$$M = \left(\left(\left(\left(C + K_4^*\right)_{\mathrm{mod}\,2^n} \times K_3^*\right)_{\mathrm{mod}\,2^n} \oplus K_2\right) \times K_1^*\right)_{\mathrm{mod}\,2^n}. \quad (11)$$

Як бачимо, операцію розшифрування можна представити у вигляді виразу, подібного до того, що використовується для зашифрування. Таким чином, процедури зашифрування і розшифрування використовують однаковий ключ K_2, і три різних ключа K_1, K_3 та K_4 для зашифрування і K_1^*, K_3^* та K_4^* для розшифрування.

Значення числа n (розрядність блоку даних) обирається довільно із міркувань швидкодії та криптостійкості, а також може змінюватись в процесі шифрування. Із збільшенням n автоматично збільшується кількість елементарних операцій, необхідних для опрацювання блока даних.

V Висновки

Запропоновано алгоритм блокового симетричного шифрування на основі арифметичних операцій за модулем 2^n. Всі операції в алгоритмі виконуються над блоками даних, які представляються як цілі числа з множини Z_{2^n}. Операції зашифрування та розшифрування використовують секретний ключ, що складається з чотирьох секретних підключів. Секретні підключі K_1, K_2, K_3 та K_4 використовуються для зашифрування, а для розшифрування необхідно попередньо обчислити підключі K_1^*, K_3^*та K_4^*. Ключ K_2 не змінюється при розшифруванні.

Запропонований БСШ володіє високою швидкістю за рахунок використання простих арифметичних операцій, які швидко виконуються на сучасних ЕОМ. Також алгоритм просто реалізується в апаратному вигляді, оскільки містить обмежений набір простих операцій. Швидкість процедур зашифрування та розшифрування приблизно однакова і залежить окрім тактової частоти від розрядності обчислювального пристрою. Для підвищення швидкості виконання операції множення великих чисел можна скористатись додатковими інструкціями процесора, кількість яких постійно збільшується.

Література: ***1.*** *А. В. Потий, О. И. Олешко. Новые требования и принципы разработки современных алгоритмов блочного шифрования (по результатам анализа алгоритмов-кандидатов в AES)// Открытые информационные и компьютерные технологии. 2000. Вып. 12. С. 30 - 45.* ***2.*** *Вильям Столлингс. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Издательский дом "Вильямс", 2001. – 452 с.* ***3.*** *Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448с.* ***4.*** *Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin. The RC4 Block Cipher, version 1.1 – 04. 1998*

УДК 681.3.067:681.3.016

МЕТОДИКА СОЗДАНИЯ ГЕНЕРАТОРОВ ПЕРИОДИЧЕСКИХ БИТОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Тарас Левченко
Национальный банк Украины

Аннотация. **Исследована возможность использования решений однородных линейных уравнений с формальными производными как генераторов периодических битовых последовательностей. Предложена методика синтеза таких генераторов. Даны рекомендации по применению методики.**
Summary. **There is investigated possibility to exploring the linear boolean equations as a periodic bits sequences generators. There is proposed methodology for such generator synthesis. There are given recommendations on application of a methodology.**
Ключевые слова: **формальная производная, разностное уравнение, псевдослучайные последовательности.**

Безопасное функционирование информационных систем в банковской сфере Украины, помимо прочих факторов [1], связано с надежной высокоскоростной генерацией битовых последовательностей, используемых для криптозащиты [2]. Существует несколько способов генерации статистически удовлетворительных битовых последовательностей [3] с некоторым, обычно весьма большим, периодом. В

банковских системах для защиты информации регулярно возникает необходимость использовать псевдослучайные последовательности для генерации различных криптообъектов: сеансовых ключей, синхропосылок и т. д. Поскольку частота сеансов генерации таких объектов в ряде случаев очень высока, то значительную роль играет скорость их выполнения. Это ограничивает сложность допустимых алгоритмов генерации и, соответственно, накладывает ограничения на качество статистических свойств генератора, то есть итоговое техническое решение должно быть результатом некоторого компромисса.

К сожалению, создание единой методики разработки таких способов наталкивается на теоретические трудности и в большинстве случаев производится полуэмпирическим путем. Представляет интерес разработка методологического подхода, позволяющего создавать слабо усложняющиеся быстродействующие генераторы битов с заранее заданным периодом.

