БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Biham E., Shamir A.* Differential Cryptanalysis of the Full 16-round DES, Crypto'92, Springer-Velgar, 1998. – P. 487.
2. *Biham E., Shamir A.* Differential Cryptanalysis of DES-like Cryptosystems, Extended Abstract, Crypto'90, Springer-Velgar, 1998. – P. 2
3. *Kelsey J., Schnier B., Wagner D.*, Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SARER, and Triple-DES // http://www.schnier.com – 1996.
4. *Бабенко Л.К., Ищукова Е.А.* Применение рекурсивного алгоритма поиска в Б-деревьях для дифференциального криптоанализа алгоритма шифрования ГОСТ 28147-89 // Материалы IX Международной научно-практической конференции «Информационная безопасность». Ч. 2. – Таганрог: Изд-во: ТТИ ЮФУ, 2007 – С. 92-97.
5. *Saarien M.-J.* A Chosen Key Attack Against the Secret S-boxes of GOST // http://www.m.-js.com – Helsinki University of Technology, Finland.
6. *Панасенко С.П.* Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Бабенко Людмила Климентьевна
Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: blk@fib.tsure.ru.
347928, г. Таганрог, ул. Чехова, 2.
Тел.: 88634312018.
Кафедра безопасности информационных технологий; профессор.

Ищукова Евгения Александровна
E-mail: jekky82@mail.ru.
Тел.: 88634371905.
Кафедра безопасности информационных технологий; доцент.

Babenko Lyudmila Klimentevna
Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: blk@fib.tsure.ru.
2, Chekhov Street, Taganrog, 347928, Russia.
Phone: +78634312018.
The Department of Security of Information Technologies; Professor.

Ischukova Evgeniya Aleksandrovna
E-mail: jekky82@mail.ru.
Phone: +78634371905.
The Department of Security of Information Technologies; Associate Professor.

УДК 519.7

С.А. Диченко, А.К. Вишневский, О.А. Финько

РЕАЛИЗАЦИЯ ДВОИЧНЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛИНЕЙНЫМИ ЧИСЛОВЫМИ ПОЛИНОМАМИ

Разработан алгоритм распараллеливания генерации псевдослучайных двоичных последовательностей (ПСП) на основе представления систем порождающих рекуррентных логических формул посредством линейных числовых полиномов. Линейные числовые полиномы, в отличие от общей (нелинейной) формы, обеспечивают высокую скорость вычислений. «Арифметизация» генераторов ПСП позволяет применить известные арифметиче-

ские коды (например, AN-коды, коды системы остаточных классов) для контроля процесса генерации ПСП. Параллельная реализация генератора ПСП в сочетании с перспективными возможностями контроля ошибок вычислений позволяет строить высокопроизводительные и безопасные средства криптографической защиты информации.

Псевдослучайная последовательность; линейный числовой полином; арифметический полином; криптография; шифры; шифрующая гамма.

S.A. Dichenko, A.K. Vishnevsky, O.A. Finko

IMPLEMENTATION OF BINARY LINEAR PSEUDORANDOM NUMERICAL POLYNOMIALS

An algorithm for parallel generation of pseudorandom binary sequences (PS) on the basis of representation systems generating recurrent logical formulas by means of numerical linear polynomials. Linear numerical polynomials, in contrast to the general (nonlinear) form, provide high-speed computing. "Arithmetization" Generator PS allows you to apply well-known arithmetic codes (eg, AN-codes, the system of residual classes) to control the generation of the PS. Parallel implementation of the PS generator coupled with promising error control capability allows you to build high-performance computing and secure means of cryptographic protection of information.

Pseudorandom sequence; numerical linear polynomial arithmetic polynomial; cryptography; ciphers encrypting range.

Введение. Генератор псевдослучайной последовательности (ПСП) имеет важнейшее значение для различных криптоалгоритмов и систем генерации ключевого материала [1–4]. Ужесточение требований к скорости шифрования и увеличение объема защищаемой информации вызывает необходимость построения параллельных алгоритмов генерации ПСП [1–6]. Наиболее распространенными и проверенными практикой являются алгоритмы генерации ПСП, основанные на рекуррентных логических выражениях и неприводимых полиномах [1–4].

В частности, регистр сдвига с обратной связью длины r, реализующий данный метод, имеет r ячеек памяти, значения которых совместно образуют (начальное) состояние $(a_0,...,a_k,...,a_{r-1}\rightarrow)$. После первого такта работы регистр сдвига выдаст a_0 и перейдет в состояние $(a_1,...,a_r)$, где $a_r = a_i = a_{i+k-r} \oplus a_{i-r}$. Продолжая, таким образом, регистр сдвига генерирует бесконечную последовательность $\{a_i\}\ i \geq 0$ [2].

