УДК 681.3.06

О.М. БЕВЗ, К.В. ДЕРЕВЕНЬКО

ОПТОЭЛЕКТРОННАЯ СИСТЕМА ПЕРЕДАЧИ ДАННЫХ С БЫСТРЫМ ДЕКОДИРОВАНИЕМ И ВЫСОКОЙ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТЬЮ

Вінницький національний технічний університет ,
21021, Хмельницьке шосе, 95, м. Вінниця, Україна,
E-mail: ezorf@mail.ru

Анотація. В статті розроблена оптоелектронна система, в якій реалізовано метод виправлення двох помилок, що грунтується на узагальненні коду Хеммінга. Також запропоновано метод інформаційного захисту від несанкціонованого доступу, що базується на дворівневій підстановочно-перестановочній мережі.

Аннотация. В статье разработана оптоэлектронная система, в которой реализован метод исправление двух ошибок, основанный на обобщении кода Хемминга. Также предложен метод информационной защиты от несанкционированного доступа, основанный на двухуровневой подстановочно-перестановочной сети.

Abstract. The article contains the optoelectronic system that has a method of correcting two errors, based on a generalization of the Hamming code. A method of information protection is developed against unauthorized access, based on a two-level Subsitution-Permutation Network-SPN also.

Ключові слова: оптоэлектронная система, несанкционированный доступ, код, исправ-ляющий две ошибки.

ВСТУП

Современные оптоэлектронные системы обладают рядом преимуществ по сравнению с другими системами передачи информации. Вместе с тем, существует ряд проблем, которые снижают эффективность процесса передачи информации. Одними из таких главных и важных проблем являются проблема искажения данных во время передачи и проблема возможности несанкционированного доступа со стороны постороннего участника.

АКТУАЛЬНОСТЬ

Искажение информации приводит к ошибкам в работе оптоэлектронной системы и возникает в результате помех, которые влияют на передаваемые в оптоэлектронных системах данные. Наиболее часто искажаются два информационных символа – возникают две ошибки. Несанкционированный доступ (НСД) участников возможен по причине открытости каналов связи, на основе которых работают оптоэлектронные системы. Современные методы исправления двух ошибок и методы защиты от несанкционированного доступа, которые используются в оптоэлектронных системах, характеризуются рядом недостатков. Самые критические из них – низкая скорость работы оптоэлектронной системы, которая приводит к снижению эффективности работы оптоэлектронной системы. Цель данной статьи – повышение эффективности работы оптоэлектронной системы, в которой реализовано исправление двух ошибок и информационная защита от несанкционированного доступа.

ПОСТАНОВКА ЗАДАЧИ

В соответствии с изложенной выше целью необходимо решить следующие задачи:
– разработать метод исправления двух ошибок с высокой скоростью работы в оптоэлектронной системе;
– разработать метод защиты информации с высокой эффективностью работы в оптоэлектронной системе.

ИЗВЕСТНЫЕ ПУТИ РЕШЕНИЯ

Наиболее распространенный метод исправления двух ошибок, которые возникают при передачи данных, в оптоэлектронных системах основывается на использовании семейства кодов Боуза-Чоудхури-Хонквингема [1].

Преимуществом данных кодов является возможность индикации наличия трех ошибок.

Декодирование кодовой последовательности, которая будет получена из оптоэлектронной системы, базируется на решении системы двух уравнений в конечном поле. Нахождение корней этой системы выполняется приведением системы к квадратному уравнению

$$x_1 + z_1 x + \frac{Z_2}{Z_1} + Z_1^2 = 0 \quad (1)$$

Корни этого уравнения являются значением позиций, на которых возникли ошибки. Существуют ряд способов решения квадратного уравнения (1).

