УДК 004.056.55

Н.А. ПОЛУЯНЕНКО, А.В. ПОТИЙ, д-р техн. наук

СРАВНЕНИЕ ОБЪЕМА АНСАМБЛЯ М-РСЛОС И М-РСНОС, СКОРОСТИ ГЕНЕРАЦИИ НА ИХ ОСНОВЕ ДЛЯ *GF*(2) И В РАСШИРЕНИЯХ ПОЛЯ *GF*(2^2)

Поточные шифры являются одним из основных механизмов обеспечения конфиденциальности. Актуальным остается вопрос обеспечения криптографической стойкости поточных шифров на основе регистров сдвига с линейной обратной связью (РСЛОС), в частности вопросы обеспечения линейной эквивалентной сложности поточных шифров на их основе.

В последнее время исследователями уделяется большое внимание альтернативным конструкциям построения поточных шифров. Одним из новых подходов являются конструкции на основе регистров сдвига с нелинейной обратной связью [1, 2]. Предполагается, что такие схемы будут обладать повышенной стойкостью из-за нелинейности в структуре регистра. Однако остаются открытыми вопросы практической реализации РСНОС и их технические характеристики.

В работе [3] показано, что РСНОС присущи практически все достоинства классических РСЛОС (скорость работы; статистические характеристики генерируемой последовательности; большой период генерируемой псевдослучайной последовательности (ПСП) в сравнении с размером регистра; простота программной и аппаратной реализации), но благодаря внесенной нелинейности в структуру обратной связи, РСНОС не обладают основным недостатком РСЛОС – восстановлением структуры регистра по известной, достаточно короткой, выходной последовательности генератора. Как показано в работе [3], РСНОС успешно, в отличиеот РСЛОС, проходит тесты на линейную сложность.

Несмотря на перспективность применения РСНОС как одного из основных элементов генератора ПСП, свойства таких регистров остаются недостаточно изучены [4].

Одной из важных характеристик [4] для конструкций, которые генерируют последовательность с максимальным периодом (М-последовательность), является объем ансамбля, т.е. количество различных М-последовательностей для заданного размера регистра сдвига с обратной связью. Под размером регистра будем понимать количество ячеек, используемых в регистре (L), а регистры которые генерируют М-последовательность назовем М-РСНОС (М-РСЛОС).

Кроме того, в доступной литературе практически отсутствует сравнение производительности, т. е. объема генерируемых данных в единицу времени, конструкций на основе РСЛОС и РСНОС.

Цель данной работы:

– определение точного значения объема ансамбля для РСНОС при небольших значениях L, приведение оценки данного объема для более высоких значений L;

– определение аналогичного объема ансамбля для РСНОС в расширенных полях Галуа для $GF(2^2)$;

– сравнение объема ансамбля РСНОС и РСЛОС;

– сравнительная оценка производительности РСНОС и РСЛОС при программной реализации алгоритма.

