УДК 004.056

Касумов В.А., д.т.н.,
orcid.org/0000-0003-3192-4225,
Маммадов Дж.И., к.т.н.,

МЕТОД ШИФРОВАНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ ОСНОВАННЫЙ НА LSFR

Азербайджанский Технический Университет

gasumov@yahoo.com
cabir_m@mail.ru

Введение

Для защиты конфиденциальности информации в процесс обмена, широко используются методы шифрования гаммированием. Суть данного метода, в основном, заключается в процессе изменения единиц шифруемой информации путем смешивания случайными числами (гаммами), образованными в определенном порядке.

Основная сложность метода шифрования гаммированием заключается в том, что гаммы должны быть генерированы непрерывно и без повторений [1]. В качестве гамм в некоторых случаях используются комбинации последовательностей генерируемых случайных битов. Уже много лет для получения последовательности случайных битов используется эффективный метод – регистры сдвига с линейной обратной связью (Linear Feedback Shift Register – LFSR). Были созданы многочисленные алгоритмы для получения псевдослучайных чисел с помощью LFSR и работы в этом направлении не утратили своей актуальности и в настоящее время. Большая часть работ в данной области является конфиденциальной и многие системы шифрования, построенные на базе LFSR, широко используются в военной области [2].

По мнению исследователей, несмотря на наличие большого количества примеров взлома генераторов случайных бит, построенных на базе регистров сдвига, интенсивность работ в данном направлении нисколько не снижается [2-4]. Это можно обосновать тем, что из-за выполнения над регистрами только простых операций сдвига и вычитания, построенные на них алгоритмы выполняются с высокой скоростью, генерируемые случайные последовательности битов имеют большую периодичность и хорошие статистические характеристики.

Использование в криптосистеме одновременно нескольких LFSR и динамическое изменение кода, записанного в регистр в качестве ключа, является одним из факторов, способствующих повышению криптостойкости систем шифрования, построенных на LFSR [2,4-6]. В работе нами была рассмотрена задача повышения эффективности системы шифрования методом синхронного использования больше регистров сдвига с линейной обратной связью, количество которых определяются количеством битов, составляющих символы шифруемой информации, и периодического изменения содержимого регистров.

Теоретические сведения

Использование LFSR для генерации случайных бит изучено достаточно широко. Суть метода заключается в том, что последовательность битов любого числа, записанного в регистр, периодически сдвигается вправо и при этом последовательность битов, взятых из крайних (последних) ячеек регистра на каждом такте, принимается в качестве псевдослучайной последовательности битов. Основным свойством, обеспечивающим случайность в регистре, является то, что он имеет функцию линейной обратной связи. Для линейных регистров эта функция состоит из операции XOR (exclusive OR), выполняемой над некоторыми битами регистра (которые иногда называют выходными битами).

На рис. 1 приведена функциональная схема, отражающая принцип работы n-разрядного LFSR. Регистр сдвига работает в дискретные моменты времени, и на каждом такте (каждый момент времени) выполняются следующие операции [6]:

1. содержимое ячейки S_0 "вынимается" из регистра сдвигом и формируется следующий элемент последовательности битов генерируемой псевдослучайной цифры;

2. содержимое ячейки S_i переносится в ячейку S_{i-1}, где i=0, 1, 2,..., n-1;

3. в пустую (освобожденную) ячейку S_{i-1} записывается бит обратной связи. Этот бит формируется умножением битов, содержащихся в ячейках S_0, S_1,..., S_{n-1} соответственно на коэффициенты a_0, a_1,..., a_{n-1}, и суммированием результатов по модулю 2. Здесь если какой-либо из коэффициентов a_0, a_1, ..., a_{n-1} равен 0, то соответствующий этому коэффициенту сумматор по модулю (изображенный на рисунке знаком плюс) удаляется из цепи обратной связи.

