УДК 519.7

С.А. Диченко, О.А. Финько

АЛГОРИТМ ГЕНЕРАЦИИ БЛОЧНОЙ ПСП, ОСНОВАННЫЙ НА ПРИМЕНЕНИИ ЛОГИКО-ЧИСЛОВЫХ ФОРМ

Обсуждается новый метод параллельной реализации псевдослучайных последовательностей ПСП, образуемых посредством комбинирующих генераторов ПСП. В статье развиваются ранее полученные результаты авторов по генерации ПСП вначале посредством, в общем случае, нелинейных логико-числовых полиномов, а затем и линейных логико-числовых полиномов. Суть новизны достигнутого результата заключается в реализации таких последовательностей (применительно к более общему случаю – комбинирующим генераторам) посредством линейных логико-числовых полиномов, которые отличаются от, в общем случае, нелинейных логико-числовых полиномов существенно более низкой сложностью реализации. Метрика сложности – длина (количество слагаемых) реализующих формул. Верхняя граница выигрыша составила (2^n+1)/(n+1) раз. Достигнутые результаты открывают новые пути для получения дальнейших результатов – повышения безопасности функционирования средств криптографической защиты информации за счет применения методов избыточного арифметического (числового) кодирования данных (обеспечения функционального диагностирования в реальном масштабе времени).

Двоичная псевдослучайная последовательность; комбинирующий генератор двоичной псевдослучайной последовательности; распараллеливание логических вычислений; логико-числовые формы; арифметический полином; линейный числовой полином; нелинейный числовой полином; криптография; шифры; шифрующая гамма.

S.A. Dichenko, O.A. Finko

ALGORITHM FOR GENERATING PSEUDORANDOM SEQUENCE OF BLOCK BASED ON THE USE LOGICAL-NUMERIC FORM

The new method of parallel realization of pseudorandom sequences of PRS constructed by means of combining PRS generators, in this article is discussed. Earlier received results of authors on PRS generation, in the beginning by means of, generally, nonlinear logic – numerical polynoms, and then and linear logic-numerical polynoms develop. The essence of novelty of the reached result consists in realization of such sequences (with reference to more general case to combining generators) by means of linear logic-numerical polynoms which differ from, generally, nonlinear logic-numerical polynoms essentially lower complexity of realization. The length (quantity composed) realizing formulas is a complexity metrics. The top border of a prize made (2^n+1)/(n+1) time. The reached results open new ways for receiving further results of increase of safety of functioning of means of cryptographic protection of information at the expense of application of methods of superfluous arithmetic (numerical) coding of data (ensuring functional diagnosing in real time).

Binary pseudorandom sequence; combining binary pseudorandom sequence generator; parallel computing logic; logic-numeric form; polynomial arithmetic; numerical polynomial linear; nonlinear numerical polynomial; cryptography; codes; ciphers gamma.

Введение. Генератор псевдослучайной последовательности (ПСП) имеет важнейшее значение для различных криптоалгоритмов и систем генерации ключевого материала [1–4]. Наиболее распространенными и проверенными практикой являются алгоритмы генерации ПСП, основанные на использовании рекуррентных логических выражениях и неприводимых полиномов [1–4].

В частности, наиболее простым по структуре является рекуррентный регистр сдвига с обратной связью, реализуемой некоторой функцией f, в результате работы которого последовательно с каждым тактом на выходе получаем один элемент ПСП (рис. 1).

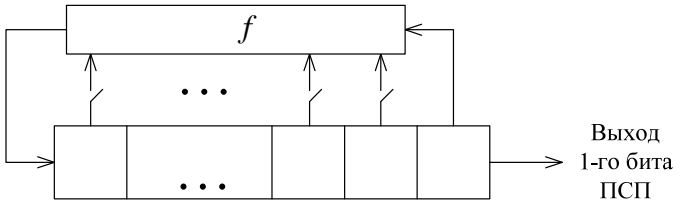


Рис. 1. Общий вид рекуррентного регистра сдвига с обратной связью

Для обеспечения максимальной длины периода ПСП используют рекуррентный регистр сдвига с обратной связью, реализуемой линейной функцией f, характеристический многочлен которого подобран по известным правилам.

Ужесточение требований к скорости шифрования и увеличение объема защищаемой информации вызывает необходимость построения параллельных алгоритмов генерации ПСП [1–6].

Из литературы известны различные методы распараллеливания алгоритма генерации ПСП, в частности с использованием логико-числовых форм, т.е. посредством применения линейных и нелинейных числовых полиномов.

