УДК 681.3

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ФУНКЦИОНИРУЮЩЕЙ В ПОЛИНОМИАЛЬНОЙ СИСТЕМЕ КЛАССОВ ВЫЧЕТОВ

Зюзякин Г.И., Калмыков М.И., Петрова Е.В.

*Федеральное государственное автономное образовательное учреждение
высшего профессионального образования «Северо-Кавказский федеральный университет»,
Ставрополь, e-mail: kia762@yandex.ru*

В интерактивных системах передачи и обработки мультимедийных данных в реальном масштабе времени возникает задача защиты информации большого объема. Степень эффективности работы таких систем защиты данных от несанкционированного доступа во многом зависит от выбранной математической модели. В работе представлена математическая модель, построенная на основе полиномиальной системы классов вычетов. Использование непозиционных систем счисления позволяет повысить скорость выполнения арифметических операций по модулю. Кроме того, на основе применения избыточных полиномиальных кодов класса вычетов может быть построена система, позволяющая обнаруживать и корректировать ошибки, которые возникают в процессе передачи и обработки данных. Показана возможность применения данных при реализации схемы разделения секрета между пользователями.

Ключевые слова: математическая модель, система защиты информации от несанкционированного доступа, полиномиальная система классов вычетов, схема разделения секрета.

MATHEMATICAL MODEL OF INFORMATION SYSTEMS, OPERATES IN A POLYNOMIAL SYSTEM OF RESIDUE CLASS

Zyuziyakin G.I., Kalmykov M.I., Petrova E.V.

*Federal state Autonomous educational institution higher professional education
«North-Caucasian federal university», Stavropol, e-mail: kia762@yandex.ru*

In the interactive data transmission and processing of the multimedia data in real time, the problem arises of a large volume of information protection. The effectiveness of such systems to protect data from unauthorized access largely depends on the mathematical model. A mathematical model constructed on the basis of a polynomial system of residue classes. Using nonpositional value systems can improve the speed performance of modulo arithmetic. In addition, based on the use of redundant residue polynomial codes class can be built a system that allows to detect and correct errors that occur during transmission and processing. Shows the possibility of the use of data in the implementation of secret sharing schemes between users.

Keywords: mathematical model, the system of information protection against unauthorized access, polynomial system of residue classes, secret sharing scheme

Введение

В современном обществе защита информации представляет собой комплекс мероприятий, направленных на предотвращение несанкционированной утечки, модификации и удаления информации, осуществляемых с применением технических, в том числе и программных, средств. Основной из основных задач обеспечения безопасности информационных компьютерных систем является защита информации от несанкционированного доступа (НСД) и ограничение круга лиц, имеющих доступ к этой критичной информации. Поэтому разработка математической модели системы защиты информации позволяющей зашифровывать поток данных в реальном масштабе времени является актуальной.

Основная часть

Развитие вычислительной техники, появление новых информационных техноло-

гий, обеспечивающих обработку и передачу больших объемов данных, требуют от современных систем защиты информации от НСД высокой производительности. В настоящее время этому требованию отвечают системы поточного шифрования [1,2]. Считается, что шифр, основанный на сложении потока псевдослучайных битов, полученных с помощью линейного регистра сдвига с обратной связью, с битами исходного текста по модулю два, в общем случае теоретически нераспознаваем. Однако такая система шифрования не отличается стойкостью и может быть мгновенно раскрыта при наличии определенного количества символов исходного и зашифрованного текста. Уязвимость системы к атакам на основе исходных и подобранных текстов обусловлено тем, что при битовом шифровании потока данных сложение символов по модулю два является единственным способом построения обратимой функции шифрования [2].

В настоящее время одним из перспективных направлений шифрования потока данных является использование математического аппарата расширенных полей Галуа $GF(p^v)$. Системы шифрования, использующие поля Галуа $GF(p^v)$, обладают более широкими возможностями по реализации различных криптографических функций обеспечения конфиденциальности и целостности информации. Применение в таких системах основных аддитивных и мультипликативных операций, к которым можно отнести сложение по модулю, умножение по модулю, возведение в степень по модулю, и их различных комбинаций позволит повысить уровень защиты информации [3-9]. Наиболее трудоемкой операцией, реализуемой в конечных полях Галуа, является операция возведения в степень по модулю. Это, конечно, приводит к увеличению времени шифрования и дешифрования, но позволяет обеспечить требуемый уровень криптографической защиты от НСД.