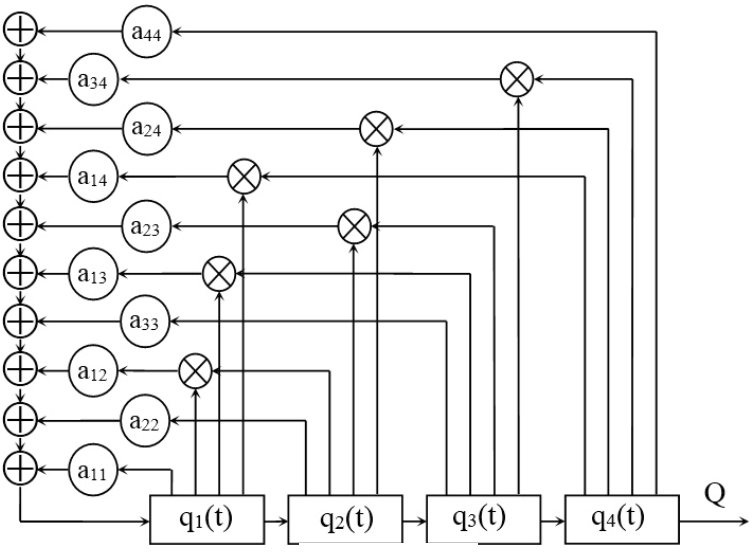


Рис. 1

Обобщенная конструкции РСНОС второго порядка, при $L=4$, для расширений в $GF(2^2)$ приведена на рис. 1. Где $a_{ij} \in \{0,1,2,3\}$ обозначает блок умножения, $q_i(t) \in \{0,1,2,3\}$ – значение i-го регистра в момент времени t, Q – генерируемая последовательность бит. Нелинейная функция – умножение (обозначенное знаком – $\otimes$) берется по модулю порождающего полинома $g(x)$. В $FG(2^2)$ каждое значение a_{ij} или q_i рассматривается как набор из двух битов $\{0,1\}$, что эквивалентно машинному слову длины 2.

Результаты сравнения РСЛОС и РСНОС второго порядка приведены в табл. 1 для $FG(2)$ и в табл. 2 – для $FG(2^2)$. Следует обратить внимание на то, что РСЛОС есть частный случай РСНОС тогда, когда все нелинейные коэффициенты обратной связи равны нулю, т.е. $a_{ij}=0$ для $i \neq j$.

Таблица 1

L	$FG(2)$						
	$T_{\max}$	РСЛОС			РСНОС		
		n_L	k	M_0	n_L	k	M_0
2	3	2	4	**1**	2	4	**1**
3	7	3	8	**2**	6	64	**2**
4	15	4	16	**2**	10	1 024	**16**
5	31	5	32	**6**	15	32 768	**128**
6	63	6	64	**6**	21	2 097 152	**1 952**
7	127	7	128	**18**	28	$2{,}6\cdot10^{8}$	**64 056**
8	255	8	256	**16**	36	$6{,}8\cdot10^{10}$	**4 017 998**
9	511	9	512	**48**	45	$3{,}5\cdot10^{13}$	**519 239 794**
10	1 023	10	1024	**60**	55	$3{,}6\cdot10^{16}$	$1\cdot10^{11}$ [2]
11	2 047	11	2048	**176**	66	$7{,}4\cdot10^{19}$	$7\cdot10^{13}$ [2]
12	4 095	12	4096	**144**	78	$3{,}0\cdot10^{23}$	$7\cdot10^{16}$ [2]
13	8 191	13	8192	**630**	91	$2{,}5\cdot10^{27}$	$1\cdot10^{20}$ [2]
14	16 383	14	16384	**756**	105	$4{,}1\cdot10^{31}$	$6\cdot10^{23}$ [2]
15	32 767	15	32768	**1 800**	120	$1{,}3\cdot10^{36}$	$5\cdot10^{27}$ [2]
16	65 535	16	65536	**2 048**	136	$8{,}7\cdot10^{40}$	$8\cdot10^{31}$ [2]
17	13 1071	17	13 1072	**7 710**	153	$1{,}1\cdot10^{46}$	$3\cdot10^{36}$ [2]
18	262 143	18	262 144	**7 776**	171	$3{,}0\cdot10^{51}$	$2\cdot10^{41}$ [2]
19	524 287	19	524 288	**27 594**	190	$1{,}6\cdot10^{57}$	$2\cdot10^{46}$ [2]
20	1 048 575	20	1 048 576	**24 000**	210	$1{,}6\cdot10^{63}$	$6\cdot10^{51}$ [2]
21	2 097 151	21	2 097 152	**84 672**	231	$3{,}5\cdot10^{69}$	$3\cdot10^{57}$ [2]
22	4 194 303	22	4 194 304	**120 032**	253	$1{,}4\cdot10^{76}$	$3\cdot10^{63}$ [2]
23	$8{,}4\cdot10^{6}$	23	$8{,}4\cdot10^{6}$	356 960 [1]	276	$1{,}2\cdot10^{83}$	$7\cdot10^{69}$ [2]
24	$1{,}7\cdot10^{7}$	24	$1{,}7\cdot10^{7}$	276 480 [1]	300	$2{,}0\cdot10^{90}$	$3\cdot10^{76}$ [2]
25	$3{,}4\cdot10^{7}$	25	$3{,}4\cdot10^{7}$	1 296 000 [1]	325	$6{,}8\cdot10^{97}$	$2\cdot10^{83}$ [2]
26	$6{,}7\cdot10^{7}$	26	$6{,}7\cdot10^{7}$	1 719 900 [1]	351	$4{,}6\cdot10^{105}$	$4\cdot10^{90}$ [2]
27	$1{,}3\cdot10^{8}$	27	$1{,}3\cdot10^{8}$	4 202 496 [1]	378	$6{,}2\cdot10^{113}$	$1\cdot10^{98}$ [2]
28	$2{,}7\cdot10^{8}$	28	$2{,}7\cdot10^{8}$	4 741 632 [1]	406	$1{,}7\cdot10^{122}$	$9\cdot10^{105}$ [2]
29	$5{,}4\cdot10^{8}$	29	$5{,}4\cdot10^{8}$	18 407 808 [1]	435	$8{,}9\cdot10^{130}$	$1\cdot10^{114}$ [2]
30	$1{,}0\cdot10^{9}$	30	$1{,}0\cdot10^{9}$	17 820 000 [1]	465	$9{,}5\cdot10^{139}$	$3\cdot10^{122}$ [2]