Указанный подход предлагается искать в виде решений рассмотренных в [4 – 6] линейных уравнений преобразований с формальной производной, полученной из определения обычной производной

$$\lim_{h\to 0}\frac{\left|f(x+h)-f(x)-B(x)h\right|}{\left|h\right|}=0. \qquad (1)$$

Линейное отображение B определяется предложенным в [4] выражением

$$\mathrm{B}y_i = y_i \oplus y_{i-1}, \qquad (2)$$

где $\oplus$ - сложение по модулю 2, y_i , i=1, 2, … ,– последовательность с элементами поля Галуа *GF*(2)**.** Свойства отображения **B,** аналогичного формальной производной**,** отличаются от свойств $B(i)$ в (1) тем, что в выражении $\mathbf{B}(y_{i-1}\ y_i)= (\mathbf{B}y_{i-1})y_i \oplus y_i\ (\mathbf{B}y_{i-1})\oplus(\mathbf{B}y_{i-1})(\mathbf{B}y_{i-1})$ слагаемым $(\mathbf{B}y_{i-1})(\mathbf{B}y_{i-1})$ нельзя пренебречь, что характерно для конечных разностей. Дискретность аргумента i позволяет трактовать это определение как разностную схему.

Пользуясь (2) на множестве i можно построить формальные производные $\mathbf{B}^{(j)}y_i$ порядка j из соотношения

$$\mathrm{B}^{(j)}y_i = \mathrm{B}^{(j-1)}y_{i-1} \oplus \mathrm{B}^{(j-1)}y_i. \qquad (3)$$

Однородным линейных уравнением с формальными производными (ОЛУФП) назовем уравнение

$$\sum_{j=0}^{J} c_j \mathrm{B}^{(j)}y_i = 0, \qquad (4)$$

где J – максимальный порядок производных, c_j - координаты некоторого битового вектора $\boldsymbol{c}$ размерности J, $c_j\neq 0$, $\mathbf{B}^{(j)}y_i$ вычисляются из (3). Здесь и в последующих выражениях знаком Σ обозначено суммирование по модулю 2**.**

В табл. 1 показан пошаговый индуктивный процесс получения формальных производных по мере увеличения i. Учтено очевидное соотношение $y_i \oplus y_i=0$.

Таблица 1 - Представление величин в ОЛУФП

		c_0	c_1	c_2	c_3	…	c_{J-1}	c_J
i	x_i	y_i	$\mathbf{B}y_i$	$\mathbf{B}^{II}y_i$	$\mathbf{B}^{III}y_i$	…	$\mathbf{B}^{(J-1)}y_i$	$\mathbf{B}^{(J)}y_i$
$-J+1$	-	y_{-J+1}	-	-	-	…	-	-
$-J+2$	-	y_{-J+2}	$y_{-J+1}\oplus y_{-J+2}$	-	-	…	-	-
…	-	…	…	…	…	…	…	…
-1	-	y_{-1}	$y_{-1}\oplus y_{-2}$	$y_{-1}\oplus y_{-3}$	$y_{-1}\oplus y_{-2}\oplus y_{-3}\oplus y_{-4}$	…	-	-
0	-	y_0	$y_0\oplus y_{-1}$	$y_0\oplus y_{-2}$	$y_0\oplus y_{-1}\oplus y_{-2}\oplus y_{-3}$	…	$\mathbf{B}^{(J-2)}y_0\oplus \mathbf{B}^{(J-2)}y_{-1}$	-
1	x_1	y_1	$y_1\oplus y_0$	$y_1\oplus y_{-1}$	$y_1\oplus y_0\oplus y_{-1}\oplus y_{-2}$	…	$\mathbf{B}^{(J-2)}y_1\oplus \mathbf{B}^{(J-2)}y_0$	$\mathbf{B}^{(J-1)}y_1\oplus \mathbf{B}^{(J-1)}y_0$
2	x_2	y_2	$y_2\oplus y_1$	$y_2\oplus y_0$	$y_2\oplus y_1\oplus y_0\oplus y_{-1}$	…	$\mathbf{B}^{(J-2)}y_2\oplus \mathbf{B}^{(J-2)}y_1$	$\mathbf{B}^{(J-1)}y_2\oplus \mathbf{B}^{(J-1)}y_1$
…	…	…	…	…	…	…	…	…
$J-1$	x_{J-1}	y_{J-1}	$y_{J-1}\oplus y_{J-2}$	$y_{J-1}\oplus y_{J-3}$	$y_{J-1}\oplus y_{J-2}\oplus$	…	$\mathbf{B}^{(J-2)}y_{J-1}\oplus \mathbf{B}^{(J-2)}y_{J-2}$	$\mathbf{B}^{(J-1)}y_{J-1}\oplus \mathbf{B}^{(J-1)}y_{J-21}$

