УДК 519.216:519.246, 004.056.5 DOI: 10.20998/2411-0558.2017.50.07

А.О. ПОДОРОЖНЯК, канд. техн. наук, с.н.с., доц., НТУ "ХПІ",
М.Г. ТОКАРЕВ, магістр, НТУ "ХПІ"

МЕТОД ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ВИСОКОЇ СТІЙКОСТІ

Розглянуто криптостійкі детерміновані генератори псевдовипадкових чисел, джерела випадкових чисел і методи генерації псевдовипадкових чисел з використанням апаратних джерел ентропії. Приведено модифікований авторами метод генерації псевдовипадкових чисел високої стійкості з використанням словника та апаратних джерел ентропії різного фізичного походження. Представлені результати роботи розробленого пристрою для генерації паролів на мікроконтролері, що реалізує запропонований модифікований метод генерації псевдовипадкових чисел та зроблений порівняльний аналіз отриманих результатів з сучасними загальновідомими методами. Іл.: 3. Табл.: 2. Бібліогр.: 11 назв.

Ключові слова: криптостійкість, генератор псевдовипадкових чисел, пароль, мікроконтролер.

Постановка проблеми та аналіз публікацій і досягнень. Сучасна інформатика широко використовує псевдовипадкові числа в самих різних галузях – від імітаційного моделювання до криптографії. При цьому від якості використаних генераторів псевдовипадкових чисел (ГПВЧ) безпосередньо залежить якість одержуваних результатів.

Розглянемо такі загально застосовувані методи генерації псевдовипадкових чисел як ISO C Random і xxHash.

ISO C Random – стандартний генератор псевдовипадкових чисел мови С. В якості початкового зсуву, як правило, використовується поточний час в мілісекундах. Дане значення перетворюється за допомогою ряду математичних перетворень у вихідний символ пароля. Наступні символи в якості початкового зсуву використовують попереднє значення до перетворення в символ пароля.

Одним з головних недоліків даного методу є те, що всі символи (крім першого) залежать від попереднього, а отже – знаючи кілька, або навіть один символ, можливо отримати всю послідовність (або кілька послідовностей). Також цей алгоритм має нерівномірність розподілу послідовностей (особливо коротких) отриманих даним методом [1].

xxHash – хеш-функція загального призначення, відрізняється високою швидкістю роботи. Дана хеш-функція формується за допомогою ряду математичних перетворень масиву вхідних значень (він може складатися і з одного елемента – наприклад, поточний час в мілісекундах) в масив вихідних значень. Алгоритм роботи даного методу представлений на рис. 1, k21-k24 – це спеціально підібрані

константи ("магічні числа"), за допомогою яких налагоджують більш рівномірний розподіл отримуваних послідовностей [2].

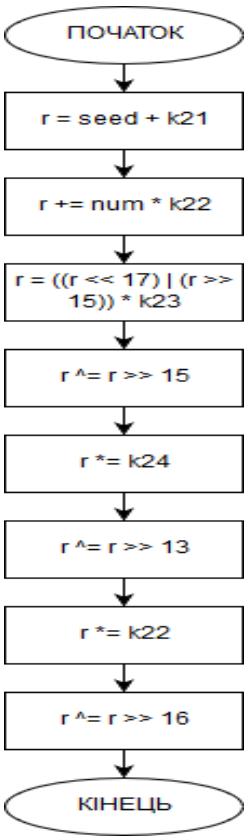

Рис. 1. Блок-схема алгоритму xxGetHash

До плюсів даного методу генерації псевдовипадкових чисел можна віднести те, що кожен символ генерується окремо і не залежить від попереднього значення, однак і цей метод слабо підходить для генерації криптостійких послідовностей псевдовипадкових чисел, так як при використанні недостатньо великого масиву вхідних значень утворюються не рівнорозподілені послідовності.

Недоліком вище перелічених методів є те, що за вхідним обмеженим масивом генеруються набагато більший масив. Це дозволяє скомпрометувати отриману послідовність за обмежений термін часу, знаючи (припускаючи) початковий зсув, або одне чи декілька значень послідовності [3].

