CRYPTOLOGY

УДК 004.056.5

СЕРГІЙ ГНАТЮК,
ТЕТЯНА ЖМУРКО,
ВАСИЛЬ КІНЗЕРЯВИЙ,
НУРГУЛЬ СЄЙЛОВА

МЕТОД ОЦІНЮВАННЯ ЯКОСТІ ТРИТОВИХ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДЛЯ КРИПТОГРАФІЧНИХ ЗАСТОСУВАНЬ

Розробки в галузі квантової криптографії ведуться практично усіма провідними західними телекомунікаційними компаніями та дослідницькими центрами. Швидкі темпи розвитку призвели до значного розширення спектру протоколів. З точки зору інформаційної місткості найбільш ефективними для протоколів квантової криптографії є тритові системи. Однак, постає проблема розробки генераторів тритових псевдовипадкових послідовностей та оцінювання їх якості, оскільки випадкові і псевдовипадкові послідовності, породжувані різними генераторами для криптографічних застосувань, підлягають обов'язковому тестуванню ймовірнісно-статистичними методами. Проте, переважна більшість відомих методик орієнтована на тестування генераторів псевдовипадкових бінарних послідовностей, отож, підтвердити псевдовипадковість згенерованих тритових послідовностей з їх допомогою практично неможливо, а програмних комплексів та методик перевірки випадковості таких послідовностей не існує, отож і виникає завдання розробки методу оцінювання якості трійкових псевдовипадкових послідовностей, що дозволить оцінити доцільність їх використання для криптографічних застосувань. Саме такий метод, що ґрунтується на підході, використаному у методиці NIST STS, розроблено у цій статті.

Ключові слова: квантова криптографія, трит, кутрит, псевдовипадкова послідовність, генератор псевдовипадкових послідовностей, оцінка якості.

Квантова криптографія (КК) [1] за останні два десятиріччя пройшла шлях від теоретичних розробок до впровадження у реальних інформаційно-комунікаційних системах. На відміну від традиційної криптографії, яка здебільшого базується на неможливості розв'язання певного класу математичних задач за деякий проміжок часу, КК ґрунтується на непорушності законів квантової фізики і використовує специфічні унікальні властивості квантових частинок [2]. Деякі протоколи КК дозволяють досягнути теоретико-інформаційної стійкості (здебільшого протоколи розподілу ключів), проте існують інші класи КК, наприклад, протоколи квантового прямого безпечного зв'язку (КПБЗ), більшість з яких мають асимптотичну стійкість. Дослідниками запропоновано низку методів підвищення стійкості таких протоколів, наприклад, в одному з таких методів [3, 4] використовується зворотне хешування із застосуванням оборотних трійкових матриць. Зазначений метод дозволяє підвищити рівень стійкості та швидкість роботи протоколів КПБЗ, проте виникає проблема генерування трійкових (тритових) матриць з високим рівнем випадковості. У роботі [5] проведено аналіз існуючих методів генерування (генераторів) псевдовипадкових послідовностей (ПВП), що вказав на неможливість їх застосування для тритових систем, які, з точки зору інформаційної місткості, є найбільш ефективними. Окрім того у роботі [5] було розроблено метод генерування тритових ПВП, який може використовуватися для потреб КК та в інших галузях, де використовуються трійкові системи числення. Проте відкритим залишилось питання оцінювання якості тритових ПВП (тобто оцінювання їх рівня

випадковості), так як для бінарних систем існує ціла низка таких методів (зокрема NIST STS [6], DIEHARD [7], тести Кнута [8] тощо), але для тритових систем вони не можуть застосовуватися в оригінальному вигляді. Отже, розробка методу оцінювання якості трійкових ПВП, що дозволить оцінити доцільність їх використання для криптографічних застосувань, є актуальною науково-практичною задачею, що має теоретичне і практичне значення. З огляду на це, **метою статті** є розробка методу оцінювання якості тритових ПВП для криптографічних застосувань (на базі кращих методик і рекомендацій для бінарних послідовностей та генераторів).

Як показав проведений аналіз [5-8], сьогодні найбільш дослідженою та популярною методикою оцінювання ПВП для криптографічних застосувань є методика NIST STS [6], яку і було взято за основу для розробки тритових тестів.