Общий вид регистров сдвига с обратной связью показан на рис. 1.

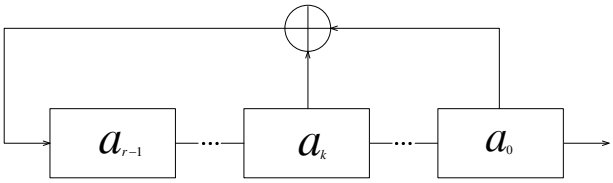

Рис. 1. Общий вид регистра сдвига с обратной связью

Цель статьи – распараллеливание алгоритма генерации ПСП с использованием ЛЧП.

Рассмотрим характеристическое уравнение тринома

$$D(x) = x^r + x^k + 1, \tag{1}$$

где r – степень тринома, $r \in N$, $r \geq 3$, $1 \leq k \leq r-1$, $k \in N$, которое имеет вид

$$a_i = a_{i+k-r} \oplus a_{i-r}, \tag{2}$$

где $a_i, a_{i+k-r}, a_{i-r} \in \{0,1\}$, $i \geq r$, $i \in N$.

Тогда, система характеристических уравнений для участка ПСП длины r $(i \div i+r-1)$ примет вид

$$\begin{cases} a_i = a_{i+k-r} \oplus a_{i-r}, \\ a_{i+1} = a_{i+k-r+1} \oplus a_{i-r+1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{i+r-1} = a_{i+k-1} \oplus a_{i-1}, \end{cases} \quad (3)$$

где $\begin{bmatrix} a_{i-r} & a_{i-r+1} & \ldots & a_{i-1} \end{bmatrix}$ – вектор начальных условий, $\begin{bmatrix} a_i & a_{i+1} & \ldots & a_{i+r-1} \end{bmatrix}$ – вектор участка ПСП, $a_k \in \{0,1\}, k = i-r+1,\ldots,i+r-1$.

Выразим правые части системы (3) через заданные начальные условия:

$$\begin{cases} a_i = a_{i+k-r} \oplus a_{i-r}, \\ a_{i+1} = a_{i+k-r+1} \oplus a_{i-r+1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{i+r-1} = \bigoplus_{t=i-r}^{i-1} g_t a_t, \end{cases} \quad (4)$$

где g_t принадлежит «0» или «1» в зависимости от вхождения в формулу a_t.

Представим систему (4) как систему r – булевых функций (БФ) от r – переменных:

$$F(\mathbf{x}) = \begin{cases} f_i(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1}) = a_{i+k-r} \oplus a_{i-r}, \\ f_{i+1}(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1}) = a_{i+k-r+1} \oplus a_{i-r+1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_{i+r-1}(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1}) = \bigoplus_{t=i-r}^{i-1} g_t a_t. \end{cases} \quad (5)$$

Используем правило представления БФ в базисе $\Omega = \{\oplus, 1\}$ посредством одного ЛЧП [7–9]:

$$f(y_1, y_2, \ldots, y_n) = \bigoplus_{i=1}^{n} y_i \rightarrow P(y_1, y_2, \ldots, y_n) = \sum_{i=1}^{n} y_i,$$

где результат вычисления БФ $f(y_1, y_2, \ldots, y_n)$ соответствует значению младшего разряда двоичного представления результата вычисления $P(y_1, y_2, \ldots, y_n)$.

Запишем систему БФ (5) как систему ЛЧП:

$$\begin{cases} P_i(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1}) = a_{i+k-r} + a_{i-r}, \\ P_{i+1}(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1}) = a_{i+k-r+1} + a_{i-r+1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ P_{i+r-1}(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1}) = \sum_{t=i-r}^{i-1} g_t a_t, \end{cases} \quad (6)$$

где $P_j(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1})$ соответствует $f_j(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1})$ системы булевых функций (5), $j = i, i+1, \ldots, i+r-1$.

Представим (6) следующим образом:

$$\begin{cases} P_i(a_{i-r}, a_{i-r+1}, ..., a_{i-1}) = \sum_{t=i-r}^{i-1} g_{i,t} a_t, \\ P_{i+1}(a_{i-r}, a_{i-r+1}, ..., a_{i-1}) = \sum_{t=i-r}^{i-1} g_{i+1,t} a_t, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ P_{i+r-1}(a_{i-r}, a_{i-r+1}, ..., a_{i-1}) = \sum_{t=i-r}^{i-1} g_{i+r-1,t} a_t, \end{cases} \quad (7)$$

где $g_{j,t}$ принимает значение «0» или «1» в зависимости от вхождения в j-й ЛЧП a_t.