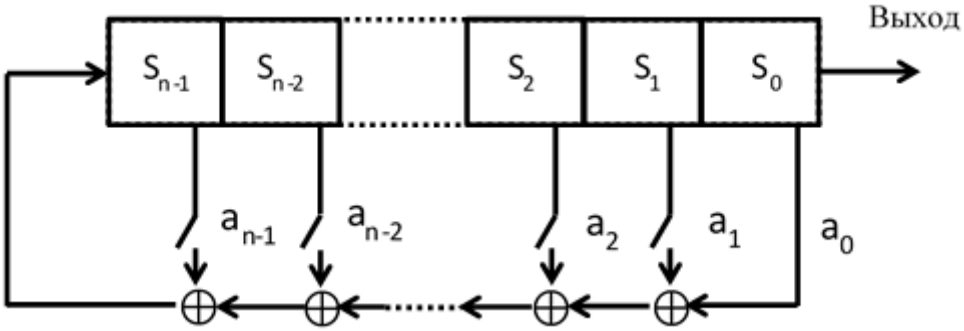

Рис. 1. Функциональная схема LSFR

Отметим, что для эффективной работы систем шифрования информации гаммированием количество битов в генерируемых гаммах не должно быть меньше, чем количества битов в шифруемых символах. В процессе генерации гамм на основе LFSR для "покрытия" (шифрования) гаммами однобайтных символов необходимо последовательно генерировать по 8 битов. После этого выполняется операция генерации новой гаммы и процесс продолжается циклически. Однако такое использование LFSR не выгодно с точки зрения быстродействия алгоритма. Так, здесь для генерации гаммы длиной в один байт используется не менее 8 тактов. С целью увеличения скорости выполнения алгоритма в каждом такте в качестве гаммы можно использовать меньший (первый справа) байт из LFSR. Несмотря на то, что в этом случае будет обеспечена максимальная скорость, но между соседними гаммами будет достаточно большая зависимость, что может негативно влиять на криптостойкость системы в целом.

Предложенная система шифрования

Генерация ключей

Криптографический ключ, используемый в предложенном методе, имеет длину 256 бит и состоит из комбинации (конкатенации) составных частей $K=K_1K_2...K_8$, записанных соответственно в регистры сдвига K_i (i=1,2,...,8) длиной 32 бита. Величины K_i вычисляются следующим образом:

$$K_i = k_i^{'} \oplus t_i \qquad (1)$$

здесь, $k_i^{'}$ (i=1,2,...,8) – составные части сеансового ключа, доставляемого сторонам по заранее определенному порядку; t_i (i=1,2,...,8) – параметры, зависящие от времени; знак $\oplus$ означает операцию суммирования по модулю 2.

Отметим, что в предложенной системе параметр t_i вычисляется следующим образом: сначала 32-битный двоичный код системых часов присваивается параметру t_0 путем упорядочения в обратном порядке. После этого, для других

регистров коды t_i (i=2,3,...,8) получаются путем периодического сдвига вправо кода t_{i-1} на 4 бита.

Алгоритм шифрования

Предлагаемая система предназначена для шифрования текстовой информации, состоящей из символов, закодированных по стандарту ASCII. С этой целью для каждого бита гаммы используется один 32-битный LFSR, а для восьми битов используются 8 штук 32-битные LFSR (LFSR1-LFSR8). Функциональная схема системы приведена на рисунке 2. В схеме Rg1 – регистр, используемый для хранения двоичного кода шифруемого символа исходного текста, Rg2 – регистр, используемый для хранения двоичного кода зашифрованного символа, Z1-Z4 – группы элементов, выполняющие суммирование (исключающее ИЛИ) по модулю 2.