Способ 1. Данный способ основан на применении операций перебора каждого значения x из данного конечного поля. Кроме операций перебора этот метод требует выполнения операций сложения, умножения и деления в конечном поле. Выполнение перечисленных выше операций в аппаратных узлах оптоэлектронной системы нуждается в использовании нескольких регистров сдвига и нескольких тактов их работы. Данный способ требует значительного времени исполнения и не является эффективным с точки зрения быстродействия. Программная интерпретация данного метода требует программных моделей регистров сдвига, которые должны работать за определенное количество итераций, и также не соответствует требованию высокой производительности и эффективности. Кроме того, он требует наличия в составе оптоэлектронной системы специализированного микропроцессорного комплекта, что ведет к дополнительным экономическим затратам.

Способ 2. Данный способ состоит в приведении в уравнении (1) к виду

$$x^2 + x + \beta = 0 \quad (2)$$

Дальнейшие решения уравнения (2) требует использования функций следа. Все математические операции этого способа выполняются в нормальном базисе, что также приводит к ряду недостатков.

В этом способе требуются меньшее количество операций умножения и деления, чем в предыдущем, но он требует большего количества итераций. В чистом виде этот метод не является быстродействующим. Одним из возможных способов повышения быстродействия является использования логарифмов и антилогарифмов Зеча. В целом эффективность этого способа также не будет достаточно высокой по причине необходимости дополнительной памяти, в которой будут храниться таблицы этих логарифмов и антилогарифмов.

Основным методом защиты информации в современных системах связи и оптоэлектронных системах является применение стандарта шифрования AES, в основу которого положен шифр Rijndael [2]. Работа данного стандарта шифрования основывается на реализации операций в конечном поле. Преимуществом данного шифра является высокая стойкость к линейному и дифференциальному криптанализу. Данное свойство является результатом «сбалансированности» операций в конечных полях. Выполнение математических операций в конечном поле требует значительного использования вычислительных ресурсов оптоэлектронных систем и характеризуется низкой скоростью работы, что снижает так же в целом эффективность.

Рассмотренные выше методы исправления двух ошибок и информационной защиты не могут по изложенным выше недостаткам (низкой эффективностью) быть использованы в оптоэлектронных системах.

РЕШЕНИЕ ЗАДАЧИ

Решение задачи выполним двумя шагами. На первом шаге разработаем код, исправляющий две ошибки, с высокой скоростью работы в оптоэлектронной системе. На втором шаге сформируем метод шифрования с высокой эффективностью работы в оптоэлектронной системе.

Шаг 1. Первый шаг будет состоять из двух этапов. На первом этапе сформируем код, исправляющий две ошибки, на втором – разработаем схему декодирования, с характеристиками, которые выше изложеных ранее методов.

Этап 1. Код исправляющий две ошибки реализуем на основе обобщения кода Хэмминга исправляющего две ошибки. Двоичный код Хэмминга – код длина которого, определяется выражением [1]

$$n = 2^m - 1, \quad (3)$$

где m – количество проверочных символов; n – длина кодового слова.

Двоичный код Хэмминга исправляет одну ошибку. Для исправления двух ошибок, очевидно, необходимо $2m$ проверочных символов. Проверочная матрица H' кода исправляющего две ошибки требует добавления m строк к проверочной матрице H кода Хэмминга. Проверочная матрица H кода Хэмминга с числом проверочных символов $m = 4$ и кодовых символов $n = 15$ содержит столбцы всех не нулевых векторов размером 4

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \quad (4)$$

Сокращенно матрицу (4) обозначим

$$H = [1, 2, 3 \ldots i \ldots 14, 15], \quad (5)$$

где i – соответствующий 4-битный вектор.