Из формулы (7) следует, что результат вычисления j-го ЛЧП системы (7) можно представить двоичным машинным словом длины

$$l_j = \left\lfloor \log\left(\sum_{t=i-r}^{i-1} g_{j,t}\right) \right\rfloor + 1.$$

Таким образом, для размещения результатов вычисления всех r ЛЧП системы (7) 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 (7).

Представим систему (7) посредством одного ЛЧП вида

$$\begin{aligned} & H(a_{i-r}, a_{i-r+1}, ..., a_{i-1}) = P_i(a_{i-r}, a_{i-r+1}, ..., a_{i-1}) + \\ & + \sum_{s=i+1}^{i+r-1} 2^{\lambda_s} P_s(a_{i-r}, a_{i-r+1}, ..., a_{i-1}) = \\ & = g_{i,i-r} a_{i-r} + ... + g_{i,i-1} a_{i-1} + ... + \\ & + 2^{\lambda_{i+r-1}} g_{i+r-1,i-r} a_{i-r} + ... + 2^{\lambda_{i+r-1}} g_{i+r-1,i-1} a_{i-1} = \\ & = d_{i-r} a_{i-r} + d_{i-r+1} a_{i-r+1} + ... + d_{i-1} a_{i-1}, \end{aligned} \quad (8)$$

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

Пример.

На рис. 2 представлен комбинирующий рекуррентный регистр сдвига (LFSR), охваченный логической обратной связью (обратная связь реализуется через сумматор по модулю два) [4]. Рассмотрим LFSR на 22 бита:

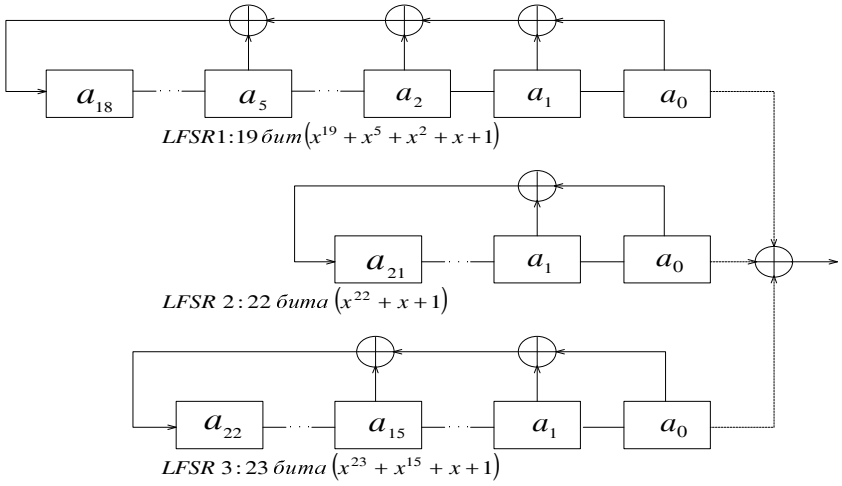

Рис. 2. Комбинирующий рекуррентный регистр сдвига

Образующий трином имеет вид

$$D(x) = x^{22} + x + 1,$$

характеристическое уравнение:

$$a_i = a_{i-21} \oplus a_{i-22.}$$

Система характеристических уравнений участка ПСП длины r имеет вид

$$\begin{cases} a_i = a_{i-21} \oplus a_{i-22}, \\ a_{i+1} = a_{i-20} \oplus a_{i-21}, \\ a_{i+2} = a_{i-19} \oplus a_{i-20}, \\ a_{i+3} = a_{i-18} \oplus a_{i-19}, \\ a_{i+4} = a_{i-17} \oplus a_{i-18}, \\ a_{i+5} = a_{i-16} \oplus a_{i-17}, \\ a_{i+6} = a_{i-15} \oplus a_{i-16}, \\ a_{i+7} = a_{i-14} \oplus a_{i-15}, \\ a_{i+8} = a_{i-13} \oplus a_{i-14}, \\ a_{i+9} = a_{i-12} \oplus a_{i-13}, \\ a_{i+10} = a_{i-11} \oplus a_{i-12}, \end{cases} \quad \begin{cases} a_{i+11} = a_{i-10} \oplus a_{i-11}, \\ a_{i+12} = a_{i-9} \oplus a_{i-10}, \\ a_{i+13} = a_{i-8} \oplus a_{i-9}, \\ a_{i+14} = a_{i-7} \oplus a_{i-8}, \\ a_{i+15} = a_{i-6} \oplus a_{i-7}, \\ a_{i+16} = a_{i-5} \oplus a_{i-6}, \\ a_{i+17} = a_{i-4} \oplus a_{i-5}, \\ a_{i+18} = a_{i-3} \oplus a_{i-4}, \\ a_{i+19} = a_{i-2} \oplus a_{i-3}, \\ a_{i+20} = a_{i-1} \oplus a_{i-2}, \\ a_{i+21} = a_{i-21} \oplus a_{i-22} \oplus a_{i-1}. \end{cases}$$

