УДК 681.3

ПРИМЕНЕНИЕ НЕЛИНЕЙНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Юртаев М.В., Калмыков М.И.

ФГАОУ ВПО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

Широкое внедрение вычислительной техники, появление новых мультимедийных приложений требуют обеспечить защиту информации от несанкционированного доступа в реальном масштабе времени. Для обеспечения высокой степени защиты предлагается использовать нелинейные алгоритмы, построенные на основе аддитивных и мультипликативных операций. С целью повышения скорости закрытия информации в работе показана возможность использования индексного представления элементов расширенного поля Галуа. Переход к индексам позволяет свести низкоскоростную операцию возведения в степень по модулю к мультипликативной операции над степенями элементов.

Ключевые слова: система защиты информации, нелинейные алгоритмы шифрования, возведения в степень по модулю, индексы.

APPLYING A NONLINEAR ENCRYPTION ALGORITHM SYSTEMS OF INFORMATION FROM UNAUTHORIZED ACCESS

Yurtaev M.V., Kalmykov M.I.

North-Caucasian federal university, Stavropol, e-mail: kia762@yandex.ru

Widespread introduction of computer technology, the emergence of new multimedia applications require information to protect against unauthorized access to realtime no. To ensure a high degree of protection offered to use nonlinear algorithms for constructing on the basis of the additive and multiplicative operations. In order to increase the speed for disclosure of information in the possibility of using the index presentation elements extended Galois field. The transition to a low-speed indices allows us to reduce operation proclaim -ing the power to the multiplicative modulo operation on degrees of elements.

Keywords: security system, nonlinear encryption algorithms, elevated to the power of modulo indices

Одним из критериев жизнеспособности современного государства является наличие защищенного, динамически развивающегося информационного пространства, пронизывающего все сферы деятельности государства. Защита информации представляет собой комплекс мероприятий, направленных на предотвращение несанкционированной утечки, модификации и удаления информации. Основной задачей обеспечения безопасности информационных компьютерных систем является защита информации и ограничение круга лиц, имеющих доступ к этой критичной информации.

С появлением новых средств мультимедиа и сетей с высокой пропускной способностью, обеспечивающих передачу мультимедийных данных большого объема, в современных вычислительных системах начинают применяться технологии, осуществляющие обработку и передачу больших массивов. Для обеспечения интерактивного обмена данными такие системы должны работать в реальном масштабе времени. Поэтому процедура обеспечения конфиденциальности и целостности информации должна реализоваться с использованием поточных алгоритмов шифрования. Для реализации эффективных методов поточного шифрования данных требуется разработка псевдослучайных последовательностей (ПСП).

Несмотря на то, что шифр, основанный на сложении потока псевдослучайных битов с битами исходного текста по модулю 2 теоретически нераспознаваем, такая система шифрования не отличается стойкостью и может быть раскрыта при наличии определенного количества символов исходного и шифрованного текста. Если известно $2k$ символов открытого и зашифрованного текста, где k – степень порождающего полинома, то с помощью системы уравнений можно раскрыть структуру генератора ПСП.

Решить данную проблему можно за счет нелинейного шифрования потока данных, которое можно реализовать с использованием операций сложения, умножения и возведения в степень элементов конечного поля, а также их комбинаций [1-4,10].

При реализации нелинейного шифрования псевдослучайная последовательность элементов расширенного поля Галуа получается с помощью регистра сдвига, генерирующего двоичную ПСП. Одновре-

менно с регистра сдвига могут сниматься несколько ПСП элементов поля Галуа $\{x, y, \ldots\}$. Данные символы могут сниматься с разных ячеек генератора двоичного ПСП. При этом такая последовательность не будет циклически сдвинутой относительно других псевдослучайных последовательностей элементов.

Рассмотрим нелинейное шифрование потока данных с операцией возведения в степень элемента конечного поля. Данная операция является одной из наиболее употребляемых криптографических процедур. Выбор данной процедуры обусловлен тем, что она нелинейна и для определения исходного текста по символам зашифрованного текста требуется вычисление дискретного логарифма [5-8].

