УДК 004.056.55

ДОКАЗУЕМО СТОЙКИЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ПОСТКВАНТОВОГО ПРИМЕНЕНИЯ

А. А. КУЗНЕЦОВ, А. С. КИЯН, Д. И. ПРОКОПОВИЧ-ТКАЧЕНКО, В. П. ЗВЕРЕВ, Е. В. КОТУХ, Т. Ю. КУЗНЕЦОВА

В данной работе рассматривается доказуемо стойкий генератор псевдослучайных последовательностей, задача криптоанализа которого сводится к решению хорошо известной и чрезвычайно сложной математической проблеме синдромного декодирования (относящейся к классу NP-сложных). Установлено, что формируемые псевдослучайные последовательности не обладают максимальным периодом, фактический период значительно ниже ожидаемого. Предлагается новая схема генератора, которая сохраняет все позитивные свойства прототипа, однако формируемые последовательности обладают максимальным периодом.

Ключевые слова: модель доказуемой безопасности, генератор псевдослучайных чисел, кодовые криптосистемы, постквантовая криптография.

ВВЕДЕНИЕ

Важным направлением в развитии постквантовых методов защиты информации является криптография, основанная на кодах, исправляющих ошибки (Code-based Cryptography) [1, 2]. В работах [3–9] показано, что использование кодовых криптосистем позволяет обеспечить высокую стойкость как к классичес-кому, так и к квантовому криптоанализу.

Первая кодовая криптосистема была предложена 40 лет назад [3] и, при соответствующих параметрах, остается стойкой по сегодняшний день [4–9]. Несмотря на многочисленные попытки криптоанализа [5–9] схема McElice на основе кодов Гоппы [10] считается надежной альтернативой современным криптосистемам с открытым ключом.

Дальнейшее развитие кодовой криптографии получило в работах [11–20]. В частности, в [11] предложена эквивалентная по стойкости криптосистема Niederreiter, которая положена в основу схем электронной цифровой подписи [14, 15]. В [16] предложен новый вариант подписи, использующий криптосистему McElice.

На сегодняшний день National Institute of Standards and Technology (NIST) США проводит открытый конкурс постквантовой криптографии [1, 2, 21–23], где анализируется 64 конкурсных предложения (из 82 предварительно поданных) по трем основным направлениям: шифрование с открытым ключом (public-key encryption), механизмы инкапсуляции ключей (key encapsulation mechanism - KEM), и электронные цифровые подписи (digital signature) [22]. Из общего числа конкурсных предложений третью часть занимает кодовая криптография [23]. Ожидается [1, 23], что в ближайшие десятилетия проект NIST PQC завершиться приятием серии стандартов постквантовой криптографии с открытым ключом.

Еще одним направлением в развитии кодовой криптографии является построение доказуемо стойких генераторов псевдослучайных последовательностей [25–27]. Суть модели доказуемой безопасности (Provable Security Model) состоит в сведении задачи криптоанализа к решению хорошо известной и чрезвычайно сложной математической задачи (относящейся к классу NP-сложных), например, факторизации, дискретного логарифмирования, и пр. [28]. Криптографические примитивы, соответствующие такой модели безопасности, принято называть доказуемо безопасными, т.к. их криптоанализ сопоставим с решением NP-сложной математической задачи. В контексте развития постквантовой криптографии построение и анализ доказуемо стойких генераторов несомненно является важным и актуальным.

Целью данной работы является анализ доказуемо стойкого генератора псевдослучайных последовательностей, задача криптоанализа которого сводится к решению проблемы синдромного декодирования (относящейся к классу NP-сложных) [25], исследование периодических свойств формируемых последовательностей. В работе показано, что формируемые последовательности не обладают максимальным периодом, фактический период значительно ниже ожидаемого. Предлагается новая схема генератора, которая сохраняет все позитивные свойства прототипа, однако формируемые псевдослучайные последовательности обладают максимальным периодом.