Согласно схеме, процесс шифрования текстовой информации осуществляется следующим образом:

1. в регистры LFSR1-LFSR8 записывается код ключа, состоящий из 8 частей (K=K1,K2,...,K8);
2. в регистр Rg1 записывается код (xi1-xi8), состоящий из 8 битов одного символа зашифрованного текста;
3. содержимое регистров LFSR1-LFSR8 сдвигается вправо на 1 бит;
4. биты 8-битного кода гаммы (gi1-gi8), полученные на выходе регистров LFSR1-LFSR8, суммируются по модулю 2 с соответствующими битами символа, записанного в регистр Rg1, с помощью элементов Z1;
5. 32-битные содержимые регистров LFSR1-LFSR8 суммируются по модулю 2 с помощью элементов Z2;
6. 32-битный код, полученный в пункте 5, разбивается на 4 части ($q_i^1 - q_i^4$) по 8 битов (1 байту), далее эти байты суммируются последовательно по модулю 2 с помощью группы элементов Z3, в результате которого получается 8-битный код;

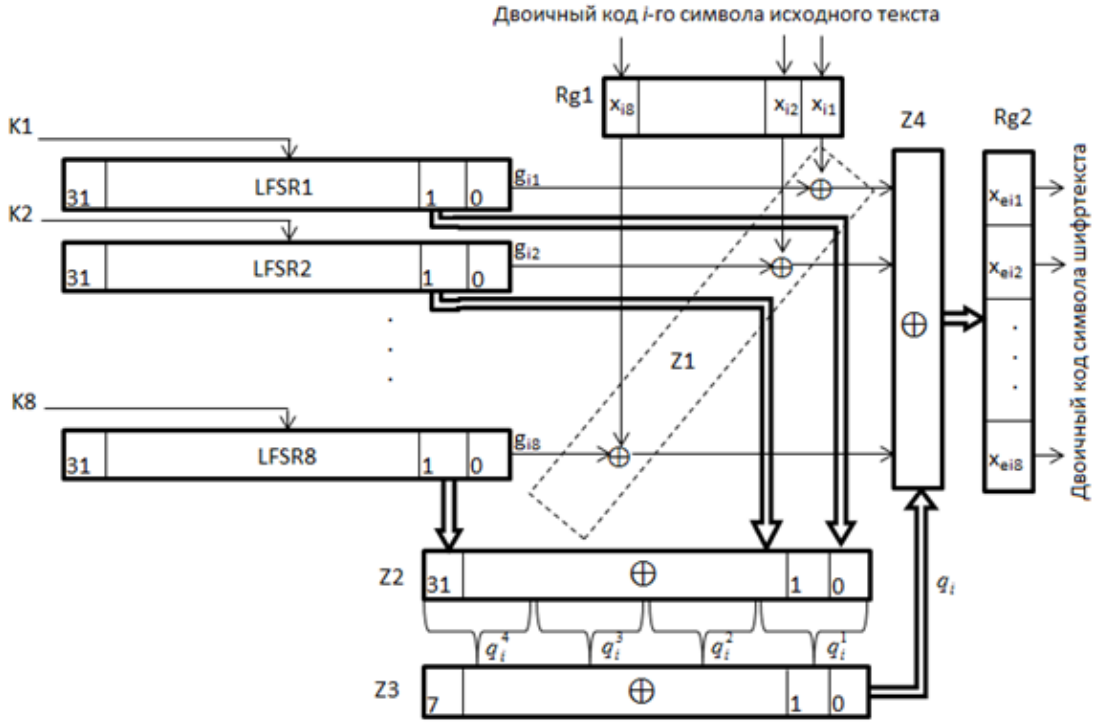

Рис 2. Функциональная схема предложенной системы шифрования

7. полученные на выходе элементов Z1 и Z3 два 8-битные коды суммируются по модулю 2 с помощью группы элементов Z4 и полученный результат (x_{ei1}-x_{ei8}) записывается в регистр Rg2 как

шифр-код, то есть зашифрованный код i-го символа исходно текста;

8. пункты 2-7 повторяются до тех пор, пока шифрование всех символов текста не будет завершено.

Предлагаемая система построена на 32-битных регистрах. Код ключа K регулярно меняется на основе выражения (1). Здесь для каждого LFSR коэффициенты обратной связи a_0, a_1,...,a_{n-1} определяются в различных комбинациях.

