УДК 681.3.06

А.А. Кузнецов, Р.В. Королёв, Ю.Н. Рябуха

Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков

УСОВЕРШЕНСТВОВАННЫЙ МЕТОД БЫСТРОГО ФОРМИРОВАНИЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Исследуются криптографические генераторы последовательностей псевдослучайных чисел (ППСЧ), стойкость которых основана на теоретико-сложностной проблеме синдромного декодирования. Предлагается усовершенствованный метод формирования ППСЧ, который позволяет обеспечить максимальный период формируемых последовательностей.

Ключевые слова: *генератор псевдослучайных чисел, псевдослучайные числа.*

Введение

Постановка проблемы в общем виде и анализ литературы. Проблема построения криптографически стойких генераторов ППСЧ имеет важное значение как для развития отдельного научного направления теории защиты информации, так и для решения прикладных задач обеспечения конфиденциальности, целостности, аутентичности и доступности информационных технологий [1 – 4].

Современные методы построения криптографических генераторов ППСЧ основаны на использовании рекуррентных правил с линейными и нелинейными обратными связями [1, 5], криптографических примитивов симметричных и несимметричных шифров [6] и др. Проведенный анализ [7] показал, что высокими показателями статистической безопасности обладают генераторы ППСЧ, стойкость которых основана на сложности решения одной из известных теоретико-сложностных задач (факторизация, дискретное логарифмирование и т.д.). В [2] такие криптоалгоритмы относят к группе т.н. «доказуемо стойких», подчеркивая тем самым сводимость задачи вычисления секретного ключа к решению хорошо известной вычислительно сложной математической задаче. Примером может служить генератор Blum-Blum-Shub (BBS), стойкость которого основана на теоретико-сложностной задаче вычисления примитивных квадратных корней по модулю числа Блюма, эквивалентной по вычислительной сложности задаче факторизации (разложения числа на сомножители) [8].

В тоже время, следует отметить существенный недостаток доказуемо стойких генераторов: чрезвычайно высокую сложность формирования ППСЧ, обусловленную необходимостью выполнять операции над большими числами. Так, например, для обеспечения криптографической стойкости, сопоставимой со стойкостью блочно-симметричного шифра AES (FIPS-197) с длиной ключа 128 бит в несимметричной криптосистеме RSA с длиной ключа 1024 бит потребуется обрабатывать числа с более 300 десятичными знаками. На практике подобные вычисления снижают производительность криптосистемы на 3 – 5 порядка и реализуются с использованием дорогих специализированных вычислительных устройств.

Особое место в развитии доказуемо стойких генераторов ППСЧ занимают методы, основанные на избыточных кодах, стойкость таких генераторов основана на теоретико-сложностной задаче синдромного декодирования [9] (Generator Provably as Secure as Syndrome Decoding – (GPSSD)) [10]. В работе [10] предложен алгоритм формирования ППСЧ и оценена его сложность, а так же показано, что соответствующий генератор GPSSD относится к категории доказуемо стойких алгоритмов. В работе [7] исследована статистическая безопасность некоторых генераторов, в том числе генератора GPSSD. Установлено, что по статистической безопасности генератор GPSSD обладает улучшенными свойствами. В [11] исследованы периодические свойства формируемых последовательностей, показано, что генератор GPSSD не обеспечивает максимальный период формируемой последовательности. Таким образом, можно констатировать, что доказуемо стойкий генератор GPSSD, построенный с использованием избыточных блоковых кодов и обладающий улучшенными показателями по статистической безопасности и быстродействию не обеспечивает формирование последовательностей максимального периода, его периодические свойства неудовлетворительные, что может стать причиной появления эффективных криптографических атак. Перспективным направлением дальнейших исследований является разработка усовершенствованного метода на основе избыточных блоковых кодов, который помимо высоких показателей статистической безопасности и быстродействия позволит формировать последовательности максимального периода.

Разработка усовершенствованного метода формирования ППСЧ

Предлагаемый усовершенствованный метод формирования ППСЧ структурно состоит из следующих этапов.

1. Этап. Формирование сеансового ключа.

2. Этап. Псевдослучайное формирование равновесной двоичной последовательности.

3. Этап. Вычисление синдромной последовательности, соответствующей сеансовому ключу.

4. Этап. Формирование фрагмента ППСЧ и последовательности для обратной связи.

