ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

УДК 681.5.011

РАЗРАБОТКА СТРУКТУРНОЙ МОДЕЛИ ОТКАЗОУСТОЙЧИВОГО ПРЕОБРАЗОВАТЕЛЯ SUBBYTES В ПОЛИНОМИАЛЬНОЙ СИСТЕМЕ КЛАССОВ ВЫЧЕТОВ

И.А. ПРОВОРНОВ, асп., И.А. КАЛМЫКОВ, д-р техн. наук,
Т.А. ГИШ, канд. техн. наук

Северо-Кавказский федеральный университет
355017, Ставрополь, ул. Пушкина, 1, e-mail: igorprovornov@yandex.ru

Статья посвящена вопросу повышения надежности реализации процедуры SubBytes криптоалгоритма AES. Обоснована актуальность развития новых методов корректирующего кодирования. Рассмотрены теоретические основы алгоритма корректирующего кодирования в полиномиальной системе классов вычетов с одним контрольным основанием и декомпозиция задачи его аппаратной реализации, первым этапом которой является разработка структурной модели устройства, отличной от классической реализации процедуры SubBytes. На основе требований к разрабатываемой структурной модели определены ее основные логические элементы (блок преобразования чисел из позиционной системы счисления в полиномиальную систему классов вычетов, блоки замены, блок обнаружения ошибок, блок коррекции ошибок), порядок их взаимодействия, количество и формат входных и выходных значений. На примерах изучен принцип работы предлагаемого устройства.

Ключевые слова: SPN-системы, AES, SubBytes, надежность, корректирующее кодирование, полиномиальная система классов вычетов, модулярная арифметика.

DOI: 10.46573/2658-5030-2023-4-62-69

ВВЕДЕНИЕ

Важным свойством системы обработки и передачи информации является защищенность, т.е. ее способность противостоять несанкционированному доступу. Один из способов обеспечения защищенности информации – применение алгоритмов шифрования, которые предназначены для преобразования исходных данных с помощью ключевой информации в данные, доступ к которым без этой информации получить невозможно. Вместе с тем к таким системам предъявляются повышенные требования надежности, так как из теории криптографии [1] известно, что сбои в работе шифратора могут привести к снижению качества стойкости шифрования. Существует целый класс криптоатак, основанных на извлечении информации из данных, генерируемых шифратором, который подвержен сбоям вследствие различных факторов, вызванных, как правило, внешними воздействиями

(повышением/понижением температуры окружающей среды, изменением напряжения питания, электромагнитным излучением и т.п.). Таким образом, в современных условиях актуальна задача повышения надежности устройств, реализующих функции шифрования.

В настоящее время криптоалгоритм AES – одна из самых распространенных технологий шифрования, являющаяся реализацией подстановочно-перестановочной сети (SPN). Основные элементы AES-шифрования – процедуры AddRoundKey, SubBytes, MixColumns и ShiftRows. Таким образом, в соответствии с принципами системного анализа сложных технических систем [2] задачу повышения надежности AES-шифратора можно представить в виде совокупности задач обеспечения надежности отдельных компонентных процедур. В настоящей статье будет рассмотрена проблема повышения надежности процедуры SubBytes криптоалгоритма AES. Целью исследования является разработка структурной модели отказоустойчивого преобразователя SubBytes, способного сохранять работоспособность в условиях сбоев и отказов его элементов.

МАТЕРИАЛЫ И МЕТОДЫ

Выделяют следующие методы повышения надежности систем цифровой обработки сигналов [3]:

аппаратную избыточность,

корректирующее кодирование.

С учетом того, что внесение дополнительной аппаратной избыточности в устройства шифрования приводит к увеличению ее стоимости и массогабаритных показателей, наиболее целесообразным является применение корректирующего кодирования [4].

Перспективным вариантом реализации корректирующего кодирования выступает использование полиномиальной системы классов вычетов (ПСКВ), в которой число A представляется в виде набора остатков от его деления на полиномы-основания $p_i(x)$:

$$A = (\alpha_1(x),\ \alpha_2(x) \ldots \alpha_i(x) \ldots \alpha_n(x)),$$

где $\alpha_i(x) = A \bmod p_i(x)$.

