УДК 004.421

О. П. Нарєжній*, канд. техн. наук,
Т. О. Гріненко,** канд. техн. наук, доцент

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

МЕТОД ПОБУДОВИ АЛГОРИТМУ ЕКСТРАКТОРА НА ОСНОВІ БАГАТОМОДУЛЬНОГО ПЕРЕТВОРЕННЯ ДЛЯ ПЕРСПЕКТИВНОГО КВАНТОВОГО ГЕНЕРАТОРА ВИПАДКОВИХ ЧИСЕЛ

В загальному вигляді сформульована і вирішена задача синтезу та аналізу алгоритму екстрактора з основою алфавіту більше двох на основі багатомодульного перетворення для перспективного квантового генератора випадкових чисел (КГВЧ). Дана робота виконувалась в рамках проведення комплексних теоретичних та експериментальних досліджень зі створення прототипу КГВЧ на основі реалізації методу подвійного радіооптичного резонансу в парах лужних металів.

Ключові слова: *квантовий генератор випадкових чисел, квантовий фазовий шум, екстрактор квантового генератора випадкових чисел, обчислювальна складність алгоритму.*

Вступ. Генерування випадкових чисел на основі квантових процесів є однією з актуальних та важливих задач криптографії. На цей час запропоновано багато методів використання квантових процесів у генераторах випадкових чисел (ГВЧ), як основні можна виділити такі [1]: метод розщеплення одиничного фотона на два шляхи та поляризації одиничного фотона; метод виявлення заплутаності шляху числа фотонів; метод підрахунку часу генерації або кількості фотонів; метод використання гомодинного виявлення флуктуації вакуумного стану; метод інтерферометричної схеми.

Постановка задачі [2] щодо теоретичного обґрунтування і практичного застосування методу вимірювання фазового шуму квантових дискримінаторів на парах лужних металів для створення прототипу КГВЧ є оригінальною, і має важливе практичне та наукове значення в криптографічних додатках. Однак даний метод має низьку швидкодію ≤ 1000 біт/с на один фотоприймач (канал). Тому швидкодія досягається використанням матриці з фотоприймачів, яка може нараховувати $\sim 10^6$ одиниць фотодіодів, що приводить до значного розширювання основи алфавіту перспективного КГВЧ.

Експериментальні дослідження макету КГВЧ показали, що квантовий фазовий шум має гауссовський закон розподілу імовірності,

тому для збільшення мінімальної ентропії та швидкодії необхідно використовувати методи та засоби збільшення ентропії [1, 2]. Тому в сучасних КГВЧ використовуються спеціальні засоби — екстрактори.

Квантовий ГВЧ — пристрій, який формує на своєму виході Y_l послідовність статистично незалежних символів з основою алфавіту m. Екстрактор КГВЧ — детермінований алгоритм чи сукупність алгоритмів та засобів, які для заданої послідовності довжиною k формують при своїй роботі послідовність Y_l символів довжиною $l >> k$, яка володіє властивістю випадкової послідовності з високою рівноймовірністю появи символів, незалежністю та однозначністю. Схема екстрактора КГВЧ включає: 1 — КГВЧ, що формує випадкові послідовності довжиною k; 2 — схему формування початкових значень k та П параметрів генератора псевдовипадкових символів; 3 — генератор псевдовипадкових символів; 4 — логіку зворотного зв'язку [1].

В загальному вигляді випадкову послідовність на виході екстрактора можна задати як залежність $Y = F(\Pi(A_s), K(A_i), A_k)$ від початкових значень ключа $K(A_i)$ та параметрів $\Pi(A_s)$, а також випадкових послідовностей A_k. При цьому зворотний зв'язок Y призводить до впливу його на параметри, початкові значення та роботу генератора псевдовипадкових символів.

Встановлення початкового стану екстрактора КГВЧ.

1. Задається початкове значення s екстрактора. Для цього використовується фізичне джерело випадкових послідовностей, що ґрунтується на випадковості квантових процесів у КГВЧ. Початковий стан екстрактора є таємним. Умови отримання початкового стану екстрактора повинні унеможливлювати доступ до нього або його частини, модифікацію, підміну або знищення.
2. Задається значення двійкового рядка B_1 та B_2 з точністю 64 двійкових розрядів. Для цього використовується поточні значення дати і часу, що отримані за допомогою приймача сигналів GPS.

На теперішній час відомо ряд алгоритмів екстракторів на основі методів та засобів генерування псевдовипадкових послідовностей (ПВП) [1]. Їх особливістю є те, що вони будуються, добре досліджені та застосовуються для алфавіту з основою $m = 2$.