1. ДОКАЗУЕМО СТОЙКИЙ ГЕНЕРАТОР, ОСНОВАННЫЙ НА СИНДРОМНОМ ДЕКОДИРОВАНИИ

Доказуемо безопасный генератор, основанный на синдромном декодировании (Pseudo-Random Generator Provably as Secure as Syndrome Decoding), был впервые предложен в работе [25], его исследование и дальнейшее развитие получило в работах [26,27].

Построение генератора основано на использовании блокового (n,k,d) кода, который задан своей проверочной матрицей H размером n столбцов и $n-k$ строк. В теории кодирования известна NP-полная проблема синдромного декодирования [29, 30]:

– по известному вектору-синдрому s длины $n-k$ и известной матрице H найти такой вектор ошибки e длины n, что $s = e \cdot H^T$, причем вес Хемминга (число ненулевых элементов) вектора e равен $w(e) = t = \left\lceil \frac{d-1}{2} \right\rceil$, где $\lceil x \rceil$ – наименьшее целое число, не меньшее x.

Величина t определяет исправляющую способность (n,k,d) кода, т.е. гарантированное число ошибок, которое возможно исправить, применив метод максимального правдоподобия. Для некоторых кодов (со специальной структурой матрицы H) известны быстрые алгоритмы алгебраического декодирования, т.е. нахождение вектора e полиномиально разрешимая задача. Однако для кодов общего положения (без специальной структуры матрицы H) нахождение вектора e является чрезвычайно сложным, наилучшие алгоритмы основаны на переборном поиске.

Для формирования псевдослучайной последовательности используется двоичный (n,k,d) код и следующее рекуррентное правило: $s_i = e_i \cdot H^T$, где: e_i – двоичный вектор длины n, $w(e_i) = t = \left\lceil \frac{d-1}{2} \right\rceil$; s_i – двоичный вектор длины $n-k$; H – двоичная проверочная матрица (n,k,d) кода.

Начальное состояние генератора e_0 задается посредством равновесного кодирования инициализирующей последовательности (*Seed*) y_0 длины

$$m = \left\lfloor \log_2 \left(\frac{n!}{t!(n-t)!} \right) \right\rfloor \text{ бит},$$

где $\lfloor x \rfloor$ – наибольшее целое число, не превосходящее x.

Равновесное кодирование преобразует двоичный вектор y_0 длины m в двоичный вектор e_0 длины n, причем $w(e_0) = t$. Очередное состояние генератора e_{i+1} также формируется посредством равновесного кодирования. Для этого двоичный вектор s_i разбивается на две части:

$$s_i = y_{i+1} \| z_{i+1},$$

(здесь $\|$ – символ конкатенации), причем длина двоичного вектора y_{i+1} равна m. Оставшиеся $n-k-m$ бит образуют вектор z_{i+1}, который подается на выход генератора как элемент псевдослучайной последовательности. Равновесное кодирование вектора y_{i+1} позволяет сформировать состояние e_{i+1} и вычисления повторяются. Алгоритмы равновесного кодирования предлагаются во многих источниках, например, в [31].

Формирование псевдослучайных последовательностей осуществляется итерационной процедурой с использованием проверочной матрицы кода H для формирования вектора-синдрома s_i (см. рис. 1). На каждом шаге алгоритма формируются $n-k-m$ бит последовательности z_{i+1}, причем задача нахождения состояния генератора e_i по известному фрагменту последовательности z_{i+1} и/или вектору-синдрому s_i сопряжена с решением теоретико-сложностной задачи синдромного декодирования.

Для проведения экспериментальных исследований периодических свойств псевдослучайных последовательностей разработана программная реализация генератора. Для небольших параметров выполнен полный перебор всех возможных векторов инициализации (*Seed*). Для каждой инициализации сформирована псевдослучайная последовательность, оценен ее период. В результате мы имеем полный набор всех длин периодов, которые могут быть порождены каждым генератором для соответствующих входных параметров.