Тому доцільно використовувати методи роботи ГСПЧ, які базуються на генерації вихідної послідовності за вхідним масивом, що дорівнює або перевищує розмірність вихідної послідовності.

Таким чином, проблемою є використання відомих програмних методів генерації псевдовипадкових чисел для створення захищених паролів, що призводить до недостатньо криптостійких та надійних результатів. Одним із шляхів вирішення даної проблеми є застосування випадкових чисел, одержуваних з фізичних джерел в якості породжуючих елементів для програмних ГСПЧ.

Для застосування у криптографії необхідний метод генерації паролів гарантованої стійкості [4, 5], який використовує перетворення джерел ентропії в символи пароля. В якості таких апаратних джерел ентропії можуть використовуватися датчики [6, 7], які можуть забезпечити ентропію не менш заданого рівня, наприклад: температурні датчики, інтервали між натисканнями клавіш тощо.

Генерація криптостійких псевдовипадкових послідовностей з використанням апаратного джерела ентропії. Даний метод генерує пароль посимвольно, перетворюючи інтервал часу між натисканнями клавіш в черговий символ – тому для 16-ти символьного пароля потрібно 16 натискань. Алгоритм роботи даного методу представлений на рис. 2.

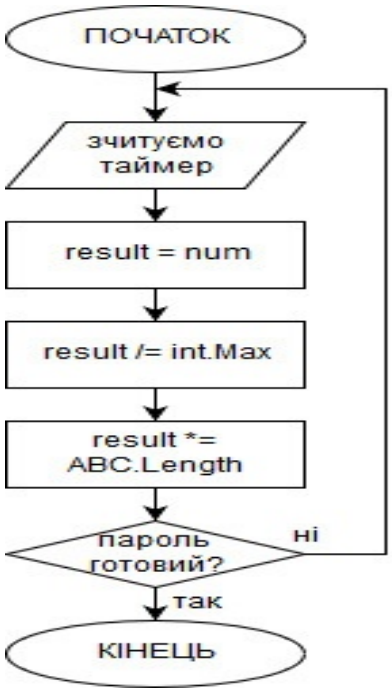

Рис. 2. Блок-схема алгоритму запропонованого методу

Слід також зазначити, що даний метод вимагає постійної безпосередньої участі користувача, через що генерація великих послідовностей, як показано на рис. 3, може зайняти багато часу. У зв'язку з цим, застосування цього методу обмежено тими областями в яких не потрібно генерувати великі послідовності псевдовипадкових чисел.

Пропонований метод дозволяє генерувати найбільш рівномірно розподілені і безпечні паролі, однак вимагає більшої участі користувача і потребує більше часу на свою реалізацію.

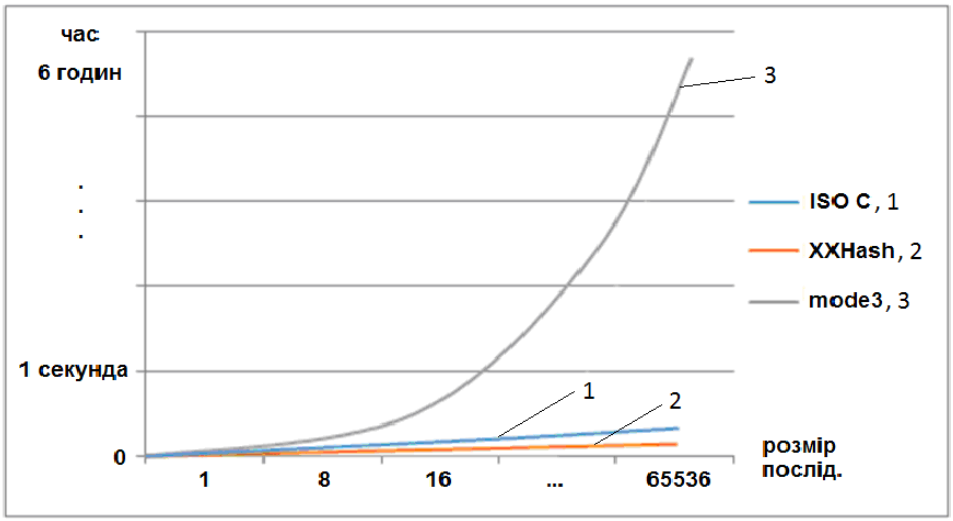

Рис. 3. Порівняння часу роботи розглянутих методів ГПВЧ

Критерій якості методів генерації псевдовипадкових чисел. Для тестування якості ГПВЧ існують різні методи. Можливо використовувати для подібних цілей ENT – програму тестування псевдовипадкових числових послідовностей. Зазвичай під якістю ГПВЧ мається на увазі як швидкість генерації послідовності певної довжини, так і рівномірність розподілу згенерованої послідовності [8, 9].