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

$$\begin{cases} f_i(a_{i-22}, ..., a_{i-1}) = a_{i-21} \oplus a_{i-22}, \\ f_{i+1}(a_{i-22}, ..., a_{i-1}) = a_{i-20} \oplus a_{i-21}, \\ f_{i+2}(a_{i-22}, ..., a_{i-1}) = a_{i-19} \oplus a_{i-20}, \\ f_{i+3}(a_{i-22}, ..., a_{i-1}) = a_{i-18} \oplus a_{i-19}, \\ f_{i+4}(a_{i-22}, ..., a_{i-1}) = a_{i-17} \oplus a_{i-18}, \\ f_{i+5}(a_{i-22}, ..., a_{i-1}) = a_{i-16} \oplus a_{i-17}, \\ f_{i+6}(a_{i-22}, ..., a_{i-1}) = a_{i-15} \oplus a_{i-16}, \\ f_{i+7}(a_{i-22}, ..., a_{i-1}) = a_{i-14} \oplus a_{i-15}, \\ f_{i+8}(a_{i-22}, ..., a_{i-1}) = a_{i-13} \oplus a_{i-14}, \\ f_{i+9}(a_{i-22}, ..., a_{i-1}) = a_{i-12} \oplus a_{i-13}, \\ f_{i+10}(a_{i-22}, ..., a_{i-1}) = a_{i-11} \oplus a_{i-12}, \end{cases} \quad \begin{cases} f_{i+11}(a_{i-22}, ..., a_{i-1}) = a_{i-10} \oplus a_{i-11}, \\ f_{i+12}(a_{i-22}, ..., a_{i-1}) = a_{i-9} \oplus a_{i-10}, \\ f_{i+13}(a_{i-22}, ..., a_{i-1}) = a_{i-8} \oplus a_{i-9}, \\ f_{i+14}(a_{i-22}, ..., a_{i-1}) = a_{i-7} \oplus a_{i-8}, \\ f_{i+15}(a_{i-22}, ..., a_{i-1}) = a_{i-6} \oplus a_{i-7}, \\ f_{i+16}(a_{i-22}, ..., a_{i-1}) = a_{i-5} \oplus a_{i-6}, \\ f_{i+17}(a_{i-22}, ..., a_{i-1}) = a_{i-4} \oplus a_{i-5}, \\ f_{i+18}(a_{i-22}, ..., a_{i-1}) = a_{i-3} \oplus a_{i-4}, \\ f_{i+19}(a_{i-22}, ..., a_{i-1}) = a_{i-2} \oplus a_{i-3}, \\ f_{i+20}(a_{i-22}, ..., a_{i-1}) = a_{i-1} \oplus a_{i-2}, \\ f_{i+21}(a_{i-22}, ..., a_{i-1}) = a_{i-21} \oplus a_{i-22} \oplus a_{i-1}. \end{cases}$$

Получим систему ЛЧП:

$$\begin{cases} P_i(a_{i-22}, ..., a_{i-1}) = a_{i-21} + a_{i-22}, \\ P_{i+1}(a_{i-22}, ..., a_{i-1}) = a_{i-20} + a_{i-21}, \\ P_{i+2}(a_{i-22}, ..., a_{i-1}) = a_{i-19} + a_{i-20}, \\ P_{i+3}(a_{i-22}, ..., a_{i-1}) = a_{i-18} + a_{i-19}, \\ P_{i+4}(a_{i-22}, ..., a_{i-1}) = a_{i-17} + a_{i-18}, \\ P_{i+5}(a_{i-22}, ..., a_{i-1}) = a_{i-16} + a_{i-17}, \\ P_{i+6}(a_{i-22}, ..., a_{i-1}) = a_{i-15} + a_{i-16}, \\ P_{i+7}(a_{i-22}, ..., a_{i-1}) = a_{i-14} + a_{i-15}, \\ P_{i+8}(a_{i-22}, ..., a_{i-1}) = a_{i-13} + a_{i-14}, \\ P_{i+9}(a_{i-22}, ..., a_{i-1}) = a_{i-12} + a_{i-13}, \\ P_{i+10}(a_{i-22}, ..., a_{i-1}) = a_{i-11} + a_{i-12}, \end{cases} \quad \begin{cases} P_{i+11}(a_{i-22}, ..., a_{i-1}) = a_{i-10} + a_{i-11}, \\ P_{i+12}(a_{i-22}, ..., a_{i-1}) = a_{i-9} + a_{i-10}, \\ P_{i+13}(a_{i-22}, ..., a_{i-1}) = a_{i-8} + a_{i-9}, \\ P_{i+14}(a_{i-22}, ..., a_{i-1}) = a_{i-7} + a_{i-8}, \\ P_{i+15}(a_{i-22}, ..., a_{i-1}) = a_{i-6} + a_{i-7}, \\ P_{i+16}(a_{i-22}, ..., a_{i-1}) = a_{i-5} + a_{i-6}, \\ P_{i+17}(a_{i-22}, ..., a_{i-1}) = a_{i-4} + a_{i-5}, \\ P_{i+18}(a_{i-22}, ..., a_{i-1}) = a_{i-3} + a_{i-4}, \\ P_{i+19}(a_{i-22}, ..., a_{i-1}) = a_{i-2} + a_{i-3}, \\ P_{i+20}(a_{i-22}, ..., a_{i-1}) = a_{i-1} + a_{i-2}, \\ P_{i+21}(a_{i-22}, ..., a_{i-1}) = a_{i-21} + a_{i-22} + a_{i-1}. \end{cases}$$