					$y_{J-3}\oplus y_{J-4}$			
J	x_J	y_J	$y_J\oplus y_{J-1}$	$y_J\oplus y_{J-2}$	$y_J\oplus y_{J-1}\oplus y_{J-2}\oplus y_{J-3}$	…	$\mathbf{B}^{(J-2)}y_J\oplus \mathbf{B}^{(J-2)}y_{J-1}$	$\mathbf{B}^{(J-1)}y_J\oplus \mathbf{B}^{(J-1)}y_{J-1}$
$J+1$	x_{J+1}	y_{J+1}	$y_{J+1}\oplus y_J$	$y_{J+1}\oplus y_J$	$y_{J+1}\oplus y_J\oplus y_{J-1}\oplus y_{J-2}$	…	$\mathbf{B}^{(J-2)}y_{J+1}\oplus \mathbf{B}^{(J-2)}y_J$	$\mathbf{B}^{(J-1)}y_{J+1}\oplus \mathbf{B}^{(J-1)}y_J$
…	…	…	…	…	…	…	…	…
i	x_i	y_i	$y_i\oplus y_{i-1}$	$y_i\oplus y_{i-2}$	$y_i\oplus y_{i-1}\oplus y_{i-2}\oplus y_{i-3}$	…	$\mathbf{B}^{(J-2)}y_i\oplus \mathbf{B}^{(J-2)}y_{i-1}$	$\mathbf{B}^{(J-1)}y_i\oplus \mathbf{B}^{(J-1)}y_{i-1}$
…	…	…	…	…	…	…	…	…

Обозначив в табл. 1 коэффициенты при y_{i-k} через g_k и подставив соответствующие формулы в выражение (3), получим

$$\sum_{j=0}^{J} c_j \left[y_i \oplus \sum_{k=1}^{J} g_k y_{i-k} \right] = 0 . \qquad (5)$$

Из (5) при выполнении условия $\sum_{j=0}^{J} c_j = 1$ (см. [6]) получим

$$y_i = \sum_{j=0}^{J} c_j \sum_{k=1}^{J} g_k y_{i-k} = \sum_{k=1}^{J} y_{i-k} \sum_{j=0}^{J} c_j g_k = \sum_{k=1}^{J} r_k y_{i-k} , \qquad (6)$$

где

$$r_k = \sum_{j=0}^{J} c_j g_k . \qquad (7)$$

Таким образом, y_i является остатком от деления на 2 линейной комбинации предыдущих значений y_{i-k}, где k=1, 2, …, J.

Рассмотрим случай J=1. В табл. 2 приведены коэффициенты (7) формул (5) для расчета нескольких первых значений y_i, i=3, 4, …, по известным y_1 и y_2.

Таблица 2 - Коэффициенты формул (5) для J=1 в первых 7 итерациях

№ итерации	Значение последовательности	Коэффициенты при	
		y_2	y_1
1	y_1	0	1
2	y_2	1	0
3	y_3	r_1	r_2
4	y_4	$r_1\oplus r_2$	$r_1 r_2$
5	y_5	r_1	$r_1 r_2\oplus r_2$
6	y_6	$r_1\oplus r_1 r_2\oplus r_2$	$r_1 r_2$
7	y_7	$r_1\oplus r_1 r_2$	r_2

По мере увеличения номера итерации i общее выражение для y_i становится все более сложным. Однако в [7 – 8] было показано, что остатки по некоторому модулю числовых последовательностей, образованных рекурсивным путем, необходимо являются периодическими. Поскольку $r_1 \in GF(2)$ и $r_2 \in GF(2)$, то путем подбора для небольших значений J можно получить аналитические соотношения, показывающие периодичность возникающих последовательностей. Формулы приведения для рассматриваемого случая при возможных нетривиальных комбинациях r_1 и r_2 сведены в табл. 3.

Таблица 3 – Формулы приведения значений возможных ОЛУФП порядка J=1

№ п/п	r_1	r_2	ОЛУФП	Формулы приведения	Период
1	0	1	$\mathbf{B}y\oplus y$=0	$y_i = y_{i-2}$	2
2	1	0	y=0	$y_i = y_{i-1}$	1
3	1	1	$\mathbf{B}y$=0	$y_i = y_{i-1}\oplus y_{i-2} = y_{i-3}$	3

Из табл. 3 следует, что решения всех возможных ОЛУФП 1 порядка могут иметь период 1

(последовательность битов не изменяется и равна 0 либо 1 в зависимости от своего первого элемента), 2 (последовательность битов поочередно принимает значения 0 и 1 за исключением, возможно, своего первого элемента), а также 3 (последовательность битов последовательно принимает некоторую комбинацию из 3 значений 0 и 1 также за исключением, возможно, своего первого элемента). Таким образом, максимальный период полученной последовательности равен $2^{J+1}-1=3$.