Значущими параметрами для оцінки якості згенерованих послідовностей були обрані такі характеристики: інформаційна ентропія, середнє значення і коефіцієнт кореляції.

Ентропія вимірює середню кількість інформації на символ джерела або, іншими словами, невизначеність, пов'язану з джерелом. $H(A) = H(a_1, \ldots, a_i, \ldots, a_q) = 0$ означає, що джерело невипадкове і $H(A)$ максимальна, коли всі a_i різновірогідні. Ентропія визначається виразом [10]

$$H_r(A) = \sum_{i=1}^{q} p(a_i) \log_r \left[\frac{1}{p(a_i)} \right], \quad (1)$$

де q – кількість можливих станів, $p(a_i)$ – імовірність появи стану a_i.

Середнє арифметичне множини чисел – сума всіх чисел, поділена на їх кількість. Визначається виразом

$$\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i \,, \quad (2)$$

де n – розмір множини, x_i – значення i-го елемента множини.

Лінійний коефіцієнт кореляції вимірює, наскільки кожен елемент псевдовипадкової послідовності залежить від попереднього. Для випадкових послідовностей це значення буде близьким до нуля. Визначається виразом [11]

$$r_{XY} = \frac{\sum_{t=1}^{n} (X_t - \bar{X})(Y_t - \bar{Y})}{\sqrt{\sum_{t=1}^{n} (X_t - \bar{X})^2 \sum_{t=1}^{n} (Y_t - \bar{Y})^2}}, \quad (3)$$

де n – розмір послідовностей, X_t, Y_t – елементи послідовностей, $\bar{X}$, $\bar{Y}$ – середні значення вибірок.

Якість окремо взятої характеристики розраховується як відношення різниці еталонного значення і поточного до різниці еталонного значення і максимально допустимого

$$Q_i = 1 - \frac{|v_e - v_i|}{|v_e - v_m|}, \quad (4)$$

де v_e – еталонне значення обраної характеристики, v_i – отримане значення обраної характеристики, а v_m – граничне значення обраної характеристики.

Граничне значення обраної характеристики v_m обирається у інтервалі від 0 до еталонного значення v_e. У часто використовуваному випадку v_m дорівнює 0, і тоді якість може бути розраховано за нижченаведеною формулою

$$Q_i = 1 - \frac{|v_e - v_i|}{|v_e|}. \quad (5)$$

Загальна якість обраного методу вважається як середнє зважене для всіх показників

$$Q_s = \frac{1}{\sum_{i=1}^{m} w_i} \sum_{i=1}^{m} w_i Q_i \,, \qquad (6)$$

де m – кількість оцінюваних характеристик; w_i – ваговий коефіцієнт (від 0 до 1); Q_i – якість i-й характеристики.

Мета статті – обґрунтування методу генерації криптостійких псевдовипадкових послідовностей з використанням анаратних джерел ентропії.

Розробка пристрою генерації паролів. Був розроблений пристрій, який забезпечує виконання таких функцій: вимірювання температури і часу між натисканнями по запиту; вибір методу генерації пароля; генерація пароля з використанням зчитаних даних в якості апаратних джерел ентропії відповідно до обраного методу; відображення даних на дисплеї. Налагодження пристрою було проведене в системі схемотехнічного моделювання та на стенді.

