УДК 004.052:004.056.55

РАЗРАБОТКА МЕТОДА НЕЛИНЕЙНОГО ШИФРОВАНИЯ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ОПЕРАЦИИ ВОЗВЕДЕНИЯ В СТЕПЕНЬ ДЛЯ КОНЕЧНОГО ПОЛЯ ГАЛУА

[1]Калмыков И.А., [1]Степанова Е.П., [1]Калмыков М.И., [2]Тынчеров К.Т.

[1]ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru;
[2]ФГБОУ ВО «Уфимский государственный нефтяной технический университет», Октябрьский

Для повышения помехозащищенности низкоорбитальных систем спутниковой связи (НССС) необходимо увеличивать информационную скрытность. Одним из наиболее эффективных методов повышения информационной скрытности является применение систем шифрования. В настоящее время широко используются системы с побитовым шифрованием. Достоинством таких поточных шифросистем является скорость закрытия данных, которая совпадает со скоростью поступления открытых данных. Однако данный метод зашифрования и расшифрования, построенный на основе суммирования по модулю два открытой информации с шифрующей гаммой, полученной из псевдослучайной последовательности (ПСП), не обладает достаточной криптостойкостью. Обладая определенным числом символов открытого и зашифрованного текста, можно однозначно определить структуру генератора ПСП. Устранить данный недостаток можно за счет применения методов нелинейного шифрования, в которых используется совокупность мультипликативных и аддитивных операций в конечных полях Галуа. Реализация метода защиты информации на основе совокупности операций по модулю в конечном поле Галуа приводит к повышению информационной скрытности НССС. Поэтому разработка метода нелинейного шифрования данных на основе процедуры возведения в степень для поля Галуа является актуальной задачей. Однако не все такие методы обладают достаточной производительностью. Поэтому цель статьи – повысить скорость выполнения нелинейного шифрования данных за счет реализации операции возведения в степень в полях Галуа.

Ключевые слова: информационная скрытность, алгоритмы поточного зашифрования, нелинейные методы зашифрования, конечные поля Галуа

DEVELOPMENT OF A METHOD NONLINEAR ENCRYPTION INFORMATION, USING THE OPERATION OF EXPONENTIATION FOR FINITE FIELD GALOIS

[1]Kalmykov I.A., [1]Stepanova E.P., [1]Kalmykov M.I., [2]Tyncherov K.T.

[1]Federal State Autonomous Educational Institution Higher Professional Education North-Caucasian Federal University, Stavropol, e-mail: kia762@yandex.ru;
[2]Branch of Ufa State Petroleum Technological University in the City, Oktyabrskiy

To increase noise immunity of low-orbit satellite communication systems (LOSCSs) it is necessary to increase information secrecy. One of the most effective methods of increasing information secrecy is the use of encryption systems. Currently, bit-encrypted systems are widely used. The advantage of such stream cipher systems is the speed of data closure, which coincides with the speed of receipt of open data. However, this method of encryption and decryption, built on the basis of summing modulo two open information with encryption gamma obtained from pseudorandom sequence (PRS), does not have sufficient cryptographic stability. Having a certain number of characters of the open and encrypted text, it is possible to define unambiguously structure of the generator of PRS. This disadvantage can be eliminated by using nonlinear encryption methods, which use a set of multiplicative and additive operations in finite Galois fields. The implementation of the method of information security based on a set of operations on the module in the final Galois field leads to an increase in the information secrecy of the LOSCSs. Therefore, the development of a method of nonlinear data encryption based on the procedure of exponentiation for the Galois field is an urgent task. However, not all such methods have sufficient performance. Therefore, the purpose of the article is to increase the speed of non-linear data encryption by implementing the exponentiation operation in Galois fields.

Keywords: information stealth, stream encryption algorithms, nonlinear encryption methods, finite Galois fields

Одним из основных составных частей помехозащищенности низкоорбитальных систем спутниковой связи (НССС) является обеспечение информационной скрытности [1–3]. Очевидно, что информационная скрытность задается способностью НССС противостоять деструктивным воздействиям, которые направлены на извлечение информации из передаваемых по каналам связи сигналов. В этом случае раскрытия смысла передаваемой информации связано с отождествлением каждой совокупности принятого сигналов с содержание сообщения [4]. Одним из наиболее эффективных методов, позволяющих повысить информационную скрытность НССС, является использование систем шифрования. В настоящее время создано значительное количество различных алгоритмов криптографической защиты. Особое место среди таких методов занимают алгоритмы нелинейные шифрования (НШ), в которых используется совокупность мультипликативных и аддитивных операций в конечных полях Галуа. Реализация метода защиты информации на основе

совокупности операций по модулю в конечном поле Галуа приводит к повышению информационной скрытности НССС. Поэтому разработка метода нелинейного шифрования данных на основе процедуры возведения в степень для поля Галуа является актуальной задачей.