Для исправления ещё одной ошибки необходимо добавить к матрице H дополнительные 4 строки. В результате матрица H' примет следующий вид

$$H' = \begin{bmatrix} 1 & 2 & 3 & & 15 \\ f(1) & f(2) & f(3) & \ldots & f(15) \end{bmatrix}. \quad (6)$$

Значением функции $f(i)$ также является 4-битный вектор. Поэтому i-й столбец матрицы H'

$$H_i = \begin{pmatrix} i \\ f(i) \end{pmatrix} \quad (7)$$

В соответствии с [2] синдром кода будет вычисляться выражением

$$S = H_i + H_j = \begin{pmatrix} i & + & j \\ f(i) & + & f(j) \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \quad (8)$$

Этап 2. Пусть y – кодовое слово, тогда декодирование происходит на основе вычисления синдрома

$$S = Hy^T = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \quad (9)$$

Если ошибки произошли на позициях i, j кодового слова, то должна выполняться система

$$\left.\begin{array}{ccccc} i & + & j & = & z_1 \\ f(i) & + & f(j) & = & z_2 \end{array}\right\} \quad (10)$$

где $i, j, f(i), z_1, z_2$ 4-битные вектора.

Наиболее целесообразно представить функции $f(i)$ и $f(j)$ в виде: $f(i) = i^3, f(j) = j^3$. Тогда система (10) примет следующий вид

$$\left.\begin{array}{ccccc} i & + & j & = & z_1 \\ i^3 & + & j^3 & = & z_2 \end{array}\right\} \quad (11)$$

Анализ системы 11 показывает, что возможны 4 варианта решения системы (11):

Вариант 1. Если $z_1 = z_2 = 0$ – ошибок не произошло.

Вариант 2. Если $z_1 \neq 0$ и $z_2 = z_1^3$ – произошла ошибка на позиции $i = z_1$.

Вариант 3. Если $z_1 \neq 0$ и $z_2 \neq z_1^3$ – ошибки произошли на позициях i, j.

Вариант 4. Если $z_1 = 0$ и $z_2 \neq 0$ – произошло три ошибки.

Решение системы (11) предлагается выполнить путем перебора всех возможных значений, которые могут принимать переменные i и j. Переменные i и j являются элементами поля Галуа $x \in GF(2^4)$. Нахождение значений корней системы (11) будет проводиться в начале для уравнения 1, а после этого, в случае выполнения равенства, необходимо проверить второе уравнение. Для реализации предложенного решения необходимо составить таблицы, в которых содержатся возможные значения 4-

битных векторов i и j и соответствующие им значения i^3 и j^3. В таблице 1 отображены значения десятичных представлений элементов поля GF (2^4), двоичные представления этих элементов, степенное представление и полиномиальное представление, а также соответствующие результаты возведений элементов в куб.

Таблица 1.

Элементы поля Галуа и соответствующие им результаты возведения в куб

Десятичное представление элемента поля x	Двоичное представление элементов поля x	Степенное представление элементов поля x	Полиномиальное представление элемента поля X	Элемент поля x^3
1	2	3	4	5
0	0000	0	0	0
1	0001	1	1	1
2	0010	x	X	x^3
3	0011	x^4	1+x	x^{12}
4	0100	x^2	x^2	x^6
5	0101	x^8	$1+x^2$	x^9
6	0110	x^5	x^2+x	1
7	0111	x^{10}	x^2+x+1	1
8	1000	x^3	x^3	x^9
9	1001	x^{14}	x^3+1	x^{12}
10	1010	x^9	x^3+x	x^{12}
11	1011	x^7	x^3+x+1	x^6
12	1100	x^6	x^3+x^2	x^3
13	1101	x^{13}	x^3+x^2+1	x^9
14	1110	x^{11}	x^3+x^2+x	x^3
15	1111	x^{12}	x^3+x^2+x+1	x^6

Нахождение корней системы (11) с использованием табличных подстановок на основе таблицы 1 требует выполнения только операций сложения и загрузки значений элементов поля из памяти.

Проведенные компьютерные эксперименты показали, что предложенный способ решения системы (11) дает возможность снизить время декодирования на 20% по сравнению с изложенными выше методами исправления двух ошибок в оптоэлектронных системах. По этой причине первый шаг поставленной задачи выполнен.