Для шифрования поступающих на вход символов исходного текста, представленного в полиномиальной форме $\alpha(z)=\{\alpha_j(z)\}$ вычисляются значения символов псевдослучайной последовательности конечного поля $x=\{x_j\}$ на различных текстах работы регистра сдвига $j = 0,1,2,\ldots$ и определяются символы шифрованного сообщения

$$\alpha(z)^x \equiv \beta(z) \bmod \pi(z). \qquad (1)$$

Для восстановления исходного значения α из получаемого значения β по модулю p используется уравнение вида:

$$\sqrt[x]{\beta} \equiv \alpha(\bmod\, p). \qquad (2)$$

Однако операция возведения элемента поля в степень трудоемка и требует больших затрат машинного времени. Для сокращения времени выполнения этой процедуры целесообразно перейти к обработке индексов элементов полей Галуа *GF(q),* где $q = p^v$, p – простое число, порожденных неприводимым полиномом $\pi(z)$. В этом случае операция умножения

$$\alpha^i \alpha^j = \alpha^k \bmod \pi(z) \qquad (1)$$

можно свести к аддитивной операции

$$k = i + j \bmod(q-1). \qquad (2)$$

Операция деления по модулю

$$\alpha^i / \alpha^j = \alpha^k \bmod \pi(z) \qquad (3)$$

может быть представлена в виде

$$k = i - j \bmod(q-1). \qquad (4)$$

При этом процедура возведения в степень по модулю

$$(\alpha^i)^j = \alpha^k \bmod \pi(z) \qquad (5)$$

представляется к виду

$$k = ij \bmod(q-1). \qquad (6)$$

Операция вычисления дискретного логарифма

$$\sqrt[j]{\alpha^k} = \alpha^i \bmod \pi(z) \qquad (7)$$

сводится к мультипликативной процедуре

$$i = ij^{-1} \bmod(q-1). \qquad (8)$$

Анализ данных выражений показывает, что степенное или индексное представления ненулевых элементов удобны для выполнения мультипликативных операций и им обратных. Переход к индексному представлению ненулевых элементов расширенного поля Галуа $GF(q)$ позволяет свести низкоскоростную операцию возведения в степень к операции умножения степеней первообразного элемента α по модулю $q-1$ [1-7].

В работах [1, 3, 4] показана структура шифратора для нелинейно шифрования потока данных с операцией возведения в степень элементов открытого текста. Символы исходного текста разбивается на блоки длиной v разрядов и в полиномиальной форме

$$a(z) = \sum_{n=0}^{v=1} a_n z^n = a_{n-1} z^{n-1} + \ldots + a_1 z^1 + a_0 z^0, \qquad (9)$$

поступает на вход устройства вычисления индекса по модулю. Данное устройство реализует следующую процедуру

$$l = \underset{\alpha}{ind}\, a(z) \bmod \pi(z), \qquad (10)$$

где $\alpha=z$; $l = l_{n-1} l_{n-2} \ldots l_1 l_0$ – показатель степени элемента поля.

Полученное значение показателя степени l подается на первый вход умножителя по модулю 2^v-1. На второй вход поступает ключ k (блок двоичных символов длиной v)

$$k(z) = \sum_{n=0}^{v=1} k_n z^n = k_{n-1} z^{n-1} + \ldots + k_1 z^1 + k_0 z^0. \qquad (11)$$

С выхода устройства снимается результат

$$\gamma = lk \bmod(2^v - 1). \qquad (12)$$

Данный результат поступает на вход преобразователя «индекс-элемент поля», где реализуется выражение

$$\beta(x) \equiv \alpha^\gamma \bmod \pi(x), \qquad (13)$$

где $\beta(x)$ – зашифрованное сообщение.

В результате получается зашифрованное сообщение, которое поступает в канал связи.

Очевидно, что эффективность процедур нелинейного шифрования данных во многом определяется эффективностью алгоритма вычисления индекса элемента поля $GF(2^v)$. В работах [6] представлена структура устройства, осуществляющего вычисление индекса элемента поля Галуа по модулю.

Рассмотрим алгоритм расшифрования сообщения с использованием нелинейных операций возведения в степень по модулю. Данный алгоритм приведен в работах [2-5, 9]. Зашифрованное сообщение $\beta(z)$ (длиной v двоичных разрядов) поступает на вход устройства вычисления индекса элемента поля $GF(2^v)$. С выхода данного устройства снимается

$$\gamma = \gamma_{v-1} z^{v-1} + \gamma_{n-2} z^{n-2} + \ldots + \gamma_1 z^1 + \gamma_0 z^0 . \quad (14)$$

Для определения значения степени l необходимо операцию деления по модулю свести к мультипликативной операции с обратным элементом

$$l = \gamma / k \bmod 2^v - 1 = \gamma \cdot k^{-1} \bmod 2^v - 1, \quad (15)$$

где $k^{-1} \bmod (2^v - 1)$ – обратный мультипликативный элемент элементу k по модулю $(2^v–1)$.

