© Gnatyuk S., Zhmurko T., Kinzeryavyy V., Seilova N. Method of trit pseudorandom sequences generating for quantum cryptography systems // Ukrainian Scientific Journal of Information Security, 2015, vol. 22, issue 2, p. 140-147.



# МЕТОД ГЕНЕРУВАННЯ ТРИТОВИХ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДЛЯ СИСТЕМ КВАНТОВОЇ КРИПТОГРАФІЇ

**Сергій Гнатюк[1], Тетяна Жмурко[1], Василь Кінзерявий[1], Нургуль Сєйлова[2]**

*[1]Національний авіаційний університет, Україна*
*[2]Казахський національний технічний університет ім. К.І. Сатпаєва, Республіка Казахстан*

**ГНАТЮК Сергій Олександрович,** к.т.н.

*Рік і місце народження:* 1985 рік, м. Нетішин, Україна.
*Освіта:* Національний авіаційний університет, 2007 рік.
*Посада:* доцент кафедри безпеки інформаційних технологій з 2012 року.
*Наукові інтереси:* інформаційна безпека, квантова криптографія, управління інцидентами інформаційної безпеки, захист критичної інформаційної інфраструктури держави.
*Публікації:* більше 100 наукових публікацій, серед яких монографії, статті у провідних вітчизняних та закордонних наукових виданнях, патенти та авторські свідоцтва.
*E-mail:* s.gnatyuk@nau.edu.ua

**ЖМУРКО Тетяна Олександрівна**

*Рік і місце народження:* 1990 рік, м. Вінниця, Україна.
*Освіта:* Національний авіаційний університет, 2012 рік.
*Посада:* аспірант кафедри безпеки інформаційних технологій з 2012 року.
*Наукові інтереси:* інформаційна безпека, програмний захист інформації, квантова криптографія.
*Публікації:* більше 20 наукових публікацій, серед яких монографія, наукові статті, тези та матеріали доповідей на конференціях, авторські свідоцтва.
*E-mail:* taniazhm@gmail.com

**КІНЗЕРЯВИЙ Василь Миколайович,** к.т.н.

*Рік і місце народження:* 1985 рік, м. Кам'янець-Подільський, Україна.
*Освіта:* Національний авіаційний університет, 2007 рік.
*Посада:* доцент кафедри безпеки інформаційних технологій з 2014 року.
*Наукові інтереси:* інформаційна безпека, криптографія та криптоаналіз блокових симетричних шифрів.
*Публікації:* більше 80 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях, патенти та авторські свідоцтва.
*E-mail:* v.kinzeryavyy@gmail.com

**СЄЙЛОВА Нургуль Абадуллаєвна,** к.т.н.

*Рік і місце народження:* 1979 рік, Кзил-Ординська область, Республіка Казахстан.
*Освіта:* КазНТУ ім. К.І. Сатпаєва, 2001 рік.
*Посада:* завідувач кафедри «Інформаційна безпека» з 2014 року.
*Наукові інтереси:* мережеві технології, захист інформації, розвиток операційних систем та систем управління базами даних.
*Публікації:* більше 25 навчально-методичних робіт і більш ніж 30 наукових статей.
*E-mail:* seilova_na@mail.ru

***Анотація.*** *Стрімкий розвиток сучасних обчислювальних технологій ставить під загрозу конфіденційність інформації, що забезпечується, як правило, традиційними криптографічними засобами і змушує дослідників шукати альтернативні методи захисту. З огляду на сучасні тенденції розвитку однією з таких альтернатив може стати квантова криптографія, що на відміну від традиційної (яка здебільшого*

*базується на неможливості розв'язання певного класу математичних задач за деякий проміжок часу) використовує специфічні унікальні властивості квантових частинок і ґрунтується на непорушності законів квантової фізики. Відомо, що деякі протоколи квантової криптографії дозволяють досягнути теоретико-інформаційної стійкості – це здебільшого протоколи розподілу ключів. Інший клас протоколів квантової криптографії – це протоколи прямого безпечного зв'язку, більшість з яких мають асимптотичну стійкість. Зважаючи на це, було запропоновано низку методів підвищення стійкості таких протоколів. Один з таких методів дозволяє підвищити асимптотичну стійкість протоколів квантового прямого безпечного зв'язку з парами переплутаних (корельованих) кутритів, проте застосування цього методу потребує генерування трійкових (тритових) псевдовипадкових послідовностей. Саме на розробку такого генератора (методу генерування) і зорієнтована ця стаття. Таким чином, у роботі запропоновано метод генерування тритових псевдовипадкових послідовностей, що базуються на необоротній функції і низці перетворень над полем GF(3). Також на базі методу розроблено відповідний алгоритм, що відображений у вигляді псевдокоду. Подальші дослідження будуть присвячені розробці методу оцінки якості згенерованих тритових псевдовипадкових послідовностей, так як усі існуючі методи орієнтовані на бінарні послідовності.*

***Ключові слова:*** *квантова криптографія, трит, кутрит, псевдовипадкова послідовність, генератор псевдовипадкових послідовностей, квантовий прямий безпечний зв'язок, пінг-понг протокол.*