В табл. 4 – 5 помещены несколько коэффициентов формул (5) и формулы приведения значений возможных ОЛУФП порядка J=2.

Таблица 4 – Коэффициенты формул (5) для J=2 в первых 7 итерациях

№ итерации	Значение последовательности	Коэффициенты при		
		y_3	y_2	y_1
1	y_1	0	0	1
2	y_2	0	1	0
3	y_3	1	0	0
4	y_4	r_1	r_2	r_3
5	y_5	$r_1 \oplus r_2$	$r_1 \cdot r_2 \oplus r_3$	$r_1 r_3$
6	y_6	$r_1 \oplus r_3$	$r_1 \cdot r_2 \oplus r_1 \cdot r_3 \oplus r_2$	$r_1 \cdot r_3 \oplus \cdot r_3$
7	y_7	$r_1 \oplus r_1 r_2 \oplus r_2$	$r_1 \cdot r_2 \oplus r_1 \cdot r_3$	$r_1 r_2 \oplus r_2$
8	y_8	$r_1 \oplus r_1 r_3 \oplus r_1 \cdot r_2$	$r_1 r_3 \oplus r_3$	$r_1 r_2 r_3 \oplus r_1 \cdot r_3 \oplus r_2 \cdot r_3$

Таблица 5 – Формулы приведения значений возможных ОЛУФП порядка J=2

№ п/п	r_1	r_2	r_3	ОЛУФП	Формулы приведения	Период
1.	0	0	1	$\mathbf{B}^{II}y \oplus y=0$	$y_i = y_{i-3}$	3
2.	0	1	0	$\mathbf{B}y \oplus y=0$	$y_i = y_{i-2}$	2
3.	0	1	1	$\mathbf{B}^{II}y \oplus \mathbf{B}y=0$	$y_i = y_{i-2} \oplus y_{i-3} = y_{i-4} \oplus y_{i-6} = y_{i-7}$	7
4.	1	0	0	$y=0$	$y_i = y_{i-1}$	1
5.	1	0	1	$\mathbf{B}^{II}y=0$	$y_i = y_{i-1} \oplus y_{i-3} = y_{i-3} \oplus y_{i-5} \oplus y_{i-6} = y_{i-4} \oplus y_{i-5} = y_{i-7}$	7
6.	1	1	0	$\mathbf{B}y=0$	$y_i = y_{i-1} \oplus y_{i-2} = y_{i-3}$	3
7.	1	1	1	$\mathbf{B}^{II}y \oplus \mathbf{B}y \oplus y =0$	$y_i = y_{i-1} \oplus y_{i-2} \oplus y_{i-3} = y_{i-4}$	4

В табл. 6 – 7 показаны несколько коэффициентов формул (5) и формулы приведения значений возможных ОЛУФП порядка J=3.

Таблица 6 – Коэффициенты формул (5) для J=3 в первых 16 итерациях

№ итерации	Значение последовательности	Коэффициенты при			
		y_4	y_3	y_2	y_1
1.	y_1	0	0	0	1
2.	y_2	0	0	1	0
3.	y_3	0	1	0	0
4.	y_4	1	0	0	0
5.	y_5	r_1	r_2	r_3	r_4
6.	y_6	$r_1 \oplus r_2$	$r_1 \cdot r_2 \oplus r_3$	$r_1 \cdot r_3 \oplus r_4$	$r_1 r_4$
7.	y_7	$r_1 \oplus r_3$	$r_2 \oplus r_1 r_2 \oplus r_1 r_3 \oplus r_4$	$r_1 r_3 \oplus r_1 r_4 \oplus r_2 r_3$	$r_1 r_4 \oplus r_2 r_4$
8.	y_8	$r_1 \oplus r_1 r_2 \oplus r_2 \oplus r_4$	$r_1 r_2 \oplus r_1 r_3 \oplus r_1 r_4$	$r_1 r_3 \oplus r_1 r_4 \oplus r_2 r_4 \oplus r_3$	$r_1 r_4 \oplus r_3 r_4$
9.	y_9	$r_1 \oplus r_1 r_2 \oplus r_1 \cdot r_3$	$r_2 \oplus r_3 \oplus r_1 r_4 \oplus$	$r_1 r_3 \oplus r_1 r_4 \oplus$	$r_1 r_4 \oplus r_1 r_2 r_4 \oplus$