[1] Значения M_0 для РСЛОС, соответствующие $L=23-30$, не вычислялись авторами и взяты из [5, 8].

[2] Значения M_0 для РСНОС, соответствующие $L=10-30$, приведены как верхняя оценка количества множества M_0, рассчитаны по эмпирической формуле, приведенной в работе [6].

Сравнение проводилось по следующим параметрам:

$T_{\max}$ – длина максимального периода, которую может сгенерировать регистр с заданным L (в таблице приведено значение в битах, а не в машинных словах);

n_L – количество коэффициентов обратной связи a_{ij}, используемое в конструкции;

k – количество возможных комбинаций, которыми можно варьировать при синтезе регистра сдвига;

M_0 – максимально возможное число различных комбинаций обратных связей для заданного L, при которых регистр будет генерировать М-последовательность. Данное значение соответствует искомому объему ансамбля для каждого L. установлено экспериментальным путем.

Дополнительно при поиске М-РСНОС подсчитывалось количество М-РСЛОС как частный случай. Начиная с $L=10$ и до длины регистров $L=22$, в связи со значительными временными затратами, производился поиск только М-РСЛОС и контроль числа найденных комбинаций с известными значениями, взятыми из [5, 8].

Таблица 2

L	$FG(2^2)$						
	$T_{\max}$	РСЛОС			РСНОС		
		n_L	k	M_0	n_L	k	M_0
2	15	4	16	**4**	6	64	**4**
3	63	6	64	**12**	12	4 096	**12**
4	255	8	256	**32**	20	1 048 576	**152**
5	1 023	10	1 024	**120**	30	1 073 741 824	**7 896**
6	4 095	12	4 096	**288**	42	$4{,}4\cdot10^{12}$	
7	16 383	14	16 384	**1 512**	56	$7{,}2\cdot10^{16}$	
8	65 535	16	65 536	**4 096**	72	$4{,}7\cdot10^{21}$	
9	262 143	18	262 144	**15 552**	90	$1{,}2\cdot10^{27}$	

Значения результатов (табл. 1 и 2), кроме M_0, можно подсчитать по формулам, приведенным в табл. 3. Следует отметить, что для расширения поля $FG(2^3)$ и более высокого порядка будет существовать более одного порождающего полинома $g(x)$ и, возможно, с учетом этого изменится соотношение для вычисления n_L и, как следствие, множества k.