Ключ k подается на вход устройства вычисления мультипликативного обратного элемента по модулю $(2^v–1)$, с выхода которого снимается значение

$$k^{-1}(z) = \sum_{n=0}^{v=1} k_n^{-1} z^n = k_{n-1}^{-1} z^{n-1} + \ldots + k_1^{-1} z^1 + k_0^{-1} z^0 . \quad (16)$$

Значения γ и $k^{-1} \bmod (2^v - 1)$ в двоичном коде поступают на вход умножителя по модулю $(2^v\text{-}1)$, с выхода которого снимается значение

$$l = l_{v-1} z^{v-1} + l_{n-2} z^{n-2} + \ldots + l_1 z^1 + l_0 z^0 . \quad (17)$$

Данный результат, представляющий собой двоичный блок длиной v разрядов, поступает на вход преобразователя «индекс-элемент поля», где реализуется выражение

$$\alpha^k(z) \equiv a(z) \bmod \pi(z), \quad (18)$$

где $\alpha = z$ – первообразный элемент поля $GF(2^v)$, порождаемый многочленом $\pi(z)$.

В результате данных преобразований получается открытое сообщение $a(z)$, которое поступает к пользователю. В работах [6-8] показана структура устройства, осуществляющего вычисление элемента поля Галуа по его индексу.

Переход к обработке индексов элементов полей Галуа позволило сократить время выполнения мультипликативных арифметических операций по модулю. Известно, что процедуры выполнения мультипликативных арифметических операций по модулю требуют значительных временных затрат. Так, чтобы вычислить степень m^n, где m – элемент некоторого кольца, а n – натуральное число, достаточно выполнить не более $2[\log_2 n]$ умножений. Тогда

$$T_1 = 2[\log_2 n] T_{\text{умн}}. \quad (19)$$

Комбинационные умножители характеризуются высоким быстродействием, которое определяется лишь задержками сигналов в логических элементах. В этом случае

$$T_{\text{умн}} = m T_{\Sigma}. \quad (20)$$

Сумматор, обладающий минимальной задержкой распространения сигнала, содержит три логических ступени, следовательно, $T_{\Sigma} = 3t_{\text{зд.р.}}$. Тогда

$$T_1 = 6mt_{\text{зд.р}} [\log_2 n]. \quad (21)$$

Рассмотрим процедуру возведения в степень с использованием индексов. Проведя анализ структуры шифратора, приведенных в работах [], можно сделать вывод, что время на выполнение операции нелинейного шифрования определяется

$$T_2 = T_{\text{эл-инд}} + T_{\text{умн}}^{\text{мод}} + T_{\text{инд-эл}}. \quad (22)$$

Время выполнения операции перевода «элемент-индекс» определяется

$$T_{\text{эл-инд}} = T_{\text{НЕ}} + T_{\text{И}} + T_{CD} = t_{\text{зд.р}} + t_{\text{зд.р}} + 3t_{\text{зд.р}} = 5t_{\text{зд.р.}} \quad (23)$$

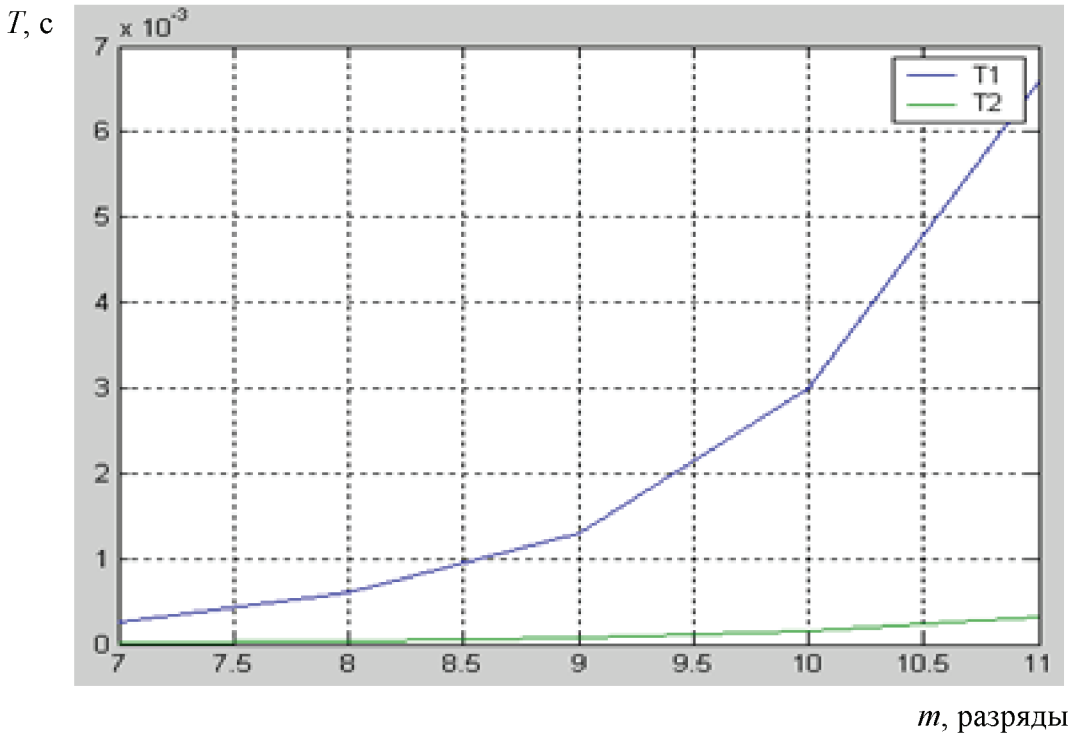
Время выполнения операции перевода «индекс-элемент» определяется из условия

