

## СТАТИСТИЧНІ ДОСЛІДЖЕННЯ СУЧАСНИХ ПОТОКОВИХ ШИФРІВ

О.О. КУЗНЕЦОВ, М.С. ЛУЦЕНКО, А.В. АНДРУШКЕВИЧ, О.М. МЕЛКОЗЕРОВА, Д.В. НОВІКОВА,  
А.В. ЛОБАН

Розглядається математична структура нового потокового симетричного шифру «Струмок». Досліджуються його криптографічні властивості шляхом статистичного тестування вихідних послідовностей (гами шифрувальної). Проводиться порівняльний аналіз показників статистичної безпеки з відомими світовими потоковими шифрами.

*Ключові слова:* потоковий симетричний шифр, криптографічні властивості, статистичне тестування.

### ВСТУП

Сучасні симетричні криптоперетворення знайшли найбільше застосування для захисту інформаційно-телекомунікаційних систем і технологій, зокрема, важливої інформації, що є власністю держави, персональних даних, таємної та комерційної інформації та інших даних, які мають підлягати захисту відповідно до законів, наказів і постанов та інших нормативно-правових актів [1 – 25]. Симетричні криптоперетворення застосовуються для захисту інформації практично в усіх криптографічних додатках, зокрема: забезпечення конфіденційності та цілісності інформації та повідомлень на усіх етапах їх життєвого циклу; шифрування в інформаційно-телекомунікаційних системах в різних режимах роботи залежно від вимог, що висуваються; генерація псевдовипадкових послідовностей; криптографічні протоколи автентифікації, встановлення таємниці та ключів, узгодження таємниці та ключів, розподілу таємниці тощо, коли висуваються складні вимоги до складності (швидкодії); криптографічні протоколи електронного цифрового підпису тощо.

Серед симетричних криптоперетворень особливе місце займають потокові алгоритми [1, 2], в яких інформація подається та обробляється у вигляді нескінченного потоку, тобто послідовності, що гіпотетично може бути нескінченної довжини. Головною перевагою такого перетворення є встановлення певної залежності між окремими символами потоку даних, що дозволяє забезпечити додатковий захист від нав'язування хибної інформації, або хибних режимів роботи апаратури захисту чи кінцевого обладнання телекомунікаційних систем і мереж. Відповідно до цього криптографічне потокове перетворення зазвичай користується більшою довірою у користувачів, оскільки потоки даних, що захищаються поточним алгоритмом, не можуть бути спотворені будь-яким чином, за результатами навмисної або ненавмисної дії користувачів та зловмисників, або якихось випадкових природних чинників чи факторів [1, 2].

Запропонований у [21 – 24] потоковий симетричний шифр «Струмок» застосовує базову структуру

алгоритму шифрування «SNOW2.0» та дозволяє збільшити швидкість формування ключового потоку в ході забезпечення високих та надвисоких показників криптографічної безпеки. Збільшення швидкості досягається за рахунок застосування таблиць передобчислень та перетворень над 64-бітними словами, які розглядаються як елементи скінченного поля  $GF(2^{64})$ . Використання РЗЛЗЗ з відводами зворотного зв'язку за примітивним поліномом над полем  $GF(2^{64})$  дозволяє формувати послідовності максимального періоду, що у сукупності із високонелінійними перетвореннями над послідовністю станів генератору забезпечує властивості випадковості та непередбачуваності формованих послідовностей. Зокрема нелінійний шар перетворень алгоритму «Струмок» засновано на компонентах із національного блокового шифру «Калина» [18, 19], який був стандартизований як ДСТУ 7624:2014 наприкінці 2014 року після тривалих та ретельних досліджень.

*Метою цієї роботи є дослідження статистичних властивостей нового потокового симетричного шифру «Струмок» та інших сучасних поточних алгоритмів. Під час дослідження застосовуються відомі методики статистичного тестування [1, 2, 26, 27], які дозволяють шляхом виконання певних розрахунків оцінити показники статистичної безпеки алгоритму, визначити непередбачуваність та випадковість формованих послідовностей.*

### 1. ПОТОКОВИЙ СИМЕТРИЧНИЙ ШИФР «СТРУМОК»

В роботах [20, 21] проведено аналіз та порівняльні дослідження сучасних алгоритмів симетричного криптоперетворення, на основі узагальнення певних математичних моделей і методів потокового шифрування запропоновано новий алгоритм «Струмок». Цей шифр за своєю структурою подібний до стандартизованого у ISO/IEC 18033-4 [7] алгоритму потокового шифрування «SNOW 2.0».