Розроблена програма дозволяє згенерувати пароль трьома різними способами: за допомогою стандартного С генератора ISOCRandom, за допомогою спрощеного варіанту швидкого xxHash і без використання ГПСЧ. ISOCRandom використовує в якості сида (джерела ентропії) поточне значення температури і поточне значення таймера, пароль генерується посимвольно. xxHash також використовує в якості джерела ентропії поточне значення температури і поточне значення таймера, однак пароль генерується одноразово. Третій метод генерує пароль посимвольно, перетворюючи інтервал часу між натисканнями клавіш в черговий символ – тому для 16-ти символьного пароля потрібно 16 натискань. Рівномірність розподілу чисел в першому випадку – мінімальна, в разі ж використання xxHash – вона зростає. Крім того, xxHash генерує за один раз весь пароль внаслідок чого пароль генерується швидше. Третій варіант дозволяє генерувати найбільш рівномірно розподілені і безпечні паролі, однак вимагає більшої участі користувача і потребує більше часу на свою реалізацію.

Для генерації паролів було застосовано мікроконтролер PIC16F877, в якості зовнішніх джерел ентропії – таймери і температурний датчик DS18S20, згенерований пароль виводився на дисплей. Для написання прошивки (програми мікроконтролера) використано середовище розробки MicroC for PIC.

Після створення програми та моделювання її роботи у середовищі Proteus 8, було проведене успішне натурне тестування роботи розробленого програмно-апаратного пристрою створення криптостійких псевдовипадкових послідовностей на стенді PIC EASY.

Для оцінки якості отриманих псевдовипадкових послідовностей використовувались згенеровані пристроєм послідовності з 65535 відліків.

Результати порівняння якості розглянутих методів генерації псевдовипадкових чисел за формулою 4 наведені в табл. 1.

Таблиця 1

Порівняння якості розглянутих методів ГПВЧ за формулою 4

Характеристики	ISO C Random		xxHash		mode3	
	значення	якість	значення	якість	значення	якість
Інформаційна ентропія	7,98208	98,21%	7,99578	99,58%	7,99758	99,76%
Середнє значення	127,225	96,33%	127,773	96,36%	127,373	98,31%
Коефіцієнт кореляції	0,00816	91,84%	0,00514	94,87%	0,00095	99,05%
Якість ГПВЧ	95,46%		96,93%		99,04%	

Результати порівняння якості розглянутих методів генерації псевдовипадкових чисел за формулою 5 наведені в табл. 2.

Таблиця 2

Порівняння якості розглянутих методів ГПВЧ за формулою 5

Характеристики	ISO C Random		xxHash		mode3	
	значення	якість	значення	якість	значення	якість
Інформаційна ентропія	7,982082	99,78%	7,995784	99,95%	7,997577	99,97%
Середнє значення	127,2246	99,78%	127,7733	99,79%	127,373	99,90%
Коефіцієнт кореляції	0,008159	99,18%	0,005135	99,49%	0,000954	99,90%
Якість ГПВЧ	99,58%		99,74%		99,92%	

Як видно з таблиці, запропонований метод дає більш рівномірний розподіл і більш непередбачувані послідовності. Проведений натурний експеримент показав збіг даних, отриманих при моделюванні у середовищі Proteus 8, з даними, отриманими на стенді PIC EASY.

Висновки. Розроблено метод генерації псевдовипадкових чисел, який використовує в якості апаратних джерел ентропії інтервали між

натисканнями клавіш і датчик температури. Було проведене тестування і порівняння запропонованого методу із загальнодоступними методами генерації псевдовипадкових чисел.

Також було розроблено мікроконтролерний пристрій, що дозволяє генерувати паролі декількома різними методами з використанням датчика температури і часу між натисканнями клавіш, як апаратних джерел ентропії. Розроблена програма дозволяє генерувати пароль одним із трьох вибраних різниих способів: за допомогою модифікованого стандартного С генератора ISOCRandom, за допомогою модифікованого спрощеного варіанту швидкого xxHash та генеруючи пароль посимвольно, перетворюючи інтервал часу між натисканнями клавіш в символ. Рівномірність розподілу чисел (а відповідно – і його криптостійкість) в першому випадку – мінімальна, в разі ж використання xxHash – вона зростає. Крім того, xxHash генерує за один раз весь пароль, внаслідок чого пароль генерується швидше. Третій варіант дозволяє генерувати найбільш рівномірно розподілені та безпечні паролі, однак вимагає більшої участі користувача і потребує більше часу на свою реалізацію.