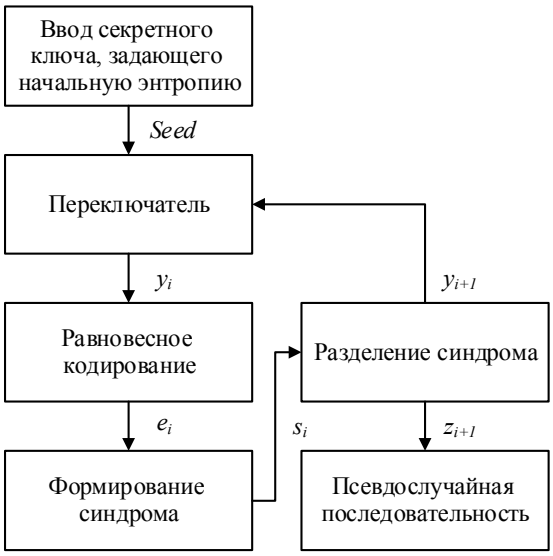

Рис. 1. Структурная схема генератора из [25]

На рисунке 2 приведены распределения числа ключей по длинам периодов в случае использования двоичного (31, 16, 7) кода. В качестве инициализирующей последовательности y_0 выбирались все двоичные вектора длины $m = 12$ бит. На рисунке 3 приведены соответствующие распределения для двоичного (31, 11,

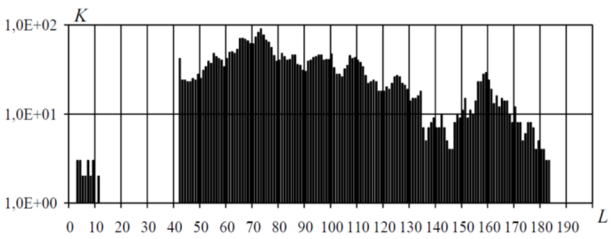

Рис. 2. Распределение количества ключей по длинам периодов формируемых последовательностей, $L_{\max} = 4095$

5) кода с $m = 17$ бит. Максимальная (ожидаемая) длина периода формируемых последовательностей составляет $L_{\max} = 2^m - 1$ бит.

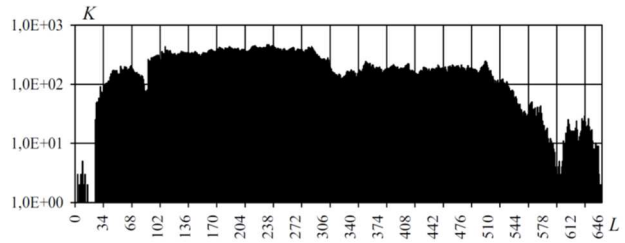

Рис. 3. Распределение количества ключей по длинам периодов формируемых последовательностей, $L_{\max} = 131073$

Полученные результаты показывают, что рассмотренный генератор формирует последовательности, период которых существенно ниже максимального. С увеличением длины инициализирующего вектора расхождения между ожидаемым и фактическим периодом увеличиваются. Например, для последнего случая фактический период меньше максимального более чем в 200 раз.

Выявленный недостаток предлагается устранить добавлением в схему генератора рекуррентных преобразований, гарантирующих максимальный период $L_{\max} = 2^m - 1$.

3. ДОКАЗУЕМО СТОЙКИЙ ГЕНЕРАТОР МАКСИМАЛЬНОГО ПЕРИОДА

В основе предлагаемой схемы генератора, как и в методе-прототипе, лежит использование проблемы синдромного декодирования. Однако правило формирования псевдослучайных последовательностей изменено. Для обеспечения максимального периода предлагается дополнительно использовать рекуррентные преобразования, например, регистры сдвига с линейной обратной связью (РСЛОС, англ. linear feedback shift register, LFSR). При размере регистра m бит и использовании обратных связей, заданных коэффициентами примитивного полинома, будет гарантирован максимальный период $L_{\max} = 2^m - 1$ выходной последовательности [29, 30].