Таблица 3

Параметр	$FG(2)$		$FG(2^{m=2})$	
	РСЛОС	РСНОС	РСЛОС	РСНОС
$T_{\max}=$	2^L-1		$2^{m\cdot L}-1$	
$n_L=$	L	$\frac{L\cdot(L+1)}{2}$	$m\cdot L$	$m\cdot\frac{L\cdot(L+1)}{2}$
$k=$	2^{n_L}			

Как видим из приведенных в табл. 1 результатов, количество различных комбинаций, которые можно составить для РСНОС, значительно превосходит аналогичное количество для РСЛОС. Причем разница увеличивается с ростом L по степенной зависимости, и если для $L=5$ количество различных комбинаций для РСНОС превосходило аналогичное количество для РСЛОС чуть более, чем в 1000 раз, то уже для $L=30$ такая разница составит 10^{130}.

Тенденция значительного превосходства в пользу РСНОС сохраняется и для более важного параметра – объема ансамбля. Уже при $L = 9$ количество М-РСНОС превышает количество М-РСЛОС более чем в 10^7 раз, а прогнозируемая разница для $L = 30$ составляет 10^{115}.

Все сказанное будет справедливо и для регистров, построенных в расширенных полях Галуа (табл. 2). Причем указанное преимущество для $FG(2^2)$ превосходит аналогичные показатели для $FG(2)$ и с ростом значения L это превосходство (прогнозируемо) также будет увеличиваться по степенному закону.

Таким образом, можно сделать еще один значимый вывод: РСНОС дают значительное преимущество по сравнению с РСЛОС по количеству возможных различных структур (возможность реализовать различные генераторы ПСП), которые будут генерировать М-последовательности при одинаковом значении L. Приведенное утверждение повышает криптографическую стойкость РСНОС по сравнению с РСЛОС при силовом взломе алгоритма из-за экспоненциального увеличения количества возможных вариантов.

Данный факт показывает, что РСНОС предпочтительнее использовать, когда есть необходимость реализовать большое количество несовместимых друг с другом генераторов ПСП при возможности использовать одинаковый базовый регистр (например, при промышленном производстве для различных потребителей). Также РСНОС целесообразно использовать для быстрой замены алгоритма работы генератора в случае его компрометации, принципиально не меняя структуру генератора. Использовав значения коэффициентов a_{ij} как параметр долговременного ключа, можно дополнительно повысить криптографическую стойкость генератора с точки зрения вероятности перекрытия генерируемой гаммы путем более частой замены коэффициентов обратной связи в сравнении с РСЛОС.

Оценка производительности РСНОС и РСЛОС в программной реализации алгоритма

Необходимо акцентировать внимание на том, что на скорость генерации (производительность) ПСП тем или иным алгоритмом оказывают влияние многие факторы, такие как: платформа, на которой производятся вычисления; подход и метод, с помощью которых на программном уровне реализованы операции, заложенные в алгоритме; используемый компилятор. При наилучшей оптимизации программного кода и соответствующем выборе компилятора иногда можно добиться лучшего результата, чем от реализации потенциально более «быстрого» генератора неподходящим способом. Авторы не утверждают, что подход, применяемый ими, является наилучшим. Приведенные результаты дают возможность провести количественное сравнение алгоритмов генераторов, основанных на РСЛОС и РСНОС.

Для компиляции всех примеров использовался FASM (flat assembler version 1.71.51). Вычисления проводились на персональном бытовом компьютере (64-разрядная Windows 7 SP 1, процессор Intel Core i5-3210M CPU 2,5GHz).

При введенной системе обозначений (см. рис. 1) обратную связь для РСНОС можно задать в виде

$$q_1(t+1) = \sum_{i=1}^{L} a_{ii} q_i(t) + \sum_{i=1}^{L-1} \sum_{j=i+1}^{L} a_{ij} q_i(t) q_j(t) \qquad (1)$$

При этом состояния РСЛОС, как частный случай РСНОС при всех нелинейных коэффициентах равных нулю, вычисляется соотношением

$$q_1(t+1) = \sum_{i=1}^{L} a_{ii} q_i(t) \qquad (2)$$

Таким образом, из (1) и (2) видно, что вычисление очередного бита можно разбить на два этапа: в первом блоке вычислений подсчитывается сумма от линейных коэффициентов; во втором блоке – вычисляется сумма от нелинейных коэффициентов.