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

$$A = (\alpha_1(x),\ \alpha_2(x) \ldots \alpha_i(x) \ldots \alpha_n(x), \alpha_{n+1}(x) \ldots \alpha_k(x)),$$

где k – количество информационных остатков; n – общее количество остатков.

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

Известно, что корректирующая способность модулярных кодов зависит от числа используемых контрольных оснований, однако их увеличение приводит также к повышению схемотехнических затрат. Таким образом, выбор количества контрольных оснований необходимо производить с учетом вероятности возникновения сбоев в конкретной схемотехнической реализации AES-шифратора. Вместе с тем в современных устройствах вероятность сбоев не превышает $1 \cdot 10^{-6}$, поэтому наиболее целесообразным является разработка кодов, корректирующих однократные ошибки.

В статье [5] предложен алгоритм, позволяющий обнаруживать и исправлять 100 % однократных и 83 % двукратных ошибок. При этом используется только одно контрольное основание.

В рассматриваемом варианте реализации SubBytes в ПСКВ обрабатываемые числа представляются в виде

$$A = (\alpha_1(x), \alpha_2(x), \alpha_3(x), \alpha_4(x)),$$

где $\alpha_1(x) = A \bmod p_1(x)$; $\alpha_2(x) = A \bmod p_2(x)$; $\alpha_3(x) = \alpha_1(x) + \alpha_2(x)$; $\alpha_4(x) = (\alpha_1 + x \cdot \alpha_2(x)) \bmod p_3(x)$.

В качестве оснований ПСКВ используются полиномы $p_1(x) = x^4 + x + 1$, $p_2(x) = x^4 + x^3 + 1$, $p_3(x) = x^4 + x^3 + x^2 + x + 1$. Коррекция ошибок проводится за счет вычисления синдромов ошибки $\delta_1(x)$ и $\delta_2(x)$, которые отражают степень изменения остатков $\alpha_3(x)$ и $\alpha_4(x)$:

$$\delta_1(x) = \alpha_3(x) \oplus \alpha_3^*(x); \quad (1)$$

$$\delta_2(x) = \alpha_4(x) \oplus \alpha_4^*(x), \quad (2)$$

где $\alpha_3^*(x)$ – остаток $\alpha_3(x)$, в котором произошла ошибка; $\alpha_4^*(x)$ – остаток $\alpha_4(x)$, в котором произошла ошибка.

Так как значения контрольных остатков $\alpha_3(x)$ и $\alpha_4(x)$ содержат информацию об информационных остатках $\alpha_1(x)$ и $\alpha_2(x)$, то на основе выражений (1), (2) и при условии уникальности $\delta_1(x)$ и $\delta_2(x)$ можно однозначно определить место возникновения и глубину ошибок. Вместе с тем для практической реализации предложенной математической модели необходимо выполнить разработку структурной модели устройства, реализующего описываемый алгоритм.

Структурная модель должны определять [6]:

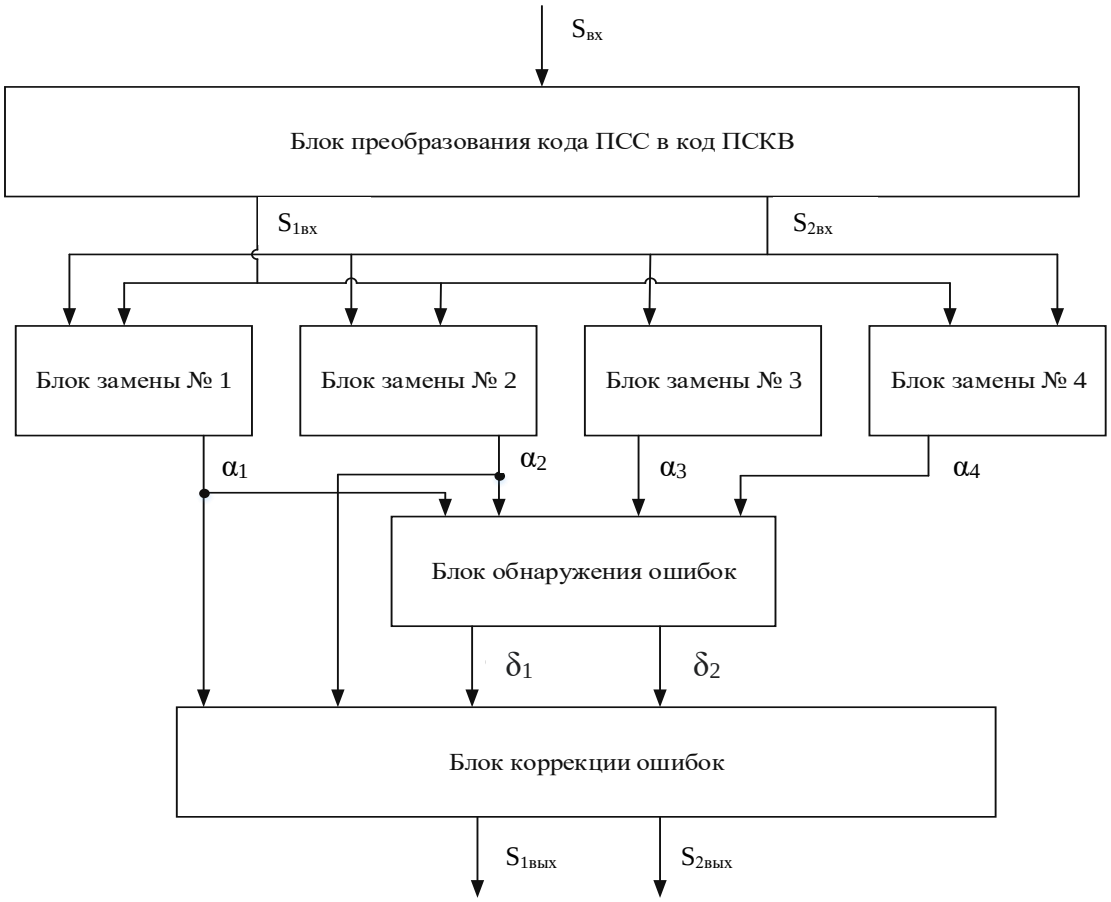
основные логические части устройства;

последовательность проведения этапов обработки информации;

связь с окружающей средой (количество и формат входных и выходных значений).

Логические элементы предлагаемого устройства целесообразно определить в соответствии с основными этапами обработки информации: 1) блок преобразования значений из позиционной системы счисления в ПСКВ; 2) блоки замены; 3) блок обнаружения ошибок; 4) блок коррекции ошибок.

С учетом особенностей математической модели разработанного алгоритма и вышеизложенных требований предлагается структурная модель устройства (рисунок).



Структурная модель устройства реализации процедуры SubBytes
в полиномиальной системе классов вычетов (ПСС – позиционная система счисления)

РЕЗУЛЬТАТЫ

Рассмотрим работу устройства при реализации процедуры SubBytes в ПСКВ.

Пусть на вход устройства (блок преобразования кода ПСС в код ПСКВ) поступает число 19_{16}. После преобразования числа в полиномиальную систему оно будет иметь вид

$$19_{16} = \left(19_{16} \bmod x^4 + x + 1, 19_{16} \bmod x^4 + x^3 + 1\right) = \left(A_{16,} 0_{16}\right).$$

Значения A_{16} и 0_{16} параллельно поступают на входы S_1-блока, S_2-блока, S_3-блока, S_4-блока. В блоках замены происходит определение выходного значения с использованием таблиц, идентификаторами строк и столбцов которых являются значения $S_{1вх}$ и $S_{2вх}$, а на их пересечении находятся значения $\alpha_1(x)$, $\alpha_2(x)$, $\alpha_3(x)$, $\alpha_4(x)$.