Запропонований метод включає у себе такі етапи перевірки тритових ПВП:

1. Перевірка частотним тритовим тестом (Freqeuncy monotrit test).
2. Дослідження частотним блоковим тестом (Frequency block trit test).
3. Перевірка тритовим тестом серій (Trit runs test).
4. Дослідження тритовим тестом найдовших серій (Test for the longest run in a block).
5. Перевірка тритовим тестом на співпадіння з шаблоном без перекриття (Trit non-overlapping template matching test).
6. Дослідження тритовим тестом шаблонів із перекриттям (Trit overlapping template matching test).

На кожному з шести зазначених етапів послідовність перевіряється таким чином:

1. Спочатку кожна вхідна трійкова послідовність A_{012} розбивається на 3 підпослідовності:
   a) A_{01} (послідовність A_{012} із видаленими 2),
   b) A_{02} (послідовність A_{012} із видаленими 1),
   c) A_{12} (послідовність A_{012} із видаленими 0).

2. Кожна із отриманих послідовностей окремо перевіряється тритовими тестами, аналогічно тестам NIST STS. У результаті перевірки кожним тестом отримуємо 3 значення $P-value$: $P-value_{01}$, $P-value_{02}$, $P-value_{12}$. Як і в тестах NIST STS $P-value_{XY}$ (під XY тут і надалі розуміємо одну із трьох можливих комбінацій послідовностей: «01», «02» та «12») відповідатиме ймовірності того, що досліджувана послідовність A_{XY} не гірша, ніж істино-випадкова, тобто якщо $P-value_{XY}=1$, то згенерована послідовність є ідеально випадковою, а якщо $P-value_{XY}=0$, то послідовність є повністю передбачуваною.

3. Визначені значення $P-value_{01}$, $P-value_{02}$, $P-value_{12}$ кожного тесту порівнюється із α (помилкою першого роду – ймовірність того, що випадкова послідовність є забракованою). Якщо $P-value_{XY}\geq\alpha$, то послідовність A_{XY} є випадковою з рівнем довіри 99%, у іншому випадку $P-value_{XY}\leq\alpha$ – послідовність A_{XY} відбраковується з рівнем довіри 99%. Будемо вважати кожен тест пройденим послідовністю A_{012}, якщо усі отримані значення $P-value_{01}$, $P-value_{02}$, $P-value_{12}$ будуть випадковими з рівнем довіри 99%, тобто виконуватимуться нерівності $P-value_{01}\geq\alpha$, $P-value_{02}\geq\alpha$ та $P-value_{12}\geq\alpha$.

Якщо досліджувана тритова послідовність пройде усі зазначені тести, то вважатимемо її псевдовипадковою. До того ж, у випадку не проходження хоча б одного із етапів, перевірка завершується і послідовність вважається передбачуваною і непридатною для криптографічних застосувань. Перейдемо до опису базових етапів реалізації методу.

I. Частотний тритовий тест

Мета тесту − визначити, чи буде кількість нулів, одиниць та двійок у трійковій послідовності A_{012} приблизно така ж як у дійсно випадковій послідовності. Тест окремо

оцінює наскільки близька пропорція нулів послідовності A_{01}, пропорція одиниць послідовності A_{12} та пропорція двійок послідовності A_{02} до $1/2$.

Позначення: n_{012} – довжина вхідної послідовності тритів $A_{012}=\{0,1,2\}^{n_{012}}$, n_{01} – довжина послідовності $A_{01}=\{0,1\}^{n_{01}}$, n_{02} – довжина послідовності $A_{02}=\{0,2\}^{n_{02}}$ та n_{12} – довжина послідовності $A_{12}=\{1,2\}^{n_{12}}$.