Структурная схема предлагаемого генератора представлена на рис. 4. Цветом выделены дополнительно внесенные блоки преобразований.

Начальное состояние генератора инициализируется последовательностью $y_0 = Seed$, которая после равновесного кодирования преобразуется в вектор e_0. Последовательность $Seed$ задает также начальное состояние u_0 рекуррентного преобразования (например, РСЛОС), обозначим его $\varphi(u)$.

На каждой итерации вычисляется состояние

$$u_{i+1} = \varphi(u_i),$$

которое поступает на сумматор (см. рис. 4).

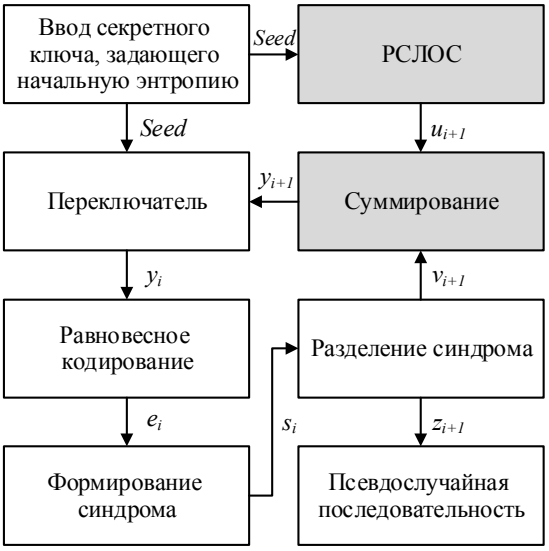

Рис. 4. Структурная схема предлагаемого генератора

Остальная часть генератора функционирует также, как и в методе-прототипе. С использованием двоичного (n,k,d) кода по правилу

$$s_i = e_i \cdot H^T$$

формируется вектор-синдром s_i, который разбивается на две части:

$$s_i = v_{i+1} \| z_{i+1},$$

причем длина двоичного вектора v_{i+1} равна m.

Оставшиеся $n-k-m$ бит образуют вектор z_{i+1}, который подается на выход генератора как элемент псевдослучайной последовательности.

Вектор v_{i+1} складывается с вектором u_{i+1} для формирования очередного значения y_{i+1}:

$$y_{i+1} = u_{i+1} + v_{i+1}$$

и вычисления повторяются.

Таким образом, за счет добавления рекуррентного преобразования (например, РСЛОС) удается обеспечить максимальный период формируемых последовательностей, причем задача нахождения состояния генератора e_i по известному фрагменту псевдослучайной последовательности z_{i+1} и/или вектору-синдрому s_i, как и в методе-прототипе, сопряжена с решением теоретико-сложностной проблемы синдромного декодирования.

Для подтверждения заявленных характеристик разработана программная реализация предложенного генератора. Для выбранных в разделе 2 параметров выполнен полный перебор всех возможных векторов инициализации (*Seed*). Для каждой инициализации сформирована псевдослучайная последовательность,

оценен ее период. Полученные результаты показывают, что все вводимые вектора инициализации приводят к формированию последовательностей максимального периода:

– при использовании двоичного (31, 16, 7) кода с инициализирующей последовательностью y_0 длины $m=12$ бит период всех формируемых последовательностей равен $L_{\max}=2^{12}-1=4095$;

– при использовании двоичного (31, 11, 5) кода с инициализирующей последовательностью y_0 длины $m=17$ бит период всех формируемых последовательностей равен $L_{\max}=2^{17}-1=131073$.

Предлагаемое улучшение генератора сопряжено с повышением вычислительной сложности. Фактически, на каждой итерации при формировании блока псевдослучайной последовательности необходимо дополнительно вычислить очередное состояние рекуррентного преобразования. В тоже время, в случае использования РСЛОС вычислительная сложность повысится не значительно – на один такт регистра сдвига с обратными связями.