Таблицы формируются таким образом, чтобы совокупность их выходных значений соответствовала представлению в ПСКВ числа, которое бы получилось при использовании классической таблицы SubBytes. С учетом того, что входному числу $19_{16} = (A_{16}, 0_{16})$ в классической таблице соответствует значение $D4_{16} = (0_{16}, 5_{16}, 5_{16}, A_{16})$, в таблице S_1-блока на пересечении значений A_{16} и 0_{16} будет находиться значение $\alpha_1(x) = 0_{16}$, в таблице S_2-блока – $\alpha_2(x) = 5_{16}$, в таблице S_3-блока – $\alpha_3(x) = 5_{16}$, в таблице S_4-блока – $\alpha_4(x) = A_{16}$.

В результате работы S-блоков осуществлено преобразование входного значения 19_{16} в значение $D4_{16}$, которое в предлагаемой ПСКВ имеет вид

$$D4_{16} = (0_{16}, 5_{16}, 5_{16}, A_{16}).$$

Таким образом, рассматриваемое преобразование обеспечивает совместимость разрабатываемого устройства с устройствами, реализующими классический алгоритм. Соответственно, на выход S_1-блока поступает значение $\alpha_1(x) = 0_{16}$, S_2-блока – $\alpha_2(x) = 5_{16}$, S_3-блока – $\alpha_3(x) = 5_{16}$, S_4-блока – $\alpha_4(x) = A_{16}$.

С выхода S-блоков значения $\alpha_1(x)$, $\alpha_2(x)$, $\alpha_3(x)$, $\alpha_4(x)$ поступают на блок обнаружения ошибок, где происходят вычисления:

$$\alpha_3^*(x) = 0_{16} + 5_{16} = 5_{16};$$
$$\alpha_4^*(x) = (0_{16} + 5_{16}) \bmod x^4 + x^3 + x^2 + x + 1 = A_{16};$$
$$\delta_1(x) = 5_{16} + 5_{16} = 0_{16};$$
$$\delta_2(x) = A_{16} + A_{16} = 0_{16}.$$

С блока обнаружения ошибок значения $\delta_1(x)$, $\delta_2(x)$ поступают на блок коррекции ошибок, где с учетом их равенства нулю происходит определение выходных значений:

$$s_{1вых} = \alpha_1 = 0_{16};$$
$$s_{2вых} = \alpha_2 = 5_{16}.$$

Значения $\alpha_1(x)$ и $\alpha_2(x)$ предварительно поступают на блок коррекции ошибок с S_1-блока и S_2-блока, где они корректируются (в случае $\delta_1(x) \neq 0$ или $\delta_2(x) \neq 0$) или подаются на выход устройства (в случае $\delta_1(x) = \delta_2(x) = 0$).

Допустим, в работе S_1-блока возник сбой при определении разряда значения $\alpha_1(x)$ и $\alpha_1(x) = 2_{16}$. Тогда в блоке обнаружения ошибок

$$\alpha_3^*(x) = 2_{16} + 5_{16} = 7_{16};$$
$$\alpha^*{}_4(x) = (2_{16} + 5_{16}) \bmod x^4 + x^3 + x^2 + x + 1 = 8_{16};$$
$$\delta_1(x) = 7_{16} + 5_{16} = 2_{16};$$
$$\delta_2(x) = 8_{16} + A_{16} = 2_{16}.$$

С блока обнаружения ошибок значения $\delta_1(x) = 2_{16}$ и $\delta_2(x) = 2_{16}$ поступают на блок коррекции, где на основе априорной информации о распределении ошибок, фрагмент которой представлен в таблице, локализируется и исправляется ошибка в первом разряде значения $\alpha_1(x)$, определяются выходные значения:

$$s_{1вых} = 0_{16};$$
$$s_{2вых} = 5_{16}.$$

Обобщенные данные
о корреляции значений $\delta_1(x)$, $\delta_2(x)$ и локализации ошибки

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

В результате моделирования функционирования устройства установлено, что оно обеспечивает выполнение процедуры SubBytes, несмотря на возникший в

процессе функционирования сбой, за счет применения корректирующих модулярных кодов.

ЗАКЛЮЧЕНИЕ

В рамках решения научной задачи, связанной с повышением надежности функционирования AES-криптосистем:

определены основные логические элементы реализации процедуры SubBytes в ПСКВ на основе анализа алгоритма корректирующего кодирования в ПСКВ с одним контрольным основанием;

разработана структурная модель устройства преобразования SubBytes в ПСКВ.