Получим ЛЧП:

$$H(a_{i-22}, ..., a_{i-1}) = \left(4 \cdot 10^{10} + 1\right)_{16} a_{i-22} + \left(4 \cdot 10^{10} + 5\right)_{16} a_{i-21} + (14)_{16} a_{i-20} +$$
$$+ (50)_{16} a_{i-19} + (140)_{16} a_{i-18} + \left(5 \cdot 10^{2}\right)_{16} a_{i-17} + \left(14 \cdot 10^{2}\right)_{16} a_{i-16} +$$
$$+ \left(5 \cdot 10^{3}\right)_{16} a_{i-15} + \left(14 \cdot 10^{3}\right)_{16} a_{i-14} + \left(5 \cdot 10^{4}\right)_{16} a_{i-13} + \left(14 \cdot 10^{4}\right)_{16} a_{i-12} +$$
$$+ \left(5 \cdot 10^{5}\right)_{16} a_{i-11} + \left(14 \cdot 10^{5}\right)_{16} a_{i-10} + \left(5 \cdot 10^{6}\right)_{16} a_{i-9} + \left(14 \cdot 10^{6}\right)_{16} a_{i-8} +$$
$$+ \left(5 \cdot 10^{7}\right)_{16} a_{i-7} + \left(14 \cdot 10^{7}\right)_{16} a_{i-6} + \left(5 \cdot 10^{8}\right)_{16} a_{i-5} + \left(14 \cdot 10^{8}\right)_{16} a_{i-4} +$$
$$+ \left(5 \cdot 10^{9}\right)_{16} a_{i-3} + \left(14 \cdot 10^{9}\right)_{16} a_{i-2} + \left(5 \cdot 10^{10}\right)_{16} a_{i-1},$$

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

Пусть $a_{i-22} = 1$, $a_{i-21} = 0$, $a_{i-20} = 0$, $a_{i-19} = 0$, $a_{i-18} = 0$, $a_{i-17} = 1$, $a_{i-16} = 0$, $a_{i-15} = 0$, $a_{i-14} = 0$, $a_{i-13} = 0$, $a_{i-12} = 0$, $a_{i-11} = 0$, $a_{i-10} = 1$, $a_{i-9} = 0$, $a_{i-8} = 0$, $a_{i-7} = 0$, $a_{i-6} = 1$, $a_{i-5} = 0$, $a_{i-4} = 0$, $a_{i-3} = 0$, $a_{i-2} = 0$, $a_{i-1} = 1$.