Статистика тесту та граничний розподіл. $Sobs_{XY}$ − абсолютна величина суми M_i по всій довжині підпослідовності A_{XY} ($A_{XY}=\left(a_1,a_2,...,a_{n_{XY}}\right), a_i=\{X,Y\}, i=\overline{1,n_{XY}}$), що поділена на корінь квадратний з довжини підпослідовності n_{XY}: $Sobs_{XY}=\dfrac{\left|S_{n_{XY}}\right|}{\sqrt{n_{XY}}}$, де $S_{n_{XY}}=\sum_{i=1}^{n_{XY}}M_i$, $M_i=-1$ – якщо $a_i=X$ та $M_i=1$ – якщо $a_i=Y$. Граничний розподіл тестової статистики при великих n_{XY} – напівнормальний. Якщо послідовність A_{XY} випадкова, тоді «+1» та «−1» будуть компенсувати один одного та статистика тесту буде мати значення близькі до нуля. Якщо в послідовності A_{XY} кількість X і Y значно відрізняються, тоді значення статистики тесту будуть значно відхилятися від нуля.

Опис тесту. Для послідовності $A_{XY}=\left(a_1,a_2,...,a_n\right)$, $a_i=\{X,Y\}$, $i=\overline{1,n_{XY}}$ виконуємо перетворення до ±1: всі X замінюємо на -1, а всі Y замінюємо на $+1$, тобто будуємо нову послідовність $M=M_1,...M_n$, $M_i=\{-1,+1\}$, $i=\overline{1,n_{XY}}$. Підраховуємо величину $S_{n_{XY}}=M_1+M_2+...+M_n$. Далі підраховуємо значення статистики тесту $Sobs_{XY}=\dfrac{\left|S_{n_{XY}}\right|}{\sqrt{n_{XY}}}$. Після чого підраховуємо $P-value_{XY}=erfc\left(\dfrac{Sobs_{XY}}{\sqrt{2}}\right)$, де $erfc$ − комплементарна функція похибки, що визначається таким чином: $erfc(z)=\dfrac{2}{\sqrt{\pi}}\cdot\int_z^{+\infty}e^{-u^2}du$.

Приклад. Якщо $A_{012}=012120001221110112110112 0$, тоді $A_{01}=011000111101111011 0$, $n_{01}=19$, $A_{02}=0220002202020$, $n_{02}=13$, $A_{12}=121212211111211112$, $n_{12}=18$.

Тоді $S_{n_{01}}=5$, $S_{n_{02}}=-1$ і $S_{n_{12}}=6$. Звідки $Sobs_{01}=\dfrac{|5|}{\sqrt{19}}=1.1470$, $Sobs_{02}=\dfrac{|-1|}{\sqrt{13}}=0.2773$, $Sobs_{12}=\dfrac{|6|}{\sqrt{18}}=1.4142$.

Тоді $P-value_{01}=erfc\left(\dfrac{1.1470}{\sqrt{2}}\right)=0.2513$, $P-value_{02}=erfc\left(\dfrac{0.2773}{\sqrt{2}}\right)=0.7815$, $P-value_{12}=erfc\left(\dfrac{1.4142}{\sqrt{2}}\right)=0.1573$.

Вирішальне правило (для рівня значущості 1%). Якщо підраховане значення $P-value_{XY}$ менше за 0.01, тоді робимо висновок, що послідовність A_{XY} не випадкова, в іншому випадку робимо висновок, що послідовність A_{XY} випадкова.

Висновки та інтерпретація результатів тесту. Так як значення $P-value_{01}$, $P-value_{02}$, $P-value_{12}$, що отримані у прикладі ≥ 0.01, робимо висновок, що послідовності A_{01}, A_{02} і A_{12} випадкові. Тому вважаємо, що послідовність A_{012} теж випадкова і пройшла цей тест.

Рекомендації щодо вхідних розмірам. Кожна послідовність A_{012}, що тестується, повинна складалася як мінімум зі 150 тритів ($n_{012} \geq 150$).

II. Частотний блоковий тритовий тест

Мета тесту. Цей тест спрямовано на визначення пропорцій X і Y послідовності A_{XY} у блоках довжиною M. Мета тесту – визначити, чи буде кількість одиниць послідовності A_{01} нулів послідовності A_{02} та двійок послідовності A_{12} у середині кожного блоку приблизно дорівнювати $M/2$, як це очікується від випадкової послідовності.