Отметим, что разрядность LFSR обычно выбирается в зависимости от задачи, для решения которой должна быть применена система. Считается целесообразным использовать LFSR большей разрядности в системах, требующих высокой криптостойкости. Так, с увеличением разрядности регистров увеличивается и общая длина криптографического ключа. Например, если регистры являются 32-разрядными (32 битными), то общая длина ключа в системе, состоящая из 8 регистров, будет $l=2^5*2^3=2^8=$ 256 бит, а если 64-разрядные, то будет $l=2^6*2^3=2^9=$ 512 бит, и при необходимости разрядность можно увеличить еще больше.

Предлагаемая система шифрования может быть реализована аппаратным, программным, а также аппаратно-программным способом. Преимущество аппаратного метода заключается в простоте его реализации и более высокой скорости выполнения. В системе, реализуемой аппаратным методом, процесс шифрования одного символа может быть выполнен всего за 1 такт. Здесь, повышая тактовую частоту до определенного предела, можно также увеличить скорость процесса шифрования в целом. Однако следует иметь в виду, что по мере увеличения разрядности в LFSR увеличивается и количество коэффициентов, используемых в обратной связи этих регистров, и время, затрачиваемое на формирование общего сигнала обратной связи, растет пропорционально этому числу. Например, предположим, что для обратной связи в 32-разрядном LFSR используется 5 коэффициентов (a_i, i=1,2,...,5). Если принять задержку сигнала на одном элементе XOR 3-4 *ns*, то сигнал обратной связи будет формироваться с задержкой 15-20 *ns*, проходя через 5 элементов XOR.

При использовании 64-разрядных LFSR, задержка сигнала будет в 2 раза больше, т.е. увеличение количества разрядов в 2 раза снижает общую скорость процесса как минимум в 2 раза. Несмотря на все это, с помощью определенных методов можно компенсировать снижение тактовой частоты за счет увеличения разрядности. Например, в качестве примера можно привести такой подход, как шифрование двух-трех или более символов исходного текста одновременно – в один такт и соответственно с этой целью увеличение количества LFSR.

Анализ результатов

Криптостойкость предлагаемой системы шифрования к атаке с применением грубой силы (“brute-force approach”), то есть к криптоанализу методом проверки всех возможных вариантов ключей достаточно высока. Так, в 32-битном варианте LFSR общая длина системного ключа равна 256 битам, а пространства ключа – 2256. Путем увеличения разрядности LFSR (на 512, 1024 и т. д.) область ключа также можно увеличить до необходимого уровня.

С точки зрения оценки времени выполнения процесса шифрования, можно отметить, что система обладает максимальным быстродействием. Таким образом, предлагаемая система реализована с помощью аппаратных средств и способна в ходе одного такта зашифровать один символ. Тем не менее, можно также увеличить скорость работы системы в несколько раз за счет параллельного шифрования нескольких символов путем увеличения количества LFSR.

Оценка криптостойкости системы с помощью анализа чувствительности к ключам и других методов криптоанализа являются задачей будущих исследований авторов.

Выводы

Для криптографической защиты текстовой информации предложена система шифрования на основе LFSR. Система, реализация которой предложена аппаратными средствами, имеет достаточно большое пространство ключей и позволяет за один такт зашифровать один символ текста. С небольшими изменениями предложенную систему также можно использовать для шифрования файлов другого типа.

Литература

1. *Касумов В.А.* Основы информационной безопасности. Учебник, Баку, 2009. – 340 с.

2. *Шнайер Б.* Практическая криптография, 2-е издание. – 610 с.

3. *Фергюсон Н., Шнайер Б.* Практическая криптография, 2005. – 424 с.

4. *Птицын Н.* Приложение теории детерминированного хаоса в криптографии. – М.: 2002. – 80 с.

5. *Маммадов Дж.И., Гасымова Н.Н., Искендерова Г.Дж.* Повышение эффективности применения последовательностей псевдослучайных чисел, основанных на детерминистическом хаосе. Баку, ВВША, Сборник Научных трудов, 2018. – № 1. – С. 67-71.

6. *Касумов В.А., Маммадов Дж.И., Акперов А.Р.* О методе шифрования на основе регистров сдвига с линейной обратной связью. Республиканская научно-техническая конференция по теме «Технологические аспекты Индустрия 4.0: интернет промышленности, киберфизические системы и интеллектуальные технологии». 26-27 ноября 2020. – С. 26-29.

