tems. *Proceedings of XIIIth International Conference CADSM'2015.* Lviv, 2015. P. 295–299.
7. Патент України на корисну модель № 68874. 10.04.2012. Бюл. № 7.
8. Деклараційний патент України на корисну модель № 71122. — 10.07.2012. Бюл. № 13.
9. Николайчук Я. М. Теорія джерел інформації. Тернопіль ТНЕУ, 2008. 536 с.

Synthesis of structure of the image-cluster model interactive monitoring many parametric states control objects based on computer aided design (CAD) algorithm rozparalelenoho processing statistics and correlation characteristics of technological objects.

Key words: *image-cluster model, interactive computer system, management of the facility.*

Одержано 16.02.2017

УДК 004.056.55

Н. А. Полуяненко, соискатель

Харьковский национальный университет
имени В. Н. Каразина, г. Харьков

РАСЧЕТ ЧИСЛА ОБРАЗУЮЩИХ ПОЛИНОМОВ ДЛЯ РЕГИСТРОВ СДВИГА С НЕЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ С НЕЛИНЕЙНОСТЬЮ ПРОИЗВОЛЬНОГО ПОРЯДКА

Рассматривается один из важных элементов генератора поточных шифров — регистры сдвига с нелинейной обратной связью (РСНОС). Рассматриваются РСНОС с нелинейностью произвольного порядка. Изучается число различных образующих полиномов, на основе которых можно построить РСНОС. В качестве результата приводятся расчетные выражения для определения числа РСНОС как произвольного порядка, так и для РСНОС максимального порядка при заданном размере регистра.

Ключевые слова: *поточные шифры, нелинейные системы, РСНОС.*

Введение. В последнее время наблюдается резкое развитие криптоаналитических систем, в том числе, перспективным направлением стало использование квантового компьютера или квантовых вычислений. Учитывая это, актуальным становится вопрос повышения уровня безопасности криптографических методов без ухудшения таких показателей, как сложность и скорость вычислений. Одним из основных требований к генераторам псевдослучайных последовательностей (ПСП) предъявляются требования неразличимости последовательностей, сложности, скорости и период повторения для ПСП [1]. Хороши-

ми криптографическими примитивами, отвечающими данным требованиям, есть конструкции на основе регистров сдвига.

Одним из перспективных подходов является конструкции на основе регистров сдвига с нелинейной обратной связью (РСНОС) [2, 3]. РСНОС представляют обобщение регистров сдвига с линейной обратной связью (РСЛОС), но в отличии от последних, в РСНОС текущее состояние является нелинейной функцией предыдущих состояний [4]. РСНОС на основе поточных шифров включаются в Achterbahn [5], Dragon [6], Grain [7], Trivium [8], VEST [9]. В работе [10] показано, что РСНОС более устойчивы к криптоаналитическим атакам, чем РСЛОС.

Обзор состояния проблемы и постановка задач исследования. Интерес к РСНОС вызван, в значительной степени, их способностью генерировать ПСП, которые, как правило, трудно поддаются существующим криптоаналитическим методам анализа [11]. В то время, как РСЛОС широко используются в тестировании и симуляции [12], для криптографических приложений, генерируемые РСЛОС ПСП не являются безопасными с криптографической точки зрения.

РСНОС присуще практически все достоинства классических РСЛОС, но благодаря внесенной нелинейности в структуру обратной связи, РСНОС не обладают основным недостатком РСЛОС — восстановлением структуры регистра по известной выходной последовательности с помощью алгоритма Берлекэмпа-Мэсси [13]. При использовании РСНОС, как показано в [14], сложность восстановления структуры L-битного РСНОС, генерирующего данную последовательность, составляет порядка $O(2^L)$.

Однако, несмотря на перспективность применения РСНОС как одного из основных элементов генератора ПСП, многие фундаментальные проблемы, связанные с РСНОС остаются недостаточно изученными [15]. Одной из важных характеристик [15] для конструкций, которые генерируют последовательность с максимальным периодом (М-последовательность), является объем ансамбля, то есть количество различных М-последовательностей для заданного размера регистра сдвига с обратной связью.