Позначення: M – довжина кожного блоку; n_{012} – довжина вхідної послідовності тритів $A_{012} = \{0,1,2\}^{n_{012}}$, n_{01} – довжина послідовності $A_{01} = \{0,1\}^{n_{01}}$, n_{02} – довжина послідовності $A_{02} = \{0,2\}^{n_{02}}$ та n_{12} – довжина послідовності $A_{12} = \{1,2\}^{n_{12}}$.

Статистика тесту та граничний розподіл. $\chi^2(\text{obs})_{XY}$ – міра того, як добре пропорція X і Y послідовності A_{XY} в межах даних блоків довжиною M відповідає пропорції, що очікується за припущенням випадковості послідовності (1/2). Граничний розподіл такої статистики є χ^2 -розподіл.

Опис тесту. Ділимо вхідну підпослідовність $A_{XY} = \left(a_1, a_2, ..., a_{n_{XY}}\right)$, $a_i = \{X, Y\}$, $i = \overline{1, n_{XY}}$ на $N_{XY} = \left\lfloor \frac{n_{XY}}{M} \right\rfloor$ блоків, що не перетинаються. Відкидаємо останні символи послідовності, що не утворюють повного блоку довжини M (якщо такі є). Визначаємо пропорцію $\pi_{j,XY}$ для кожного з блоків $j = 1,2...N_{XY}$ за формулою: $\pi_{j,XY} = \frac{\sum_{l=1}^{M} \varepsilon_{(j-1)\cdot \mathrm{M}+l}}{M}$, де $\varepsilon_i = 0$ – якщо $a_i = X$, $\varepsilon_i = 1$ – якщо $a_i = Y$, $i = \overline{1, n_{XY}}$.

Підраховуємо значення статистики $\chi^2(\text{obs})_{XY} = 4 \cdot \mathrm{M} \cdot \sum_{j=1}^{N_{XY}} \left(\pi_{j,XY} - \frac{1}{2} \right)^2$ та вираховуємо значення $P - value_{XY} = igamc\left(\frac{N_{XY}}{2}, \frac{\chi^2(\text{obs})_{XY}}{2} \right)$, де $igams(.)$ – неповна гамма функція, що визначається таким чином $igamc(a,b) = \frac{1}{\Gamma(\mathrm{a})} \cdot \int_b^{+\infty} e^{-u} \cdot u^{a-1} du$.

Приклад. Якщо $A_{012} = 012120001221110112110120$, тоді $A_{01} = 0110001111011110110$, $n_{01} = 19$, $A_{02} = 0220002202020$, $n_{02} = 13$, $A_{12} = 121212211111211112$, $n_{12} = 18$. Нехай $M = 4$.

Тоді із послідовності A_{01} сформуються 4 блоки ($N_{01} = \left\lfloor \frac{19}{4} \right\rfloor = 4$): 0110 0011 1101 1110, із послідовності A_{02} сформуються 3 блоки ($N_{02} = \left\lfloor \frac{13}{4} \right\rfloor = 3$): 0220 0022 0202, і відповідно з A_{12} – 4 блоки ($N_{12} = \left\lfloor \frac{18}{4} \right\rfloor = 4$): 1212 1221 1111 2111.

Для кожної послідовності A_{XY} визначаємо пропорцію $\pi_{j.XY}$ для кожного з блоків $j = 1,2...N_{XY}$. Для A_{01}: $\pi_{1,01} = 1/2$, $\pi_{2,01} = 1/2$, $\pi_{3,01} = 3/4$, $\pi_{4,01} = 3/4$; для A_{02}: $\pi_{1,02} = 1/2$, $\pi_{2,02} = 1/2$, $\pi_{3,02} = 1/2$; для A_{12}: $\pi_{1,12} = 1/2$, $\pi_{2,12} = 1/2$, $\pi_{3,12} = 0$, $\pi_{4,12} = 1/4$.