Шаг 2. В соответствии с изложеной выше целью работы необходимо обеспечить высокую скорость работы и стойкость метода защиты информации (криптографического преобразования) в оптоэлектронных системах. Наиболее мощными видами криптоанализа являются линейный и дифференциальный. Криптографическая стойкость преобразования к линейному и диференциальному криптанализу является функцией количества активных S-боксов [3]. Одним из путей увеличения количества активных S-боксов является использование двух уровневой подстановочно-перестановочной сети (Subsitution-Permutation Network-SPN). Для формирования максимального количества активных S-боксов на двух уровнях SPN-сети (верхнего и нижнего) необходимо применить коды с максимальной длиной - $КМД_н$ и $КМД_в$. Для SPN такого типа количество активных S-боксов равно [4]

$$N = (m_2 + 1)(m_1 + 1), \tag{12}$$

где m_2 – длина слова $КМД_н$; m_1 – длина слова $КМД_в$.

В качестве кода с максимальным расстоянием целесообразно использовать код

$КМД\left(2m, m, m+1\right)$. Код $КМД\left(2m, m, m+1\right)$ – код с образующей матрицей G=[I][C], где C – образующая матрица размером *m* x *m*, I-единичная матрица, *m* – длина слова кода. Для формирования преобразования в шифрах на основе SPN-сетей с использованием кода с максимальным расстоянием необходимо применять только матрицу – C.

Преобразование одного уровня гнездовой SPN согласно КМД определяет отображение результатов S-боксов X в вектор Y через произведение матриц над полем Галуа $GF(2^n)$. Параметр n определяет длину S-бокса

$$\begin{bmatrix} y_0 \\ . \\ . \\ . \\ y_{m-1} \end{bmatrix} = \begin{bmatrix} c_{0,0} \ldots c_{0,\mathrm{m}-1} \\ \\ c_{ij} \\ \\ c_{m-1,0} \ldots c_{m-1,m-1} \end{bmatrix} * \begin{bmatrix} x_0 \\ . \\ . \\ . \\ x_{m-1} \end{bmatrix}, \tag{13}$$

где x_j – результирующее значение определенного S-бокса, $x_i \in GF(2^n);$ y_j – результирующее значение определенного уровня гнездовой SPN. $y_i \in GF(2^n);$ c_{ij} – коэффициенты образующей матрицы *КМД* – преобразования $c_{ij} \in GF(2^n)$; m – длина слова *КМД*.

Следующим параметром, который определяет стойкость шифра к линейному и дифференциальному криптоанализу, кроме количества активных S-боксов раунда, являются значения вероятности линейной *p* и дифференциальных *q* характеристик S-боксов, что применяются в раунде [5].

Вероятность дифференциальной характеристики раунда определяется выражением

$$P = p_s^n, \tag{14}$$

где p_s – вероятность дифференциальной характеристики S-бокса, что применяется в раунде; n – количество активных S-боксов в раунде.

Вероятность линейной характеристики раунда определяется выражением

$$Q = q_s^n, \tag{15}$$

где q_s – вероятность линейной характеристики S-бокса, что применялся в раунде; n – количество активных S-боксов в раунде.

Нижняя граница вероятности линейной q_s и дифференциальной p_s характеристик одного S-бокса зависит от его размера. Как указано в роботе [5], нижняя граница дифференциальной и линейной характеристики S-бокса размером *n* x *n* определяется выражением

$$q_s = p_s = \frac{n}{2^{n-1}}, \tag{16}$$

где n – размер S-бокса.

Размер S-бокса также влияет на тип кода с максимальным расстоянием. Наиболее целесообразно в оптоэлектронной системе использовать S-боксы размером 16 x 16 бит. Такие S-боксы для длины блока шифрования 128 бит могут формировать 4 типа двухуровневых SPN-сетей.

Эффективность защиты информации, которая будет реализована в оптоэлектронной системе определяется отношением двух составляющих. Первое составляющее – вероятность линейной (дифференциальной) характеристики одного раунда двухуровневой SPN-сети. Второе составляющее – количество операций, за которые данный раунд будет выполнен оптоэлектронной системой [6].