			$r_1 r_3$	$r_1 r_2 r_3 \oplus r_2 r_3$	$r_2 r_4 \oplus r_4$
10.	y_{10}	$r_1 \oplus r_1 r_2 \oplus r_1 \cdot r_4 \oplus r_2 \oplus r_3$	$r_2 r_3 \oplus r_1 r_3 \oplus r_1 r_4$	$r_1 r_4 \oplus r_1 r_2 r_4 \oplus r_1 r_2 r_3 \oplus r_2 r_4 \oplus r_4$	$r_4 (r_1 \oplus r_1 r_3 \oplus r_1 r_2)$
11.	y_{11}	$r_1 \oplus r_2 r_3$	$r_2 \oplus r_2 r_3 \oplus r_1 r_3 \oplus r_1 r_4 \oplus r_2 r_4 \oplus r_1 r_2 r_3 \oplus r_4$	$r_1 r_3 \oplus r_2 r_3 \oplus r_1 r_2 r_3 \oplus r_1 r_4 \oplus r_1 r_2 r_4 \oplus r_3$	$r_4 (r_1 \oplus r_1 r_4 \oplus r_1 r_2 \oplus r_2)$
12.	y_{12}	$r_1 \oplus r_2 \oplus r_1 r_4 \oplus r_2 r_3 \oplus r_2 r_4 \oplus r_4$	$r_3 \oplus r_1 r_2 \oplus r_1 r_4 \oplus r_1 r_3 \oplus r_1 r_2 r_4 \oplus r_1 r_2 r_3$	$r_2 r_3 \oplus r_1 r_3 \oplus r_2 r_4 \oplus r_3 r_4 \oplus r_1 r_2 r_4$	$r_4 (r_1 \oplus r_2 r_3)$
13.	y_{13}	$r_1 \oplus r_3 \oplus r_1 r_4 \oplus r_1 r_3$	$r_2 \oplus r_1 r_2 \oplus r_1 r_3 \oplus r_2 r_4 \oplus r_3 r_4$	$r_1 r_3 \oplus r_1 r_4 \oplus r_3 r_4 \oplus r_1 r_3 r_4$	$r_4 (r_1 \oplus r_2 \oplus r_4 \oplus r_1 r_4 \oplus r_2 r_3 \oplus r_3 r_4)$
14.	y_{14}	$r_1 \oplus r_2 \oplus r_1 r_2 \oplus r_1 r_4 \oplus r_1 r_3 \oplus r_3 r_4 \oplus r_2 r_4$	$r_1 r_2 \oplus r_1 r_3 \oplus r_2 r_3 \oplus r_1 r_4 \oplus r_3 r_4 \oplus r_1 r_2 r_3 \oplus r_1 r_2 r_4 \oplus r_1 r_3 r_4$	$r_2 r_3 r_4 \oplus r_1 r_3 r_4 \oplus r_3 \oplus r_4$	$r_3 r_4 \oplus r_1 r_3 r_4$
15.	y_{15}	$r_1 \oplus r_1 r_2 \oplus r_1 r_3 \oplus r_2 r_3 \oplus r_3 r_4 \oplus r_1 r_2 r_3$	$r_2 \oplus r_3 \oplus r_4 \oplus r_2 r_4 \oplus r_1 r_2 r_3 \oplus r_1 r_2 r_4$	$r_1 r_2 r_3 \oplus r_2 r_3 r_4 \oplus r_2 r_3$	$r_3 r_4 \oplus r_1 r_3 r_4 \oplus r_1 r_2 r_4$
16.	y_{16}	$r_1 \oplus r_2 \oplus r_3 \oplus r_4 \oplus r_2 r_4 \oplus r_1 r_2 \oplus r_1 r_2 r_3 \oplus r_1 r_2 r_4$	0	$r_2 r_3 \oplus r_1 r_4 \oplus r_1 r_3 \oplus r_1 r_3 r_4 \oplus r_1 r_2 r_4$	$r_1 r_4 \oplus r_3 r_4 \oplus r_1 r_2 r_4 \oplus r_2 r_3 r_4 \oplus r_1 r_2 r_3 r_4$