Список літератури: **1.** *Лобода Є.О.* Мікропроцесорний генератор паролів / *Є.О. Лобода, А.О. Подорожняк, М.Г. Токарев* // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали сьомої НТК. – Харків: ДП "ХНДІ ТМ", ПНТУ, Полтава; КЛА НАУ, Кропивницький; Військова академія ЗС Азербайджанської республіки, Баку, 2017. – С. 58-59. **2.** *Токарев М.Г.* Генерація і побудова тривимірних зображень ландшафту в реальному часі / *М.Г. Токарев, А.О. Подорожняк* // XI Міжнародна науково-практична конференція магістрантів та аспірантів: матеріали конференції: у 3-х ч. – Ч. 3. – Харків: НТУ "ХПІ", 2017. – С. 142-143. **3.** *Шнейер Б.* Прикладная криптография / *Б. Шнейер*. – М.: Триумф, 2016. – 1024 с. **4.** *Фороузан Б.А.* Математика криптографии и теория шифрования / *Б.А. Фороузан*. – М.: НОУ "Интуит", 2016. – 510 с. **5.** *Тилборг ван Х.К.А.* Основы криптологии. Профессиональное руководство и интерактивный учебник / *Х.К.А. Тилборг ван*. – М.: Мир, 2006. – 471 с. **6.** *Cheung R.C.C.* Hardware generation of arbitrary random number distributions from uniform distributions via the inversion method / *R.C.C. Cheung, D.U. Lee, W. Luk, J.D. Villasenor* // IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2007. – Vol. 15. – № 8. – P. 952-962. **7.** *Шарапов В.М.* Датчики / *В.М. Шарапов, Е.С. Полищук, Н.Д. Кошевой, Г.Г. Ишанин, И.Г. Минаев, А.С. Совлуков*. – М.: Техносфера, 2012. – 624 с. **8.** *Rukhin A.* A statistical test suite for random and pseudorandom number generators for cryptographic applications / *A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo,* available at: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf (accesed 14 September 2017). **9.** *Верещагин Н.К.* Колмогоровская сложность и алгоритмическая случайность / *Н.К. Верещагин, В.А. Успенский, А. Шень*. – М.: МЦНМО, 2013. – 576 с. **10.** *Hamming R.W.* Coding and Information Theory. Englewood Cliffs NJ: Prentice-Hall, 1980 – 104 p. **11.** *Knuth D.E.* Art of Computer Programming, Vol. 2: Seminumerical Algorithms. Reading MA: Addison-Wesley Professional, 2014. – 784 p.

References:

1. Loboda, Ye.O., Podorozhnyak, A.O. and Tokarev, M.G. (2017), "Microprocessor Password Generator", *Modern directions of development of information and communication technologies*

and means of management. Proceedings of the 7th International Conference, April 20-21, State Enterprise "KhNDI TM", Kharkiv; PNTU, Poltava; Military Academy of the Armed Forces of the Republic of Azerbaijan, Baku, pp. 58-59.
2. Tokarev, M.G. and Podorozhnyak, A.O. (2017),. "Generation and construction of three-dimensional landscape images in real time", *Proceedings of the 11th International scientific and practical conference of graduate students and postgraduate students, April 18-21*, 2017, Kharkiv, NTU "KhPI", Vol. 3, pp. 142-143.
3. Schneier, B. (2016), *Applied Cryptography*, Triumph, Moskow, 1024 p.
4. Forouzan, B.A. (2016), *Mathematics of cryptography and the theory of encryption*, National Open University "Intuit", Moskow, 510 p.
5. Tilborg, H.C.A. (2006), *Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial*, Mir, Moskow, 471 p.
6. Cheung R.C.C., Lee, D.U., Luk, W. and Villasenor, J.D. *(*2007), *"*Hardware generation of arbitrary random number distributions from uniform distributions via the inversion method", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 15, No. 8, pp. 952–962.
7. Sharapov, V.M., Polishchuk, E.S., Koshevoi, N.D., Ishanin, G.G., Minaev, I.G. and Sovluskov, A.S. (2012), *Sensors*, Technosphere, Moskow, 624 p.
8. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J. and Vo, S. (2010), "A statistical test suite for random and pseudorandom number generators for cryptographic applications", available at: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.
9. Vereshchagin, N.K. Uspensky, V.A. and Shen, A. (2013), *Kolmogorov complexity and algorithmic randomness*, Moscow Center for Continuous Mathematical Education, Moscow, 576 p.
10. Hamming, R.W. (1980), *Coding and Information Theory*, Englewood Cliffs NJ, Prentice-Hall, 104 p.
11. Knuth, D.E. (2014), *Art of Computer Programming, Volume 2: Seminumerical Algorithms*, Reading MA, Addison-Wesley Professional, 784 p.