В работе [16] показано, что РСНОС второго порядка дают значительное преимущество по сравнению с РСЛОС по количеству возможных различных структур, которые будут генерировать *M*-последовательности при одинаковом значении L. Например, для РСЛОС размерностью $L = 9$, количество возможных комбинаций (k), которыми можно варьировать при синтезе регистра сдвига составляет 512, из которых только 48 комбинаций генерируют *M*-последовательность. Для РСНОС второго порядка того же размера: $k = 3{,}5 \cdot 10^{13}$, из которых 519 239 794 комбинаций генерируют *M*-последовательность.

В данной работе рассматривается модель РСНОС с нелинейностью произвольного порядка. Изучается число различных образующих полиномов, на основе которых можно построить РСНОС. В качестве результата приводятся расчетные выражения для определения числа РСНОС произвольного порядка.

Общая модель РСНОС. Общая конструкция РСНОС третьего порядка для регистра, состоящего из $L = 4$ ячеек, приведена на рисунке 1. Если в регистрах используется произведение только двух ячеек, то такие РСНОС называем РСНОС второго порядка. Если используется произведение от трех ячеек (см. рисунок) — РСНОС третьего порядка. В общем случае, при максимальном произведении r числа ячеек, будем говорить о нелинейности r-го порядка. Предельный случай, когда $r = L$ будет соответствовать нелинейности максимального порядка. В данной работе под РСНОС будем понимать РСНОС только в $GF(2)$.

На рисунке введены следующие обозначения: $a \in \{0,1\}$ — коэффициент обратной связи, соответствует наличию ($a = 1$) или отсутствию ($a = 0$) обратной связи от произведения соответствующих ячеек регистра; $q_i(t) \in \{0,1\}$ — значение i-ого регистра в момент времени t; Q — генерируемая последовательность бит. Знаком $\otimes$ обозначена нелинейная функция умножения (соответствующая логической операции «и» — AND), а $\oplus$ — линейная функция сложения (соответствующая логической операции исключающего «или» — XOR).

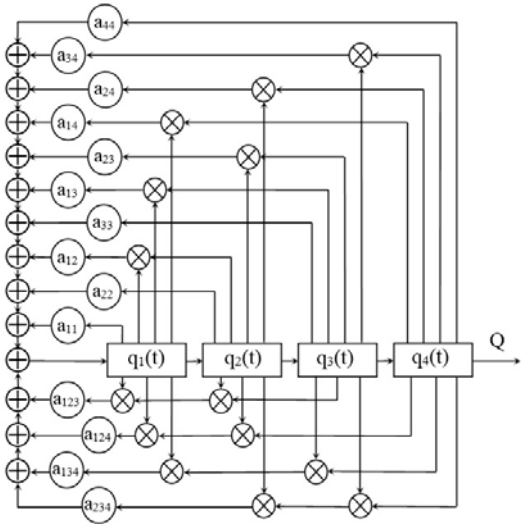

Рисунок. *Общая конструкция РСНОС третьего порядка*

Расчет числа РСНОС r-го порядка. Число различных образующих полиномов, с помощью которых можно построить РСНОС r-го порядка, определяется соотношением:

$$k = 2^{n_L^r}.$$

Выражения для определения числа различных образующих полиномов (n_L^r) можно получить исходя из принципов комбинаторики, рассматривая количество ячеек в регистре L как генеральную совокупность, а произведение между различными ячейками — как выборку из r неупорядоченного набора. Тогда число сочетаний из L элементов по r (C_L^r) можно вычислить по формуле:

$$C_L^r = \frac{L!}{r!\cdot(L-r)!}.$$

Откуда получаем для РСЛОС:

$$C_L^1 = \frac{L!}{1!\cdot(L-1)!} = L.$$

Нелинейность второго порядка будет соответствовать $r = 2$ и число нелинейных комбинаций второго порядка будет определяться соотношением:

$$C_L^2 = \frac{L!}{2!\cdot(L-2)!} = \frac{L\cdot(L-1)}{2}.$$

Общее количество комбинаций, которое можно составить из линейных и нелинейных коэффициентов второго порядка, задается выражением:

$$n_L = C_L^1 + C_L^2 = \frac{L\cdot(L+1)}{2},$$

что соответствует результатам, приведенным в [16].