**Вступ.** Особливе занепокоєння у надійності традиційних криптографічних систем захисту, які використовуються для потреб дипломатії (держави), торгівлі, військової справи та інших галузей, з'явилось з огляду на активний розвиток досліджень та практичну реалізацію квантового комп'ютера (автор терміну Нобелівський лауреат Р. Фейнман), мінімальною одиницею інформації якого є кубіт (*qubit*). Реалізувати його можна різними способами, але головною особливістю його є те, що окрім традиційних станів «0» та «1», він може перебувати одночасно у двох цих станах – стан суперпозиції (*superposition*). При збільшенні кількості кубітів у процесорі квантового комп'ютера його потужність зростає експоненціально, адже замість двох бітів (у класичному процесорі) у квантовому комп'ютері дії будуть проводитися над суперпозицією вже чотирьох станів «00», «01», «10» і «11». У результаті, квантовий комп'ютер обіцяє для вирішення деяких завдань набагато більшу обчислювальну потужність. Однак, для цього необхідно створити ідеальні умови, щоб точно провести операції і не дозволити зруйнуватися квантовому стану до того, як буде здійснене вимірювання. Власне, над цим складним завданням зараз працюють науковці-фізики, яким за останні декілька років вдалося зробити великий прорив і представити на ринок комерційний квантовий комп'ютер (D-Wave Two, який успішно пройшов низку випробувань і використовується у спільному проекті між NASA, Google і USRA під назвою Quantum Artificial Intelligence Lab [1]). Окрім збільшення обчислювальної потужності, квантовий комп'ютер може набагато швидше розв'язувати NP-складні задачі, неможливість швидкого розв'язання яких є основою забезпечення надійності більшості методів асиметричної криптографії.

Отож, постає питання пошуку нових технологій, які могли б стати альтернативою традиційній криптографії. Одним з варіантів є *квантова криптографія* (КК, *quantum cryptography*) – це порівняно новий міждисциплінарний напрям досліджень, що дозволяє застосовувати ефекти квантової фізики і базується на принциповій непорушності постулатів квантової механіки для створення захищених каналів передачі даних [2]. Вона поєднує у собі цілу низку наукових напрямів, таких як квантова механіка, інформатика, теорія інформації, квантові обчислення та криптографія, а сформувалась внаслідок виникнення задач, що не мали класичного розв'язку, у зазначених галузях. Ідея КК з'явилась в 1984 р. завдяки співробітникам фірми IBM (команда науковців на чолі з Ч. Беннетом) спільно з науковцями Монреальського університету (Ж. Брассард) [2], а лабораторні дослідження ведуться з кінця XX сторіччя.

**Постановка завдання.** На сьогодні існує багато напрямів і технологій КК, зокрема, у роботі [4] представлена найбільш широка їх класифікація: квантовий розподіл ключів (*quantum key distribution*) – КРК; квантовий прямий безпечний зв'язок (*quantum secure direct communication*) – КПБЗ; квантове розділення секрету (*quantum secret sharing*); квантовий потоковий шифр (*quantum stream cipher*); квантовий цифровий підпис (*quantum digital signature*); квантова стеганографія (*quantum steganography*).

Як зазначається у [2, 5, 6] основна задача КК полягає у створенні каналу передачі інформації, абсолютна захищеність якого буде гарантуватись фундаментальними законами природи [2, 5, 6], що дозволяють зафіксувати будь-яку спробу проникнення ззовні, тобто надійне виявлення порушника (основна перевага КК над традиційними методами). Процес створення секретного ключа в деяких протоколах КК здійснюється за допомогою передачі оптичним волокном одиночних фотонів (*single photons*), закодованих у певному базисі, і спирається на важливу теорему квантової механіки про неможливість клонування (*no-cloning theorem*) попередньо невідомого квантового стану [2, 5, 6]. У цьому випадку будь-яка спроба прослухати такий канал призведе до виникнення підвищеного рівня помилок, що може бути зафіксовано.

Теоретичні та експериментальні роботи з квантової криптографії ведуться в багатьох науково-дослідних центрах Великобританії, Швейцарії, Франції, Японії, США, а також активні дослідження ведуться компаніями MagiQ, IBM, SmartQuantum, GAP-Optique, ID Quantique, WISeKey, British Telecom, Toshiba Research Europe, SwissCom, BBN Technologies, Mitsubishi Electric Corporation, NEC

Research Institute та холдингом QinetiQ. За минулі два десятиріччя, з моменту початку активних досліджень, запропоновано багато квантових криптографічних протоколів [3, 8-15], виконано значну кількість лабораторних експериментів з їх практичної реалізації [16], виконана важлива робота з доведення стійкості запропонованих протоколів до деяких видів атак [17-19], а також розроблені перші комерційні системи КРК [20-23]. В Україні робота у цій галузі ведеться декількома науково-дослідними групами науковців: Інституту фізики НАН України, Національного технічного університету України «Київський політехнічний університет», Одеської національної академії зв'язку ім. О.С. Попова та Національного авіаційного університету.

Найбільш розвинутим напрямом КК, який вже вийшов на комерційний рівень, є КРК. Швейцарською компанією ID Quantique випущено декілька комерційних рішень (Cerberis QKD for Commercial Applications, Clavis2 QKD for R&D, а також Centauris CN8000, ARCIS, Centauris – з додатковими можливостями додавання Cerberis QKD, для більш надійного захисту інформації), які використовуються у банківських, державних та приватних установах. У роботі [24] представлений детальний аналіз існуючих комерційних систем КРК.

Ще один напрям КК, який використовується сьогодні та викликає значний інтерес у наукової спільноти, це КПБЗ. Протоколи КПБЗ призначені для безпосередньої передачі секретних повідомлень за допомогою переплутаних станів фотонів (*entangled states*), квантовим каналом, без їх попереднього шифрування. Оскільки в КПБЗ відсутні криптографічні перетворення, відповідно – відсутня і проблема розподілу ключів шифрування – а ця проблема є досить критичною у сучасній симетричній криптографії. Відповідно до [4] на сьогодні існують такі протоколи КПБЗ: пінг-понг протокол, протоколи з передаванням переплутаних кубітів блоками, протоколи з одиничними кубітами та протоколи з групами переплутаних кудитів.