Второй блок разбивается на субблоки для каждого q_i. В каждом субблоке проверяется значение регистра q_n, где $n = \overline{\{1, L-1\}}$, и если $q_n = 1$, проводится проверка четности суммы значений регистров q_j (для $j = \overline{\{n+1, L\}}$) и только при тех значениях j, при которых $a_{nj} \neq 0$. Если сумма значений регистров q_j – число нечетное, то изменяется значение, предварительно вычисленное для линейной составляющей, которое по завершении проверок всех субблоков подается на вход регистра.

Таким образом, применяя описанный подход для вычисления очередного состояния в РСНОС, может проводиться дополнительно от одного до $L-1$ блоков операций, в зависимости от присутствующих нелинейных коэффициентов обратной связи.

В первом блоке (для линейных коэффициентов) содержится семь команд процессора, во втором – восемь команд для каждого субблока. Кроме того, для проверки четности регистра в каждом блоке использовался флаг четности (бит PF регистра флагов RFLAGS). Однако флаг четности применим только при значениях $L \leq 8$. Для регистров длиной $L > 8$ производилось разбиение проверяемого непрерывного фрагмента регистра на части длиной в 8 бит и проверялась каждая из этих частей по отдельности. Дополнительное разбиение ведет к увеличению количества операций и, соответственно, – к увеличению затрачиваемого времени на генерацию.

В табл. 4 приведены результаты измерения времени, которое затрачивается на генерацию 1 Гбайт данных по приведенному алгоритму. Генерировалась только М-последовательность. В случае генерации не М-последовательностей, могут встречаться серии из одних единиц или из нулей, что будет сказываться на результате эксперимента.

Таблица 4

№ п/п	Полиномиальное представление	Затраченное время на генерацию 1 Гбайта
	РСЛОС[3)]	
1	$x^8 + x^7 + x^2 + x^1 + 1$	21 с
2	$x^8 + x^7 + x^6 + x^5 + x^2 + x^1 + 1$	21 с
3	$x^8 + x^7 + x^6 + x^3 + x^2 + x^1 + 1$	21 с
4	$x^{24} + x^{23} + x^{22} + x^{17} + 1$	21 с
5	$x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x^1 + 1$	34 с
6	$x^{24} + x^{10} + x^4 + x^3 + 1$	34 с
	РСНОС	
7	$x^8 + x^4 \cdot x^2 + x^3 \cdot x^2 + x^1 + 1$	34 с
8	$x^8 + x^7 + x^5 + x^4 + x^6 \cdot x^1 + x^4 \cdot x^1 + x^3 \cdot x^1 + x^2 \cdot x^1 + 1$	34 с
9	$x^8 + x^7 + x^7 \cdot x^6 + x^6 + x^7 \cdot x^5 + x^6 \cdot x^5 + x^5 + x^7 \cdot x^4 + + x^6 \cdot x^4 + x^5 \cdot x^4 + x^4 + x^7 \cdot x^3 + x^6 \cdot x^3 + x^5 \cdot x^3 + x^4 \cdot x^3 + + x^3 + x^7 \cdot x^2 + x^6 \cdot x^2 + x^5 \cdot x^2 + x^2 + x^7 \cdot x^1 + x^1 + 1$	76 с
10	$x^{24} + x^{23} \cdot x^{21} + x^{22} + x^{21} + x^{19} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + + x^{10} + x^7 + x^6 + x^4 + 1$	43с
11	$x^{24} + x^{23} \cdot x^{21} + x^{22} + x^{22} \cdot x^{21} + x^{21} + x^{19} + x^{17} + x^{16} + x^{13} + + x^{12} + x^{11} + x^{10} + x^6 + x^5 + 1$	43 с

[3)] Полиномы для М-РСЛОС взяты из работы [8].