Структура усовершенствованного метода формально представлена на рис. 1. На рисунке выделены элементы – отличные от метода-прототипа [10].

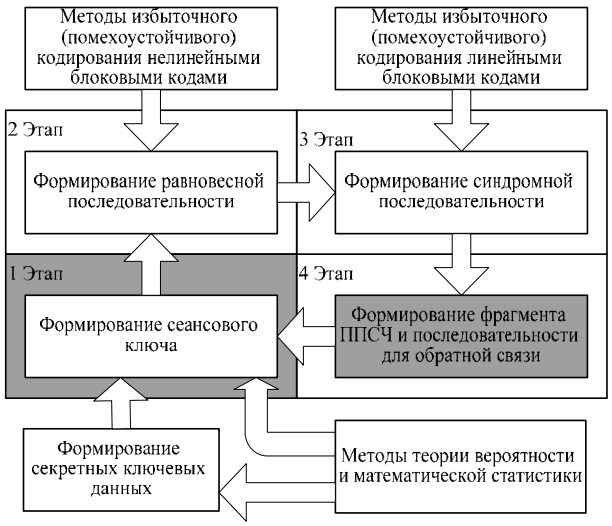

Рис. 1. Структурная схема усовершенствованного метода быстрого формирования ППСЧ

На первом этапе предлагаемого метода с использованием приемов и операций теории защиты информации формируются сеансовые ключевые данные – последовательности максимального периода [1, 12]. Этот этап является основным отличительным элементом предлагаемого метода от известного метода прототипа. Реализация процедур формирования последовательностей максимального периода может быть выполнена различными способами, например, с использованием линейных рекуррентных регистров с обратными связями (ЛРР) [1, 5, 12]. Начальное заполнение регистра соответствует значению введенных секретных ключевых данных.

Введем следующие обозначения:

– $K = \{K_1, K_2, ..., K_M\}$ – множество секретных ключей, $|K| = M$, где $M = q^m$, $m = \left\lfloor \log_q \left(C_n^w\right) \right\rfloor$, $C_n^w = n!/\left(w! \cdot (n-w)!\right)$, n – длина равновесной последовательности, w – заранее заданная константа (вес последовательности – число ненулевых элементов равновесной последовательности),

$$K_i = \left(K_{i_0} \quad K_{i_1} \quad ... \quad K_{i_{m-1}}\right),$$

$$K_i \in K \subseteq GF^M(q),\ K_{i_j} \in GF(q);$$

– $C_K = \left\{C_{K1}, C_{K2}, ..., C_{K_M}\right\}$ – множество последовательностей сеансовых ключей:

$$C_{K_i} = \left(C_{Ki_0} \quad C_{Ki_1} \quad ... \quad C_{Ki_{m-1}}\right),$$

$$C_{Ki} \in C_K \subseteq GF^M(q),\ C_{Ki_j} \in GF(q);$$

– $C^*_K = \left\{C^*_{K1}, C^*_{K2}, ..., C^*_{K_{q^m}}\right\}$ – множество равновесных последовательностей, т.е. множество кодовых слов равновесного кода:

$$C^*_{K_i} = \left(C^*_{Ki_0} \quad C^*_{Ki_1} \quad ... \quad C^*_{Ki_{n-1}}\right),$$

$$C^*_{Ki} \in C^*_K \subseteq GF^n(q),\ C^*_{Ki_j} \in GF(q),$$

$$w\left(C^*_{Ki}\right) = w;$$

– $S_K = \left\{S_{K1}, S_{K2}, ..., S_{K_{q^m}}\right\}$ – множество синдромных последовательностей линейного блокового (n, k, d) кода, $r = n - k$:

$$S_{K_i} = \left(S_{Ki_0} \quad S_{Ki_1} \quad ... \quad S_{Ki_{r-1}}\right),$$

$$S_{Ki} \in S_K \subseteq GF^r(q),\ S_{Ki_j} \in GF(q);$$

– $S^*_K = \left\{S^*_{K1}, S^*_{K2}, ..., S^*_{K_{q^r}}\right\}$ – множество последовательности для обратной связи:

$$S^*_{K_i} = \left(S^*_{Ki_0} \quad S^*_{Ki_1} \quad ... \quad S^*_{Ki_{m-1}}\right),$$

$$S^*_{Ki} \in S^*_K \subseteq GF^M(q),\ S^*_{Ki_j} \in GF(q).$$

На первом этапе предлагаемого метода по введенной секретной ключевой последовательности

$$K_i = \left(K_{i_0} \quad K_{i_1} \quad ... \quad K_{i_{m-1}}\right)$$

и последовательности для обратной связи

$$S^*_{K_i} = \left(S^*_{Ki_0} \quad S^*_{Ki_1} \quad ... \quad S^*_{Ki_{m-1}}\right)$$