Тогда

$$H = \left(4 \cdot 10^{10} + 1\right)_{16} \cdot 1 + \left(4 \cdot 10^{10} + 5\right)_{16} \cdot 0 + (14)_{16} \cdot 0 + (50)_{16} \cdot 0 + (140)_{16} \cdot 0 +$$
$$+ \left(5 \cdot 10^{2}\right)_{16} \cdot 1 + \left(14 \cdot 10^{2}\right)_{16} \cdot 0 + \left(5 \cdot 10^{3}\right)_{16} \cdot 0 + \left(14 \cdot 10^{3}\right)_{16} \cdot 0 + \left(5 \cdot 10^{4}\right)_{16} \cdot 0 +$$
$$+ \left(14 \cdot 10^{4}\right)_{16} \cdot 0 + \left(5 \cdot 10^{5}\right)_{16} \cdot 0 + \left(14 \cdot 10^{5}\right)_{16} \cdot 1 + \left(5 \cdot 10^{6}\right)_{16} \cdot 0 + \left(14 \cdot 10^{6}\right)_{16} \cdot 0 +$$
$$+ \left(5 \cdot 10^{7}\right)_{16} \cdot 0 + \left(14 \cdot 10^{7}\right)_{16} \cdot 1 + \left(5 \cdot 10^{8}\right)_{16} \cdot 0 + \left(14 \cdot 10^{8}\right)_{16} \cdot 0 + \left(5 \cdot 10^{9}\right)_{16} \cdot 0 +$$
$$+ \left(14 \cdot 10^{9}\right)_{16} \cdot 0 + \left(5 \cdot 10^{10}\right)_{16} \cdot 1 = (90141400501)_{16} =$$
$$= (1\ \underbrace{0\ 0}_{f_{i+21}}\ \underbrace{1}_{f_{i+20}}\ \underbrace{0\ 0}_{f_{i+19}}\ \underbrace{0\ 0}_{f_{i+18}}\ \underbrace{0\ 0}_{f_{i+17}}\ \underbrace{0}_{f_{i+16}}\ \underbrace{1}_{f_{i+15}}\ \underbrace{0}_{f_{i+14}}\ \underbrace{1}_{f_{i+13}}\ \underbrace{0\ 0}_{f_{i+12}}\ \underbrace{0\ 0}_{f_{i+11}}\ \underbrace{0}_{f_{i+10}}\ \underbrace{1}_{f_{i+9}}\ \underbrace{0}_{f_{i+8}}\ \underbrace{1}_{f_{i+7}}\ \underbrace{0}_{f_{i+6}}\ \underbrace{1}_{f_{i+5}}\ \underbrace{0}_{f_{i+4}}\ \underbrace{0\ 0}_{f_{i+3}}\ \underbrace{0}_{f_{i+2}}\ \underbrace{0}_{f_{i+1}}\ \underbrace{0\ 1}_{f_i})_2.$$

Таким образом, в данном примере с помощью одного ЛЧП мы получим фрагмент ПСП длины r. В табл. 1 представлен пример для начальных условий: $a_{i-22} = 1$, $a_{i-21} = 0$, $a_{i-20} = 0$, $a_{i-19} = 0$, $a_{i-18} = 0$, $a_{i-17} = 1$, $a_{i-16} = 0$, $a_{i-15} = 0$,

$a_{i-14}=0$, $a_{i-13}=0$, $a_{i-12}=0$, $a_{i-11}=0$, $a_{i-10}=1$, $a_{i-9}=0$, $a_{i-8}=0$, $a_{i-7}=0$, $a_{i-6}=1$, $a_{i-5}=0$, $a_{i-4}=0$, $a_{i-3}=0$, $a_{i-2}=0$, $a_{i-1}=1$.

Таблица 1

Таблица истинности для тринома $D(x)=x^{22}+x\ +1$

№ такта	a_{i-1}	a_{i-2}	a_{i-3}	a_{i-4}	…	a_{i-19}	a_{i-20}	a_{i-21}	a_{i-22}	Выходная послед-ть	f_n
0	1	0	0	0	…	0	0	0	1	1	f_{i-22}
1	1	1	0	0	…	0	0	0	0	0	f_{i-21}
2	0	1	1	0	…	1	0	0	0	0	f_{i-20}
3	0	0	1	1	…	0	1	0	0	0	f_{i-19}
4	0	0	0	1	…	0	0	1	0	0	f_{i-18}
5	1	0	0	0	…	0	0	0	1	1	f_{i-17}
6	1	1	0	0	…	0	0	0	0	0	f_{i-16}
7	0	1	1	0	…	0	0	0	0	0	f_{i-15}
8	0	0	1	1	…	0	0	0	0	0	f_{i-14}
9	0	0	0	1	…	1	0	0	0	0	f_{i-13}
10	0	0	0	0	…	0	1	0	0	0	f_{i-12}
11	0	0	0	0	…	0	0	1	0	0	f_{i-11}
12	1	0	0	0	…	0	0	0	1	1	f_{i-10}
13	1	1	0	0	…	1	0	0	0	0	f_{i-9}
14	0	1	1	0	…	0	1	0	0	0	f_{i-8}
15	0	0	1	1	…	0	0	1	0	0	f_{i-7}
16	1	0	0	1	…	0	0	0	1	1	f_{i-6}
17	1	1	0	0	…	0	0	0	0	0	f_{i-5}
18	0	1	1	0	…	1	0	0	0	0	f_{i-4}
19	0	0	1	1	…	1	1	0	0	0	f_{i-3}
20	0	0	0	1	…	0	1	1	0	0	f_{i-2}
21	1	0	0	0	…	0	0	1	1	1	f_{i-1}
22	0	1	0	0	…	0	0	0	1	1	f_i
23	1	0	1	0	…	1	0	0	0	0	f_{i+1}
24	0	1	0	1	…	1	1	0	0	0	f_{i+2}
25	0	0	1	0	…	0	1	1	0	0	f_{i+3}