Применение нелинейных числовых полиномов (НЧП) вызывает ряд трудностей, так как длина НЧП, равная $2^n - 1$ (где n – степень многочлена), существенно возрастала с увеличением степеней характеристических многочленов, на основе которых строится генератор ПСП. А, как известно, для обеспечению безопасности функционирования средств криптографической защиты информации в целом используют именно генераторы ПСП, построенные на многочленах больших степеней.

Поэтому, применение линейных числовых полиномов (ЛЧП), длина которых значительно короче длины НЧП и составляет $n+1$, обеспечивает значительный выигрыш в скорости вычислений и, как следствие, является практически наиболее перспективным для дальнейшего использования в исследованиях.

В частности, метод распараллеливания алгоритма генерации двоичной ПСП с использованием ЛЧП представлен в [7].

Общая схема реализации метода представлена на рис. 2.

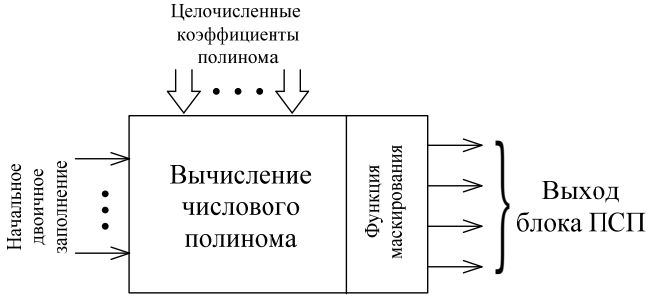


Рис. 2. Схема реализации ПСП ЛЧП

В [7] сам алгоритм генерации двоичной ПСП, подлежащий распараллеливанию, реализован посредством линейного рекуррентного регистра сдвига (ЛРРС).

Благодаря этому методу на выходе генератора мы получим не один, а целый блок элементов ПСП.

Кратко опишем этот метод.

На основе характеристического уравнения полинома (частный случай: образующий полином - трином)

$$D(x) = x^r + x^k + 1,$$

где r – степень тринома, $r \in N$, $1 \le k \le r-1$, $k \in N$, которое имеет вид:

$$a_i = a_{i+k-r} \oplus a_{i-r},$$

где $a_i, a_{i+k-r}, a_{i-r} \in \{0,1\}$; $i \ge r$; $i \in N$, построим систему характеристических уравнений для участка ПСП длины d:

$$\begin{cases} a_i = a_{i+k-r} \oplus a_{i-r}, \\ a_{i+1} = a_{i+k-r+1} \oplus a_{i-r+1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{i+d-1} = a_{i+k-1} \oplus a_{i-1}, \end{cases}$$

где $[a_{i-r} \quad a_{i-r+1} \quad \ldots \quad a_{i-1}]$ – вектор начальных условий; $[a_i \quad a_{i+1} \quad \ldots \quad a_{i+d-1}]$ – вектор участка ПСП; $a_k \in \{0,1\}$; $k = i-r+1, \ldots, i+r-1$.

Систему характеристических уравнений представим, как систему БФ, в свою очередь которую, используя правило представления БФ в базисе $\Omega = \{\oplus, 1\}$ посредством одного ЛЧП [8–10], преобразуем в систему ЛЧП:

$$\begin{cases} P_i(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1}) = \sum_{t=i-r}^{i-1} g_{i,t} a_t, \\ P_{i+1}(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1}) = \sum_{t=i-r}^{i-1} g_{i+1,t} a_t, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ P_{i+d-1}(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1}) = \sum_{t=i-r}^{i-1} g_{i+r-1,t} a_t, \end{cases} \quad (1)$$

где $g_{j,t}$ (здесь и далее) принимает значение «0» или «1» в зависимости от вхождения в j-ый ЛЧП a_t;. $j = i, i+1, \ldots, i+d-1$

Результат вычисления j-го ЛЧП системы (1) представим двоичным машинным словом длины $l_j = \left\lfloor \log\left(\sum_{t=i-r}^{i-1} g_{j,t}\right) \right\rfloor + 1.$

Далее систему (1) представим посредством одного ЛЧП вида:

$$H(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1}) = P_i(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1}) + \sum_{s=i+1}^{i+r-1} 2^{\lambda_s} P_s(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1}) =$$

$$= g_{i,i-r} a_{i-r} + \ldots + g_{i,i-1} a_{i-1} + \ldots + 2^{\lambda_{i+d-1}} g_{i+d-1,i-r} a_{i-r} + \ldots + 2^{\lambda_{i+d-1}} g_{i+d-1,i-1} a_{i-1} = \quad (2)$$

$$= h_{i-r} a_{i-r} + h_{i-r+1} a_{i-r+1} + \ldots + h_{i-1} a_{i-1},$$

где $\lambda_s = \sum_{t=i}^{s-1} (l_j + 1)$; $h_t \in Z$; $t = i-r, i-r+1, \ldots, i-1$.