формируется последовательность сеансового ключа

$$C_{K_i} = \left(C_{Ki_0} \quad C_{Ki_1} \quad ... \quad C_{Ki_{m-1}}\right)$$

как результат отображения

$$\varphi : (K) \times \left(S^*_K\right) \to C_K. \qquad (1)$$

Отображение (1) реализуется совокупностью операций формирования последовательностей максимального периода по введенной секретной ключевой последовательности

$$K_i = \left(K_{i_0} \quad K_{i_1} \quad ... \quad K_{i_{m-1}}\right)$$

в комбинации с итеративной процедурой над последовательностью обратной связи

$$S^*_{K_i} = \left(S^*_{Ki_0} \quad S^*_{Ki_1} \quad ... \quad S^*_{Ki_{m-1}}\right).$$

В простейшем варианте отображение (1) реализуется посредством использования ЛРР с начальным состоянием равным введенной секретной ключевой последовательности

$$K_i = \left(K_{i_0} \quad K_{i_1} \quad ... \quad K_{i_{m-1}}\right)$$

с последующим поэлементным суммированием в арифметике конечного поля с последовательностью обратной связи на каждой итерации процесса фор-

мирования ППСЧ.

Структурная схема устройства формирования последовательностей сеансового ключа приведена на рис. 2 (в конфигурации Галуа).

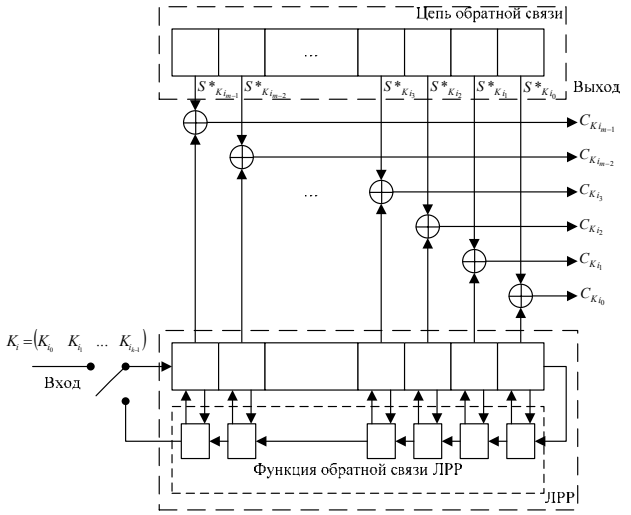

Рис. 2. Структурная схема устройства формирования сеансовых ключей с использованием ЛРР (конфигурация Галуа)

Устройство, структурная схема которого приведена на рис. 2, функционируют следующим образом. В течении первых m временных отсчетов ключ (переключатель) находится в верхнем положении а регистр сдвига заполняется ключевой последовательностью

$$K_i = \left(K_{i_0} \quad K_{i_1} \quad \ldots \quad K_{i_{m-1}}\right).$$

В течение последующих $q^m - 1$ временных отсчетов ключ (переключатель) находится в нижнем положении и на выход устройства подаются значения, хранимые в ячейках регистра сдвига. На каждом временном интервале информация, хранимая в регистре сдвига, перемещается на одну ячейку вправо, а по цепи обратной связи ЛРР поступает значение, хранимое в крайней правой ячейке. Функция обратной связи задает конкретный вид коммутаций цепи обратной связи и обеспечивает формирование псевдослучайной последовательности максимального периода.

На втором этапе предлагаемого метода с использованием алгоритмов равновесного кодирования осуществляется преобразование последовательности сеансового ключа в равновесную последовательность, т.е. осуществляется отображение

$$\gamma : C_K \to C^*_K, \qquad (2)$$

где $C^*_{K_i} = \left(C^*_{Ki_0} \quad C^*_{Ki_1} \quad \ldots \quad C^*_{Ki_{n-1}}\right)$;

$C^*_{Ki} \in C^*_K \subseteq GF^n(q)$; $C^*_{Ki_j} \in GF(q)$; $w(C^*_{Ki}) = w$;

n – длина равновесной последовательности; w – число ненулевых элементов последовательности (вес последовательности).