Тоді $\chi^2(\text{obs})_{01} = 4\cdot 4\cdot \sum_{j=1}^{4}\left(\pi_{j,01}-\frac{1}{2}\right)^2 = 2$, $\chi^2(\text{obs})_{02} = 4\cdot 4\cdot \sum_{j=1}^{3}\left(\pi_{j,02}-\frac{1}{2}\right)^2 = 0$, $\chi^2(\text{obs})_{12} = 4\cdot 4\cdot \sum_{j=1}^{4}\left(\pi_{j,12}-\frac{1}{2}\right)^2 = 5$. Звідки $P-value_{01} = igamc\left(\frac{4}{2},\frac{2}{2}\right) = 0.7358$, $P-value_{02} = igamc\left(\frac{3}{2},\frac{0}{2}\right) = 1$, $P-value_{12} = igamc\left(\frac{4}{2},\frac{5}{2}\right) = 0.2873$.

Вирішальне правило (для рівня значущості 1%). Якщо підраховане значення $P-value_{XY} \geq 0.01$, тоді робимо висновок, що A_{XY} випадкова.

Висновки та інтерпретація результатів тесту. Так як значення $P-value_{01}$, $P-value_{02}$, $P-value_{12}$, що отримані в прикладі ≥ 0.01, робимо висновок, що послідовності A_{01}, A_{02} і A_{12} випадкові. Тому вважаємо, що послідовність A_{012} теж є випадковою і пройшла цей тест.

Рекомендації щодо вхідних розмірів. Кожна послідовність A_{012}, що тестується, повинна складалася як мінімум зі 150 тритів ($n_{012} \geq 150$). Зауважимо, що $M \geq 20$, $M \geq 0.01\cdot n_{012}$.

III. Тритовий тест серій

Мета тесту. Тест спрямований на загальну кількість серій в усій послідовності A_{XY}. Під серією розуміється неперервна послідовність однакових символів X та Y. Мета тесту – визначити, чи буде загальна кількість серій з «0» і «1» послідовності A_{01}, кількість серій з «0» і «2» послідовності A_{02} та кількість серій з «1» і «2» послідовності A_{12} такою, яка очікується від випадкової послідовності.

Позначення. n_{012} – довжина вхідної послідовності тритів $A_{012} = \{0,1,2\}^{n_{012}}$, n_{01} – довжина послідовності $A_{01} = \{0,1\}^{n_{01}}$, n_{02} – довжина послідовності $A_{02} = \{0,2\}^{n_{02}}$ та n_{12} – довжина послідовності $A_{12} = \{1,2\}^{n_{12}}$.

Статистика тесту та граничний розподіл. $\mathrm{V}_n(\text{obs})_{XY}$ – загальна кількість серій (тобто загальна кількість серій з X + загальна кількість серій з Y) для усіх n_{XY} символів послідовності A_{XY}. Граничний розподіл такої статистики є χ^2-розподіл.

Опис тесту. Визначаємо пропорцію π_{XY} Y у підпослідовності $A_{XY} = \left(a_1, a_2, ..., a_{n_{XY}}\right)$, $a_i = \{X, Y\}$, $i = \overline{1, n_{XY}}$: $\pi_{XY} = \frac{1}{n_{XY}}\cdot \sum_{i=1}^{n_{XY}} \varepsilon_i$, де $\varepsilon_i = 0$ – якщо $a_i = X$, $\varepsilon_i = 1$ – якщо $a_i = Y$, $i = \overline{1, n_{XY}}$.

Потім перевіряємо нерівність: $\left|\pi_{XY} - 1/2\right| \geq 2/\sqrt{n_{XY}}$ Якщо вона виконується, тоді $P-value_{XY} = 0$ і далі тест можна не виконувати, якщо нерівність не виконується – виконуємо тест далі. Підраховуємо значення статистики тесту для послідовності A_{XY}: $V_{n_{XY}} = \sum_{i=1}^{n_{XY}-1} r(i) + 1$, де $r(i) = 0$ – якщо $a_i = a_{i+1}$, $r(i) = 1$ – якщо $a_i \neq a_{i+1}$, . $i = \overline{1, n_{XY}-1}$.