В основі потокового шифру «Струмок» [22 – 24] лежить класична схема підсумовуючого генератора. Криптоалгоритм орієнтований на 64-розрядні

обчислювальні системи, і, відповідно, розмір слова в шифрі визначено рівним 64 бітам. Як вхідні дані використовується 512 (або 1024)-бітний секретний ключ  $K$  та 512-бітний вектор ініціалізації  $IV$ .

Основними структурними компонентами шифру є регістр зсуву з лінійним зворотним зв'язком (РЗЛЗЗ) та кінцевий автомат (finite-state machine – FSM), в якому виконується нелінійне перетворення. Вхідні дані використовуються для ініціалізації змінної стану  $S_i (i \geq 0)$ , яка складається з вісімнадцяти 64-бітових блоків, до складу яких входить дві компоненти: 16 змінних  $s^{(i)}$  – комірок регістра зсуву з лінійним зворотним зв'язком:  $s^{(i)} = (s_{15}^{(i)}, s_{14}^{(i)}, \dots, s_0^{(i)})$  і двох регістрів кінцевого автомату  $r^{(i)}: r^{(i)} = (r_2^{(i)}, r_1^{(i)})$ . На виході отримуємо ключовий потік (гаму шифрувальну), який формується з 64-бітових слів  $Z_i$ .

Схематичне зображення потокового шифру «Струмок» у режимі генерації гами шифрувальної наведено на рис. 1. На рисунку зображено функціонування генератора в довільний момент часу  $i$ . Змінну часової залежності  $i$  не наведено.

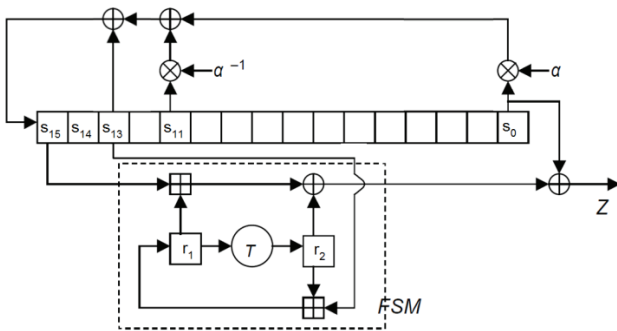


Рис. 1. – Схематичне зображення потокового шифру «Струмок» у режимі генерації ключового потоку

Відводи зворотного зв'язку у РЗЛЗЗ будуються за примітивним над полем  $GF(2^{64})$  поліномом  $f(x) = x^{16} + x^{13} + \alpha^{-1}x^{11} + \alpha$ , де  $\alpha$  є коренем примітивного над полем  $GF(2^8)$  поліному

$$g(z) = z^8 + g_7z^7 + \dots + g_1z + g_0.$$

В свою чергу поле  $GF(2^8)$  будується за примітивним над полем  $GF(2)$  поліномом

$$p(y) = y^8 + y^4 + y^3 + y^2 + 1,$$

а коефіцієнти  $g_0, g_1, \dots, g_7$  подаються через ступінь примітивного елементу  $\beta$  поля  $GF(2^8)$ , тобто  $\beta$  – корінь поліному  $p(y)$ .

Таким чином, маємо вежу полів:

$$GF(2) \subset GF(2^8) \subset GF(2^{64}) \subset GF(2^{1024}),$$

де

– поле  $GF(2^{1024})$  задається відводами зворотного зв'язку РЗЛЗЗ як факторкільце  $GF(2^{64})[x]/(f(x))$ ,

– поле  $GF(2^{64})$  задається як факторкільце  $GF(2^8)[z]/(g(z))$ ,

– поле  $GF(2^8)$  задається як факторкільце  $GF(2)[y]/(p(y))$ .

Отже період вихідної послідовності РЗЛЗЗ є максимальним і дорівнює  $2^{1024} - 1$ . Нижче розглянуто різні варіанти побудови примітивного многочлена  $g(z)$  із дослідженням властивостей відповідних вихідних послідовностей.