Однак в порівнянні з протоколами КРК, які досягають теоретико-інформаційної стійкості (*information-theoretic security*), більшість протоколів КПБЗ мають лише асимптотичну стійкість (*asymptotic security*) до атак, тому потребують наукових досліджень та розробки методів підвищення їх стійкості (*privacy amplification*). На сьогодні запропоновано декілька методів підвищення стійкості КПБЗ [25-34]. В одному з таких методів [33, 34] використовується зворотне хешування із застосуванням оборотних трійкових матриць. Зазначений метод дозволяє підвищити рівень стійкості та швидкість роботи протоколів КПБЗ, проте виникла проблема генерування трійкових (тритових) послідовностей з високим рівнем випадковості. З огляду на це, *метою роботи* є розробка методу генерування тритових псевдовипадкових послідовностей (ПВП) для застосування в системах квантової криптографії.

**Основна частина дослідження.** Історично перший електронний цифровий комп'ютер загального призначення ЕНІАК (розробник Дж. Моклі) використовував десяткову систему числення, однак був дуже громіздким та потребував багато елементів, використання ж двійкової логіки значно все спрощувало, адже у розповсюджених сьогодні логічних елементів лише два стани, тому запис даних є заздалегідь простішим. Проте, питома натуральнологарифмічна щільність запису інформації описується функцією [35]:

$$Y(\mathrm{a}) = \frac{\ln y(\mathrm{a})}{a} = \frac{\ln a}{a}, \qquad (1)$$

де $a$ – це основа системи числення. З рівняння (1) випливає (і з рис. 1 видно), що найбільшу щільність запису інформації має система числення з основою рівною основі натуральних логарифмів, тобто рівною числу Ейлера (e ≈ 2,718281828459045), а з цілочислених – це трійкова система.

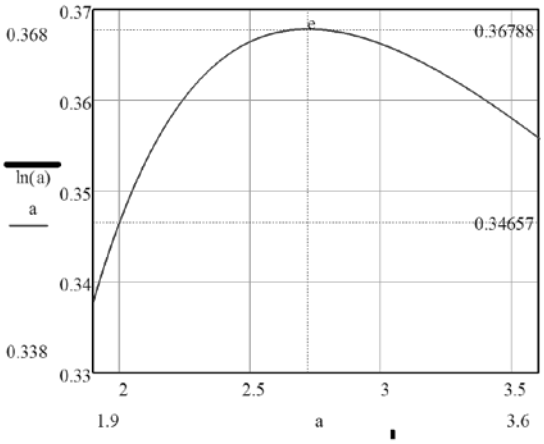


Рис. 1. Питома натуральнологарифмічна щільність запису інформації

Ідея використання трійкової логіки не нова, ще у 1840 р. Т. Фоулер побудував механічну трійкову обчислювальну машину (помножувач з 55-тритним регістром результату), одну з найбільш ранніх механічних обчислювальних машин [36]. А у 1959 р., під керівництвом Н. Брусенцова розроблена перша серійна трійкова ЕОМ «Сетунь» [37, 38]. З 1962 р до 1964 р. Казанським заводом математичних машин було вироблено 46 ЕОМ «Сетунь». У 1970 р., Н. Брусенцов побудував в Московському державному університеті другу електрону трійкову ЕОМ (комп'ютер) «Сетунь-70». 2008 р. – Д. Коннеллі, К. Патель і А. Чавез за підтримки професора Ф. Ніко (California Polytechnic State University of San Luis Obispo, San Luis Obispo, Каліфорнія, США) побудували трьохтритову цифрову комп'ютерну систему TCA2, версія v2.0, в трирівневій (3-Level CodedTernary, 3L CT) системі трійкових логічних елементів на 1484-х інтегральних транзисторах [39]. 2013 р. на конкурсі Intel ISEF представлена робота молодого науковця щодо порівняння швидкості роботи двійкових та трійкових систем [40].

Застосування зазначеного методу [33, 34] потребує генерування трійкових (тритових) ПВП. Проведений аналіз дозволив виявити достатню кількість існуючих генераторів ПВП (ГПВП), які можуть використовуватись для різного роду застосувань [41-44]. Стандарт ISO/IEC 18031, який встановлює концептуальні моделі, термінологію і

вимоги, що відносяться до конструктивних елементів і властивостей систем, які використовуються для генерації випадкових бітів в криптографічних застосування, визначає два типи генераторів: *недетерміновані* (механізм генерації випадкових бітів, який використовує джерело ентропії для генерації випадкового потоку бітів) і *детерміновані* (механізм генерації бітів, який використовує детерміновані механізми, такі як криптографічні алгоритми, на джерелі ентропії для генерації випадкового потоку бітів. Використовує особливі вхідні дані, і, якщо необхідно, деякі необов'язкові вхідні дані, які, залежно від їх застосування можуть бути загальнодоступними) генератори випадкових бітів [41].

За способом отримання ГПВП діляться на три принципово різних класи: *табличні* – основний недолік є скінченими, *фізичні* (радіоактивне випромінювання, фізичні генератори шумів, квантові генератори, генератори імпульсних послідовностей тощо) - спільними і найбільш суттєвими недоліками, що утрудняють їх застосування є обмежена швидкодія, низька стабільність основних імовірнісних характеристик, що пояснюється нестабільністю первинних джерел, дрейфом параметрів перетворюючих схем, джерел живлення та вимагає періодичної статистичної перевірки якості; складність апаратурної реалізації, *алгоритмічні* (ГПВП, наприклад, метод серединних квадратів, метод серединних добутків, метод перемішування, лінійний конгруентний метод) [42].