Таким образом, представленный метод позволяет с помощью одного ЛЧП реализовать блок ПСП длины d. Значения полученного блока ПСП будут являться начальным заполнением для ЛЧП, реализующего следующий блок последовательности длины равной d.

Однако свойства ЛРРС показывают, что, несмотря на достаточно большой период и хорошие статистические качества, линейные рекуррентные последовательности имеют очень простое строение. Поэтому в большинстве известных криптоалгоритмов используют различные способы усложнения аналитического строения линейных рекуррент [11].

Один из таких способов усложнения связан с использованием в одной схеме нескольких ЛРРС, объединенных одной общей функцией усложнения. В этом случае генератор ПСП называется *комбинирующим,* в результате работы которого последовательно с каждым тактом на выходе получаем один элемент ПСП [11] (рис. 3).

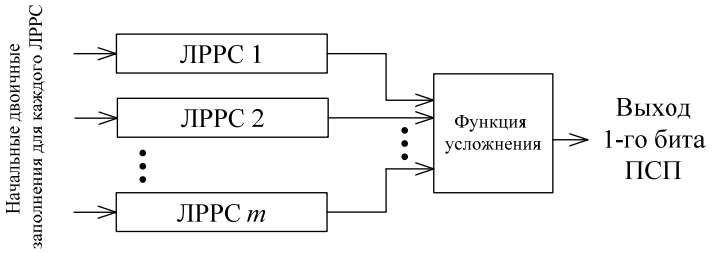


Рис. 3. Общий вид комбинирующего генератора ПСП

Настоящая статья является продолжением работы [7]. В ней реализован метод распараллеливания алгоритма генерации ПСП, полученной на основе применения комбинирующего генератора ПСП, состоящего из двух и более $r^{(v)}$ ЛРРС различной или равной длины (где $v = 1, \ldots, m$), объединенных функцией усложнения (частный случай: функция усложнения – линейная).

Общая схема реализации метода представлена на рис. 4.

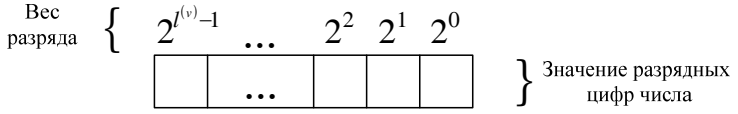
Рис. 4. Схема реализации ПСП ЛЧП

Цель статьи – распараллеливание алгоритма генерации ПСП с использованием ЛЧП, полученной на основе применении комбинирующего генератора ПСП.

Для каждого ЛРРС, входящего в состав комбинирующего генератора ПСП произведем ряд вычислений, описанных в [7], и получим систему ЛЧП (1), которую представим следующим образом:

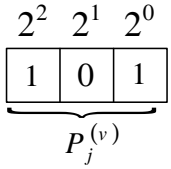
$$\begin{cases} P_i^{(v)}(a_{i-r}^{(v)}, a_{i-r+1}^{(v)}, \ldots, a_{i-1}^{(v)}) = \sum_{t=i-r}^{i-1} g_{i,t} a_t^{(v)}, \\ P_{i+1}^{(v)}(a_{i-r}^{(v)}, a_{i-r+1}^{(v)}, \ldots, a_{i-1}^{(v)}) = \sum_{t=i-r}^{i-1} g_{i+1,t} a_t^{(v)}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ P_{i+d-1}^{(v)}(a_{i-r}^{(v)}, a_{i-r+1}^{(v)}, \ldots, a_{i-1}^{(v)}) = \sum_{t=i-r}^{i-1} g_{i+d-1,t} a_t^{(v)}. \end{cases} \quad (3)$$

Результат вычисления j-го ЛЧП системы (3) можно представить двоичным машинным словом вида:

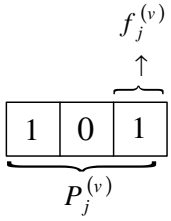


длины $l^{(v)} = \left\lfloor \log_2 r^{(v)} \right\rfloor + 1.$

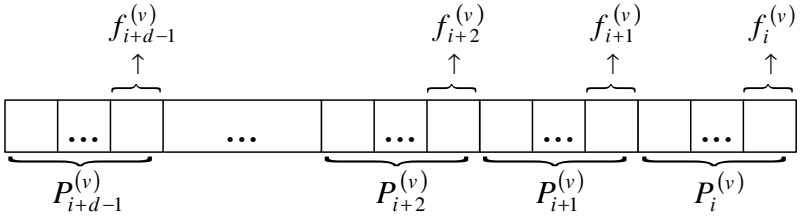
Пример 1. *При* $P_j^{(v)} = 5$ *длина двоичного машинного слова равна* $l^{(v)} = \lfloor \log_2 5 \rfloor + 1 = 3$, *который примет вид:*



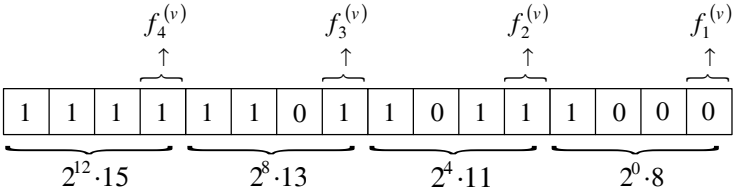
При этом результат вычисления БФ $f_j^{(v)}$ соответствует значению младшего разряда двоичного представления результата вычисления $P_j^{(v)}$.



И, таким образом, для размещения результатов вычисления всех $d^{(v)}$ ЛЧП системы (3) в одном машинном слове необходимо произвести сдвиг влево результата вычисления j-го ЛЧП на количество разрядов занимаемых результатами вычислений предшествующих ему ЛЧП в порядке, указанном в системе (3). Получим



Пример 2. *При* $l^{(v)} = 4,\ P_1^{(v)} = 8,\ P_2^{(v)} = 11,\ P_3^{(v)} = 13,\ P_4^{(v)} = 15$, *получим*



По примеру (2) представим систему (3) посредством одного ЛЧП вида:

$$H^{(v)}(a_{i-r}^{(v)}, a_{i-r+1}^{(v)}, ..., a_{i-1}^{(v)}) = \sum_{u=0}^{d-1} 2^{s_u \cdot l^{(v)}} P_{i+s_u}^{(v)}(a_{i-r}^{(v)}, a_{i-r+1}^{(v)}, ..., a_{i-1}^{(v)}) =$$

$$= 2^{s_0 \cdot l^{(v)}} g_{i,i-r} a_{i-r}^{(v)} + ... + 2^{s_0 \cdot l^{(v)}} g_{i,i-1} a_{i-1}^{(v)} + ...$$

$$... + 2^{s_1 \cdot l^{(v)}} g_{i+1,i-r} a_{i-r}^{(v)} + ... + 2^{s_1 \cdot l^{(v)}} g_{i+1,i-1} a_{i-1}^{(v)} + ... \quad (4)$$

$$... + 2^{s_{d-1} \cdot l^{(v)}} g_{i+d-1,i-r} a_{i-r}^{(v)} + ... + 2^{s_{d-1} \cdot l^{(v)}} g_{i+d-1,i-1} a_{i-1}^{(v)} =$$

$$= h_{i-r} a_{i-r}^{(v)} + h_{i-r+1} a_{i-r+1}^{(v)} + ... + h_{i-1} a_{i-1}^{(v)},$$

где $s_0 = 0;\ s_u = s_{u-1} + 1;\ h_t \in Z;\ t = i-r,\ i-r+1,\ ...,\ i-1.$

Для всех m регистров сдвига, входящих в состав комбинирующего генератора ПСП, выполним преобразования (3), (4), получим общий ЛЧП (5):

$$H_{общ}(a_{i-r}^{(1)}, a_{i-r+1}^{(1)}, ..., a_{i-1}^{(1)}; ...; a_{i-r}^{(m)}, a_{i-r+1}^{(m)}, ..., a_{i-1}^{(m)}) =$$

$$= 2^{s_0 \cdot l} g_{i,i-r} a_{i-r}^{(1)} + ... + 2^{s_0 \cdot l} g_{i,i-1} a_{i-1}^{(1)} + ... + 2^{s_0 \cdot l} g_{i,i-r} a_{i-r}^{(m)} + ...$$

$$... + 2^{s_0 \cdot l} g_{i,i-1} a_{i-1}^{(m)} + ... + 2^{s_1 \cdot l} g_{i+1,i-r} a_{i-r}^{(1)} + ... + 2^{s_1 \cdot l} g_{i+1,i-1} a_{i-1}^{(1)} + ...$$