В ході дослідження були сформовані чотири варіанти поліному  $g(z)$ :

$$1) \quad g(z) = z^8 + \beta^{170}z^7 + \beta^{166}z^6 + \beta^2z^5 + \beta^{224}z^4 + \beta^{70}z^3 + \beta^2,$$

або при шістнадцятковому поданні коефіцієнтів:

$$g(z) = z^8 + D7z^7 + 3Fz^6 + 04z^5 + 12z^4 + 5Ez^3 + 04;$$

$$2) \quad g(z) = x^8 + \beta^{153}z^7 + \beta^{63}z^6 + \beta^{172}z^5 + \beta^{186}z^4 + \beta^{123}z^3 + \beta^{184}z^2 + \beta^{242},$$

або при шістнадцятковому поданні коефіцієнтів:

$$g(z) = z^8 + 92z^7 + A1z^6 + 7Bz^5 + 6Ez^4 + C5z^3 + 95z^2 + B0;$$

$$3) \quad g(z) = z^8 + \beta^{228}z^7 + \beta^{237}z^6 + \beta^{200}z^5 + \beta^{37}z^4 + \beta^{64}z^3 + \beta^{64}z^2 + \beta^{149},$$

або при шістнадцятковому поданні коефіцієнтів:

$$g(z) = z^8 + 3Dz^7 + 8Bz^6 + 1Cz^5 + 4Az^4 + 5Fz^3 + 5Fz^2 + A4;$$

$$4) \quad g(z) = z^8 + \beta^{14}z^7 + \beta^{151}z^6 + \beta^{158}z^5 + \beta^{117}z^4 + \beta^{95}z^3 + \beta^8z^2 + \beta^{112},$$

або при шістнадцятковому поданні коефіцієнтів:

$$g(z) = z^8 + 13z^7 + AAz^6 + B7z^5 + EDz^4 + E2z^3 + 1Dz^2 + 70,$$

де  $\beta = y$  – примітивний елемент поля  $GF(2^8)$ , корінь двійкового поліному  $p(y) = y^8 + y^4 + y^3 + y^2 + 1$  (у шістнадцятковому поданні  $\beta = 02$ ).

Структурно в алгоритмі потокового шифрування «Струмок» можна виділити три основні функції:

– функція ініціалізації  $Init$ , яка приймає як вхідні дані ключ  $K$  (512 біт або 1024 біта) і вектор ініціалізації  $IV$  (256 біт або 512 біт), і виробляє початкове значення змінної стану  $S_0 = (s^{(0)}, r^{(0)})$ ;

– функція наступного стану  $Next$ , яка приймає на вхід змінну стану  $S_i = (s^{(i)}, r^{(i)})$  і виробляє наступне значення змінної стану  $S_{i+1} = (s^{(i+1)}, r^{(i+1)})$ . Функція  $Next$  може виконуватися в двох режимах, залежно від способу виконання ітерації – як частини реалізації або як частини нормального режиму генерації вихідних даних;

– функція ключового потоку  $Strm$ , що приймає на вході змінну стану  $S_i = (s^{(i)}, r^{(i)})$  і виробляє на виході 64-бітний ключовий потік  $Z_i$ .

Схематичне зображення потокового шифру «Струмок» у ході виконання функції  $Next$  у режимі ініціалізації  $INIT$  наведено на рис. 2.

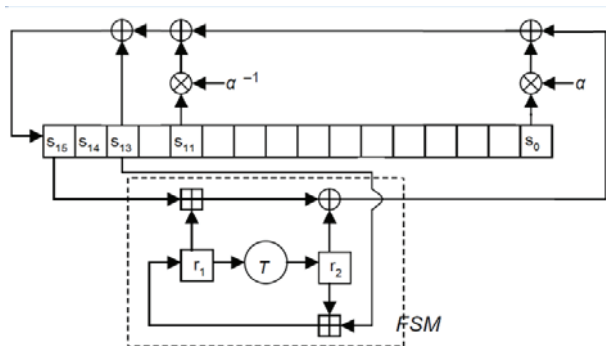


Рис. 2. Схематичне зображення потокового шифру «Струмок» у режимі ініціалізації функції  $Next$

Одним з важливих показників криптографічної стійкості генератора ключових потоків є період формованих псевдовипадкових послідовностей. Розглянутий поточковий шифр «Струмок» виконано за схемою 64-розрядного слово-орієнтованого синхронного поточного криптоалгоритму. За рахунок застосування перетворень над 64-бітними словами, які розглядаються як елементи скінченного поля  $GF(2^{64})$ , та використання РЗЛЗЗ із 16 64-бітними словами забезпечується формування псевдовипадкових послідовностей максимального періоду, що дорівнює  $(2^{64})^{16} - 1 = 2^{1024} - 1$  бітів. У сукупності із нелінійними перетвореннями над послідовністю станів генератору забезпечуються властивості випадковості та непередбачуваності формованих послідовностей.