Розраховуємо три $P-value$ для кожної підпослідовності A_{XY}:

$$P-value_{XY} = erfc\left(\frac{\left|V_{n_{XY}} - 2\cdot n_{XY}\cdot \pi_{XY}\cdot(1-\pi_{XY})\right|}{2\cdot\sqrt{2\cdot n_{XY}}\cdot \pi_{XY}\cdot(1-\pi_{XY})}\right).$$

Приклад. Якщо $A_{012} = 012120001221110112110112 0$, тоді $A_{01} = 0110001111011110110$, $n_{01} = 19$, $A_{02} = 0220002202020$, $n_{02} = 13$, $A_{12} = 121212211111211112$, $n_{12} = 18$.

Тоді $\pi_{01} = \frac{1}{19} \cdot \sum_{i=1}^{19} \varepsilon_i = 0.6315$, $\pi_{02} = \frac{1}{13} \cdot \sum_{i=1}^{13} \varepsilon_i = 0.4615$, $\pi_{12} = \frac{1}{18} \cdot \sum_{i=1}^{18} \varepsilon_i = 0.3333$.

Перевіряємо нерівність $|\pi_{01} - 1/2| \geq 2/\sqrt{n_{01}}$: $|0.6315 - 0.5| = 0.1315 < 2/\sqrt{19} = 0.4588$ – можна виконувати тест далі. Перевіряємо нерівність $|\pi_{02} - 1/2| \geq 2/\sqrt{n_{02}}$: $|0.4615 - 0.5| = 0.0385 < 2/\sqrt{13} = 0.5547$ – можна виконувати тест далі. Перевіряємо нерівність $|\pi_{12} - 1/2| \geq 2/\sqrt{n_{12}}$: $|0.3333 - 0.5| = 0.1667 < 2/\sqrt{18} = 0.4714$ – можна виконувати тест далі.

Підраховуємо значення статистики тесту для послідовностей:

$$V_{n_{01}} = 1+0+1+0+0+1+0+0+0+1+1+0+0+0+1+1+0+1+1 = 9,$$

$$V_{n_{02}} = 1+0+1+0+0+1+0+1+1+1+1+1+1 = 9,$$

$$V_{n_{12}} = 1+1+1+1+1+0+1+0+0+0+0+1+1+0+0+0+1+1 = 10.$$

Розраховуємо три $P-value$:

$$P-value_{01} = erfc\left(\frac{|9 - 2 \cdot 19 \cdot 0.6315 \cdot (1 - 0.6315)|}{2 \cdot \sqrt{2 \cdot 19} \cdot 0.6315 \cdot (1 - 0.6315)}\right) = 0.9379,$$

$$P-value_{02} = erfc\left(\frac{|9 - 2 \cdot 13 \cdot 0.4615 \cdot (1 - 0.4615)|}{2 \cdot \sqrt{2 \cdot 13} \cdot 0.4615 \cdot (1 - 0.4615)}\right) = 0.1566,$$

$$P-value_{12} = erfc\left(\frac{|10 - 2 \cdot 18 \cdot 0.3333 \cdot (1 - 0.3333)|}{2 \cdot \sqrt{2 \cdot 18} \cdot 0.3333 \cdot (1 - 0.3333)}\right) = 0.2888.$$

Вирішальне правило (для рівня значущості 1%). Якщо підраховане значення $P-value_{XY} \geq 0.01$, тоді робимо висновок, що A_{XY} випадкова.

Висновки та інтерпретація результатів тесту. Так як значення $P-value_{01}$, $P-value_{02}$, $P-value_{12}$, що отримані у прикладі ≥ 0.01, робимо висновок, що послідовності A_{01}, A_{02} і A_{12} випадкові. Тому вважаємо, що трійкова послідовність A_{012} теж є випадковою і пройшла цей тест. Зауважимо, що великі значення $V_n(obs)_{XY}$ свідчать про дуже швидкі коливання між X та Y, малі значення $V_n(obs)_{XY}$ свідчать про занадто повільні коливання. Швидкі коливання спостерігаються при великій кількості переходів. Послідовність з повільними коливаннями має менше серій, ніж очікується від випадкової послідовності.

Рекомендації щодо вхідних розмірів. Кожна послідовність A_{012}, що тестується, повинна складалася як мінімум зі 150 тритів ($n_{012} \geq 150$).