$$... + 2^{s_1 \cdot l} g_{i+1,i-r} a_{i-r}^{(m)} + ... + 2^{s_1 \cdot l} g_{i+1,i-1} a_{i-1}^{(m)} + ... + 2^{s_{d-1} \cdot l} g_{i+d-1,i-r} a_{i-r}^{(1)} + ... \quad (5)$$

$$... + 2^{s_{d-1} \cdot l} g_{i+d-1,i-1} a_{i-1}^{(1)} + ... + 2^{s_{d-1} \cdot l} g_{i+d-1,i-r} a_{i-r}^{(m)} + ...$$

$$... + 2^{s_{d-1} \cdot l} g_{i+d-1,i-1} a_{i-1}^{(m)} = h_{i-r}^{(1)} a_{i-r}^{(1)} + h_{i-r+1}^{(1)} a_{i-r+1}^{(1)} + ... + h_{i-1}^{(1)} a_{i-1}^{(1)} + ...$$

$$... + h_{i-r}^{(m)} a_{i-r}^{(m)} + h_{i-r+1}^{(m)} a_{i-r+1}^{(m)} + ... + h_{i-1}^{(m)} a_{i-1}^{(m)},$$

где $l = \left\lfloor \log_2 \left(r^{(1)} + ... + r^{(m)} \right) \right\rfloor + 1;\ h_t^{(v)} \in Z;\ t = i-r,\ i-r+1,\ ...,\ i-1;\ s_0 = 0;$ $s_u = s_{u-1} + 1.$

Таким образом, с помощью одного ЛЧП мы получим i-й блок участка ПСП вида $\left\{ a_i^*, a_{i+1}^*, \ldots, a_{i+d-1}^* \right\}$.

Представленный алгоритм реализован для комбинирующего генератора ПСП следующего вида (рис. 5):

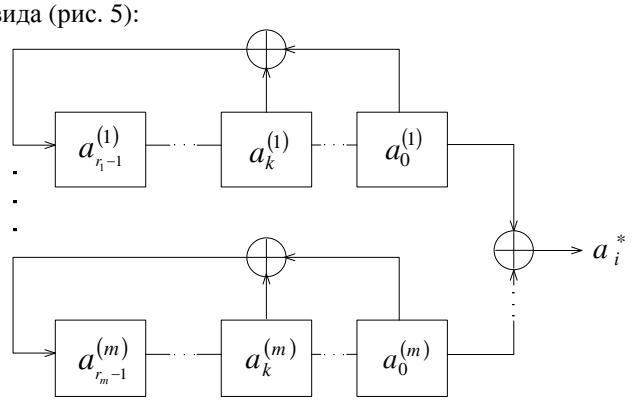


Рис. 5. Комбинирующий генератор ПСП (частный случай: образующий полином – трином)

При различных длинах регистров сдвига $r^{(v)}$ перед получением общего ЛЧП (5) необходимо выполнить выравнивание ПСП $\left\{a_i^{(1)}, a_{i+1}^{(1)}, \ldots, a_{i+r-1}^{(1)}\right\}$ ЛРРС, состоящего из меньшего числа ячеек памяти, по отношению к ПСП $\left\{a_i^{(m)}, a_{i+1}^{(m)}, \ldots, a_{i+r-1}^{(m)}\right\}$ ЛРРС, состоящего из большего числа ячеек памяти.

Числовая и логическая схемы реализации i-го блока ПСП представлены на рис. 6, 7.