Рассмотрим процедуру шифрования потока данных с операцией возведения в степень символов поля Галуа $GF(p^v)$. В данной системе выбирается неприводимый полином $\pi(z)$ $\deg \pi(z) = v$, порождающий все элементы мультипликативной группы данного поля. Входная последовательность разбивается на блоки по v символов в каждом. Такой блок в полиномиальной форме имеет вид

$$A(z) = a_{v-1}z^{v-1} + a_{v-2}z^{v-2} + \dots + a_2z^2 + a_1z^1 + a_0z^0, \quad (1)$$

где $a_{v-1}, a_{v-2}, \dots, a_2, a_1, a_0$ – двоичный код блока, $a_i \in \{0, 1\}$, $i = 0, 1, \dots, v-1$.

Этот блок считается элементом расширенного поля Галуа $GF(p^v)$. Для реализации процедуры шифрования на основе возведения в степень вычисляются значения псевдослучайной последовательности (ПСП) X , значения которой снимаются с разных v выходов линий задержки генератора. Тогда псевдослучайная последовательность можно представить в виде последовательности

$$X = \{X_0, X_1, X_2, \dots\}. \quad (2)$$

В этом случае процедура шифрования определяется равенством

$$\beta_i = A_i^{X_i}(z) \bmod \pi(z) \quad (3)$$

где β_i – i -й блок зашифрованного сообщения; $i = 0, 1, \dots$

Повысить скорость шифрования можно за счет перехода и индексному представлению элементов полей Галуа, что позволяет свести низкоскоростную операцию возведения в степень по модулю к аддитивной операции [1-4]. В этом случае блок исходных данных в двоичном коде подается на входы устройства вычисления индекса, реализующего

$$l_j = \text{ind } A(z) \bmod \pi(z) = \log_2 A(z) \quad (4)$$

где l – индекс блока $A(z)$; α – порождающий элемент мультипликативной группы поля Галуа $GF(p^v)$.

Вычисленный l_j индекс в виде параллельного кода подается на первые входы умножителя по модулю p^v-1 . На вторые входы этого умножителя поступает параллельный двоичный код ключа x_j , снятого с выходов генератора ПСП. Умножитель по модулю p^v-1 реализует модульную операцию

$$\gamma_j = l_j x_j \bmod p^v - 1. \quad (5)$$

Полученный результат γ_j представляет индекс элемента поля $GF(p^v)$, который является результатом зашифрованного блока A_j согласно выражения (3). Он в параллельном виде подается на вход преобразователя «индекс – элемент поля»

$$\beta_j = \alpha^{\gamma_j} \bmod \pi(z) \quad (6)$$

В результате зашифрованный блок данных β_j , передается на приемную сторону.

Для дешифрования сообщения на приемной стороне решается обратная задача выражению (3). В этом случае j -й блок открытого сообщения $j = 0, 1, 2, \dots$ вычисляется согласно

$$x_j \sqrt[\gamma_j]{\beta_j(z)} \equiv A_j(z) \bmod \pi(z). \quad (7)$$

Применение полиномиальной системы классов вычетов (ПСКВ) позволяет повысить степень защиты информации от НСД, а также скорость закрытия информации [5]. Если взять для выработки генератор ПСП, в котором число линий задержек значительно превосходит степень $\pi(z)$, то есть $n \gg \deg \pi(z)$, то число символов, которые можно использовать как показатели степени равно

$$N_{\text{псп}} \gg \deg \pi(z)!(C_n^{\deg \pi(z)}). \quad (8)$$

Так уже при $n = 255$ и седьмой степени полинома число возможных ПСП, снимаемых параллельно с выходов различных линий задержки, превысит число 1018, что свидетельствует о высокой степени криптографической защиты.

Кроме того, применение полиномиальной системы классов вычетов позволяет обеспечить защиту информации от возникающих ошибок в процессе передачи и обработки данных. В работах [6-9] представлены различные алгоритмы, позволяющие обнаруживать и корректировать ошибки с использованием избыточных кодов ПСКВ. Для этого необходимо вычислитель соответствующую позиционную характеристику, величина которой позволит однозначно определить местоположение ошибки и ее глубину. Проведенный анализ работ [6-9] показал, что наиболее перспективным методом коррекции ошибок выступает спектральный метод, аппаратная реализация которого приведена в работе [9].