Обобщая результаты для произвольного порядка нелинейности получаем формулу для определения количества коэффициентов обратной связи a, используемое в конструкции в случае нелинейности r-го порядка для регистра размерности L:

$$n_L^r = \sum_{i=1}^{r} C_L^i = L\cdot\left(1 + \sum_{i=1}^{r-1}\frac{\prod_{j=1}^{i}(L-j)}{(1+i)!}\right).$$

В предельном случае, когда задействована нелинейность максимального порядка, для данного размера регистра, n_L принимает вид:

$$n_L^{r=L} = 2^L - 1.$$

Расчетные значения n_L^r для нелинейности r-го порядка приведены в табл. 1.

Таблица 1

Количество коэффициентов обратной связи (n_L^r), используемое в РСНОС, в случае нелинейности r-го порядка для регистра размерности L

L	**Порядок нелинейности, r**									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
2	2	3	–	–	–	–	–	–	–	–
3	3	6	7	–	–	–	–	–	–	–
4	4	10	14	15	–	–	–	–	–	–
5	5	15	25	30	31	–	–	–	–	–
6	6	21	41	56	62	63	–	–	–	–
7	7	28	63	98	119	126	127	–	–	–
8	8	36	92	162	218	246	254	255	–	–
9	9	45	129	255	381	465	501	510	511	–
10	10	55	175	385	637	847	967	1 012	1 022	1 023

В качестве примера, в табл. 2, приведено n_L^r, а также число различных комбинаций, которое можно из них составить при максимальной нелинейности для $L = 32$ и $L = 64$. Для сравнения приведем аналогичные значения для РСЛОС и РСНОС второго порядка, взятые из работы [16].

Таблица 2

Сравнительная таблица числа возможных комбинаций для РСНОС при нелинейности различного порядка

L	**РСЛОС**		**РСНОС второго порядка**		**РСНОС максимального порядка**	
	n_L	k	n_L	k	$n_L^{r=L}$	k
32	32	$4{,}3\cdot10^{9}$	528	$8{,}8\cdot10^{158}$	4 294 967 295	$\sim10^{1\,292\,820\,256}$
64	64	$1{,}8\cdot10^{19}$	2 080	$1{,}4\cdot10^{626}$	18 446 744 073 709 551 615	$\sim10^{5\,552\,620\,721\,900\,791\,247}$

Как видим, число различных образующих полиномов, с помощью которых можно построить РСНОС максимального порядка, значительно превышает аналогичное число для РСЛОС или же РСНОС второго порядка. При этом, если тенденция числа РСНОС генерирующих *M*-последовательность будет также сохраняться, как и для нелинейности второго порядка, то при нелинейности третьего и более высокого порядка есть все основания полагать о существовании колоссального числа различных РСНОС генерирующих *M*-последовательность даже при небольших размерах используемых регистров.

Выводы. Количество коэффициентов обратной связи, для РСНОС произвольного порядка, вычисляется по формуле:

$$n_L^r = L \cdot \left(1 + \sum_{i=1}^{r-1} \frac{\prod_{j=1}^{i} (L-j)}{(1+i)!} \right).$$

В предельном случае, когда $r = L$, что соответствует РСНОС максимального порядка, n_L^r будет определяться как:

$$n_L^{r=L} = 2^L - 1.$$

Количество различных РСНОС r-го порядка значительно превосходит аналогичное количество для РСЛОС или РСНОС второго порядка и, потенциально, может также многократно превосходить по числу регистров, генерирующих М-последовательность.