$$T_{\text{эл-инд}} = T_{\text{инд-эл}} = 5t_{\text{зд.р}}. \quad (24)$$

Положим, что $T_{\text{умн}}^{\text{мод}} = T_{\text{умн}} = 3mt_{\text{зд. р.}}$ Тогда время возведение в степень равно

$$T_2 = 5t_{\text{зд. р}} + 3mt_{\text{зд. р}} + 5t_{\text{зд. р}} = (3m + 10)t_{\text{зд. р.}} \quad (25)$$

На рисунке приведена сравнительная характеристика времени выполнения нелинейного шифрования без использования индексного представления (кривая Т1) и с использованием индексов (кривая Т2).



Сравнительная характеристика времени выполнения нелинейного шифрования

Полученные результаты свидетельствуют о том, что применение индексов позволил повысить быстродействие выполнения нелинейного шифрования не мене чем в 2,6 раза. При чем при увеличении разрядности обрабатываемых данных возрастает выигрыш в производительности систем.

Проведенные исследования показали, что применение в нелинейных системах шифрования индексного представления элементов расширенных полей Галуа позволяет реализовать адаптивные средства защиты информации, для которых наличие исходного и шифрованного текста не снижает криптостойкость системы. При этом использование индексирования позволяет обеспечить защиту информации от НСД в интерактивных системах передачи и обработки мультимедийных данных в реальном масштабе времени.

Список литературы

1. Дагаева О.И., Калмыков И.А., Кихтенко О.А., Барильская А.В. Криптографическая система на базе непозиционных полиномиальных алгебраических структур // Вестник Северо-Кавказского федерального университета. 2010. № 2. С. 51-57

2. Дагаева О.И., Калмыков И.А., Разработка псевдослучайной функции повышенной эффективности // Известия Южного федерального университета. Технические науки. 2011. Т.125. № 12. С.160-169.

3. Калмыков И.А., Стрекалов Ю.А., Щелкунова Ю.О., Кихтенко О. А., Барильская А.В. Технология нелинейного шифрования данных в высокоскоростных сетях связи // Инфокоммуникационные технологии. 2010. Т.8. № 2. С. 14-22

4. Калмыков И.А. Чипига А.А. Алгоритм обеспечения информационной скрытности для адаптивных средств передачи информации // Инфокоммуникационные технологии. Самара. – 2007. – Т.5. № 2. – С. 159-162.

5. Калмыков И.А., Чипига А.Ф., Барильская А.В., Кихтенко О. А. Криптографическая защита данных в информационных технологиях на базе непозиционных полиномиальных систем // Известия Южного федерального университета. Технические науки. 2009. Т.100. № 11. С.210-220.

6. Калмыков И.А., Барильская А.В., Кихтенко О. А. Устройство для вычисления индекса элементов поля Галуа по модулю// Современные наукоемкие технологии. 2007. № 11. С.76-78.

7. Калмыков И.А., Барильская А.В., Кихтенко О. А. Разработка математической модели криптографической защиты информации, функционирующей в полиномиальной системы классов вычетов// Информационные системы и технологии. 2010. № 4. С.138-145.

8. Лободин М.В., Калмыков И.А. Разработка алгоритма обратного преобразования для непозиционных для адаптивных средств защиты информации // Инфокоммуникационные технологии. Самара. – 2007. – Т.5. № 2. – С. 156-159.

9. Тимошенко Л.И., Калмыков И.А., Хайватов А.Б., Гахов В.Р. Применение полиномиальной системы классов вычетов для повышения скорости функционирования спецпроцессора адаптивных средств защиты информации // Успехи современного естествознания. 2007. № 5. С.76.

10. Чипига А.Ф., Калмыков И.А., Яковлева Е.М., Калмыков М.И. Применение полиномиальной системе классов вычетов в схеме разделения секрета // Информационное противодействие угрозам терроризма. 2012. № 19. С.45-49.