В таблице 2 представлены типы кодов с максимальным расстоянием, которые могут формировать SPN-сеть с размерами S-боксов 16 x 16, длиной 128 бит и соответствующие значения эффективности защиты информации в оптоэлектронной системе.

Таблица 2.

Варианты гнездовых SPN-сетей с S-боксами размеров 16 х 16 и соответствующие показатели эффективности реализации

Номер варианта	Тип КМД нижнего уровня	Тип КМД верхнего уровня	Коэффициент эффективности
1	2	3	4
1	(2, 1, 2)	(16, 8, 9)	11,7
2	(4, 2, 3)	(8, 4, 5)	18,3
3	(8, 4, 5)	(4, 2, 3)	20,6
4	(16, 8, 9)	(2, 1, 2)	11

Анализ таблицы 2 демонстрирует, что наиболее эффективным вариантом для защиты информации в оптоэлектронной сети является SPN-сеть, которая состоит из кода максимальной длины нижнего уровня типа (8, 4, 5) и кода максимальной длины верхнего уровня типа (4, 2, 3). Значение эффективности одного раунда стандарта AES составляет – 15, 6 [6], что на 30% ниже чем предложенный метод шифрования.

ВЫВОДЫ

В результате выполненного исследования разработана оптоэлектронная система, в которой используется метод исправления двух ошибок при передачи данных и метод защиты информации от несанкционированного доступа. Метод исправления двух ошибок основанный на обобщении кода Хемминга, реализация которого в оптоэлектронной системе повысит скорость работы на 20%, по сравнению с существующими методами. Метод защиты информации основанный на двухуровневой подстановочно-перестановочной сети. Реализация данного метода в оптоэлектронной системе передачи данных повысит эффективность работы по сравнению с существующими методами на 30%.

СПИСОК ЛИТЕРАТУРЫ

1. Ф. Дж. Мак - Вильямс. Теория кодов исправляющих ошибки / Ф. Дж. Мак – Вильямс, Н. Дж. А. Слоэн // Связь. – 1979. – 743 с.
2. Daemen J. The Design of Rijndael. AES: The Advanced Encryption Standard / Joahn Daemen, Vincent Rijmen // Springer – Berlin. – 2002. – V.234. – P. 24 – 28.
3. O'Connor L. On the distribution of characteristics in bijective mappings / O'Connor L. // Advances in Cryptology – EUROCRYPT '93. – Springer-Verlag. – 1994. – Vol.678. – P. 360 – 370.
4. The block cipher Hierocrypt / [Ohkuma K., Muratani H., Sano F., Kawamura S]. // Proceedings of Selected Areas in Cryptography – SAC 2000, Lecture Notes in Computer Science. – Springer-Verlag. – 2001. – Vol. 2012. – P. 72 – 88.
5. Kanda M. Practical security evaluation against differential and linear cryptanalysis for Feistel ciphers with SPN round function. / Kanda M. // Seventh Annual International Workshop on Selected Areas in Cryptography-SAC`00, Lecture Notes in Computer Science – Springer-Verlag. – 2001. -Vol. 2012. – P.324 – 338.
6. Бевз О. М. Методи шифрування на основі високонелінійних бульових функцій та кодів з максимальною відстанню: дис. ... канд. техн. наук: 05.13.05 / Бевз Олександр Миколайович – Вінниця: 2008. – 181 с.

Надійшла до редакції 11.12.2013р.

БЕВЗ ОЛЕКСАНДР МИКОЛАЙОВИЧ – к.т.н, доцент кафедри автоматики та інформаційно-вимірювальної техніки, Вінницький національний технічний університет, м. Вінниця, Україна.

ДЕРЕВЕНЬКО КАТЕРИНА ВАСИЛІВНА – студентка гр. 1СІ-11 кафедри автоматики та інформаційно-вимірювальної техніки, Вінницький національний технічний університет, м. Вінниця, Україна.