ВЫВОДЫ

В данной работе исследованы доказуемо безопасные генераторы, криптоанализ которых основан на решении проблемы синдромного декодирования (относящейся к классу NP-сложных). Ожидается, что этот класс криптопримитивов будет надежным и безопасным даже в условиях применения квантовых методов криптографического анализа.

Рассмотренный генератор, предложенный в работе [25], был реализован программно, для небольших параметров кодов исследованы периодические свойства формируемых псевдослучайных последовательностей. Установлено, что для всех вводимых векторов инициализации генератор формирует последовательности с очень малыми длинами периодов, которые меньше ожидаемого (максимального) периода на несколько порядков.

Для устранения выявленных недостатков предложено усовершенствовать генератор посредством дополнительного выполнения рекуррентных преобразований, гарантирующих максимальный период формируемых последовательностей (например, РСЛОС). Экспериментальные исследования подтвердили заявленные характеристики. Кроме того, задача нахождения состояния генератора по известному фрагменту последовательности, как и в методе-прототипе, сопряжена с решением теоретико-сложностной задачи синдромного декодирования. Следовательно, предлагаемый генератор, как и генератор из [25], будет устойчив к атакам квантового криптоанализа.

Вычислительная сложность реализации предлагаемого генератора незначительно превосходит прототип. На каждой итерации (для формирования каждого блока выходной последовательности) необходимо дополнительно вычислять очередное состояние рекуррентного преобразования. В случае использования РСЛОС вычислительная сложность повысится не значительно (на один такт регистра).

Литература

[1] *D. Moody.* “Post-Quntum Cryptography: NIST’s Plan for the Future.” The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. [On-line]. Internet: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf [March 8, 2016].

[2] *Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta*, Ray Perlner and Daniel Smith-Tone. “NISTIR 8105. Report on Post-Quantum Cryptography”, National Institute of Standards and Technology, Internal Report 8105, April 2016, 10 p.

[3] *R.J. McEliece* “A public-key cryptosystem based on algebraic coding theory”. DSN Progress Report 42-44, Jet Propulsion Lab., Pasadena, CA, January-February, 1978, pp. 114-116.

[4] *D. Bernstein, J. Buchmann and E.Dahmen*. Post-Quantum Cryptography. Springer-Verlag, Berlin-Heidleberg, 2009, 245 p.

[5] *Сидельников В.М.* Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22 с.

[6] *Anne Canteaut and Nicolas Sendrier*. “Cryptanalysis of the original McEliece cryptosystem”. In Kazuo Ohta and Dingyi Pei, editors, Advances in cryptology - ASIACRYPT’98, volume 1514 of Lecture Notes in Computer Science, pp. 187–199.

[7] *Сидельников В.М., Шестаков С.О.* О системе шифрования, построенной на основе обобщенных кодов Рида – Соломона // Дискретная математика. – 1992. – Т.4., №3. – С.57–63.

[8] *L.Minder and A. Shokrollahi.* “Cryptanalysis of the Sidelnikov Cryptosystem”, Advances in Cryptology - EUROCRYPT 2007: 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007, Proceedings, Springer Berlin Heidelberg, 2007, pp. 347–360.

[9] *D.J.Bernstein, T.Lange and C.Peters*. “Attacking and Defending the McEliece Cryptosystem”. In: Buchmann J., Ding J. (eds) Post-Quantum Cryptography. PQCrypto 2008. Lecture Notes in Computer Science, vol 5299. Springer, Berlin, Heidelberg, pp. 31–46.

[10] *Гонна В. Д.* Новый класс линейных корректирующих кодов // Проблемы передачи информации. – 1970. – Т. 6, вып.3. – С. 24–30.

[11] *Niederreiter H.* “Knapsack-type cryptosystems and algebraic coding theory”. Problem Control and Inform Theory, 1986, v. 15. pp. 19–34.