Современные низкоорбитальные системы спутниковой связи должны обладать высокой информационной скрытностью. По мере увеличения трафика передаваемых данных и повышения скорости передачи информации особое внимание приобретают методы поточного шифрования. Однако, обеспечивая высокую скорость закрытия информации, поточные шифры, построенные на основе сложения по модулю два потока открытых данных с шифрующей гаммой, представляющей собой набор псевдослучайных символов, не обладают достаточной информационной стойкостью. Это связано с тем, что обратная функция шифрования базируется на выполнении одной аддитивной операции. Устранить данный недостаток позволяют методы нелинейного шифрования. Однако не все они обладают достаточной производительностью. Поэтому цель статьи – повысить скорость выполнения нелинейного шифрования данных за счет реализации операции возведения в степень в полях Галуа.

Материалы и методы исследования

Информационная скрытность низкоорбитальной системы спутниковой связи во многом определяется степенью защищенности информации от случайных и преднамеренных воздействий нарушителей. Такие деструктивные воздействия могут привести к значительному ущербу субъектам, которые являются владельцами передаваемой по НССС информации. Для устранения данного недостатка широко используются методы шифрования. Особое место занимают поточные системы шифрования, так как обеспечивают достаточно высокую скорость зашифрования [5]. В качестве генератора шифрующей гаммы в таких системах предлагается использовать генераторы, вырабатывающие псевдослучайную последовательность. В работах [5–7] показаны методы и схемные решения систем поточного шифрования, которые реализуются с использованием целочисленных алгебраических систем на основе регистров сдвига с линейной обратной связью. При этом поточный шифр, построенный на основе модульной операции сложении потока псевдослучайных битов, полученных с помощью многотактных кодовых фильтров, с битами потока открытых данных теоретически имеет высокую информационную скрытность. Однако такие системы имеют недостаток – недостаточная криптостойкость из-за возможности вскрытия при наличии определенного числа символов открытого текста и соответствующему ему зашифрованного текста.

Устранить отмеченный недостаток позволяют методы нелинейного шифрования, которые эффективно реализуются в конечных полях Галуа. В отличие от поточного шифрования, в котором прямое и обратное криптопреобразование выполняется с помощью одной операции, методы нелинейного шифрования имеют более широкие возможности по обеспечению информационной скрытности передаваемых данных [8]. Это связано с тем, что в таких системах НШ используются преобразования, реализующие как отдельные аддитивные и мультипликативные операции, так и их различные комбинации В качестве примера можно представить следующие методы НШ

$$\tilde{p}(x)+\tilde{k}(x)\equiv\tilde{c}(x)\bmod\eta(x)\,, \qquad (1)$$

$$\tilde{p}(x)\tilde{k}(x)\equiv\tilde{c}(x)\bmod\eta(x)\,, \qquad (2)$$

$$\tilde{p}(x)^{\tilde{k}}\equiv\tilde{c}(x)\bmod\eta(x)\,, \qquad (3)$$

где $\tilde{p}(x)$ – полиномиальная форма блока открытых данных длиной L разрядов; $\tilde{c}(x)$ – полиномиальная форма блока зашифрованных данных длиной L разрядов; $\tilde{k}(x)$ – полиномиальная форма ключа длиной L разрядов; $\deg\eta(x)=L$ – степень порождающего полинома $\eta(x)$ – множество ключевых данных.

Рассмотрим метод нелинейного шифрования, реализуемый в поле Галуа, который в своей основе имеет метод возведения в степень элементов $GF(2^L)$. Для реализации данного метода необходимо использовать неприводимый полином $\eta(x)$. На основе данного полинома порождаются ненулевые элементы мультипликативной группы. Если положить, что степень порождающего полинома равна L, то входной поток открытых данных необходимо разделить на блоки длиной L бит. Тогда полиномиальная форма полученного блока открытых данных имеет вид

$$p_j(x)=p_{L-1}x^{L-1}+p_{L-2}x^{L-2}+\ldots+p_2x^2+p_1x^1+p_0\,, \qquad (4)$$

где $p_{L-1},\ldots,p_0$ – двоичные разряды j-го блока открытых данных; $p_v\in\{0,1\}$, $v=0,1,\ldots,L-1$.