Розглянемо метод побудування алгоритму екстрактора з певним алфавітом символів, скажімо m, на основі багатомодульних перетворень у скінченному полі Галуа $GF\left(p^n\right)$. Для загального випадку будемо вважати, що здійснюється k перетворень елементів розширення

поля Галуа $GF\left(p^n\right)$, відповідно за модулями $\left(f\left(X\right),f_1\left(X\right)\right)$, $\left(f_1\left(X\right),f_2\left(X\right)\right),\ldots,\left(f_{k-2}\left(X\right),f_{k-1}\left(X\right)\right)$ та останнім модулем m. Загальними параметрами, яких достатньо для того, щоб генерувати елементи a_i поля $GF\left(p^n\right)$, є кортеж $\left(f\left(X\right),p,n,\theta_j\right)$, де $f\left(X\right)$ — незвідний поліном степеня n над полем $GF\left(p\right)$, а θ_j — первісний елемент, вибраний із множини $\left\{\theta\right\}$ порядку $\varphi\left(p^n-1\right)$, де $\varphi\left(*\right)$ — функція Ейлера. В такому випадку генерування (формування) елементів поля здійснюється за правилом:

$$a_i=\left(\theta_j\right)^i\left(\mathrm{mod}\left(f\left(X\right),p,n\right)\right). \tag{1}$$

Показано [1, 3], що при виконанні зазначених вище вимог до кортежу $\left(f\left(X\right),p,n,\theta_j\right)$, перетворення (1) породжує скінченне поле Галуа з періодом повторення p^n-1. Відзначимо, що вказане є справедливим для $p=2,3,5,7$ і наступних простих чисел.

Далі нехай $\left(f_s\left(X\right),p_s,n_s\right)$ будуть кортежами загальних параметрів, наприклад, поліномів (у тому числі незвідних) $f_s\left(X\right)$, $s=\left(1,k-1\right)$, а n_s — їх степені. Незвідність поліномів нам потрібна для того, щоб за необхідності забезпечити їх взаємну простоту.

Також нехай степені поліномів (у тому числі незвідних) n_s задовольняють вимогам:

$$n_1>n_2,\ n_2>n_3,\ \ldots,\ n_{k-2}>n_{k-1}, \tag{2}$$

причому основа алфавіту m є довільним числом, а також виконуються нерівності:

$$p^{n_1}>>p^{n_2},\ p^{n_2}>>p^{n_3},\ldots,p^{n_{k-2}}>>p^{n_{k-1}},\ p^{n_{k-1}}>>m. \tag{3}$$

Справедливими є твердження 1 та 2.

Твердження 1. Детермінований генератор ПВП, що функціонує згідно з алгоритмом багатомодульного перетворення:

$$b_i=\Big(\left(\theta_j\right)^i\left(\mathrm{mod}\left(f\left(X\right),p,n\right),\left(f_1\left(X\right),p_1,n_1\right),\left(f_2\left(X\right),p_2,n_2\right),\ldots\right.$$
$$\left.\ldots,\left(f_{k-1}\left(X\right),p_{k-1},n_{k-1}\right),\left(f_m\left(X\right),m\right)\right), \tag{4}$$

параметрів, *m* — певне натуральне число, *k* — ступінь багатомодульності, p_m — число (не обов'язково просте), забезпечує генерування ПВП (символів) з періодом повторення p^n-1, рівноймовірно і з певною основою алфавіту *m* за умови, що:

1) виконуються умови (1)–(3);
2) модулі (пари поліномів)

$$\left(f(X), f_1(X)\right), \left(f_1(X), f_2(X)\right), \ldots, \left(f_{k-2}(X), f_{k-1}(X)\right) \qquad (5)$$

є взаємно простими, а кортеж ($f_m(X), m$) є довільним.

В умові (4) запис $\left(f_m(x), m\right)$ означає, що модуль m подається у вигляді полінома.

При виконанні умов (4)–(5) забезпечується генерування ПВП (символів) з такими властивостями і характеристиками: довільною основою алфавіту m; періодом повторення $p^n - 1$; символи генеруються рівноймовірно або «практично» рівноймовірно; ансамблем ізоморфізмів $\varphi\left(p^n - 1\right)$.

Твердження 2. Детермінований генератор ПВП, що функціонує згідно з алгоритмом багатомодульного перетворення

$$b_i = \left(\left(\theta_j\right)^{K_0+i}\left(\mathrm{mod}\left(f(X), p, n\right), \left(f_1(X), p_1, n_1\right), \ldots \right.\right.$$
$$\left.\left. \ldots, \left(f_{k-1}(X), p_{k-1}, n_{k-1}\right), \left(f_m(X), \overleftarrow{m}\right)\right)\right), \qquad (6)$$

де $K_0 + i$ — поточний ключ генератора, K_0 — початковий ключ, а i — ключ сеансу, є необоротним зі складністю не нижче за $O(n)$ [1].