Також ГПВП можна класифікувати за різними законами розподілу [43], проте найбільш повна класифікація представлена у роботі [44] та відображена на рис. 1. Відповідно до цієї класифікації методи формування ПВП поділяються на *криптостійкі* та *не криптостійкі*. До яких у свою чергу відносять *криптостійкі*: на основі потокових шифрів (наприклад, Dragon-128, SEAL, RC4, RC5, RC6, Grain, Yamb, Phelix), на основі блокових шифрів (наприклад, ГОСТ 28147-89, AES, ANSI X9.17, DES), на основі односторонніх функцій (наприклад, генератори BBS, RSA, Dual_EC_DRBG (еліптичні криві), GPSSD (лінійні коди) та ін.) і *не криптостійкі:* на основі елементарних рекурентів (наприклад, лінійний конгруентний генератор, поліноміальний конгруентний генератор, адитивний генератор Фібоначчі, адитивний генератор Фібоначчі з запізненням, мультиплікативний генератор Фібоначчі з запізненням), на основі операцій в кінцевих полях (наприклад, генератори Галуа, Де Брейна, Фібоначчі, адитивний, Голмана, стискаючий тощо).

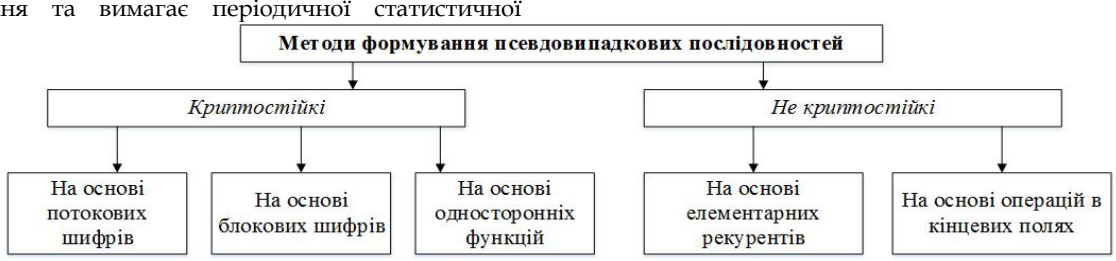


Рис. 2. Методи формування ПВП

**Запропонований метод.** Проте всі розроблені на сьогодні методи генерування ПВП (генератори) орієнтовані на бінарні послідовності, а отже розробка методу генерування тритових ПВП є актуальним науковим завданням. З огляду на це, запропоновано метод генерування тритових ПВП $\xi$ із множиною векторів внутрішніх станів $V_p$ ($V_p = \{0, 1, 2\}^p$), множиною секретних ключів $V_n$, множиною векторів ініціалізації $V_e$ та множиною вихідних послідовностей $V_m$, де $p = 14 \cdot l$, $n = 4 \cdot l$, $e = p - n = 10 \cdot l$, $m = b \cdot n$, $l = d \cdot s$ і $b$, $d$, $s$ – натуральні числа.

*Для генерації вихідної тритової послідовності виконується наступне*:

*Етап 1.* Виконується початкова ініціалізація вектора внутрішнього стану $U$ на основі вектора ініціалізації $VI$ та секретного ключа $K$, $U \in V_p$, $VI \in V_e$, $K \in V_n$.

Нехай $U = (x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3, y_4, k_1, k_2, k_3, k_4)$, де $x_i$, $y_j$, $k_j$ – частини вектора внутрішнього стану $U$ ($x_i \in V_l$, $y_j \in V_l$, $k_j \in V_l$, $i \in \overline{1,6}$, $j \in \overline{1,4}$); $VI = (VI_1, VI_2, VI_3, VI_4, VI_5, VI_6, VI_7, VI_8, VI_9, VI_{10})$, де $VI_o$ – частини вектора ініціалізації $VI$ ($VI_o \in V_l$, $o \in \overline{1,10}$); $K = (K_1, K_2, K_3, K_4)$, де $K_w$ – частини секретного ключа $K$ ($K_w \in V_l$, $w \in \overline{1,4}$).

Тоді внутрішній стан вектора $U$ ініціалізується таким чином:

$x_i = VI_i$, $y_j = VI_{6+j}$, $k_j = K_j$, $i \in \overline{1,6}$, $j \in \overline{1,4}$.

*Етап 2.* На основі поточних значень внутрішнього стану вектора $U$ виконується поступова генерація вихідної послідовності $M = (M_1, ..., M_b)$, $M \in V_m$, $M_q$ – частини вихідної послідовності $M$, $M_q \in V_n$, $q \in \overline{1,b}$. Зауважимо, що при генерації кожного $M_q$ поточні значення внутрішнього стану вектора $U$ весь час змінюються.

**2.1.** Для генерації частини вихідної послідовності $M_q$ $r$-разів ($q \in \overline{1,b}$, $r$ – натуральне число) виконується наступне:

2.1.1. Розраховуються нові значення векторів $x_1$, $x_2$, $x_3$:

$$x_1 = \left(Sbox\left(x_1 + k_1\right) \oplus x_4\right) <<< k_4;$$

$$x_2 = \left(Sbox\left(x_2 + k_2\right) + x_5\right) >>> k_3;$$

$$x_3 = Mix\left(\left(x_3 + x_6\right) \oplus y_3\right) <<< x_1.$$

2.1.2. Обчислюється нові значення векторів $k_1$, $k_2$, $y_1$, $y_2$:

$$k_1 = Sbox\left(\left(Sbox\left(x_1 \oplus k_1\right) + x_5\right) \oplus y_1\right);$$

$$k_2 = Sbox\left(Mix\left(x_2 + k_2 + x_6\right) \oplus y_2\right);$$

$$y_1 = Sbox\left(\left(\left(k_1 + y_1\right) <<< x_2\right) \oplus k_3\right);$$

$$y_2 = Mix\left(Sbox\left(\left(\left(k_2 + y_2\right) >>> x_3\right) \oplus k_4\right)\right).$$