Кроме того, рассматривая вопросы разработки математической модели системы защиты информации от НСД, функционирующей в ПСКВ, нельзя не отметить возможность использования данных кодов для построения схемы разделения секрета [4,10]. Построение такой схемы вызвано необходимостью организации безопасной связи внутри групп абонентов с динамически меняющимся составом. Применение ПСКВ позволяет решить данную задачу на основе усовершенствования модулярной пороговой схемы (m, n) разделения секрета. Для этого выбирается полином $p_i(z)$, степень которого превышает полиномиальную форму секрета $M(z)$.

Затем выбираются неприводимые полиномы $p_i(z)$, удовлетворяющие условию

$$\deg p_i(z) \leq \deg p_l(z) \quad i = 1, 2, \dots, n, \quad (9)$$

которые упорядочены по возрастанию степеней

$$\begin{aligned} \deg p_1(z) &\leq \deg p_2(z) \leq \\ &\leq \deg p_3(z) \leq \dots \leq \deg p_n(z) \quad . \quad (10) \end{aligned}$$

Для создания (m, n) схемы проверяется выполнение условия

$$\begin{aligned} \deg(p_1(z) p_2(z) \dots p_m(z)) &> \\ &> \deg(p_1(z) p_{n-m+2} \dots p_n(z)) \quad . \quad (11) \end{aligned}$$

Чтобы определить доли секрета и их распределить между абонентами группы, выбирается полином $r(z)$ и вычисляется значение

$$M^*(z) = M(z) + r(z) p_l(z). \quad (12)$$

В качестве долей для каждого пользователя выступают остатки

$$M_i^*(z) \equiv M^*(z) \pmod{p_l(z)}. \quad (13)$$

Используя китайскую теорему об остатках, m пользователей способны восстановить значение $M^*(z)$, а затем, зная $r(z)$ и $p_l(z)$, определить секрет $M(z)$. При этом группа из $m-1$ абонентов не способна будет получить значение $M(z)$. Для эффективной работы схемы разделения секрета в ПСКВ необходимо вычислить предельное значение полинома $r(z)$, которое позволило бы при меньших временных затратах вычислить $M^*(z)$, и найти значение $M(z)$.

Рассмотрим пороговую схему разделения секрета, функционирующую в полиномиальной системе классов вычетов. Если в (m, n) модулярной полиномиальной пороговой схеме, в которой справедливо

$$\begin{aligned} \deg p_1(z) &\leq \deg p_2(z) \leq \\ \deg p_1(z) &\leq \deg p_2(z) \leq \dots \leq \deg p_n(z) \quad , \quad (14) \end{aligned}$$

имеет место условие

$$\deg r(z) < \deg(P(z)/p_l(z)) \quad , \quad (15)$$

где $P(z) = \prod_{i=1}^n p_i(z)$ – полный диапазон,

то такая пороговая схема обеспечивает восстановление секрета $M(z)$ для любого набора m пользователей группы, состоящей из n абонентов.

Проведенные исследования показали, что использование полиномиальной системы классов вычетов в схеме разделения секрета позволяет в 2 раза сократить размер вспомогательного полинома $r(z)$ при сохранении уровня защиты от НСД при использовании уже 11 разрядных оснований ПСКВ. При чем при увеличении разрядности оснований ПСКВ данных возрастает выигрыш в системе разделения секрета.

Выводы

В работе показано, что эффективность работы системы защиты информации от НСД во многом зависит от математического аппарата,

положенного в основу ее работы. Применение в математической модели ПСКВ в нелинейных системах шифрования позволяет не только повысить скорость шифрования за счет применения индексного представления элементов расширенных полей Галуа, но и осуществлять процедуры поиска и коррекции ошибок, которые возникают в процессе передачи и обработки закрытых данных.

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., Петлеванный С.В., Сагдеев А.К., Емарлукова Я.В. Устройство для преобразования числа из полиномиальной системы классов вычетов в позиционный код с коррекцией ошибки // Патент России № 2309535. 31.03.2006. Бюл. № 30 от 27.10.2007.
7. Калмыков И.А. Устройство для коррекции ошибок в полиномиальной системе классов вычетов с использованием псевдоортогональных полиномов // Патент России № 2294529. 05.05.2005.
8. Калмыков И.А., Гахов В.Р., Емарлукова Я.В. Устройство обнаружения и коррекции ошибок в кодах полиномиальной системы классов вычетов // Патент России № 2300801. 30.06.2005.
9. Чипига А.А., Калмыков И.А., Лободин М.В. Устройство спектрального обнаружения и коррекции в кодах полиномиальной системы классов вычетов // Патент России № 2301441. 01.08.2005.
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.