Список использованной литературы:

1. Горбенко Ю. І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації. Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем: За заг. ред. д.т.н., професора І.Д. Горбенка. Харків: Видавництво «Форт», 2015. 960 с.
2. An NLFSR-Based Stream Cipher. Berndt M. Gammel, Rainer G¨ottfert and Oliver Kniffler Infineon Technologies AG, Munich, Germany. Режим доступа: https://www.researchgate.net/ publication/224647778
3. Martin Hell, Thomas Johansson, Willi Meier, Grain — A Stream Cipher for Constrained Environments, Estream submissionmany. Режим доступа: http://www.ecrypt.eu.org/stream/p3ciphers/ grain/Grain_p3.pdf
4. Golomb S. Shift Register Sequences. Aegean Park Press. 1982.
5. Gammel B., Gottfert R., Kniffler O. Achterbahn-128/80: Design and analysis. in SASC'2007: Workshop Record of The State of the Art of Stream Ciphers. 2007. P. 152–165.
6. Chen K., Henricken M., Millan W., Fuller J., Simpson L., Dawson E., Lee H., Moon S. (2005) Dragon: A fast word based stream cipher. in eSTREM, ECRYPT Stream Cipher Project. Report 2005/006.
7. Hell M., Johansson T., Meier W. (2005). Grain — a stream cipher for constrained environments. Режим доступа: citeseer.ist.psu.edu/732342.html.
8. Canniere C., Preneel B. TRIVIUM specifications. Режим доступа: citeseer.ist.psu.edu/734144.html. 2006.
9. Gittins B., Landman H., O'Neil S., Kelson R. A presentation on VEST hardware performance, chip area measurements, power consumption estimates and benchmarking in relation to the aes, sha-256 and sha-512. Cryptology ePrint Archive, Report 2005/415. Режим доступа: http://eprint.iacr.org/. 2005.
10. Canteaut A. Open problems related to algebraic attacks on stream ciphers. in WCC. 2005. P. 120–134.

11. Zeng K., Yang C., Wei D., and Rao T.R.N. «Pseudo-random bit generators in stream-cipher cryptography». Computer. 1991.
12. David R. Random Testing of Digital Circuits. New York: Marcel Dekker. 1998.
13. Massey J. L. «Shift-register synthesis and BCH decoding». IEEE Transactions on Information Theory, Vol. 15. 1969. P. 122–127.
14. Dubrova E., Teslenko M., and Tenhunen H. «On analysis and synthesis of (n,k)-non-linear feedback shift registers», in Design and Test in Europe. 2008. P. 133–137.
15. Коробейников А. Г., Гатчин Ю. А. Математические основы криптологии. Учебное пособие. Санкт-Петербург. 2004. Режим доступа: http://books.ifmo.ru/file/pdf/56.pdf.
16. Полуяненко Н. А., Потий А. В. Сравнение объема ансамбля М-РСЛОС и М-РСНОС, скорости генерации на их основе, для GF(2) и в расширениях поля GF(22). *Радиотехника.* Всеукраинский межведомственный научно-технический сборник. 2016. № 186/216. С. 153–160.

In this paper, one of the important elements of generator of stream ciphers — the nonlinear feedback shift registers (NLFSR) are considered. NLFSR with nonlinearity of random order are considered. The amount of different forming polynomials that can be used for NLFSR are studied. The result — calculated equations for determination of the number of NLFSR of random and maximal order (for a given size of the register) are showed.

Key words: *stream ciphers, nonlinear systems, SRNLF.*

Получено 24.03.2017

УДК 004.056.055

В. А. Пономар, аспірант

Харківський національний університет імені В. Н. Каразіна, м. Харків

СТАН, МЕТОДИКА ТА ПРОМІЖНІ ПІДСУМКИ РОЗРОБКИ ПРОЕКТІВ ПОСТКВАНТОВИХ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ

Наводяться вимоги, пропозиції з порівняння та проміжні результати порівняння кандидатів у постквантові стандарти асиметричних крипто перетворень.

Ключові слова: *асиметричні крипто перетворення, методи порівняння, проміжні результати порівняння постквантових крипто примітивів в ході конкурсу NIST США.*

Вступ. В 2015–2016 роках відбувся ряд значущих подій, які уже суттєво вплинули на інтенсивний розвиток постквантової криптографії. NIST США, розуміючи необхідність пошуку нових асиметричних криптографічних примітивів електронного підпису та асиметричного направленого шифрування, які будуть актуальними та можуть застосовуватись