Інші етапи методу виконуються аналогічним чином, тобто тритова послідовність оцінюється у три кроки:

- аналізується послідовність «0» та «1», «2» виключаються;
- аналізується послідовність «0» і «2», «1» виключаються;
- аналізується послідовність «1» і «2», «0» виключаються.

Тритова послідовність, яка проходить усі етапи тестування, є псевдовипадковою та придатною до використання у криптографічних застосуваннях. Як уже зазначалось, якщо послідовність не проходить хоча б один з тестів її не можна розглядати як надійну. Таким чином, у цій статті, на базі кращих методик і рекомендацій для бінарних послідовностей та генераторів, розроблено метод оцінювання якості тритових ПВП.

СПИСОК ВИКОРИСТАННОЇ ЛІТЕРАТУРИ

1. Korchenko O. Modern quantum technologies of information security / O. Korchenko, E. Vasiliu, S. Gnatyuk // Aviation. Vilnius: Technika. – 2010. – Vol. 14, No. 2. – P. 58-69.

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

3. 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.

4. Gnatyuk S. Efficiency Increasing Metod for Quantum Secure Direct Communication Protocols / S. Gnatyuk, T. Zhmurko, P. Falat // 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.

5. Гнатюк С. О. Метод генерування тритових псевдовипадкових послідовностей для систем квантової криптографії / С. О. Гнатюк, Т. О. Жмурко , В. М. Кінзерявий, Н. А. Сєйлова // Безпека інформації. – 2015. – № 2 (22). – С. 140-147.

6. NIST STS [Electronic resource]. – Access mode : http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html. – Access data : Oktober 2015. – The title of the screen.

7. Кнут Д. Искусство программирования для ЭВМ. Получисленные алгоритмы / Д. Кнут. – М. : Мир, 1977. – Т. 2.– 700 с.

8. Marsaglia G. DIEHARD Statistical Tests [Electronic resource]. – Access mode : http://stat.fsu.edu/~geo/ diehard.html. – Access data : Oktober 2015. – The title of the screen.

Стаття надійшла до редакції 19 жовтня 2015 року.

REFERENCES

1. Korchenko, O., Vasiliu, E., Gnatyuk, S. (2010), *Modern quantum technologies of information security*, Aviation. Vilnius: Technika, Vol. 14, No. 2, pp. 58-69.

2. Nilsen, M., Chang, I. (2006), *Kvantovye vychisleniia i kvantovaia informatciia* [Quantum computing and quantum information], Mir Publ., Moskow, 824 p.

3. Kinzeryavyy, V., Vasiliu, E., Gnatuyk, S., Zhmurko, T. (2012), *Novyi metod pidsylennia sekretnosti pinh-ponh protokolu z paramy pereplutanykh kutrytiv* [The new method of ping-pong protocol secrecy amplification with pairs of entangled qutrits], Ukrainian scientific journal of information security, №2 (55), pp. 5-13.

4. Gnatyuk, S., Zhmurko, T., Falat, P. (2015), *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, Warsaw, Poland, pp. 125-130.

5. Gnatyuk, S., Zhmurko, T., Kinzeryavyy, V., Seilova, N. (2015), *Metod heneruvannia trytovykh psevdovypadkovykh poslidovnostei dlia system kvantovoi kryptohrafii* [Method of pseudorandom trit sequences generating for quantum cryptography systems], Ukrainian Scientific Journal of Information Security, Vol. 22, Iss. 2, pp. 140-147.

6. NIST STS, available at : http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html (accessed : 26 September 2015).

7. Knuth, D. (1977), *Iskusstvo programmirovaniia dlia EVM Poluchislennye algoritmy* [The Art of Computer Programming. Seminumerical Algorithms. Vol. 2] Mir Publ., Moskow, 700 p.

8. Marsaglia G. DIEHARD StatisticalTests, available at : http://stat.fsu.edu/~geo/diehard.html (accessed : 06 Oktober 2015).