Розглянемо окремий випадок тверджень 1 і 2 для трьох модульного перетворення. Елементи розширення поля Галуа також генеруються згідно з (1), але (2)–(6) набувають вигляду:

$$n_1 > m, \qquad (7)$$

$$p^{n_1} >> p^m,\ a_i\ p^n - 1 \qquad (8)$$

$$b_i = \left(\left(\theta_j\right)^i\left(\mathrm{mod}\left(f(X), p\right), \left(f_1(X), p_1, n_1\right), \left(f_m(X), \overleftarrow{m}\right)\right)\right), \qquad (9)$$

$$b_i = \left(\left(\theta_j\right)^{K_0+i}\left(\mathrm{mod}\left(f(X), p\right), \left(f_1(X), p_1, n_1\right), \left(f_m(X), \overleftarrow{m}\right)\right)\right). \qquad (10)$$

Для умов (7)–(10) твердження 1 для трьох модульного перетворення подамо у вигляді теореми 1.

Теорема 1. Детермінований генератор ПВП, що функціонує згідно трьох модульного перетворення на основі (1) за правилами:

$$b_i = \left(\left(\theta_j\right)^i\left(\mathrm{mod}\left(f(X), p, n\right), \left(f_1(X), p_1, n_1\right), \left(f_m(X), \overleftarrow{m}\right)\right)\right) \qquad (11)$$

або

$$b_i = \left(\left(\theta_j \right)^{k_0 + i} \left(\mathrm{mod}\left(f\left(X \right), p, n \right), \left(f_1\left(X \right), p_1, n_1 \right), \left(f_m\left(X \right), \overleftarrow{m} \right) \right) \right), \qquad (12)$$

при виконанні умов (2)–(8), забезпечує генерування ПВП (символів) чисел з довільною основою алфавіту m, з періодом повторення $p^n - 1$, рівноймовірною появою символів на періоді повторення та ансамблем ізоморфізмів $\varphi\left(p^n - 1 \right)$.

Доведення теореми 1 для трьох модульного перетворення наведено [3]. У цілому, алгоритм екстрактору, що реалізує рівноймовірність появи *m*-символів (кінцевого алфавіту) для перспективного КГВЧ на основі багатомодульного перетворення може бути зведений до такого.

1. Увести або генерувати загальносистемні параметри — кортежі загальних параметрів $\left(f_s\left(X \right), p_s, n_s \right)$ згідно з вимогами твердження 1.
2. Увести або інсталювати таємний ключ генератора k, $k = 1 \div p^n - 1$.
3. Обчислити початкове значення генератора a_0, використовуючи правило:

$$a_0 = \theta^k \left(\mathrm{mod}\left(f\ \left(x \right), n \right) \right),$$

де $\left(f\ \left(x \right), n \right)$ — основний модуль перетворення.

4. Обчислити елемент a_i генератора, використовуючи правило:

$$a_i = a_{i-1} \theta \left(\mathrm{mod}\left(f\ \left(x \right), n \right) \right) = R_{\left(f(x), n_1 \right)} \left(a_0 \theta^i \right),$$

де $i \geq 1$ —— номер елемента ПВП, що генерується, a_{i-1} — $\left(i - 1 \right)$-й елемент послідовності над полем поширення p^n.

5. Обчислити елемент b_i ПВП, використовуючи правило:

$$b_i = a_i (\mathrm{mod}\left(f_1\left(x \right), n_1 \right)) = R_{\left(f_1(x), n_1 \right)} \left(a_i \right) = R_{\left(f_1(x), n_1 \right)} \left(R_{\left(f\ (x), n \right)} \left(a_0 \theta^i \right) \right),$$

де $1 < \left(f_1\left(x \right), n_1 \right) < \left(f\left(x \right), n \right)$.

6. Обчислити елемент c_i ПВП, використовуючи правило:

$$c_i = R_{\left(f_n(x), m_n \right)} \left(R_{\left(f_{n-1}(x), m_{n-1} \right)} \left(\ldots \left(R_{\left(f_1(x), m_1 \right)} \left(a_0 \theta^i \right) \right) \ldots \right) \right),$$

де $0 \leq i \leq \varphi\left(p \right)$, а $i \geq 1$ — номер елемента ПВП, що генерується, $\left(f_1\left(x \right), n_1 \right), \ldots, \left(f_n\left(x \right), n_n \right)$ — проміжні модулі.

7. За необхідності обчислити i-те геш-значення від b_i та прийняти його в якості i-го випадкового слова, тобто $y_i = H(b_i)$.

Схема, яка реалізує метод побудови алгоритму екстрактору на основі багатомодульного перетворення для КГВЧ, показана на рисунку.