2.1.3. Розраховуються нові значення векторів $x_4$, $x_5$, $x_6$:

$$x_4 = \left(Sbox\left(x_4 + k_3\right) \oplus x_1\right) <<< k_2;$$

$$x_5 = \left(Sbox\left(x_5 + k_4\right) + x_2\right) >>> k_1;$$

$$F = Mix\left(\left(x_6 + x_3\right) \oplus y_1\right) <<< x_4.$$

2.1.4. Обчислюється нові значення векторів $k_3$, $k_4$, $y_3$, $y_4$:

$$k_3 = Sbox\left(\left(Sbox\left(x_4 \oplus k_3\right) + x_2\right) \oplus y_3\right);$$

$$k_4 = Sbox\left(Mix\left(x_5 + k_4 + x_3\right) \oplus y_4\right);$$

$$y_3 = Sbox\left(\left(\left(k_3 + y_3\right) <<< x_5\right) \oplus k_1\right);$$

$$y_4 = Mix\left(Sbox\left(\left(\left(k_4 + y_4\right) >>> x_6\right) \oplus k_2\right)\right).$$

**2.2.** За допомогою конкатенації векторів $y_i$ обраховується вихідна послідовності $M_q$: $M_q = \left(y_1 \mid y_2 \mid y_3 \mid y_4\right)$.

У зазначених вище формулах, символи $\oplus$ та $+$ відповідають операціям покоординатного додавання за модулем 3 та алгебраїчну операцію додавання за модулем $3^l$ відповідно. Під операцією $X <<< Y$ розуміємо операцію циклічного зсув вліво числа $X$ на $Y$ разів, а під $X >>> Y$ − циклічного зсуву вправо числа $X$ на $Y$ разів. Під операцією $Sbox(X)$ розуміємо операцію в якій $X$ розбивається на $d$ частин довжиною $s$ тритів, над кожною з яких виконується підстановка на множині $V_s$: $Sbox(X) = \left(S(X_1),...,S(X_d)\right)$, де $X = \left(X_1,...,X_d\right)$, $X \in V_l$, $X_i \in V_s$, $i \in \overline{1,d}$, а $S$ − підстановка на зазначеній множині. $Mix\left(X\right)$ відповідає операції у якій виконується лінійне розсіювання тритів вектора $X$ (у якості $Mix\left(X\right)$ можуть бути використані МДР-коди).

**Алгоритм TriGen.** На основі запропоновано метода генерування тритових ПВП $\xi$ розроблено алгоритм TriGen (псевдокод алгоритму див. на рис. 3). У алгоритмі TriGen використовуються такі параметри $d = 4$, $s = 6$, $l = d \cdot s = 24$, $p = 14 \cdot l = 336$, $n = 4 \cdot l = 96$, $e = p - n = 10 \cdot l = 240$, $m = b \cdot n = 96 \cdot b$, $r = 4$, $b$ − натуральне число.

В операції $Sbox(X)$ виконується нелінійна заміна кожних шести тритів числа $X$ на відповідне їм значення таблиці підстановок. Використовується лише одна таблиця підстановок, що побудована за допомогою обрахунку зворотного елементу поля $\left(X\right)^{-1} \in GF(3^6)$ з подальшим виконанням афінного перетворення над полем $GF(3)$: $S(X) = M \cdot \left(X\right)^{-1} + V$, де $X, V \in GF(3^6)$, а $M$ − квадратна не вироджена матриця над полем $GF(3)$ розміром $6 \times 6$. Кінцеве поле GF($3^6$) фіксується кільцем многочленів з операціями за модулем незвідного многочлена $m(x) = x^6 + x + 2$.

**TriGen**

Input: вектор ініціалізації $VI$, секретний ключ $K$, $VI \in V_{240}$, $K \in V_{96}$, параметр $b$.

Output: вихідна послідовність $M = \left(M_1,...,M_b\right)$, $M \in V_{96b}$, $M_q \in V_{96}$, $q \in \overline{1,b}$.

1. $x_i = VI_i$, $y_j = VI_{6+j}$, $k_j = K_j$, $i \in \overline{1,6}$, $j \in \overline{1,4}$.
2. *For* $q = 1, q \le b, q{+}{+}$ *do*

2.1. *For* $j = 0, j < 4, j{+}{+}$ *do*

2.1.1. $x_1 = \left(Sbox\left(x_1 + k_1\right) \oplus x_4\right) <<< k_4$;

2.1.2. $x_2 = \left(Sbox\left(x_2 + k_2\right) + x_5\right) >>> k_3$;

2.1.3. $x_3 = Mix\left(\left(x_3 + x_6\right) \oplus y_3\right) <<< x_1$;

2.1.4. $k_1 = Sbox\left(\left(Sbox\left(x_1 \oplus k_1\right) + x_5\right) \oplus y_1\right)$;

2.1.5. $k_2 = Sbox\left(Mix\left(x_2 + k_2 + x_6\right) \oplus y_2\right)$;

2.1.6. $y_1 = Sbox\left(\left(\left(k_1 + y_1\right) <<< x_2\right) \oplus k_3\right)$;

2.1.7. $y_2 = Mix\left(Sbox\left(\left(\left(k_2 + y_2\right) >>> x_3\right) \oplus k_4\right)\right)$;

2.1.8. $x_4 = \left(Sbox\left(x_4 + k_3\right) \oplus x_1\right) <<< k_2$;

2.1.9. $x_5 = \left(Sbox\left(x_5 + k_4\right) + x_2\right) >>> k_1$;

2.1.10. $F = Mix\left(\left(x_6 + x_3\right) \oplus y_1\right) <<< x_4$;

2.1.11. $k_3 = Sbox\left(\left(Sbox\left(x_4 \oplus k_3\right) + x_2\right) \oplus y_3\right)$;

2.1.12. $k_4 = Sbox\left(Mix\left(x_5 + k_4 + x_3\right) \oplus y_4\right)$;

2.1.13. $y_3 = Sbox\left(\left(\left(k_3 + y_3\right) <<< x_5\right) \oplus k_1\right)$;

2.1.14. $y_4 = Mix\left(Sbox\left(\left(\left(k_4 + y_4\right) >>> x_6\right) \oplus k_2\right)\right)$.