Таблица 7 – Формулы приведения значений возможных ОЛУФП порядка J=3

№ п/п	r_1	r_2	r_3	r_4	ОЛУФП	Формулы приведения	Период
1.	0	0	0	1	$\mathbf{B}^{III}y \oplus \mathbf{B}^{II}y \oplus \mathbf{B}y \oplus y=0$	$y_i = y_{i-4}$	4
2.	0	0	1	0	$\mathbf{B}^{II}y \oplus y=0$	$y_i = y_{i-3}$	3
3.	0	0	1	1	$\mathbf{B}^{III}y \oplus \mathbf{B}y=0$	$y_i = y_{i-3} \oplus y_{i-4} = y_{i-6} \oplus y_{i-8} = y_{i-9} \oplus y_{i-10} \oplus y_{i-11} \oplus y_{i-12} = y_{i-15}$	15
4.	0	1	0	0	$\mathbf{B}y \oplus y=0$	$y_i = y_{i-2}$	2
5.	0	1	0	1	$\mathbf{B}^{III}y \oplus \mathbf{B}^{II}y=0$	$y_i = y_{i-2} \oplus y_{i-4} = y_{i-6}$	6
6.	0	1	1	0	$\mathbf{B}^{II}y \oplus \mathbf{B}y=0$	$y_i = y_{i-2} \oplus y_{i-3} = y_{i-4} \oplus y_{i-6} = y_{i-7}$	7
7.	0	1	1	1	$\mathbf{B}^{III}y \oplus y=0$	$y_i = y_{i-2} \oplus y_{i-3} \oplus y_{i-4} = y_{i-7}$	7
8.	1	0	0	0	$y=0$	$y_i = y_{i-1}$	1
9.	1	0	0	1	$\mathbf{B}^{III}y \oplus \mathbf{B}^{II}y \oplus \mathbf{B}y=0$	$y_i = y_{i-1} \oplus y_{i-4} = y_{i-2} \oplus y_{i-4} \oplus y_{i-5} = y_{i-3} \oplus y_{i-6} \oplus y_{i-8} = y_{i-4} \oplus y_{i-8} \oplus y_{i-10} = y_{i-5} \oplus y_{i-10} = y_{i-6} \oplus y_{i-9} \oplus y_{i-10} = y_{i-7} \oplus y_{i-10} \oplus y_{i-13} = y_{i-8} \oplus y_{i-13} \oplus y_{i-14} = y_{i-9} \oplus y_{i-12} \oplus y_{i-13} \oplus y_{i-14} = y_{i-10} \oplus y_{i-12} \oplus y_{i-14} = y_{i-11} \oplus y_{i-12} = y_{i-15}$	15
10.	1	0	1	0	$\mathbf{B}^{II}y=0$	$y_i = y_{i-1} \oplus y_{i-3} = y_{i-2} \oplus y_{i-6} = y_{i-3} \oplus y_{i-5} \oplus y_{i-6} = y_{i-7}$	7
11.	1	0	1	1	$\mathbf{B}^{III}y \oplus \mathbf{B}y \oplus y=0$	$y_i = y_{i-1} \oplus y_{i-3} \oplus y_{i-4} = y_{i-2} \oplus y_{i-3} \oplus y_{i-5} = y_{i-6}$	6
12.	1	1	0	0	$\mathbf{B}y=0$	$y_i = y_{i-1} \oplus y_{i-2} = y_{i-3}$	3
13.	1	1	0	1	$\mathbf{B}^{III}y \oplus \mathbf{B}^{II}y \oplus y=0$	$y_i = y_{i-1} \oplus y_{i-2} \oplus y_{i-4} = y_{i-3} \oplus y_{i-4} \oplus y_{i-5} = y_{i-7}$	7
14.	1	1	1	0	$\mathbf{B}^{II}y \oplus \mathbf{B}y \oplus y=0$	$y_i = y_{i-1} \oplus y_{i-2} \oplus y_{i-3} = y_{i-4}$	4
15	1	1	1	1	$\mathbf{B}^{III}y=0$	$y_i = y_{i-1} \oplus y_{i-2} \oplus y_{i-3} \oplus y_{i-4} = y_{i-5}$	5

Можно отметить следующее.

1. Для рассмотренных порядков существует $2^{J+1}-1$ нетривиальных различных ОЛУФП.

2. Каждое из возможных ОЛУФП имеет 2^{J+1} периодических решений, определяемых (J+1) возможными начальными элементами.

3. Периоды указанных решений образуют дискретную сетку от 1 до $2^{J+1}-1$.

4. При некоторых значениях начальных элементов период может быть уменьшен.

5. Практическое значение имеют последовательности с максимальным возможным периодом, равным $2^{J+1}-1$.