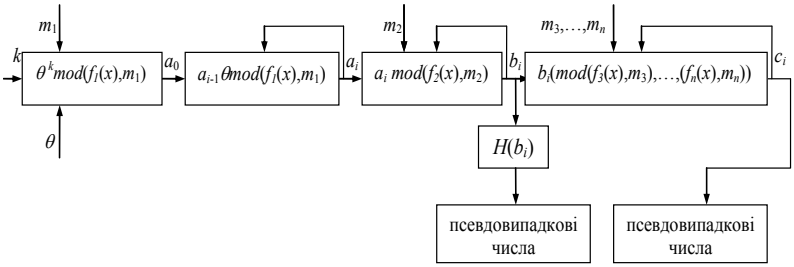

Рисунок. *Схема алгоритму екстрактора перспективного КГВЧ*

Детермінований екстрактор, що функціонує згідно з трьох модульним перетворенням на основі (11) або (12) при виконанні умов (2)–(8), забезпечує генерування ПВП (символів) чисел з певною основою алфавіту m, періодом повторення $p^n - 1$, рівноймовірною появою символів на періоді повторення $p^n - 1$ та ансамблем ізоморфізмі $\varphi\left(p^n - 1\right)$.

Для детального аналізу обчислювальної складності екстрактору необхідні додаткові дослідження. Як грубі оцінки можна використати оцінки, що наведені в роботі [1] відносно обчислювальної складності криптографічних перетворень у скінченному полі $GF\left(p^n\right)$.

Висновки. На цей час розроблено ряд алгоритмів та засобів формування екстракторів [1]. Їх особливістю є те, що вони будуються, як правило, для двійкової основи $m = 2$. Тому, важливою є задача розробки методів і засобів формування екстракторів із необхідними властивостями випадковості та довільною (певною) основою алфавіту. Найбільш перспективним, на наш погляд, серед класів таких перетворень є клас багатомодульних перетворень.

У цілому метод побудови алгоритму екстрактора на основі багатомодульного перетворення може знайти застосування у криптографічних додатках, в яких висуваються умови високої рівноймовірності та довільної основи появи символів ПВП.

Список використаних джерел:

1. Горбенко Ю. І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних сис-

тем за заг. ред. д.т.н., професора І. Д. Горбенко. Харків: Видавництво «Форт», 2016. 960 с.
2. Горбенко І. Д., Гріненко Т. О., Нарєжній О. П. Методика вимірювання спектральної щільності потужності шума квантової радіооптичної системи генератора випадкових чисел. *Радиотехника: всеукр. межвед. науч.-техн. сб.* Харьков: ХТУРЕ, 2016. Вып. 186. С. 172-183.
3. Gorbenko Y., Grinenko T. A pseudorandom sequences generator based on the multimodulo transformation. Computer science and cybersecurity. International electronic scientific journal. 2016 Issue. 1(1). P. 5-19, [Електронний ресурс]. Режим доступу: http://periodicals.karazin.ua/cscs/article/view/6194/5739.

In general form it is stated and solved the task of synthesis and analysis of extractor algorithm on the multi-module transformation with alphabet basis greater than two for prospective quantum random numbers generator (QRNG). The work was lead within a framework of complex theoretical and experimental researches for creation of QRNG prototype based on double radio-optic resonance in alkaline metal pairs.

Key words: *quantum random numbers generator; physical quantum noise; extractor of quantum random numbers generator; computation complexity of the algorithm.*

Одержано 05.03.2017

УДК 519.6

М. О. Недашковський*, д-р фіз.-мат. наук, професор,
Т. І. Крошка,** старший викладач

*Університет Казимира Великого, м. Бидгощ, Польща,
**Буковинський державний фінансово-економічний університет,
м. Чернівці

РОЗВ'ЯЗУВАННЯ МАТРИЧНИХ ПОЛІНОМІАЛЬНИХ РІВНЯНЬ ІЗ ВЕКТОРНИМИ НЕВІДОМИМИ

Пропонуються нові обчислювальні схеми розв'язання поліноміальних матричних рівнянь з векторними невідомими за допомогою ланцюгових дробів.

Ключові слова: *поліноміальні матричні рівняння, ланцюгові дроби.*

Вступ. У роботах В. С. Григорківа [1–4] було розглянуто пряму нелінійну балансову модель міжгалузевої еколого-економічної взаємодії а також двоїсту до неї модель відносно цін. Аторами показано [5], що ця нелінійна модель зводиться до поліноміального матричного рівняння із векторними невідомими вигляду

$$A_n diag(X)^{n-1} X + A_{n-1} diag(X)^{n-2} X + ... + A_1 X + B = 0. \qquad (1)$$