2.2. $M_q = \left(y_1 \mid y_2 \mid y_3 \mid y_4\right)$

Рис. 3. Псевдокод алгоритму TriGen

Для побудови запропонованої таблиці замін були обрані такі значення матриці $M$ та вектора $V$:

$$M = \begin{pmatrix} 1 & 2 & 0 & 1 & 1 & 2 \\ 2 & 1 & 2 & 0 & 1 & 1 \\ 1 & 2 & 1 & 2 & 0 & 1 \\ 1 & 0 & 2 & 1 & 2 & 0 \\ 0 & 1 & 0 & 2 & 1 & 2 \\ 2 & 0 & 1 & 1 & 2 & 1 \end{pmatrix}, V = \begin{pmatrix} 0 \\ 2 \\ 2 \\ 1 \\ 0 \\ 2 \end{pmatrix}.$$

В операції $Mix\left(X\right)$ квадратна не вироджена матриця $M'$ над полем $GF(3)$ розміром $24 \times 24$ тритів множиться на $X$ (представлений у вигляді вектора-стовпчика) над полем $GF(3)$. Матриця $M'$ побудована на основі масиву $U$ таким чином:

$M'[i][j]=U[(j+24-i) \bmod 24]$, де $i, j = \overline{0,...,23}$, а масив $U$ приймає значення: $U$ = { 1, 0, 2, 2, 1, 0, 2, 0, 1, 1, 1, 2, 0, 1, 2, 1, 0, 2, 0, 0, 1, 2, 0, 2 }.

**Висновки.** Таким чином, у роботі проведено аналіз існуючих методів генерування ПВП, що вказав на неможливість їх застосування для тритових систем. З огляду на це, було розроблено метод генерування тритових ПВП, який може використовуватися для потреб КК та в інших галузях, де використовуються трійкові системи числення. Проте відкритим залишається питання оцінювання якості ПВП (тобто оцінювання рівня випадковості), так як для бінарних систем існує ціла низка таких методів (зокрема NIST STS, DIEHARD, тести Кнута тощо), але для тритових систем вони не можуть застосовуватися (в оригінальному вигляді). Отже, подальші дослідження будуть орієнтовані на розробку методу оцінювання якості трійкових ПВП, що дозволить оцінити доцільність використання запропонованого у цій статті методу для криптографічних застосувань.

**Література**

[1] Choi, Charles (May 16, 2013). Google and NASA Launch Quantum Computing AI Lab. MIT Technology Review [Online] Available: http://www.technologyreview.com/news/514846/google-and-nasa-launch-quantum-computing-ai-lab.

[2] Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. – М.: Мир, 2006. – 824 с.

[3] Bennett C., Brassard G., Quantum cryptography: Public key distribution and coin tossing, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (Institute of Electrical and Electronics Engineers, New York, 1984), pp. 175-179.

[4] Korchenko O., Vasiliu E., Gnatyuk S. Modern quantum technologies of information security, Aviation. Vilnius: Technika, Vol. 14, No. 2, p. 58-69 2010. [Online]. Available: arXiv: 1005.5553v2 [Accessed Aug. 5, 2015].

[5] Килин С.Я. Квантовая криптография: идеи и практика / Килин С.Я., Хорошко Д.Б., Низовцев А.П. – Минск: ИД «Белорусская наука», 2008. – 392 с.

[6] Gisin N. Quantum cryptography / N. Gisin, G. Ribordy, W.Tittel, H. Zbinden // Rewiews of Modern Physics – 2002. – V. 74, №1. – P. 145-195.

[7] Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк // Захист інформації. – 2010, № 1. – С. 77–89.

[8] Scarani V. The security of practical quantum key distribution / V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf et al. // Review of Modern Physics. – 2009. – V. 81, issue 3. – P. 1301–1350.

[9] Василиу Е.В. Проблемы развития и перспективы использования квантово-криптографических систем / Е.В. Василиу, П.П. Воробиенко // Наукові праці ОНАЗ ім. О.С. Попова. – 2006. – № 1. – С. 3–17.

[10] Korchenko O., Vorobiyenko P., Lutskiy M., Vasiliu Ye., Gnatyuk S. Quantum Secure Telecommunication Systems, Telecommunications Networks – Current Status and Future Trends, 2012, Ed. Dr. Jesus Ortiz, InTech, Available from: http://www.intechopen.com/books/telecommunications-networks-current-status-and-future-trends/quantum-secure-telecommunication-systems.

[11] Корченко О.Г. Квантові технології конфіденційного зв'язку / О.Г. Корченко, С.О. Гнатюк, В.М. Кінзерявий // Защита информации: Сб. науч. трудов. – К.: НАУ, 2010. – Вип. 1. – С. 179–184.

[12] Корченко О.Г. Система квантового розподілу ключів на основі одиничної поляризації фотонів // О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк, В.М. Кінзерявий // Вісник інженерної академії України. – 2009. – № 2. – С. 114–117.