По мере увеличения J анализ, аналогичный приведенному в табл. 2 – 7, становится весьма громоздким. Его целесообразно проводить на быстродействующих ЭВМ в два этапа. Вначале осуществим последовательный перебор всех возможных значений $r_k^{/}$ и получим массивы периодически повторяющихся битов. Величина периода полученных последовательностей устанавливается путем расчета их автокорреляционных функций. В связи с последним из вышеуказанных замечаний достаточно рассмотреть последовательности с максимальным возможным периодом l_{max}.

На втором этапе полученным значениям $r_k^{/}$ необходимо сопоставить совокупность бинарных производных, удовлетворяющих соотношениям (5) – (6). С этой целью для каждого J по схеме, показанной на рис. 1, формируется массив коэффициентов g_k.

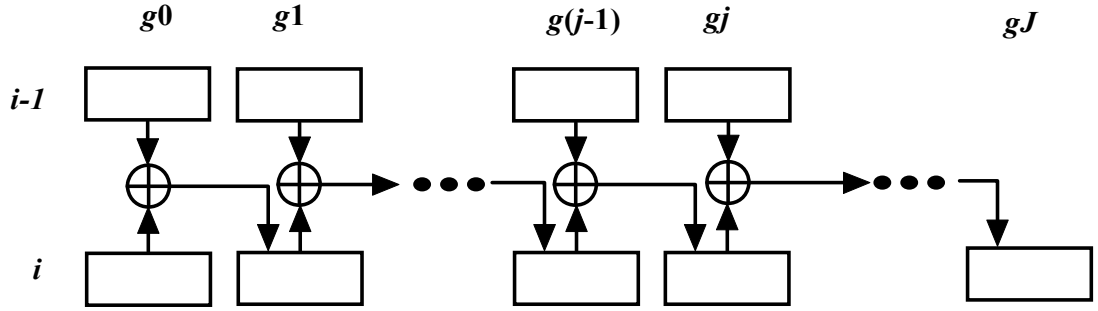

Рисунок1 - Схема формирования массива коэффициентов g_k на i-м шаге итерации.

Посредством (6) из g_k. определяются все возможные значения $r_{k.}$. Методом последовательного перебора находятся последовательности бинарных производных , для которых $r_k^{/} = r_k$.

На рис. 2 изображена зависимость количества ОЛУФП, имеющих решения с максимальным периодом, от порядка уравнения.

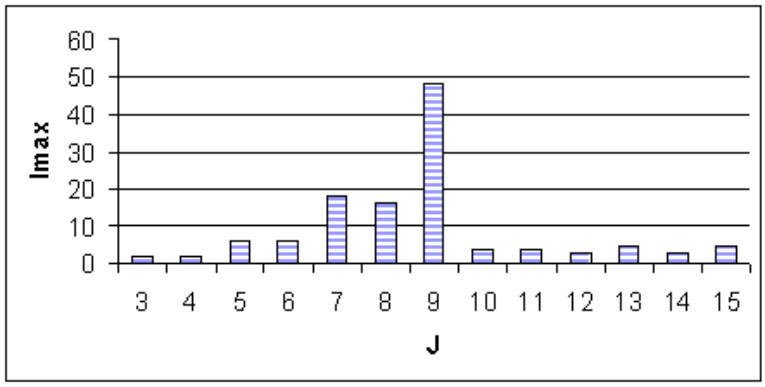

Рисунок 2 – Количество l_{max} ОЛУФП, имеющих решения с максимальным периодом $2^{J+1}-1$, в зависимости от порядка уравнения J.

Отметим, что по мере увеличения порядка уравнения до J=9 наблюдается ожидаемый рост числа ОЛУФП, имеющих решения с максимальным периодом. Однако дальнейшее увеличение J вплоть до прослеженных значений J=15 не приводит к увеличению количества таких уравнений. Объяснение этого факта может быть найдено в связи с четвертым из вышеуказанных замечаний. Период получающихся последовательностей оказывается большим, но не максимальным.

Таким образом, предлагается следующая методика создания генераторов периодических битовых последовательностей.

1. Исходя из допустимой сложности технической реализации генератора, определить максимальный порядок используемых формальных производных J и их количество.
2. Исходя из общесистемных требований к генератору, выбрать его период, не превышающий $2^{J+1}-1$.
3. С помощью наличных в системе генераторов псевдослучайных последовательностей создать начальное заполнение генератора нолями и единицами длиной J.
4. Путем последовательного перебора коэффициентов $r_{k.}$ провести итерационные расчеты y_i по формулам (6) с последующим определением периодов возникающих последовательностей. Произвести отбор массивов коэффициентов, порождающих последовательности необходимой длины, в соответствии с п. 2.
5. Путем последовательного перебора коэффициентов g_k определить значения c_j, в максимальной

степени удовлетворяющие п. 1.