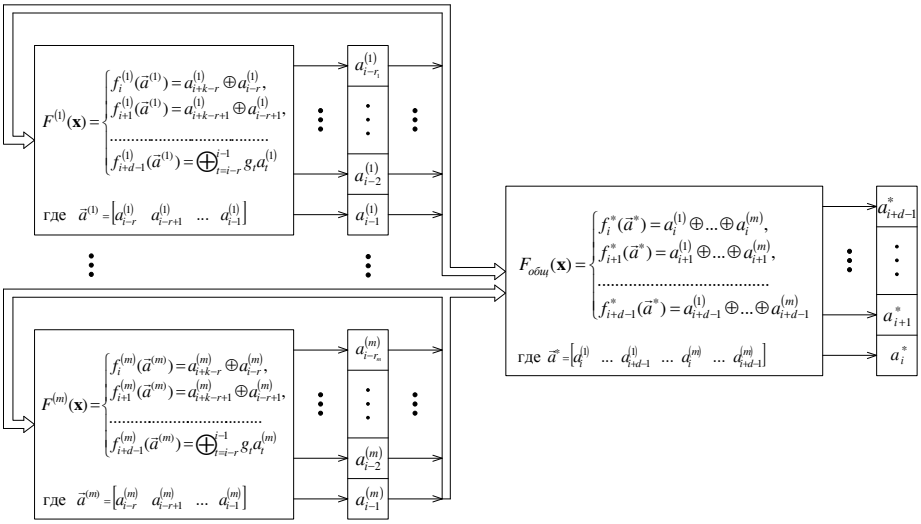


Рис. 6. Логическая схема реализации двоичной ПСП системой БФ

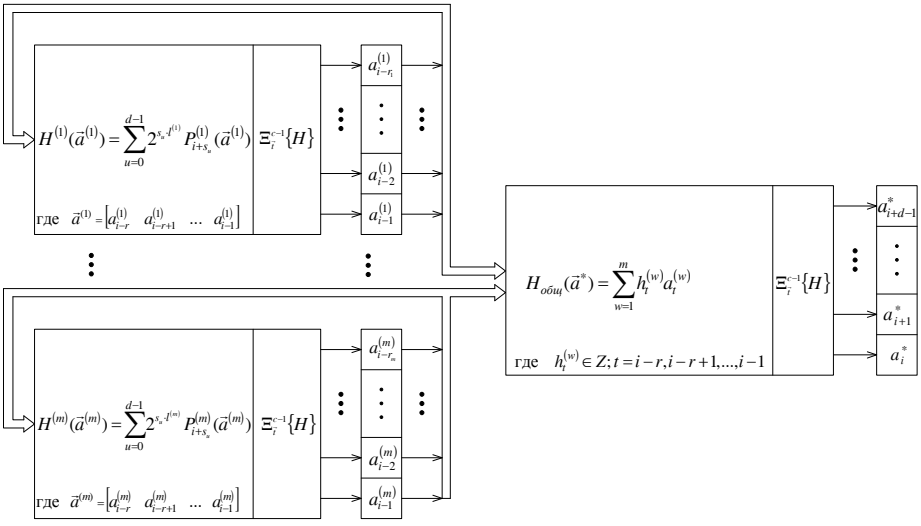


Рис. 7. Числовая схема реализации двоичной ПСП одним ЛЧП (где оператор маскирования $\Xi_i^{c-1}\{H\}$ необходим для определения $\vec{t}$ -го двоичного разряда)

Пример 3. *На рис. 8 представлен комбинирующий генератор ПСП, состоящий из двух 3-х и 4-х разрядных ЛРРС, объединенных общей функцией усложнения (функция усложнения реализуется через сумматор по модулю два).*

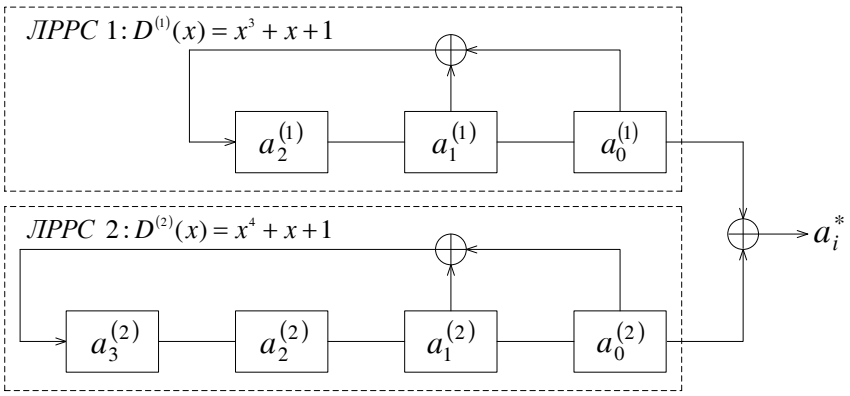


Рис. 8. Комбинирующий рекуррентный регистр сдвига

Подробно рассмотрим 3-х разрядный ЛРРС:
Образующий трином имеет вид:

$$D^{(1)}(x) = x^3 + x + 1,$$

характеристическое уравнение:

$$a_i^{(1)} = a_{i-3}^{(1)} \oplus a_{i-2}^{(1)}.$$

Система характеристических уравнений участка ПСП длины 7 имеет вид:

$$\begin{cases} a_i^{(1)} = a_{i-3}^{(1)} \oplus a_{i-2}^{(1)}, \\ a_{i+1}^{(1)} = a_{i-2}^{(1)} \oplus a_{i-1}^{(1)}, \\ a_{i+2}^{(1)} = a_{i-1}^{(1)} \oplus a_i^{(1)}, \\ a_{i+3}^{(1)} = a_i^{(1)} \oplus a_{i+1}^{(1)}, \\ a_{i+4}^{(1)} = a_{i+1}^{(1)} \oplus a_{i+2}^{(1)}, \\ a_{i+5}^{(1)} = a_{i+2}^{(1)} \oplus a_{i+3}^{(1)}, \\ a_{i+6}^{(1)} = a_{i+3}^{(1)} \oplus a_{i+4}^{(1)}. \end{cases}$$

Запишем систему характеристических уравнений, как систему БФ, с выраженными правыми частями равенств через начальные условия:

$$\begin{cases} f_i^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-3}^{(1)} \oplus a_{i-2}^{(1)}, \\ f_{i+1}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-2}^{(1)} \oplus a_{i-1}^{(1)}, \\ f_{i+2}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-3}^{(1)} \oplus a_{i-2}^{(1)} \oplus a_{i-1}^{(1)}, \\ f_{i+3}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-3}^{(1)} \oplus a_{i-1}^{(1)}, \\ f_{i+4}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-3}^{(1)}, \\ f_{i+5}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-2}^{(1)}, \\ f_{i+6}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-1}^{(1)}. \end{cases}$$

Получим систему ЛЧП:

$$\begin{cases} P_i^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-3}^{(1)} + a_{i-2}^{(1)}, \\ P_{i+1}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-2}^{(1)} + a_{i-1}^{(1)}, \\ P_{i+2}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-3}^{(1)} + a_{i-2}^{(1)} + a_{i-1}^{(1)}, \\ P_{i+3}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-3}^{(1)} + a_{i-1}^{(1)}, \\ P_{i+4}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-3}^{(1)}, \\ P_{i+5}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-2}^{(1)}, \\ P_{i+6}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-1}^{(1)}. \end{cases}$$

Так как длины ЛРРС различны и длина рассматриваемого ЛРРС короче, выполним выравнивание его выходной ПСП по отношению к ПСП второго ЛРРС. Система (3) примет вид:

$$\begin{cases} P_{i+1}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-2}^{(1)} + a_{i-1}^{(1)}, \\ P_{i+2}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-3}^{(1)} + a_{i-2}^{(1)} + a_{i-1}^{(1)}, \\ P_{i+3}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-3}^{(1)} + a_{i-1}^{(1)}, \\ P_{i+4}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-3}^{(1)}, \\ P_{i+5}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-2}^{(1)}, \\ P_{i+6}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-1}^{(1)}, \\ P_{i+7}^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = a_{i-3}^{(1)} + a_{i-2}^{(1)}. \end{cases}$$

Получим ЛЧП:

$$H^{(1)}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}) = (1054)_{16} a_{i-3}^{(1)} + (1105)_{16} a_{i-2}^{(1)} + (415)_{16} a_{i-1}^{(1)},$$

где запись $(...)_{16}$ *означает запись в 16-ричной системе счисления.*

Для 4-х разрядного ЛРРС выполним преобразования аналогичные для 3-х разрядного, получим ЛЧП:

$$H^{(2)}(a_{i-4}^{(2)}, ..., a_{i-1}^{(2)}) = (41201)_{16} a_{i-4}^{(2)} + (48209)_{16} a_{i-3}^{(2)} + (41048)_{16} a_{i-2}^{(2)} + (8240)_{16} a_{i-1}^{(2)}.$$

Получим общий ЛЧП (5):

$$H_{общ}(a_{i-3}^{(1)}, ..., a_{i-1}^{(1)}; a_{i-4}^{(2)}, ..., a_{i-1}^{(2)}) = (40248)_{16} a_{i-3}^{(1)} + (41009)_{16} a_{i-2}^{(1)} + (8049)_{16} a_{i-1}^{(1)} +$$

$$+ (41201)_{16} a_{i-4}^{(2)} + (48209)_{16} a_{i-3}^{(2)} + (41048)_{16} a_{i-2}^{(2)} + (8240)_{16} a_{i-1}^{(2)}.$$

Пусть $a_{i-3}^{(1)} = 0,\ a_{i-2}^{(1)} = 1,\ a_{i-1}^{(1)} = 1,\ a_{i-4}^{(2)} = 1,\ a_{i-3}^{(2)} = 0,\ a_{i-2}^{(2)} = 0,\ a_{i-1}^{(2)} = 1.$

