \delta_4(x) = x$, то выполняется коррекция первого остатка комбинации согласно (24):

$$a_1(0) = \tilde{a}_1(0) + \delta_3(x) = (x^3 + x + 1) + x = x^3 + 1.$$

Ошибка, возникшая при выполнении S-преобразования, исправлена.

Пусть при выполнении S-преобразования на выходе второй таблицы получится ошибочный остаток $\tilde{a}_2^*(0) = x^3 + x^2 + x + 1$. Тогда ошибочная комбинация имеет вид $\tilde{a}^*(0) = (x^3 + 1 \| x^3 + x^2 + x + 1 \| x^2 \| x^3 + x^2)$. Используя (22) вычислим избыточные остатки:

$$a_3'''(0) = (x^3 + 1) + (x^3 + x^2 + x + 1) = x^2 + x,$$

$$a_4'''(0) = \left|(x^3 + 1) + x \cdot (x^3 + x^2 + x + 1)\right|_{x^4+x^3+x^2+x+1} = x^3.$$

Произведем проверку полученного результата, используя (23):

$$\delta_3(x) = a_3^*(0) + a_3'''(0) = x^2 + (x^2 + x) = x,$$

$$\delta_4(x) = a_4^*(0) + a_4'''(0) = (x^3 + x^2) + x^3 = x^2.$$

Если $\delta_3(x) = x, \delta_4(x) = x^2$, то выполняется коррекция второго остатка комбинации согласно (25):

$$a_2(j) = \tilde{a}_2(j) + \delta_3(x) = (x^3 + x^2 + x + 1) + x = x^3 + x^2 + 1.$$

Ошибка, возникшая при выполнении S-преобразования, исправлена.

Полученные результаты свидетельствуют о том, что разработанная математическая модель с использованием [16] позволяет корректировать однократные ошибки, которые возникают при выполнении нелинейного преобразования в SPN-шифре, в то время как метод [15] способен только обнаруживать факт ошибки. Таким образом, поставленная цель достигнута.

Заключение

Для борьбы с преднамеренными помехами, поставленными средствами РЭБ, в системах НССИ используют режим ССЧ совместно с технологией OFDM. Чтобы обеспечить более высокую скорость передачи данных в системах OFDM, предлагается применять модулярные коды при выполнении ортогонального преобразования сигналов. Однако модулярные коды не

только обеспечивают высокую скорость вычислений, но могут быть использованы в качестве средства, позволяющего повысить отказоустойчивость вычислительного устройства. В статье показана реализация нелинейного преобразования SPN-шифра Кузнечик в ПМККВ. На основе проведенного анализа был выбран метод обнаружения и коррекции ошибок на основе невязки, в котором для коррекции искаженного остатка предлагается использовать одно контрольное основание. С использованием данного метода была разработана математическая модель отказоустойчивого блока нелинейного преобразования SPN-шифра Кузнечик. Приведен пример использования данной математической модели. Полученные результаты показали, что с помощью разработанной математической модели можно обнаруживать и исправлять однократные ошибки при выполнении нелинейного преобразования в SPN-шифре, в то время как в работе [15] ПМККВ с одним контрольным основанием только обнаруживает ошибки.

Исследование выполнено за счет гранта Российского научного фонда № 23-21-00036, https://rscf.ru/project/23-21-00036/».

Литература

1. Shreehari H.S., Makam Supreeth Starlink Satellite Internet Service. International Journal of Research Publication and Reviews, 2022, vol 3, no 6, pp. 4501-4504.

2. Макаренко С.И., Иванов М.С. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. СПб.: Свое издательство, 2013. 166 с.

3. Kalmykov, I.A., Dukhovnyj, D.V., Kalmykova, N.I. Development of a Mathematical Model for Performing the Haar Wavelet Transform in Parallel

Modular Codes // International Russian Automation Conference. Moscow, 2023. - pp. 466-470.

4. Калмыков И.А., Чистоусов Н.К., Калмыкова Н.И., Духовный Д.В. Ортогональная обработка сигналов с использованием математических моделей целочисленных вейвлет-преобразований, реализованных в модулярных кодах классов вычетов // Инженерный вестник Дона, 2023, №1 URL: ivdon.ru/ru/magazine/archive/n3y2023/8273.

5. Калмыков И.А., Чистоусов Н.К., Духовный Д.В. Разработка структурных моделей системы OFDM, использующих преобразования Добеши в GF(m) и кодах классов вычетов // Современные наукоемкие технологии. Междисциплинарный журнал. 2023. № 8. С. 84-90.

6. Лось, А. Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации для изучающих компьютерную безопасность. Учебник для вузов. Москва: Юрайт, 2024. 473 с.

7. Schneier, B. Applied Cryptography: Protocols, Algorithms and Source Code in C. New York: Wiley, 2017, 784 p.

8. Вульф А. Криптография. Основы практического шифрования и криптографии. Москва: Ridero, 2023. 216 с.