Касумов В.А., Маммадов Дж.И.

МЕТОД ШИФРОВАНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ ОСНОВАННЫЙ НА LSFR

*Статья посвящена вопросам разработки LFSR основанного метода шифрования текстовой информации. Предлагается метод шифрования информации с использованием регистра сдвига с линейной обратной связью (Linear Feedback Shift Register – LFSR) и динамических ключей. Большой период и хорошая статистическая характеристика последовательности выработанной LFSR, выполняя при этом простые операции сдвига и сложения, обеспечивает высокую надежность и скорость процесса шифрования. В предложенной системе предполагается использовать несколько регистров одновременно, число которых определяется разрядностью шифруемого символа. Используемый криптографический ключ является соединением (конкатенацией) величин Ki (i=1,2,...,8), вводимых в сдвигающие регистры: K= K1K2...K8. А величины Ki вычисляются на основе составляющих частей сеансового ключа (i=1,2,...,8) и параметра системного времени. Имеется возможность расширения криптографического ключа посредством увеличения разрядности регистров. В системе с 32-разрядными регистрами, общая длина ключа составляет l=25*23=28= 256 бит, а с 64-разрядными – 512 бит. Предложенный метод может реализовываться аппаратно, программно и аппаратно-программной комбинацией. Максимальная скорость процесса достигается в системе с аппаратной реализацией, т.к., шифрование одного символа в такой системе выполняется всего за один такт. Имеется возможность увеличения скорости процесса также шифрованием несколько символов одновременно, используя с этой целью регистров в соответственном количестве. Устойчивость предложенной криптосистемы к атакам методом грубой силы достаточно высока, т.к. при использовании 32-битных регистров длина ключей составит 256 битов и ключевая область будет равна 2256. Повышение ключевой области и применение динамически меняющийся криптографических ключей обеспечивает необходимый уровень процесса шифрования. Система реализована для*

шифрования текстовой информации, однако она может быть использована и для шифрования информации других форматов.

Ключевые слова: *регистр сдвига с линейной обратной связью, LFSR, регистр сдвига, шифр, ключ шифрования, криптографическая система, гамма, псевдослучайные биты, статистическая зависимость.*

Gasimov V.A., Mammadov J.I.

METHOD OF ENCRYPTION OF TEXT INFORMATION BASED ON LSFR

*The article is devoted to the development of an LFSR-based method for encrypting text information. A method for encrypting information using a Linear Feedback Shift Register (LFSR) and dynamic keys is proposed. The long period and good statistical characterization of the sequence generated by the LFSR, while performing simple shift and addition operations, ensures high reliability and speed of the encryption process. In the proposed system, it is assumed to use several registers at the same time, the number of which is determined by the bit depth of the encrypted character. The cryptographic key used is a concatenation of the values Ki (i=1,2,...,8) entered in the shift registers: K= K1K2...K8. And the values Ki are calculated based on the components of the session key (i=1,2,...,8) and the system time parameter. It is possible to extend the cryptographic key by increasing the bit depth of the registers. In a system with 32-bit registers, the total key length is l=25*23=28= 256 bits, and with 64-bit registers, 512 bits. The proposed method can be implemented in hardware, software, and hardware-software combination. The maximum speed of the process is achieved in a system with a hardware implementation, since the encryption of a single character in such a system is performed in just one clock cycle. It is also possible to increase the speed of the process by encrypting several characters at the same time, using the appropriate number of registers for this purpose. The resistance of the proposed cryptosystem to brute force attacks is quite high, since when using 32-bit registers, the key length will be 256 bits and the key area will be equal to 2256. Enhancing the key domain and applying dynamically changing cryptographic keys provides the necessary level of encryption process. The system is implemented to encrypt text information, but it can also be used to encrypt information in other formats.*

Keywords: *linear feedback shift register, LFSR, shift register, chiper, encryption key, cryptographic system, gamma, pseudo-random bits, statistical dependence.*