СЕРГЕЙ ГНАТЮК,
ТАТЬЯНА ЖМУРКО,
ВАСИЛИЙ КИНЗЕРЯВЫЙ,
НУРГУЛЬ СЕЙЛОВА

МЕТОД ОЦЕНКИ КАЧЕСТВА ТРИТОВЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ КРИПТОГРАФИЧЕСКИХ ПРИЛОЖЕНИЙ

Разработки в области квантовой криптографии ведутся практически всеми ведущими западными телекоммуникационными компаниями и исследовательскими центрами. Быстрые темпы развития привели к значительному расширению спектра протоколов. С точки зрения информационной емкости наиболее эффективными для протоколов квантовой криптографии является тритовые системы. Однако, возникает проблема разработки генераторов тритовых псевдослучайных последовательностей и оценки их качества, поскольку случайные и псевдослучайные последовательности, порождаемые различными генераторами для криптографических приложений, подлежат обязательному тестированию вероятностно-статистическими методами. Однако, подавляющее большинство известных методик ориентированы на тестирование генераторов псевдослучайных бинарных последовательностей, так что подтвердить псевдослучайность сгенерированных тритовых последовательностей с их помощью практически невозможно, а программных комплексов и методик проверки случайности таких последовательностей не существует, поэтому и возникает задача разработки метода оценки качества тритовых псевдослучайных последовательностей, что позволит оценить целесообразность их использования для криптографических приложений. Именно такой метод, основанный на подходе, использованном в методике NIST STS, разработан в этой статье.

Ключевые слова: квантовая криптография, трит, кутрит, псевдослучайная последовательность, генератор псевдослучайных последовательностей, оценка качества.

SERHII HNATIUK,
TETIANA ZHMURKO,
VASYL KINZERIAVYI,
NURHUL SEILOVA

METHOD FOR QUALITY EVALUATION OF TRIT PSEUDORANDOM SEQUENCE TO CRYPTOGRAPHIC APPLICATIONS

Developments in quantum cryptography are carried by almost all major western telecommunication companies and research centers. Rapid development led to a significant expansion of the protocols range. From viewpoint of information capacity the most effective protocols for quantum cryptography system is trit systems. However, there is a problem of developing trit pseudorandom sequences generators and assessing their quality. This is because random and pseudo-random sequence generated by different generators for cryptographic applications must be tested by probabilistic and statistical methods. However, the vast majority of known techniques focused on testing generators pseudorandom binary sequences, so confirm pseudorandom generated trit sequences using them is almost impossible. Also there are not existed software and methods of such sequences assessment and arises the task of method developing for evaluation the quality of ternary pseudorandom sequences to evaluate the feasibility of using them for cryptographic applications. That method was developed in this paper and it is based on the approach used in NIST STS.

Key words: quantum cryptography, trit, qutrit, pseudorandom sequence, pseudorandom sequences generator, quality assessment.

Сергій Олександрович Гнатюк, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна.
E-mail: S.Gnatyuk@nau.edu.ua

Тетяна Олександрівна Жмурко, асистент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна.
E-mail: TaniaZhm@gmail.com

Василь Миколайович Кінзерявий, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна.
E-mail: V.Kinzeryavyy@gmail.com

Нургуль Абадуллаєвна Сєйлова, кандидат технічних наук, завідувач кафедри інформаційної безпеки, Казахський національний дослідницький технічний університет ім. К.І.Сатпаєва, Алмати, Республіка Казахстан.
E-mail: Seilova_NA@mail.ru

Сергей Александрович Гнатюк, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.

Татьяна Александровна Жмурко, ассистент кафедры безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.

Василий Николаевич Кинзерявый, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.

Нургуль Абадуллаевна Сейлова, кандидат технических наук, заведующая кафедрой информационной безопасности, Казахский национальный исследовательский технический университет им. К.И. Сатпаева, Алматы, Республика Казахстан.

Serhii Hnatiuk, candidate of technical sciences, associate professor of IT-security academic department, National Aviation University, Kyiv, Ukraine.

Tetiana Zhmurko, assistant of IT-security academic department, National Aviation University, Kyiv, Ukraine.

Vasyl Kinzeriavyi, candidate of technical sciences, associate professor of IT-security academic department, National Aviation University, Kyiv, Ukraine.

Nurhul Seilova, candidate of technical sciences, head of information security academic department, Kazakh National Research Technical University n. a. K.I. Satpayev, Almaty, Republic of Kazakhstan.