Как видим, для генерации на основе РСНОС затрачивается время примерно в 1,2-1,6 раз больше, чем на генерацию РСЛОС. Обратим внимание на три момента:

1. В примененном способе количество операций для РСЛОС не зависит от числа обратных связей (если есть такая зависимость, то она настолько мала, что в ходе тестирования не отслеживалась). И независимо от того, будет ли только один линейный коэффициент не равен нулю или все, на скорость выполнения всего цикла это не влияет. Как пример можно привести образующие полиномы № 5 и 6 (табл. 4). В первом случае образующий полином плотный, а во втором – разряженный. Аналогично и для РСНОС (полиномы № 7 и 8 табл. 4), если все нелинейные коэффициенты имеют общий член, то все коэффициенты можно рассчитать за один субблок.

2. Можно подобрать полиномы, при которых ненулевые коэффициенты обратных связей в субблоках будут находиться друг от друга на расстоянии не более чем 8 бит. Это позволит не разбивать вычисления на блоки по 8 бит и вычислять их одновременно. В качестве примера приведен полином под № 4, который вычисляется за время, равное времени, затраченному на вычисление регистра в три раза меньшего размера (полиномы № 1, 2, 3).

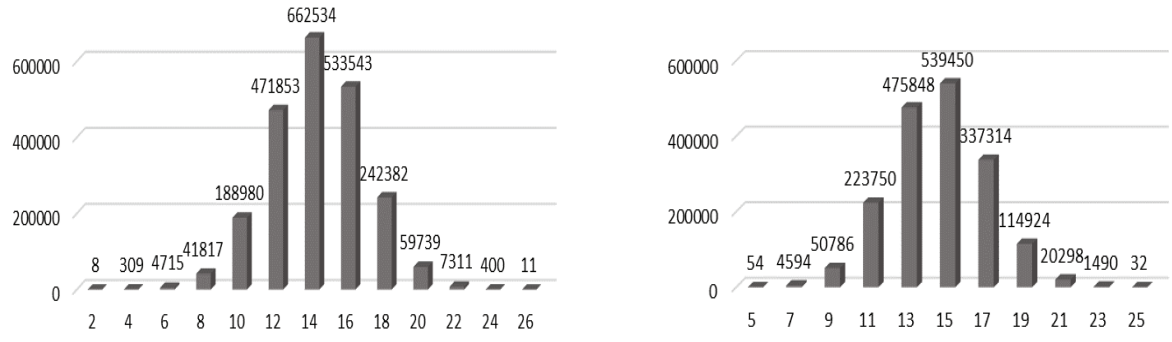
3. Время, затраченное на выполнение одного такта в РСНОС, увеличивается (приблизительно на 30 %) с каждой новой комбинацией q_n. Например, в полиноме № 9 присутствуют все различные нелинейные комбинации, что приводит к двукратному увеличению времени на вычисления. В связи с этим для РСНОС имеет смысл применять полиномы, в которых будут только комбинации нелинейных коэффициентов a_{ij}, входящие в один субблок (как, например, полиномы № 10, 11).

Оптимизация вычислений под определенные обратные связи позволяет увеличить быстродействие алгоритма. Так, для $L = 8$ (полином № 1при тех же условиях удалось сгенерировать 1 Гбайт за 16 с, а для РСНОС, соответствующему полиному № 9, – за 41 с. Однако при этом теряется универсальность метода и алгоритм необходимо подстраивать под отдельно взятые полиномы.

Как показывают приведенные результаты, подбор определенным образом коэффициентов обратных связей напрямую влияет на скорость работы алгоритма (при программной реализации). Обратим внимание на распределение количества нелинейных обратных связей в М-РСНОС (при любых линейных коэффициентах обратных связей).