[12] *A. Kuznetsov, A. Kiian, M. Lutsenko, I. Chepurko and S. Kavun,* "Code-based cryptosystems from NIST PQC," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 282–287.

[13] *T. R. N. Rao and K. H. Nam*. “Private-key algebraic-coded cryptosystem”. Advances in Cryptology - CRYPTO 86, New York, NY: Springer, pp. 35–48.

[14] *Courtois, N., Finiasz, M., and N.Sendrier*. “How to achieve a McEliece-based digital signature scheme”. In Advances in

Cryptology - ASIACRYPT 2001, volume 2248, pp. 157–174.

[15] *M.Finiasz.* “Parallel-CFS: Strengthening the CFS McEliece-based signature scheme”. In Biryukov, A., Gong, G., Stinson, D., eds.: Selected Areas in Cryptography. Volume 6544 of LNCS., Springer (2010), pp. 159–170.

[16] *Alexandr Kuznetsov, Andriy Pushkar’ov, Nastya Kiyan and Tetiana Kuznetsova.* “Code-Based Electronic Digital Signature”, The 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT’2018, 24-27 May, 2018, Kyiv, Ukraine.

[17] *A. Kuznetsov, I. Svatovskij, N. Kiyan and A. Pushkar'ov*, "Code-based public-key cryptosystems for the post-quantum period," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 125–130.

[18] *Yu. V. Stasev, A. A. Kuznetsov.* “Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes”. Cybernetics and Systems Analysis, Volume 41, Issue 3, pp. 354–363, May 2005.

[19] *A. Kuznetsov, R. Serhiienko and D. Prokopovych-Tkachenko,* "Construction of cascade codes in the frequency domain," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 131–136.

[20] *Yu.V. Stasev, A.A. Kuznetsov*. “Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes”. Kibernetika i Sistemnyi Analiz, No. 3, pp. 47–57, May-June 2005.

[21] “Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”, National Institute of Standards and Technology, 25 p. [On-line].Internet: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[22] *Ray A. Perlner and David A. Cooper.* “Quantum Resistant Public Key Cryptography: A Survey”, IDtrust ’09, April 14-16, 2009, Gaithersburg, MD, pp. 85-93. [On-line]. Internet: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=901595

[23] *Dustin Moody.* “Let’s Get Ready to RumbleThe NIST PQC “Competition”, National Institute of Standards and Technology, April 18, 2018, 37 p. [On-line]. Internet: https://csrc.nist.gov/CSRC/media/Presentations/Let-s-Get-Ready-to-Rumble-The-NIST-PQC-Competiti/images-media/PQCrypto-April2018_Moody.pdf

[24] “Computer Security Resource Center”. Round 1 Submissions. Created January 03, 2017, Updated June 25, 2018. [On-line] Internet: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions

[25] *Jean-Dernard Fisher, Jacques Stern*. “An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding”. EUROCRYPT’96 Proceeding, LNCS 1070, p. 245–255.

[26] *P. Gaborit, C. Lauradoux and N. Sendrier*, "SYND: a Fast Code-Based Stream Cipher with a Security Reduction," 2007 IEEE International Symposium on Information Theory, Nice, 2007, pp. 186–190.

[27] *T. Wu and R. Wang*, "Stream cipher by reed-solomon code," 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2017, pp. 422–427.

[28] “Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption”, April 19, 2004 - Version 0.15 (beta), Springer-Verlag, 829 p.

[29] *F. J. MacWilliams and N. J. A. Sloane*. The theory of error-correcting codes. North-Holland, Amsterdam, New York, Oxford, 1977, 762 p.

[30] *R.E. Blahut.* Theory and Practice of Error Control Codes. Addison Wesley Publishing Company, Inc., Reading, Massachusetts, 1983, 1983, 500 p.