[13] Слепов Н. Квантовая криптография: передача квантового ключа. Проблемы и решения / Н. Слепов // Электроника: наука, технология, бизнес. – 2006. – № 2. – С. 54–61.

[14] Алексеев Д.А. Практическая реальность квантово-криптографических систем распределения ключей / Д.А. Алексеев, А.В. Корнейко // Захист інформації. – 2007. – № 1. – С. 72–76.

[15] Waks E. Security of Quantum Key Distribution with Entangled Photons Against Individual Attacks / E. Waks, A. Zeevi, Y. Yamamoto // Physical Review A. – 2002. – V. 65, issue 5. – 052310.

[16] Applied Quantum Cryptography / Kollmitzer C., Pivk M. (eds.). – Springer-Verlag, Berlin, Heidelberg, 2010. – 227 p.

[17] Василиу Е.В. Анализ атаки на пинг – понг протокол с триплетами Гринбергера – Хорна – Цайлингера / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова. – 2008. – № 1. – С. 15–24.

[18] Василиу Е.В. Анализ атаки пассивного перехвата на пинг – понг протокол с полностью перепутанными парами кутритов / Е.В. Василиу, Р.С. Мамедов // Восточноевропейский журнал передовых технологий. – 2009. – № 4/2 (40). – С. 4–11.

[19] Василиу Е.В. Анализ атаки двух злоумышленников на протокол квантовой прямой безопасной связи / Е.В. Василиу, С.В. Николаенко // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2013. – С.324–330.

[20] ID Quantique SA, Cerberis Encryption Solution: Layer 2 Encryption with Quantum Key Distribution [Online] Available: http://www.idquantique.com/products/cerberis.htm [Accessed Aug. 5, 2015].

[21] Toshiba Research Europe Ltd. «Quantum Key Distribution System» [Online] Available: http://www.toshiba-europe.com/research/crl/qig/quantum keyserver.html [Accessed Aug. 5, 2015].

[22] MagiQ Technologies, Inc. QPN-8505 Security Gateway: Data Sheet [Online] Available: http://www.magiqtech.com/MagiQ/Products_files/8505_Data_Sheet.pdf [Accessed Aug. 5, 2015].

[23] Bovino F.A., Giardina M. Practical Quantum Cryptography: The Q-KeyMaker [Online] Available:http://arxiv.org/ftp/arxiv/papers/1104/1104.2475.pdf [Accessed Aug. 5, 2015].

[24] Gnatyuk S., Riabyi M., Zhmurko T. Contemporary Commercial Quantum Information Security Systems Computer Science & Engineering: 6th International Conference of Young Scientists CSE-2013, November 21-23: Proceedings. – Lviv, 2013. – P. 74-77.

[25] Василиу Е.В. Безопасные системы передачи конфиденциальной информации на основе протоколов квантовой криптографии / Е.В. Василиу, В.Я. Мильчевич, С.В. Николаенко, А.В. Мильчевич // Монография. – Краснодар: Кубанский институт информзащиты, 2013.– 168 с.

[26] Василіу Є.В. Оцінки обчислювальної складності способу підсилення безпеки пінг–понг протоколу з переплутаними станами кубітів та кутритів / Є.В. Василіу, Р.С. Мамедов // Наукові праці ОНАЗ ім. О.С. Попова. – 2009. – № 2. – С. 14–25.

[27] Василіу Є. Підсилення безпеки пінг-понг протоколу квантового безпечного зв'язку з n-кубітними ГХЦ – станами / Є. Василіу, С. Ніколаєнко // Комп'ютерні науки та інженерія: Матеріали III Міжнародної конференції молодих вчених CSE–2009. – Львів: Видавництво Національного університету «Львівська політехніка». – 2009. – С. 299–301.

[28] Патент України на корисну модель № 59732. Спосіб підсилення безпеки пінг-понг протоколу квантового безпечного зв'язку / П.П. Воробієнко, Є.В. Василіу, С.В. Ніколаєнко; заявник і патентовласник Одеська національна академія зв'язку ім. О.С. Попова; заявлено 19.11.2010; опубліковано 25.05.2011, бюл. № 10.

[29] Vasiliu Ye. Security amplification of the ping-pong protocol with many-qubit Greenberger-Horne-Zeilinger states / Ye. Vasiliu, S. Gnatyuk, S. Nikolayenko, T. Zhmurko// Безпека інформації. – 2012. – № 2. С. 84–88.

[30] Николаенко С.В. Усиление безопасности методом гаммирования протокола квантовой прямой безопасной связи / С.В. Николаенко // Applied radio electronics. Special issue devoted to problems of ensuring information security. – 2013.– V. 12.– № 2. – P. 347–350.

[31] Ніколаєнко С.В. Гамування як метод підсилення стійкості пінг-понг протоколу з парами переплутаних кубітів / С.В. Ніколаєнко // Інформаційна безпека, СНУ ім. В. Даля. – 2013– № 1(9). – С. 21–28.

[32] Ніколаєнко С.В. Підсилення стійкості пінг-понг протоколу з парою переплутаних кубітів методом гамування / С.В. Ніколаєнко., О.О. Буз // XX семинар «Моделирование в прикладных научных исследованиях». – Одесса, Одесский национальный политехнический университет. – 2012. – С. 18–20.].

[33] Кінзерявий В.М. Новий метод підсилення секретності пінг-понг протоколу з парами переплутаних кутритів / В.М. Кінзерявий, Є.В. Василіу, С.О. Гнатюк, Т.О. Жмурко// Захист інформації. – 2012, №2 (55). – С. 5–13.

[34] Gnatyuk S., Zhmurko T., Falat P. Efficiency Increasing Metod for Quantum Secure Direct Communication Protocols - The 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 24-26 September 2015, Warsaw, Poland, p. 125-130.