Был проведен анализ на распределение количества М-РСНОС по числу не равных нулю нелинейных коэффициентов обратной связи для фиксированной комбинации линейных коэффициентов для всего множества М-РСНОС при $L \le 9$.

В качестве примера на рис. 2 приведены две гистограммы распределения количества нелинейных коэффициентов $a_{ij} \neq 0$ для двух различных коэффициентов a_{ii} при $L = 9$ (четное количество линейных коэффициентов обратная связь a_{ii}, соответствующая полиному $x^9 + x^1 + 1$, представлена на рис. 2, *а*; нечетное количество a_{ii}, соответствующее полиному $x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + 1$, – на рис. 2, *б*. Для остальных комбинаций линейных коэффициентов распределение имеет примерно такой же вид.



а *б*

Рис. 2

Таким образом, если искать (или проектировать) РСНОС, то оптимальным подходом будет искать ненулевые нелинейные коэффициенты, рассчитывая их количество, близкое к $L/2$. Если нелинейных связей всего одна или две (или же почти все), то число возможных М-РСНОС будет несколько единиц (независимо от того, какие при этом берутся линейные обратные связи).

Выводы

Показано, что РСНОС дают значительное преимущество, по сравнению с РСЛОС, по количеству возможных различных структур, которые будут генерировать М-последовательности при одинаковом значении L. Приведены числовые значения для регистров длины до $L = 9$ для $FG(2)$ и для регистров длины до $L = 5$ для $FG(2^2)$.

Показано, что в программной реализации время, затраченное на генерацию РСНОС, соизмеримо со временем, затраченным на генерацию РСЛОС и увеличивается приблизительно в 1,2 – 1,6 раз. Даны рекомендации по подбору коэффициентов обратных связей для сокращения времени на генерацию, в том числе и для РСНОС.

Список литературы: 1. *An NLFSR*-Based Stream Cipher. Berndt M. Gammel, Rainer G¨ottfert and Oliver Kniffler Infineon Technologies AG, Munich, Germany. Электронный ресурс: https://www.researchgate.net/publication/224647778. 2. *Martin Hell, Thomas Johansson, Willi Meier, Grain*. A Stream Cipher for Constrained Environments, eSTREAM submission, Электронный ресурс: http://www.ecrypt.eu.org/stream/p3ciphers/grain/Grain_p3.pdf. 3. *Аналіз,* розробка та дослідження постквантових криптографічних примітивів та обґрунтування умов їх застосування в Україні : звіт про НДР (проміжний). Т.1. Аналіз та порівняльні дослідження симетричних криптографічних перетворень на постквантовий період / ХНУ ім. В.Н. Каразіна ; кер. Кузнецов О.О. ; вик.: Сватовський І.І. [та інш.,]. – Х. : ХНУ ім. В.Н. Каразіна. – 2016. – 119 с. 4. *Математические* основы криптологии / А. Г. Коробейников, Ю.А.Гатчин : учеб. пособие. – Санкт-Петербург, 2004. Электронный ресурс: http://books.ifmo.ru/file/pdf/56.pdf 5. *Pseudo* Random Number Generation Using Linear Feedback Shift Registers. Электронный ресурс: https://www.maximintegrated.com/en/app-notes/index.mvp/id/4400 6. *Потий, А.В., Полуяненко, Н.А*. Анализ свойств регистров сдвига с нелинейной обратной связью второго порядка генерирующих, последовательность с максимальным периодом // Прикладная радиоэлектроника. – 2008. – № 3. – С. 282-290. 7. *Регистр* сдвига с линейной обратной связью. Электронный ресурс: https://ru.wikipedia.org/wiki/Регистр_сдвига_с_линейной_обратной_связью 8. *Maximal* Length LFSR Feedback Terms. Philip Koopman. Электронный ресурс: https://users.ece.cmu. edu/~koopman/lfsr/

Харьковский национальный
университет имени В.Н.Каразина

Поступила в редколлегию 12.09.2016