Таким образом, для j-го блока, представленного в полиномиальной форме в виде многочлена $p_j(x)$, справедливо

$$\deg p_j(x)<\deg\eta(x). \qquad (5)$$

В этом случае данный блок, длиной L двоичных разрядов, считается элементом $GF(2^L)$. Для реализации процедуры шифрования на основе возведения в степень элемента расширенного поля Галуа вычисляются значения псевдослучайной последовательности X. Если обеспечить устранение блока, состоящего из L нулей, то ключевую последовательность, представляющую собой ПСП, можно записать в виде кортежа ненулевых числе

$$\tilde{k}=\{k_0,k_1,k_2,\ldots\}. \qquad (6)$$

Тогда зашифрование потока данных для $j=0$, 1, …. будет выполняться согласно

$$c_j(x)=p_j^{k_{ji}}(x)\bmod\eta(x), \qquad (7)$$

где $c_j(x)$ – j-й блок зашифрованных данных, представленный в полиномиальной форме;

Процедура расшифрования потока на приемной стороне является обратной задачей уравнения (7). Тогда для получения j-й блока открытых данных необходимо реализовать

$$\sqrt[k_j]{c_j(x)}\equiv p_j(x)\,. \qquad (8)$$

Для получения ключевой последовательности $\tilde{k} = \{k_0, k_1, k_2, ...\}$ можно использовать многотактовые кодовые фильтры, построенные на основе регистров сдвига. Так как операция возведения в степень элементов конечного поля реализуется по модулю порождающего полинома η(x), то для повышения скорости выполнения данной процедуры целесообразно использовать быстрый алгоритм возведения в степень. Согласно [крипт] на данную итерацию зашифрования потребуется не более $2[\log_2 k_j]$ операций умножений. Если считать, что *j*-й блок ключевой последовательности удовлетворяет условию

$$2^{L-1} \le k_j < 2^L, \tag{9}$$

то очевидно, что $[\log_2 k_j] = L - 1$. Таким образом, очевидно следующее противоречие. Для обеспечения высокой информационной скрытности НССС необходимо увеличивать порядок конечного поля Галуа. Но при этом происходит снижение скорости выполнения шифрования. Устранить данное противоречие позволит разработанный метод нелинейного шифрования информации с использованием операции возведения в степень в сумме полей Галуа. Такой переход от шифрования блока данных $p_j(x)$ длиной L бит, к параллельному шифрованию блоков меньшей длины $m_i^j(x)$ позволяет повысить скорость шифрования. Это обусловлено изоморфизмом китайской теоремы об остатках (КТО).

В этом случае используется сумма конечных полей Галуа, имеющая вид

$$GF(2^L) = GF(2^{L_1}) + GF(2^{L_2}) + GF(2^{L_3}) + ... + GF(2^{L_n}), \tag{10}$$

где $L = L_1 + L_2 + ... + L_n$.

Для реализации разработанного метода нелинейного шифрования с использованием операции возведения в степень в сумме конечных полей Галуа необходимо разбить исходный блок $p_j(x)$ длиной L бит согласно

$$p_j(x) = m_j^1(x) \,||\, m_j^2(x) \,||\, m_j^3(x) \,||\, ... \,||\, m_j^n(x), \tag{11}$$

где || – операция конкатенация; $\deg \eta(x) = \sum_{i=1}^{n} \deg \eta^i(x)$; $\eta^i(x)$ – порождающий полином конечного поля Галуа $GF(2^{L_i})$; $L_i = \deg \eta^i(x)$.

Тогда процесс зашифрования описывается выражением

$$\begin{cases} c_j^1(x) = (m_j^1(x))^{k_j^1} \bmod \eta^1(x), \\ \vdots \\ c_j^n(x) = (m_j^n(x))^{k_j^n} \bmod \eta^n(x). \end{cases} \tag{12}$$

Процедура расшифрования в сумме конечных полей Галуа будет определяться

$$\begin{cases} \sqrt[k_j^1]{c_j^1(x)} \equiv m_j^1(x) \bmod \eta^1(x), \\ \vdots \\ \sqrt[k_j^n]{c_j^n(x)} \equiv m_j^n(x) \bmod \eta^n(x). \end{cases} \tag{13}$$

Если в выбранном наборе конечных полей справедливо $\max \deg \eta^i(x) = w$, то при использовании быстрого алгоритма возведения в степень на выполнение одной итерации зашифрования потребуется не более $2[\log_2 k_j^w]$ операций умножений. Если учесть, что имеем $w < L$, то, очевидно, разработанный метод нелинейного шифрования с использованием операции возведения в степень в сумме конечных полей Галуа позволяет повысить скорость закрытия информации.