Окончание табл. 1

№ такта	a_{i-1}	a_{i-2}	a_{i-3}	a_{i-4}	…	a_{i-19}	a_{i-20}	a_{i-21}	a_{i-22}	Выходная послед-ть	f_n
26	1	0	0	1	…	0	0	1	1	1	f_{i+4}
27	0	1	0	0	…	0	0	0	1	1	f_{i+5}
28	1	0	1	0	…	0	0	0	0	0	f_{i+6}
29	0	1	0	1	…	0	0	0	0	0	f_{i+7}
30	0	0	1	0	…	1	0	0	0	0	f_{i+8}
31	0	0	0	1	…	1	1	0	0	0	f_{i+9}
32	0	0	0	0	…	0	1	1	0	0	f_{i+10}
33	1	0	0	0	…	0	0	1	1	1	f_{i+11}
34	0	1	0	0	…	1	0	0	1	1	f_{i+12}
35	1	0	1	0	…	1	1	0	0	0	f_{i+13}
36	0	1	0	1	…	0	1	1	0	0	f_{i+14}
37	1	0	1	0	…	0	0	1	1	1	f_{i+15}
38	0	1	0	1	…	0	0	0	1	1	f_{i+16}
39	1	0	1	0	…	1	0	0	0	0	f_{i+17}
40	0	1	0	1	…	0	1	0	0	0	f_{i+18}
41	0	0	1	0	…	1	0	1	0	0	f_{i+19}
42	1	0	0	1	…	0	1	0	1	1	f_{i+20}
43	1	1	0	0	…	0	0	1	0	0	f_{i+21}

Преимуществом представления систем характеристических уравнений посредством ЛЧП является небольшая длина ЛЧП

$$L(D(\mathbf{x})) = n,$$

которая определяется количеством слагаемых, и всегда равна количеству переменных, в отличие от сложности системы булевых формул, определяемой их длиной.

Длина булевой формулы $C(f(\mathbf{x}))$ определяется количеством вхождений в булеву формулу переменных.

Подсчитав общее количеством вхождений переменных во все булевы формулы системы (5), можно определить сложность $C(F(\mathbf{x}))$ системы (5).

Таким образом, сложность системы БФ (5) при $n = 2b$ и $1 \le k \le \frac{n}{2} - 1$, $n = 2b+1$ и $1 \le k \le \frac{n-1}{2}$ определяется выражением $C(F(\mathbf{x})) = 2(n-k) + 3k$.

На рис. 3 демонстрируется зависимость выигрыша от представления систем характеристических уравнений посредством ЛЧП для заданного k и длины участка генерируемой ПСП n:

$$V = \frac{C(F(\mathbf{x}))}{L(D(\mathbf{x}))}.$$

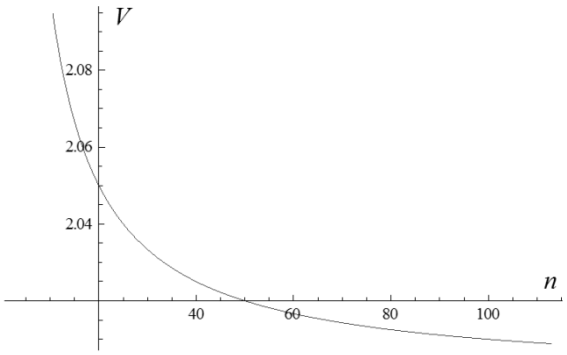

Рис. 3. Оценка выигрыша представления системы характеристических уравнений посредством ЛЧП

Полученный выигрыш от представления систем характеристических уравнений посредством ЛЧП будет равен $V > 2$.

Для условий $n = 2b$ и $k = \frac{n}{2}$ определяется выражением $C(F(\mathbf{x})) = \frac{3n}{2}$.

На рис. 4 демонстрируется зависимость выигрыша от представления систем характеристических уравнений посредством ЛЧП для заданного k и длины участка генерируемой ПСП n:

$$V = \frac{C\ (F(\mathbf{x}))}{L(D(\mathbf{x}))}.$$

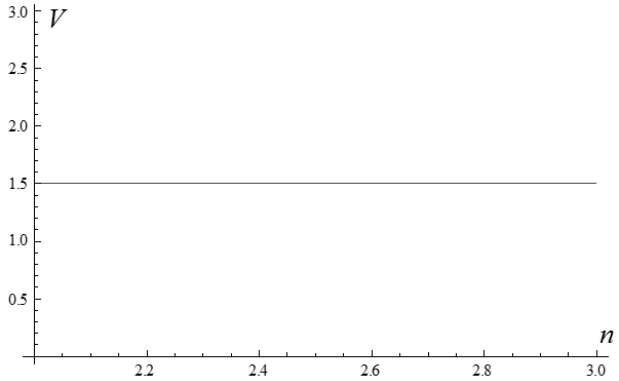

Рис. 4. Оценка выигрыша представления системы характеристических уравнений посредством ЛЧП

Полученный выигрыш от представления систем характеристических уравнений посредством ЛЧП будет равен $V = 1{,}5$.