Тогда

$$H_{общ} = (40248)_{16} \cdot 0 + (41009)_{16} \cdot 1 + (8049)_{16} \cdot 1 + (41201)_{16} \cdot 1 + (48209)_{16} \cdot 0 +$$

$$+ (41048)_{16} \cdot 0 + (8240)_{16} \cdot 1 = (92493)_{16} =$$

$$= (1\ \underbrace{0}_{f_{i+6}^*}\ \underbrace{0}_{f_{i+5}^*}\ 1\ \underbrace{0}_{f_{i+4}^*}\ \underbrace{0}_{f_{i+3}^*}\ 1\ \underbrace{0}_{f_{i+2}^*}\ \underbrace{0}_{f_{i+1}^*}\ 1\ \underbrace{0}_{f_{i}^*}\ 0\ 1\ 1)_2.$$

Вывод. Разработан метод распараллеливания алгоритма генерации ПСП на основе представления систем БФ посредством ЛЧП. Решение необходимо для построения высокопроизводительных средств криптографической защиты информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Бабаш, А.В., Шанькин Г.П.* Криптография / Под ред. В.П. Шерстюка, Э.А. Применко. – М.: СОЛОН-ПРЕСС, 2007. – 512 с.
2. *Тилборг.* Основы криптологии. – М.: Мир, 2006. – 472 с.
3. *Шнайер, Б.* Практическая криптография. – М.: Вильямс, 2005. – 424 с.
4. *Фороузан, Б.А.* Криптография и безопасность сетей: Учеб. пособие: пер. с англ. под ред. А.Н. Берлина. – М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. – 784 с.
5. *Вишневский А.К., Финько О.А.* Реализация типовых функций гибридных криптосистем арифметико-логическими полиномами // Теория и техника радиосвязи. – 2011. – № 1. – С. 32-36.
6. *Вишневский А.К., Финько О.А.* Параллельная реализация систем подстановок числовыми полиномами // V Международная конференция «Параллельные вычисления и задачи управления» (PACO-2010). – М., 26-28 октября 2010.
7. *Диченко С.А., Вишневский А.К., Финько О.А.* Реализация двоичных псевдослучайных последовательностей линейными числовыми полиномами // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 130-140.
8. *Малюгин В.Д.* Параллельные логические вычисления посредством арифметических полиномов / В.Д. Малюгин. – М.: Физматлит, 1997. – 192 с.
9. *Финько, О.А.* Реализация систем булевых функций большой размерности методами модулярной арифметики // Автоматика и телемеханика. – 2004. – № 6. - С. 37-60.
10. *Yanushkevich L., Shmerko V., Lyshevski S.* Logic design of nanoICs. CRC Press, 2005.
11. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии: Учеб. пособие. – М.: Гелиос АРВ, 2001. – 480 с.

Статью рекомендовал к опубликованию д.т.н., профессор В.Н. Марков.

Диченко Сергей Александрович – Филиал Военной академии связи (г. Краснодар); e-mail: dichenko.sa@yandex.ru; 350063, г. Краснодар, ул. Красина, 4; тел.: +79618588866; адъюнкт очной адъюнктуры.

Финько Олег Анатольевич – e-mail: ofinko@yandex.ru; тел.: +79615874848; профессор.

Dichenko Sergey Alexsandrovich – Branch of the Military Academy of Communications (Krasnodar); e-mail: dichenko.sa @yandex.ru; 4, Krasina, Krasnodar, 350063, Russia; phone: +79618588866; associate postgraduate full-time.

Finko Oleg Anatolievich – e-mail: ofinko@yandex.ru; phone: +79615874848; professor.

УДК 81.93.29

О.Ю. Пескова, Ю. Г. Халабурда

ПРИМЕНЕНИЕ СЕТЕВОЙ СТЕГАНОГРАФИИ ДЛЯ СКРЫТИЯ ДАННЫХ, ПЕРЕДАВАЕМЫХ ПО КАНАЛАМ СВЯЗИ*

Представлены основные понятия сетевой стеганографии, приведена классификация и рассмотрены базовые методы сетевой стеганографии. Наиболее подробно проанализированы методы модификации полей заголовков, методы SCTP-стеганографии, а также гибридные методы. Приведена сравнительная таблица характеристик рассмотренных

* Работа поддержана грантом РФФИ №10-07-00464-а.