9. Бабаш А.В., Баранова Е.К. Криптографические методы защиты информации. Москва.: КНОРУС, 2016. 192 с.

10. Mohan A. Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland, 2016, 351 p.

11. Pashintsev V.P., Tyncherov K T, Olenev A.A. Error-Correction Coding Using Polynomial Residue Number System. // Applied Sciences, 2022. URL: //doi.org/10.3390/app12073365.

12. Samoilenko D.V, Finko O.A. Noise-resistant data transmission in radio channels of robotic systems based on polynomial classes of residues. // High technology in space exploration of the Earth, 2016; pp. 49-55.

13. Omondi A, Premkumar B. Residue Number Systems: Theory and Implementation // Imperial College Press, 2007. 254 p.

14. Емарлукова Я.В., Гиш Т.А., Дунин А.В., Макарова А.В., Гостев Д.В. Математические модели и схемные решения отказоустойчивых непозиционных вычислительных систем: коллективная монография. Ставрополь: СКФУ, 2016. 216 с.

15. Chu, J., Benaissa, M. Error Detecting AES Using Polynomial Residue Number System // Microprocessors and Microsystems, 2013. 37, C. 228-234.

16. Калмыков И.А., Сляднев В.С., Калмыков М.И., Пелешенко Т.А., Проворнов И.А. Алгоритм коррекции ошибок в модулярном коде классов вычетов, обеспечивающий повышение отказоустойчивости систем OFDM // - Ставрополь: Инженерный вестник Дона, 2024, №2 URL: ivdon.ru/ru/magazine/archive/n2y2024/9038.

References

1. Shreehari H.S. International Journal of Research Publication and Reviews, 2022, vol 3, № 6, pp. 4501-4504.

2. Makarenko S.I., Ivanov M.S. Pomehozashhishhennost' sistem svjazi s psevdosluchajnoj perestrojkoj rabochej chastoty [Noise immunity of communication systems with pseudorandom adjustment of the operating frequency]. Monographia. St. Peterburg: Svoe izdatelstvo, 2013. 166 p.

3. Kalmykov, I.A., Dukhovnyj, D.V., Kalmykova, N.I. Mezhdunarodnaja rossijskaja konferencija po avtomatizacii (International Russian Automation Conference). Moskva, 2023. - pp. 466-470.

4. Kalmykov I.A., Chistousov N.K., Kalmykova N.I., Dukhovny D.V. Inzhenernyj vestnik Dona, 2023, №1. URL: ivdon.ru/ru/magazine/archive/n3y2023/8273.

5. Kalmykov I.A., Chistousov N.K., Dukhovny D.V. Sovremennye naukoemkie tehnologii. Mezhdisciplinarnyj zhurnal. 2023. No. 8. pp. 84-90.

6. Los, A. B., Nesterenko A.Yu., Rozhkov M.I. Kriptograficheskie metody zashhity informacii dlja studentov, izuchajushhih komp'juternuju bezopasnost'. Uchebnoe posobie dlja vuzov. [Cryptographic methods of information protection for students of computer security. Textbook for universities]. Moskva: Yurait, 2024. 473 p.

7. Schneier, B. Applied Cryptography: Protocols, Algorithms and Source Code in C. New York: Wiley, 2017, 784 p.

8. Wolf A. Kriptografija. Osnovy prakticheskogo shifrovanija i kriptograficheskoj tehniki [Cryptography. Fundamentals of practical encryption and cryptograph]. Moskva: Ridero, 2023. 216 p.

9. Babash A.V., Baranova E.K. Kriptograficheskie metody zashhity informacii [Cryptographic methods of information protection]. Moskva: KNORUS, 2016. 192 p.

10. Mohan A. Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland, 2016, 351 p.

11. Pashintsev V.R., Tyncherov K T, Olenev A.A Prikladnye nauki, Mezhdistsiplinarnyy zhurnal. 2022. URL: doi.org/10.3390/app12073365

12. Samoilenko D.V., Finko O.A. High technology in space exploration of the Earth, 2016; pp. 49-55.

13.Omondi A, Premkumar B. Imperial College Press, 2007. 254 p.

14. Emarlukova Ya.V., Gish T.A., Dunin A.V., Makarova A.V., Gostev D.V. Matematicheskie modeli i shemnye reshenija otkazoustojchivyh nepozicionnyh vychislitel'nyh sistem: kollektivnaja monografija [Mathematical models and circuit solutions of fault-tolerant non-positional computing systems: a collective monograph]. Stavropol: NCFU, 2016. 216 p.

15. Chu, J., Benaissa, M. Microprocessors and Microsystems, 2013. 37, pp. 228-234.

16. Kalmykov I.A., Slyadnev V.S., Kalmykov M.I., Peleshenko T.A., Skornov I.A. Inzhenernyj vestnik Dona, 2024, №2. URL: ivdon.ru/ru/magazine/archive/n2y2024/9038.

Дата поступления: 30.08.2024

Дата публикации: 12.10.2024