## 2. МЕТОДИКА СТАТИСТИЧНОГО ТЕСТУВАННЯ

Для проведення експериментальних досліджень криптографічних властивостей потокового шифру «Струмок» було використано статистичне тестування вихідних послідовностей (ключового потоку або гами шифрувальної). До найбільш відомих наборів статистичних тестів належать [1, 2, 26]: DIEHARD, NIST Statistical Test Suite (NIST STS), DieHarder. Їх сутність полягає в перевірці гіпотези про випадковий характер вихідної послідовності досліджуваного криптоалгоритму, тобто в перевірці припущення про те, що сформовані дані не відрізняються в статистичному сенсі від деякої гіпотетичної «випадкової» послідовності.

Під час проведенні експериментальних досліджень було застосовано пакет статистичного тестування NIST STS, який був розроблений в ході проведення конкурсу AES для дослідження генераторів випадкових або псевдовипадкових чисел.

За методикою NIST STS гіпотеза перевіряється за 15 незалежними статистичними тестами (з урахуванням різних вхідних параметрів виконуються 188 тестів), по кожному з яких обчислюється відповідна ймовірність  $P_j, j=1, \dots, 188$  проходження тесту. Ця ймовірність використовується правилом прийняття суджень (критерієм згоди) про істинність чи хибність гіпотези, тобто якщо значення ймовірності  $P_j$  проходження  $j$ -го тесту не нижче деякого порогового значення  $\alpha \in [0.96, 0.99]$ , наприклад, якщо  $P_j \geq 0.99$ , тоді гіпотеза  $H_0$  приймається (на  $j$ -му тесті). В іншому випадку приймається альтернативна гіпотеза. Аналіз елементів  $P_j$  вектора  $P$  дозволяє вказати на конкретні дефекти «випадковості» протестованої послідовності, тобто низькі значення  $P_j$  вказують на явну відмінність досліджуваної послідовності від реалізації випадкового процесу, виявлене  $j$ -м статистичним тестом.

Отже, пакет статистичного тестування NIST STS містить 15 статистичних тестів, але, фактично, залежно від вхідних параметрів обчислюються 188 значень ймовірності  $P$ , які можна розглядати як результат роботи окремих тестів. До 15 тестів належать наступні.

1. *Частотний побітовий тест.* Спрямований на визначення співвідношення між нулями та одиницями у двійковій послідовності певної довжини. Для дійсно випадкової бінарної послідовності кількість нулів та одиниць має бути майже однакова. Отже, тест оцінює, на скільки близькою є доля одиниць до 0,5.

2. *Частотний блоковий тест.* Суть тесту полягає у визначенні долі одиниць всередині блоку довжиною  $m$  бітів, тобто необхідно з'ясувати, чи дійсно частота повторення одиниць в блоці довжиною  $m$  бітів приблизно є рівною  $m/2$ , як можна було б припустити у випадку випадкової послідовності.

3. *Тест на послідовність однакових бітів.* У цьому тесті відбувається пошук рядків, тобто неперервних послідовностей однакових бітів. Ряд (серія) довжиною  $k$  бітів складається з  $k$  абсолютно ідентичних бітів, починається та закінчується з біту, який містить протилежне значення. В даному тесті необхідно з'ясувати швидко чи повільно чергуються одиниці та нулі у початковій послідовності.

4. *Тест на найдовшу послідовність одиниць в блоці.* В даному тесті визначається найдовший рядок одиниць всередині блоку довжиною  $m$  бітів. Необхідно з'ясувати відхилення від теоретичного закону розподілу максимальної довжини серії одиниць.

5. *Тест рангів бінарних матриць.* Тут здійснюється розрахунок рангів неперетинних підматриць, побудованих з початкової двійкової

послідовності. Метою цього тесту є перевірка на лінійну залежність підрядків фіксованої довжини, що складають початкову послідовність..