Результаты исследования и их обсуждение

Рассмотрим реализацию разработанного метода нелинейного шифрования с использованием операции возведения в степень в сумме конечных полей Галуа. В качестве конечных полей Галуа выбираем $GF(2^3)$ с порождающим полиномом $\eta^1(x) = x^3 + x + 1$, $GF(2^4)$ с порождающим полиномом $\eta^2(x) = x^4 + x + 1$ и $GF(2^5)$ с порождающим полиномом $\eta^3(x) = x^5 + x^2 + 1$. Пусть задан поток открытых данных, представленный в шестнадцатеричной системе счисления $\tilde{p} = DEDF354FF$. Для получения ключевой последовательности был использован генератор ПСП, с выхода которого была снята последовательность чисел $\tilde{k} = 92F57DD17$. Так как степень первого порождающего полинома равна $\deg \eta^1(x) = 3$, второго полинома – $\deg \eta^2(x) = 4$, а третьего многочлена – $\deg \eta^3(x) = 5$, входной поток разбиваем по блоками по 12 бит. Аналогично поступаем и с ключевой последовательностью.

Рассмотрим первую итерацию процесса зашифрования. Для этого представим данные в двоичном коде. Тогда получаем

$$\tilde{p}_1 = DED = 110\ 1111\ 01101_2;\ \tilde{k}_1 = 92F_{16} = 100\ 1001\ 01111_2.$$

Таким образом, для поля Галуа $GF(2^3)$ получаем значения первого блока данных $m_1^1(x) = 110_2 = x^2 + x$ и ключа $k_1^1(x) = 100_2 = 4$. Для поля Галуа GF(2^4) значение первого блока данных равно $m_1^2(x) = 1111_2 = x^3 + x^2 + x + 1$, а значение ключа $k_1^2(x) = 1001_2 = 9$. Для поля Галуа $GF(2^5)$ получаем первый блок данных равный $m_1^3(x) = 01101_2 = x^3 + x^2 + 1$, а значение ключа $k_1^3(x) = 01111_2 = 15$. Воспользуемся выражением (12). Получаем

$$\begin{cases} c_1^1(x) = (m_1^1(x))^{k_1^1} \bmod \eta^1(x) = (x^2 + x)^4 \bmod x^3 + x + 1 = x^2 = 100, \\ c_1^2(x) = (m_1^2(x))^{k_1^2} \bmod \eta^2(x) = (x^3 + x^2 + x + 1)^9 \bmod x^4 + x + 1 = x^3 = 1000, \\ c_1^3(x) = (m_1^3(x))^{k_1^3} \bmod \eta^3(x) = (x^3 + x^2 + 1)^{15} \bmod x^5 + x^2 + 1 = x^3 + x + 1 = 01011. \end{cases}$$

Выполним вторую итерацию шифрования. Тогда получаем

$$\tilde{p}_2 = F35_{16} = 111\ 1001\ 10101_2;\ \tilde{k}_2 = 57D_{16} = 101\ 0111\ 11011_2.$$

Таким образом, для поля Галуа $GF(2^3)$ получаем значения первого блока данных равный $m_2^1(x) = 111_2 = x^2 + x + 1$ и ключа $k_2^1(x) = 010_2 = 2$. Для поля Галуа $GF(2^4)$ значение первого блока данных равно $m_2^2(x) = 1001_2 = x^3 + 1$, а значение ключа $k_2^2(x) = 1011_2 = 11$. Для поля Галуа $GF(2^5)$ получаем первый блок данных равный $m_2^3(x) = 10101_2 = x^4 + x^2 + 1$, а значение ключа $k_2^3(x) = 11101_2 = 29$. Тогда получаем

$$\begin{cases} c_2^1(x) = (m_2^1(x))^{k_2^1} \bmod \eta^1(x) = (x^2 + x + 1)^2 \bmod x^3 + x + 1 = x + 1 = 011, \\ c_2^2(x) = (m_2^2(x))^{k_2^2} \bmod \eta^2(x) = (x^3 + 1)^{11} \bmod x^4 + x + 1 = x + 1 = 0011, \\ c_2^3(x) = (m_2^3(x))^{k_2^3} \bmod \eta^3(x) = (x^4 + x^2 + 1)^{29} \bmod x^5 + x^2 + 1 = x + 1 = 00011. \end{cases}$$