Алгоритмы равновесного кодирования, в том числе недвоичными последовательностями, подробно рассмотрены в третьем разделе.

На третьем этапе по сформированной равновесной последовательности

$$C^*_{K_i} = \left(C^*_{Ki_0} \quad C^*_{Ki_1} \quad \ldots \quad C^*_{Ki_{n-1}}\right)$$

с использованием методов избыточного кодирования линейными блоковыми кодами формируется синдромная последовательность, т.е. осуществляется отображение:

$$\phi : C^*_K \to S_K, \qquad (3)$$

где $S^*_{K_i} = \left(S^*_{Ki_0} \quad S^*_{Ki_1} \quad \ldots \quad S^*_{Ki_{m-1}}\right)$;

$S^*_{K_i} \in S^*_K \subseteq GF^M(q)$; $S^*_{Ki_j} \in GF(q)$.

Выше показано, что значение синдромной последовательности линейного блокового кода может быть получено посредством матричного умножения вектора-строки

$$C^*_{K_i} = \left(C^*_{Ki_0} \quad C^*_{Ki_1} \quad \ldots \quad C^*_{Ki_{n-1}}\right)$$

на транспонированную проверочную матрицу кода. Проверочная матрица кода (обозначим ее символом H_X) используется как секретный долговременный ключ. Если используемый код допускает полиномиальное описание, синдромная последовательность может быть получена посредством взятия многочлена с коэффициентами из вектора

$$C^*_{K_i} = \left(C^*_{Ki_0} \quad C^*_{Ki_1} \quad \ldots \quad C^*_{Ki_{n-1}}\right)$$

по модулю порождающего многочлена кода. Порождающий многочлен такого кода (обозначим его символом $g(x)_X$) используется как секретный долговременный ключ.

На четвертом этапе полученная синдромная последовательность подвергается простейшему преобразованию, например, как в методе-прототипе GPSSD [10], с целью формирования последовательности для обратной связи и фрагмента искомой ППСЧ. Процесс формирования последовательности для обратной связи формализуем в виде отображения

$$\varphi : S_K \to S^*_K, \qquad (4)$$

где $S_{K_i} = \left(S_{Ki_0} \quad S_{Ki_1} \quad \ldots \quad S_{Ki_{r-1}}\right)$;

$S_{Ki} \in S_K \subseteq GF^r(q)$; $S_{Ki_j} \in GF(q)$.

Сформированная в результате выполнения операций метода ППСЧ есть результат нескольких функциональных отображений, в общем виде

$$\text{ППСЧ} = \phi\left(H_X, \gamma\left(\varphi\left((K_i) \times \left(\varphi\left(S_{K_j}\right)\right)\right)\right)\right). \qquad (5)$$

Следует отметить, что функциональное соответствие $\varphi\left(S_{K_j}\right)$ реализует отображение множества синдромных последовательностей в множество последовательностей обратной связи, т.е. выражение (5) справедливо только для того фрагмента ППСЧ, который формируется на итерации, соответствующей аргументу функции $\varphi\left(S_{K_j}\right)$. На следующей итерации при фиксированном значении ключа K_i фрагмент ППСЧ зависит от другого значения аргу-

мента функции, т.е. от S_{K_l}, $l \neq j$.

Нахождение ключевых данных K_i по известной (перехваченной) ППСЧ сопряжено с поиском вычислительно эффективных алгоритмов выполнения обратного отображения ϕ^{-1}(ППСЧ). Эта задача эквивалентна теоретико-сложностной задаче декодирования случайного кода. Кроме того, наличие в структуре метода операций формирования последовательностей максимального периода (реализуемого, например, с помощью ЛРР), позволяет формировать ППСЧ с гарантированным максимальным периодом $L = q^m - 1$.