Таким образом, создан элемент модели системы передачи и обработки информации, способной сохранять работоспособное состояние в условиях сбоев и отказов SPN-преобразователя. Дальнейшим направлением исследования является разработка функциональных схем логических элементов данной структурной модели.

ЛИТЕРАТУРА

1. Адаменко М. Основы классической криптологии. Секреты шифров и кодов. М.: Машиностроение. 2014. 256 с.
2. Системный анализ и принятие решений в деятельности учреждений реального сектора экономики, связи и транспорта / М.А. Асланов [и др.]; под ред. В.В. Кузнецова. М.: Экономика. 2010. 406 с.
3. 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.
4. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир. 1986. 536 с.
5. 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.
6. Модулярные параллельные вычислительные структуры нейропроцессорных систем / Н.И. Червяков [и др.]. М.: Физматлит. 2003. 287 с.

Для цитирования: Проворнов И.А., Калмыков И.А., Гиш Т.А. Разработка структурной модели отказоустойчивого преобразователя SubBytes в полиномиальной системе классов вычетов // Вестник Тверского государственного технического университета. Серия «Технические науки». 2023. № 4 (20). С. 62–69.

DEVELOPMENT OF A STRUCTURAL MODEL OF A FAULT-TOLERANT SUBBYTES CONVERTER IN A POLYNOMIAL SYSTEM OF RESIDUE CLASSES

I.A. PROVORNOV, Graduate, I.A. KALMYKOV, Dr. Sc.,
T.A. GISH, Cand. Sc.

North-Caucasus Federal University
1, Pushkin st., 355017, Stavropol, Russian Federation, e-mail: igorprovornov@yandex.ru

The article is devoted to the issue of increasing the reliability of the implementation of the SubBytes procedure of the AES cryptoalgorithm. The relevance of the development of new methods of corrective coding is substantiated. The theoretical foundations

of the corrective coding algorithm in a polynomial system of residue classes with one control base and the decomposition of the problem of its hardware implementation are considered, the first stage of which is the development of a structural model of the device different from the classical implementation of the SubBytes procedure. Based on the requirements for the developed structural model, its main logical elements are determined (a block for converting numbers from a positional number system to a polynomial system of residue classes, replacement blocks, an error detection block, an error correction block), the order of their interaction, the number and format of input and output values. The examples show the principle of operation of the proposed device.

Keywords: SPN systems, AES, SubBytes, reliability, corrective coding, polynomial system of residue classes, modular arithmetic.

Поступила в редакцию/received: 21.07.2023; после рецензирования/revised: 10.08.2023;
принята/accepted: 30.08.2023

УДК 681.51

К ПРОБЛЕМЕ ФОРМАЛИЗАЦИИ ЗНАНИЙ ПРИ СОЗДАНИИ CALS-ТЕХНОЛОГИЙ В ОБЛАСТИ МАШИНОСТРОЕНИЯ

Е.В. ПОЛЕТАЕВА, канд. техн. наук, И.В. ГОРЛОВ, д-р техн. наук

Тверской государственный технический университет
170026, Тверь, наб. Аф. Никитина, 22, e-mail: epolet2010@mail.ru

Рассмотрены вопросы, связанные с формализацией знаний предметной области машиностроения. Особое внимание уделено понятию «свойство», определяющему место термина в терминологической системе и являющемуся основой для проведения оптимизационных расчетов на разных этапах проектирования. Предложен метод структурирования знаний для представления вещественных объектов, процессов, концептуальных объектов и их свойств в рамках терминологической системы предметной области машиностроения. Отмечено, что данный метод позволяет создать основу как для решения инженерных задач, так и для согласования уже существующих моделей знаний, реализуемых в автоматизированных системах на разных этапах проектирования с целью интеграции всех этапов машиностроительного производства.

Ключевые слова: машиностроение, автоматизация проектирования, технологическая подготовка производства, онтология, структурное моделирование, терминологическая система, ИПИ-технологии, базы знаний.

DOI: 10.46573/2658-5030-2023-4-69-76