Статтю представив д-р техн. наук. завідувач кафедри НТУ "ХПІ" Семенов С.Г.

Поступила (*received*) *11.11.2017*

Podorozhniak Andrii, Ph.D, associate Professor
National Technical University "Kharkiv Polytechnic Institute"
Str. Kirpichova, 2, Kharkov, Ukraine, 61002
Tel.: (057) 707-00-00, , e-mail: andpod2@mail.ru
ORCID ID: 0000-0002-6688-8407

Tokarev Marko, student
National Technical University "Kharkiv Polytechnic Institute"
Str. Kirpichova, 2, Kharkov, Ukraine, 61002
Tel.: (057) 707-00-00, e-mail: tokarevmarko@gmail.com
ORCID ID: 0000-0001-7689-8556

УДК 519.216:519.246, 004.056.5

Метод генерації псевдовипадкових чисел високої стійкості / Подорожняк А.О., Токарев М.Г. // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2017. – № 50 (1271). – С. 36 – 45.

Розглянуто криптостійкі детерміновані генератори псевдовипадкових чисел, джерела випадкових чисел і методи генерації псевдовипадкових чисел з використанням апаратних джерел ентропії. Приведено модифікований авторами метод генерації псевдовипадкових чисел високої стійкості з використанням словника та апаратних джерел ентропії різного фізичного походження. Представлені результати роботи розробленого пристрою для генерації паролів на мікроконтролері, що реалізує запропонований модифікований метод генерації псевдовипадкових чисел. Зроблений порівняльний аналіз отриманих результатів з сучасними загальновідомими методами. Іл.: 3. Табл.: 2. Бібліогр.: 11 назв.

Ключові слова: криптостійкість, генератор псевдовипадкових чисел, пароль, мікроконтролер.

УДК 519.216:519.246, 004.056.5

Метод генерации псевдослучайных чисел высокой стойкости / Подорожняк А.А., Токарев М.Г. // Вестник НТУ "ХПИ". Серия: Информатика и моделирование. – Харьков: НТУ "ХПИ". – 2017. – № 50 (1271). – С. 36 – 45.

Рассмотрены криптостойкие детерминированные генераторы псевдослучайных чисел, источники случайных чисел и методы генерации псевдослучайных чисел с использованием аппаратных источников энтропии. Приведен модифицированный авторами метод генерации псевдослучайных чисел высокой стойкости с использованием словаря и аппаратных источников энтропии различного физического происхождения. Представлены результаты работы разработанного устройства для генерации паролей на микроконтроллере, реализующем предложенный модифицированный метод генерации псевдослучайных чисел. Сделан сравнительный анализ полученных результатов с современными общеизвестными методами. Ил.: 3. Табл.: 2. Библиогр.: 11 назв.

Ключевые слова: криптостойкость, генератор псевдослучайных чисел, пароль, микроконтроллер.

UDC 519.216:519.246, 004.056.5

The method of generating high crypto pseudo-random numbers / Podorozhniak A.O., Tokarev M.G. // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2017. – № 50 (1271). – P. 36 – 45.

Cryptographic stability deterministic pseudo-random number generators, random number sources and methods for generating pseudo-random numbers using hardware entropy sources are considered. A modified method for generating high crypto pseudo-random numbers using a dictionary and hardware sources of entropy of various physical origin is presented. The results of the developed device for generating passwords on a microcontroller implementing the proposed modified method for generating pseudo-random numbers are presented. Comparative analysis of the results obtained with modern well-known methods. Figs.: 3. Tabl.: 2. Refs.: 11 titles.

Keywords: cryptographic stability, pseudo-random number generator, password, microcontroller