Выводы

Таким образом, в результате проведенных исследований разработан усовершенствованный метод формирования ППСЧ, выполнение всех этапов которого (см. выражения (1) – (5)) позволяет по заданным ключевым данным K_i и по введенному долговременному ключу – проверочной матрице H_X за конечное число шагов формировать ППСЧ со сведением задачи криптоанализа к решению теоретико-сложностной задачи декодирования случайного кода по известному вектору-синдрому как функции от секретного вектора-ключа. Основным достоинством усовершенствованного метода перед методом-прототипом GPSSD является обеспечение максимального периода формируемых ППСЧ. По своей структуре предложенный метод предполагает выполнение простых и вычислительно эффективных операций. В тоже время значительное повышение длины периода ППСЧ может быть достигнуто исключительно за счет повышения размерности векторов

$$C_{K_i} = \left(C_{Ki_0} \quad C_{Ki_l} \quad \ldots \quad C_{Ki_{m-1}} \right)$$

$$\text{и } C^*_{K_i} = \left(C^*_{Ki_0} \quad C^*_{Ki_l} \quad \ldots \quad C^*_{Ki_{n-1}} \right),$$

что влечет за собой существенное усложнение процедуры равновесного кодирования.

Перспективным направлением исследований в этом смысле является разработка метода быстрого формирования ППСЧ со сведением задачи криптоанализа к решению теоретико-сложностной задачи декодирования случайного кода по известному кодовому слову с ошибками как функции от секретного вектора-ключа. Это позволит за счет использования двух векторов секретных ключевых данных при неизменной разрядности равновесных векторов существенно повысить длину периода формируемой ППСЧ.

Список литературы

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: ТРИУМФ, 2002. – 816 с.

2. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004. – Version 0.15 (beta), Springer-Verlag. – p. 829.

3. Landau S. Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard / S. Landau // The mathematical association of America. – February 2004. – 111. – P. 89-117.

4. Аунг Т.М. Разработка и исследование стохастических методов защиты программных систем: автореф. дисс. ... канд. техн. наук: 05.13.11, 05.13.19 / Т.М. Аунг, Московский инженерно-физический институт (государственный университет). – М., 2007. – 20 с.

5. Поточные шифры Результаты зарубежной открытой криптологии. – М., 1997. – [Електронний ресурс]. – Режим доступу к документу: www.ssl.stu.neva.ru/psw/crypto/potok/str_ciph.htm.

6. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22. Technology Administration U.S. Department of Commerce. – Washington: National Institute of Standards and Technology. – 2000. – P. 164.

7. Кузнецов А.А. Исследование статистической безопасности генераторов псевдослучайных чисел / А.А. Кузнецов, Р.В. Королев, Ю.Н. Рябуха // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип. 3 (70). – С. 79-82.

8. Эллиптические кривые и современные алгоритмы теории чисел / Ю.П. Соловьев, В.А. Садовничий, Е.Т. Шавгулидзе, В.В. Белокуров. – Москва – Ижевск: Институт компьютерных исследований, 2003. – 192 с.

9. Мак-Вильямс Ф.Дж. Теория кодов, исправляющих ошибки / Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн. – М.: Связь, 1979. – 744 с.

10. Jean-Dernard Fisher An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding / Jean-Dernard Fisher, Jacques Stern. // EUROCRYPT'96 Proceeding, LNCS 1070. – P. 245-255.

11. Корольов Р.В. Дослідження періодичних властивостей генераторів псевдовипадкових чисел, заснованих на використанні надмірних блокових кодів / Р.В.Корольов // Системи озброєння і військова техніка. – 2008. – № 3 (15). – С. 126-128.

12. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

Поступила в редколлегию 25.11.2008

Рецензент: д-р тех. наук, проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ВДОСКОНАЛЕНИЙ МЕТОД ШВИДКОГО ФОРМУВАННЯ ПОСЛІДОВНОСТЕЙ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

О.О. Кузнецов, Р.В. Корольов, Ю.М. Рябуха

Досліджуються криптографічні генератори послідовностей псевдовипадкових чисел (ППВЧ), стійкість яких заснована на теоретико-складової проблемі синдромного декодування. Пропонується вдосконалений метод формування ППВЧ, який дозволяє забезпечити максимальний період формованих послідовностей.

Ключові слова: *генератор псевдовипадкових чисел, псевдовипадкові числа.*

METHOD OF RAPID FORMING OF SEQUENCES OF PSEUDO-RANDOM NUMBERS IS IMPROVED

O.O. Kuznecov, R.V. Korolev, Yu.M. Ryabukha

The cryptographic generators of sequences of pseudo-random numbers (PRN) firmness of which is based on theorist of intricate problem of the syndromic decoding are probed. The improved method of forming of PRN is offered, which allows to pro-

vide the maximal period of mouldable sequences.

Keywords: *generator of pseudo-random number , of pseudo-random numbers.*