[31] Методи та алгоритми адаптивного рівноважного кодування на основі біноміальних чисел для інформаційних систем: автореф. дис. / О.В. Бережная; Харк. нац. ун-т радіоелектрон. – Х., 2002. – С. 19.

Поступила в редколлегию 25.12.2018

Кузнецов Александр Александрович, доктор технических наук, профессор, заместитель главного конструктора АТ «ИИТ», профессор кафедры Харьковского национального университета им. В.Н. Каразина. Область научных интересов – криптография и аутентификация, обработка, передача и защита информации.

Киян Анастасия Сергеевна, магистрант кафедры безопасности информационных систем и технологий Харьковского национального университета им. В.Н. Каразина. Область научных интересов – криптография и аутентификация, алгебраическая теория кодов и кодовые криптосистемы.

Прокопович-Ткаченко Дмитрий Игоревич, кандидат технических наук, заведующий кафедрой кибербезопасности Университета таможенного дела и финансов. Заместитель Председателя Государственной службы специальной связи и защиты информации Украины (2013-2014 г.). Область научных интересов – аутентификация и безопасность беспроводных сетей.

Зверев Владимир Павлович, кандидат технических наук, старший научный сотрудник, Помощник Председателя Национальной полиции Украины, Председатель Государственной службы специальной связи и защиты информации Украины (2014-2015 г.). Область научных интересов – информационная и кибернетическая безопасность государства.

Котух Евгений Владимирович, кандидат технических наук, доцент, доцент кафедры кибербезопасности Университета таможенного дела и финансов. Область научных интересов – информационная и кибербезопасность государства, кодовая криптография и аутентификация.

Кузнецова Татьяна Юрьевна, научный сотрудник кафедры безопасности информационных систем и технологий Харьковского национального университета имени В.Н. Каразина. Область научных интересов – криптография и аутентификация, блочные симметричные шифры.

УДК 004.056.55

Кузнецов О. О. **Доказово стійкий генератор псевдовипадкових послідовностей для постквантового застосування** / О. О. Кузнецов, А. С. Кіян, Д. І. Прокопович-Ткаченко, В. П. Звєрєв, Е. В. Котух, Т. Ю. Кузнецова // Прикладна радіоелектроніка: наук.–техн. журнал. – 2018. –Том 17. № 3, 4. – С. 115–120.

У даній роботі розглядається доказово стійкий генератор псевдовипадкових послідовностей, завдання криптоаналізу якого зводиться до вирішення добре відомої і надзвичайно складної математичної проблеми синдромного декодування (що належить до класу NP-складних). Встановлено, що формовані псевдовипадкові послідовності не володіють максимальним періодом, фактичний період значно нижчий за очікуваний. Пропонується нова схема генератора, яка зберігає всі позитивні властивості прототипу, проте формовані послідовності мають максимальний період.

Ключові слова: модель доказової безпеки, генератор псевдовипадкових чисел, кодові криптосистеми, постквантова криптографія.

Іл.: 4. Бібліогр.:31 наім.

UDC 004.056.55

Kuznetsov A. A. **Provably strong pseudorandom sequence generator for post-quantum applications** / A. A. Kuznetsov, A. S. Kiian, D. I. Prokopovich-Tkachenko, V. P. Zverev, E. V. Kotukh, T. Yu. Kuznetsova // Applied Radio Electronics: Sci. Journ. – 2018. – Vol. 17, № 3, 4. – P. 115–120.

This paper considers a provably secure pseudorandom sequence generator whose task of cryptanalysis is reduced to solving a well-known and extremely complex mathematical problem of syndromic decoding (which belongs to a NP-complex class). It is found that formed pseudorandom sequences do not have the maximum period, the actual period is much lower than an expected one. A new generator scheme is proposed which retains all positive properties of the prototype, but formed sequences have a maximum period.

Keywords: proof-security model, pseudorandom number generator, code-based cryptosystems, post-quantum cryptography.

Fig. 4. Ref.: 31 items.