[35] Porat D.I. Three valued digital system, Proc. IEEE Vol. 116 , No. 6, pp.947-955, June 1969.

[36] The ternary calculating machine of Thomas Fowler http://www.mortati.com/glusker/fowler/index.htm.

[37] Брусенцов Н. П. Вычислительная машина "Сетунь" Московского государственного университета. "Новые разработки в области вычислительной математики и вычислительной техники". Материалы научно-технической конференции. Киев, 1960, стр. 226-234.

[38] Брусенцов Н.П., Маслов С.П., Розин В.П., Тишулина А.М. Малая цифровая вычислительная машина «Сетунь», Изд-во МГУ Москва, 1962, 140 с.

[39] Ternary Computing Testbed: 3-Trit Computer Architecture Jeff Connelly, Chirag Patel, Antonio Chavez 193 p.

[40] Макарычев А. Битва за скорость: троичная логика против двоичной https://www.societyforscience.org/.

[41] Горбенко І.Д. Обґрунтування вимог до генераторів випадкових бітів згідно ISO/IEC 18031 / І.Д. Горбенко, Н.В. Шапочка, О.О. Козулін // Радіоелектронні і комп'ютерні системи. – 2009. – № 6 (40). – С. 94-97.

[42] Назаров Є.О. Генератори псевдо-випадкових послідовностей для криптографічних систем / Є.О. Назаров, А.В. Чернишова, Н.Є. Губенко // Збірник наукових праць міжнародної науково-технічної конференції «Інформатика і комп'ютерні технології – 2012», Донецький національний технічний університет, с. 139-144.

[43] Гарасимчук О.І., Максимович В.М. Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості / Захист інформації. – №3. – 2003. – С. 29-36.

[44] Євсеєв С.П., Корольов Р.В., Краснянська М.В. Аналіз сучасних методів формування псевдо-випадкових послідовностей / Восточно-Европейский журнал передовых технологий. – № 3/4 (45). – 2010. – С. 11-15.

**УДК 003.26:004.056.55:621.39 (045)**

***Гнатюк С.А., Жмурко Т.А., Кинзерявый В.Н., Сейлова Н.А. Метод генерирования тритовых псевдослучайных последовательностей для систем квантовой криптографии***

***Аннотация.*** *Стремительное развитие современных вычислительных технологий ставит под угрозу конфиденциальность информации, которая обеспечивается, как правило, традиционными криптографическими средствами и заставляет исследователей искать альтернативные методы защиты. Учитывая современные тенденции развития, одной из таких альтернатив может стать квантовая криптография, которая в отличие от традиционной*

*(которая обычно базируется на невозможности решения определенного класса математических задач за некоторый промежуток времени) использует специфические уникальные свойства квантовых частиц и основывается на нерушимости законов квантовой физики. Известно, что некоторые протоколы квантовой криптографии позволяют достичь теоретико-информационной устойчивости – это в основном протоколы распределения ключей. Другой класс протоколов квантовой криптографии - это протоколы прямой безопасной связи, большинство из которых имеют асимптотической устойчивости. Несмотря на это, был предложен ряд методов повышения устойчивости таких протоколов. Один из таких методов позволяет повысить асимптотической устойчивости протоколов квантовой прямой безопасной связи с парами перепутанных (коррелированных) кутритов, тем не менее, применение этого метода требует генерирования троичных (тритовых) псевдослучайных последовательностей. Именно на разработку такого генератора (метода генерирования) и ориентирована эта статья. Таким образом, в работе предложен метод генерирования тритовых псевдослучайных последовательностей, основанных на необратимой функции и ряде преобразований над полем GF (3). Также на основе метода разработан соответствующий алгоритм, который отражен в виде псевдокода. Дальнейшие исследования будут посвящены разработке метода оценки качества сгенерированных тритовых псевдослучайных последовательностей, так как практически все существующие методы ориентированы на бинарные последовательности.*

***Ключевые слова:*** *квантовая криптография, трит, кутрит, псевдослучайная последовательность, генератор псевдослучайных последовательностей, квантовая прямая безопасная связь, пинг-понг протокол.*

***Gnatyuk S., Zhmurko T., Kinzeryavyy V., Seilova N. Method of trit pseudorandom sequences generating for quantum cryptography systems***

***Abstract.*** *The rapid development of modern computing technology threatens the confidentiality of information that is provided, usually, by traditional cryptographic means and forces researchers to look for alternative methods of security. Considering the development tendencies one of these alternatives may be quantum cryptography that unlike traditional (which is mostly based on the impossibility of solving a certain class of mathematical problems by certain period of time) uses specific unique properties of quantum particles, based on the inviolability of the quantum physics laws. It is known that some quantum cryptography protocols allowing to achieve information-theoretic stability – a key distribution protocols mostly. Another class of quantum cryptography protocols - secure direct communication protocols, most of which have asymptotic stability. Therefore, it was suggested a number of methods to increase the stability of such protocols. One of these methods will increase the asymptotic stability of quantum secure direct connection protocols with entangled pairs (correlated) of qutrit, but this method requires the generation of ternary (trit) pseudorandom sequences. In the work proposed generating pseudorandom trit sequences method based on the number of irreversible functions and transformation over the field GF (3). Also at the basis of a method developed appropriate algorithm that reflected as pseudo code. Further research will focus on the development of a quality evaluation of trit generated pseudorandom sequences method, as virtually all existing methods focused on binary sequence.*

***Key words:*** *quantum cryptography, trit, qutrit, pseudorandom sequence, pseudorandom sequence generator, quantum secure direct communication, ping-pong protocol.*

Отримано *26 травня 2015 року*, затверджено редколегією *10 червня 2015 року*