СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ МОДУЛЯРНОЙ СИСТЕМЫ СЧИСЛЕНИЯ

Калмыков И.А., Науменко Д.О., Березкина М.В., Макарова А.В.,
Калмыков М.И.
Северо-Кавказский федеральный университет.
Институт информационных технологий и телекоммуникаций
г. Ставрополь, Россия

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 [1,2]. Основной задачей обеспечения безопасности информационных компьютерных систем является защита информации и ограничение круга лиц, имеющих доступ к этой критичной информации.

Развитие вычислительной техники, появление новых информационных технологий, 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]. Несмотря на то, 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, сама система шифрования не отличается стойкостью и может быть мгновенно раскрыта при наличии определенного количества символов исходного и шифрованного 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].

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 (сложение по модулю, умножение по модулю, возведение в степень по модулю) и их различных комбинаций позволит повысить уровень защиты информации [2,3]. 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 $\pi(z), \deg\pi(z) = \nu$, порождающий все элементы мультипликативной группы данного поля. Входная последовательность разбивается на блоки по ν символов в каждом. Такой блок в полиномиальной форме имеет вид

$$A(z) = a_{\nu-1}z^{\nu-1} + a_{\nu-2}z^{\nu-2} + a_{\nu-3}z^{\nu-3} + ... + a_2z^2 + a_1z^1 + a_0z^0, \qquad (1)$$

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

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 ν выходов линий задержки генератора. Тогда ПСП

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

Процедура зашифрования определяется равенством

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

где β_i – i-й блок зашифрованного сообщения; i = 0, 1, ….

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. В этом слу-

чае блок исходных данных в двоичном коде подается на входы устройства вычисления индекса, реализующего

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

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»

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

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… вычисляется согласно

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

Применение ПСКВ позволяет повысить степень защиты информации от НСД. Если взять для выработки генератор ПСП, в котором число линий задержек значительно превосходит степень $\pi(z)$, то есть $n >> \deg \pi(z)$, то число символов, которые можно использовать как показатели степени равно

$$N_{ПСП} >> \deg \pi(z)!(C_n^{\deg \pi(z)}). \quad (8)$$

Так уже при n = 255 и седьмой степени полинома $\pi(z)$ число возможных ПСП, снимаемых параллельно с выходов различных линий задержки, превысит число 10^{18}, что свидетельствует о высокой степени криптографической защиты.

Рассматривая вопросы разработки систем защиты информации от НСД, функционирующей в ПСПВ, нельзя не отметить необходимость организации безопасной связи внутри групп абонентов с динамически меняющимся составом. Решить данную задачу возможно на основе разработки пороговой схемы (m, n) разделения секрета с использованием ПСКВ. Для этого выбирается полином $p_l(z)$, степень которого превышает полиномиальную форму секрета M(z). Затем выбираются неприводимые полиномы $p_i(z)$, удовлетворяющие условию

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

которые упорядочены по возрастанию степеней

$$\deg p_1(z) \le \deg p_2(z) \le \deg p_3(z) \le ... \le \deg p_n(z). \quad (10)$$

Для создания (m, n) схемы проверяется выполнение условия

$$\deg(p_1(z)p_2(z)...p_m(z)) > \deg(p_l(z)p_{n-m+2}...p_n(z)). \quad (11)$$

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

$$M_i^*(z) \equiv M^*(z) \bmod p_l(z). \quad (13)$$

Используя китайскую теорему об остатках, m пользователей способны восстановить значение, 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 была доказана теорема, определяющее предельное значение полинома r(z), которое позволило бы при меньших временных затратах вычислить M*(z), а также найти значение M(z).

ТЕОРЕМА.

Если в (m, n) модулярной полиномиальной пороговой схеме, в которой справедливо $\deg p_1(z) \le \deg p_2(z) \le \deg p_3(z) \le ... \le \deg p_n(z)$, имеет место

$$\deg r(z) < \deg(P(z)/p_l(z)), \quad (17)$$

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.

Литература:

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / М.: − ТРИУМФ, 2003. – 816 с.
2. Иванов М.А., Чугунов И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.: КУДИЗ-ОБРАЗ, - 2003. – 240 с.
3. Х.К.А.ван Тилборг. Основы Криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2007. – 346 с.
4. Калмыков И.А., Чипига, А.А. Алгоритм обеспечения информационной скрытности для адаптивных средств передачи информации // Инфокоммуникационные технологии: №3. − 2007. − С. 159-162.