Выполним третью итерацию шифрования. Тогда получаем

$$\tilde{p}_3 = 4FF_{16} = 010\ 0111\ 11111_2;\ \tilde{k}_3 = D17_{16} = 110\ 1000\ 10111_2.$$

Для поля Галуа $GF(2^3)$ получаем значения первого блока данных равные $m_3^1(x) = 010_2 = x$ и ключа $k_3^1(x) = 110_2 = 6$. Для поля Галуа $GF(2^4)$ значение первого блока данных равно $m_3^2(x) = 0111_2 = x^2 + x + 1$, а значение ключа $k_3^2(x) = 1000_2 = 8$. Для поля Галуа $GF(2^5)$ получаем первый блок данных равный $m_3^3(x) = 11111_2 = x^4 + x^3 + x^2 + x + 1$, а значение ключа $k_3^3(x) = 10111_2 = 23$. Тогда получаем

$$\begin{cases} c_3^1(x) = (m_3^1(x))^{k_3^1} \bmod \eta^1(x) = (x)^6 \bmod x^3 + x + 1 = x^2 + 1 = 101, \\ c_3^2(x) = (m_3^2(x))^{k_3^2} \bmod \eta^2(x) = (x^2 + x + 1)^8 \bmod x^4 + x + 1 = x^2 + x = 0110, \\ c_3^3(x) = (m_3^3(x))^{k_3^3} \bmod \eta^3(x) = (x^4 + x^3 + x^2 + x + 1)^{23} \bmod x^5 + x^2 + 1 = x^4 = 10000. \end{cases}$$

В рассмотренном примере имеем $\max \deg \eta^i(x) = 5$. Тогда при использовании быстрого алгоритма возведения в степень на выполнение одной итерации зашифрования потребуется $N_1 = 2[\log_2 k_j^w] = 10$ операций умножений. Так как $\deg \eta(x) = \sum_{i=1}^{3} \deg \eta^i(x) = 12$ бит, то для выполнения операции возведения в степень по модулю $\eta(x)$ потребуется $N_2 = 2[\log_2 \tilde{k}_j] = 24$ операций умножения. Таким образом очевидно, что разработанный метод нелинейного шифрования с использованием операции возведения в степень в сумме конечных полей Галуа позволяет повысить скорость закрытия информации в 2,4 раза по сравнению с использованием одного модуля разрядностью 12 бит.

Выводы

В статье рассмотрен вопрос повышения помехозащищенности низкоорбитальных

систем спутниковой связи за счет увеличения информационной скрытности НССС. Для достижения поставленной цели было предложено использовать криптографические методы защиты информации. Проведенные исследования систем шифрования показали целесообразность применения нелинейных методов зашифрования, в которых применяются мультипликативные и аддитивные операции в полях Галуа. В статье приведен разработанный метод нелинейного шифрования данных на основе процедуры возведения в степень для поля Галуа. Проведенные исследования показали, что использование данного метода нелинейного шифрования, реализованного в сумме конечных полей Галуа, позволяет повысить скорость закрытия информации в 2,4 раза по сравнению с использованием одного модуля разрядностью 12 бит.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-07-01020.

Список литературы

1. Pashintsev V.P., Zhuk A.P., Kalmykov M.I., Rezenkov D.N. Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication. International Journal of Mechanical Engineering and Technology. 2018. № 9 (5). P. 958–965.

2. Максимов М.В. Защита от радиопомех. М.: «Сов. радио», 1976. 496 с.

3. Дворников С.В. Оценка имитостойкости каналов управления с частотной модуляцией // Информация и космос. 2016. № 1. С. 32–35.

4. Куприянов А.И., Шустов Л.Н. Радиоэлектронная борьба. Основы теории. М.: Вузовская книга, 2016. 800 с.

5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Издательство ТРИУМФ, 2003. 816 с.

6. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Горячая линия – Телеком, 2017. 229 с.

7. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. М.: Горячая линия – Телеком, 2015. 256 с.

8. Клен Р.М., Борисов Е.А. Нелинейные системы на службе защиты данных // Информационная безопасность. 2014. № 6. С. 38–39.