Для условий $n = 2b$, $n = 2b+1$ и $k = n-1$ определяется выражением

$$C(F(\mathbf{x})) = \frac{n^2 + 3n - 4}{2}.$$

На рис. 5 демонстрируется зависимость выигрыша от представления систем характеристических уравнений посредством ЛЧП для заданного k и длины участка генерируемой ПСП n:

$$V = \frac{C(F(\mathbf{x}))}{L(D(\mathbf{x}))}.$$

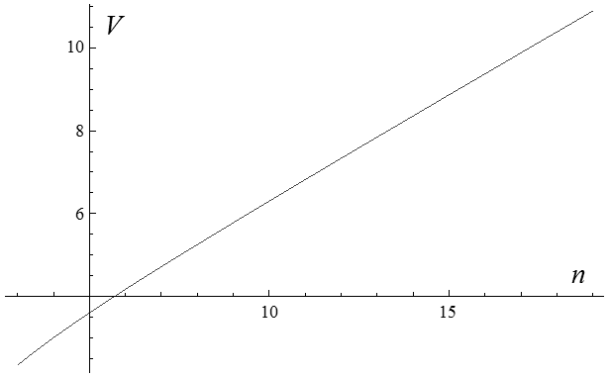

Рис. 5. Оценка выигрыша представления системы характеристических уравнений посредством ЛЧП

Полученный выигрыш от представления систем характеристических уравнений посредством ЛЧП будет равен $V \geq 3$.

Вывод. Таким образом, разработан метод распараллеливания алгоритма генерации ПСП на основе представления систем булевых функций числовыми формулами (ЛЧП), в отличие от общепринятых методов, основанных на алгебре логики. Данный метод является эффективным для реализации скоростных криптографических алгоритмов защиты больших объемов данных (например, мультимедиа). Кроме того, как показано в [8], для числовых методов легко реализовать контроль (коррекцию) ошибок вычислений в реальном масштабе времени посредством избыточных арифметических кодов (например, AN-кодов, кодов системы остаточных классов и др.), что является чрезвычайно важным для обеспечения безопасности функционирования 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: Учебное пособие / Фороузан Б.А.: 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. – Воронеж, 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., 2010.

7. *Малюгин В.Д.* Параллельные логические вычисления посредством арифметических полиномов. – М.: Физматлит, 1997. – 192 с.
8. *Финько О.А.* Модулярная арифметика параллельных логических вычислений. – М.: ИПУ РАН, 2003. – 224 с.
9. *Yanushkevich S., Shmerko V., Lyshevski S.* Logic design of nanoICs. – CRCPress, 2005.

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

Диченко Сергей Александрович
Филиал Военной академии связи (г. Краснодар).
E-mail: dichenko.sa@yandex.ru.
350035, г. Краснодар, ул. Красина, 4.
Тел.: +79618588866.
Адъюнкт очной адъюнктуры.

Вишневский Артем Константинович
E-mail: vishn.artem@yandex.ru.
Тел.: +79181811798.
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, 350035, Russia.
Phone: +79618588866.
Associate Postgraduate Full-time.

VishnevskyArtemKonstantinovich
E-mail: vishn.artem@yandex.ru.
Phone: +79181811798.
Associate Postgraduate Full-time.

Finko Oleg Anatolievich
E-mail: ofinko@yandex.ru.
Phone: +79615874848.
Professor.

УДК 004.91

Д.А. Ржевский, Н.И. Елисеев, Н.Д. Абасов, О.А. Финько

ЭЛЕКТРОННАЯ ПОДПИСЬ, УСТОЙЧИВАЯ К ДЕСТРУКТИВНЫМ ВОЗДЕЙСТВИЯМ

Рассматривается устойчивая к ошибкам многоканальная криптосистема, которая при соответствующих условиях может быть использована и для построения устойчивой к ошибкам системы групповой электронной подписи, функционирующей в кольце положительных целых чисел по модулю p. Предложены решения, позволяющие обеспечить электронную подпись новым свойством самовосстановления с заданной вероятностью при различных деструктивных воздействиях на нее. По отношению к методам кратного дублирования достигается существенное уменьшение избыточности. Представлены оценки обнаруживающей способности.

Китайская теорема об остатках; модулярная арифметика; электронная подпись; электронный документооборот.