Найденные коэффициенты позволяют построить ОЛУФП, решения которого представляют собой массивы периодических булевозначных последовательностей. Они могут использоваться в генераторах псевдослучайных битов, применяемых при защите банковских информационных систем.

Литература: ***1.*** *Анин Б. Ю. Защита компьютерной информации. - СПб.: БХВ - Санкт-Петербург. - 2000. – 384 с.* ***2.*** *Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452с. – С. 241 - 254.* ***3.*** *Б. Шнайер. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М. : Триумф, 2002.* ***4.*** *J. M. Carroll, L. E. Robbins. Using binary derivatives to test an enhancement of DES //Cryptologia. - 1988. - V. 12. - № 4. - Pp. 193 - 208.* ***5.*** *Березюк Н. Г., Холодный М. Ф. Булевы дифференциальные уравнения и методы их решения. - В сб.: Математическое и программное обеспечение задач оптимизации технических систем. - Киев . - "Наукова думка". - 1987. - С. 61 - 65.* ***6.*** *В. Н. Куценко, Т. В. Левченко, В. В. Мясоедов. Модель цифровой подписи//Захист інформації. - 2004. - Спеціальний випуск № 22. - С. 29 - 35.* ***7.*** *В. Мясоедов. Золотое сечение в шифровании данных.// В сб.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - Науково-технічний збірник. - Випуск 4. - К.: НДЦ "Тезіс" НТУУ "КПІ". - 2002. - 213 с. - С. 105.* ***8.*** *В. Мясоедов, В. Куценко, Оценка случайности по избыточности // В сб.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - Науково-технічний збірник. - Випуск 8. - К.: НДЦ "Тезіс" НТУУ "КПІ". - 2004. - 166 с.- С. 90 - 94.*

УДК 681.3.067:681.3.016

ОЦЕНКА АСИММЕТРИИ ПО АВТОКОРРЕЛЯЦИИ

Геннадий Куценко
КП НТК «Импульс»

Аннотация: **На примере псевдослучайной последовательности генератора Фибоначчи подробно описаны результаты экспериментального исследования асимметрии методами автокорреляции. Введенный в статье коэффициент ранговой упорядоченности двоичных слов из полезной длины периода последовательности в рассмотренном примере очень мал.**
Summary: **On example of the pseudorandom sequence of Fibonacci generator in detail described results of the experimental study to asymmetries by methods of autocorrelation.**
Ключевые слова: **Генератор Фибоначчи, псевдослучайные числа, асимметрия последовательностей, автокорреляционная функция, ранговая корреляция, ранговая упорядоченность.**

Известные методы оценки качества псевдослучайных последовательностей «в целом» [1] являются недостаточными, так как их применение не гарантирует отсутствия простых симметрий – повторений отрезков последовательности – в псевдослучайных последовательностях, порождаемых определёнными алгоритмами. Это недопустимо с точки зрения применений псевдослучайных последовательностей в области защиты данных.

Удобным инструментом локальных оценок, в частности для проверки отсутствия простых симметрий в псевдослучайных последовательностях, является вычисление автокорреляционной функции, малые значения которой несовместимы с наличием в последовательностях простых симметрий. Это выражено как постулат в [2]. Имеется также средство оценки бинарных последовательностей, позволяющее локализовать вычисления автокорреляционной функции, трактуемой как совокупность коэффициентов корреляции отрезков последовательности, попадающих в пару подвижных «окон» одинакового размера. Отсутствие простых симметрий в псевдослучайной последовательности может быть проверено с помощью оценок автокорреляции и в более широком случае, когда ко второму экземпляру последовательности применён некоторый простой оператор. Кроме того, автокорреляционные схемы оценки асимметрии могут быть применены также при минимальных предположениях о свойствах шкалы генерируемых объектов – тогда необходимо вычислять ранговые корреляции [3].

Теоретические средства локального оценивания хотя и возможны, но всегда ориентированы на конкретные алгоритмы генерации. При этом весьма полезны предварительные эмпирические исследования.

Предметом подробного рассмотрения в статье являются результаты экспериментальных исследований асимметрии методами автокорреляции на примере псевдослучайных последовательностей двоичных слов, порождаемых генератором Фибоначчи.