6. *Спектральний тест.* Суть тесту полягає в оцінці висоти піків дискретного перетворення Фур'є початкової послідовності. Метою є виявлення періодичних властивостей вхідної послідовності, наприклад, близько розташованих один до одного повторюваних ділянок.

7. *Тест на співпадіння шаблонів, що не перекриваються.* У даному тесті підраховується кількість заздалегідь визначених шаблонів, які знайдені в початковій послідовності. Необхідно виявити генератори псевдовипадкових чисел, що формують занадто часто задані неперіодичні шаблони. Як і в тесті №8 на співпадіння шаблонів, що перекриваються, для пошуку конкретних шаблонів довжиною  $m$  бітів використовується вікно також довжиною  $m$  бітів. Якщо шаблон не знайдено, вікно зсувається на один біт. Якщо ж шаблон знайдено, тоді вікно пересувається на біт, який є наступним за знайденим шаблоном, та пошук продовжується далі.

8. *Тест на співпадіння шаблонів, що перекриваються.* Суть даного тесту полягає в підрахунку кількості заздалегідь визначених шаблонів, які знайдені в початковій послідовності. Пошук проводиться майже аналогічним способом як у тесті №7.

9. *Універсальний статистичний тест Маурера.* Тут визначається число бітів між однаковими шаблонами в початковій послідовності (міра, що має безпосереднє відношення до довжини стиснутої послідовності). Необхідно з'ясувати, чи може дана послідовність бути значно стиснута без втрат інформації. У разі, якщо це можливо зробити, то вона не є дійсно випадковою.

10. *Тест на лінійну складність.* В основі тесту лежить принцип роботи лінійного регістра зсуву зі зворотним зв'язком. Необхідно з'ясувати, чи є вхідна послідовність досить складною для того, щоб вражатися абсолютно випадковою. Абсолютно випадкові послідовності характеризуються довгими лінійними регістрами зсуву зі зворотним зв'язком. Якщо ж такий регістр занадто короткий, то передбачається, що послідовність не є повною мірою випадковою.

11. *Тест на періодичність.* Даний тест полягає в підрахунку частоти всіх можливих перекривань шаблонів довжини  $m$  бітів протягом початкової послідовності бітів. Метою є визначення, чи дійсно кількість появ  $2m$  шаблонів, що перекриваються, довжиною  $m$  бітів, є приблизно такою як і у випадку абсолютно випадкової вхідної послідовності бітів. Остання, як відомо, володіє одноманітністю, тобто кожен шаблон довжиною  $m$  біт з'являється в послідовності з однаковою ймовірністю.

12. *Тест приблизної ентропії.* В даному тесті акцент робиться на підрахунку частоти всіх можливих

перекривань шаблонів довжини  $m$  бітів у початкової послідовності бітів. Необхідно порівняти частоти перекривання двох послідовних блоків початкової послідовності з довжинами  $m$  та  $m+1$  з частотами перекривання аналогічних блоків в абсолютно випадковій послідовності. Цей тест виявляє регулярність властивостей генератора.

13. *Тест кумулятивних сум.* Тест полягає в максимальному відхиленні (від нуля) при довільному обході, визначеному кумулятивною сумою заданих  $(-1,+1)$  цифр у послідовності. Необхідно визначити, чи є кумулятивна сума часткових послідовностей, що виникають у вхідній послідовності, занадто великою або занадто маленькою порівняно з очікуваною поведінкою такої суми для абсолютно випадкової вхідної послідовності.

14. *Тест на довільні відхилення.* Суть даного тесту полягає в підрахунку числа циклів, що мають суворо  $k$  відвідувань при довільному обході кумулятивної суми. Довільний обхід кумулятивної суми починається з часткових сум після послідовності  $(0,1)$  перекладеної у відповідну послідовність  $(-1,+1)$ . Цикл довільного обходу складається з серії кроків одиничної довжини, виконаних у випадковому порядку. Мета даного тесту полягає у визначенні того, чи відрізняється число відвідувань певного стану всередині циклу від аналогічного числа в разі абсолютно випадкової вхідної послідовності. Фактично даний тест є набором, що складається з восьми тестів, які проводяться для кожного з восьми станів циклу:  $-4, -3, -2, -1$  та  $+1, +2, +3, +4$ .

15. *Інший тест на довільні відхилення.* У цьому тесті підраховується загальна кількість відвідувань певного стану при довільному обході кумулятивної суми. Метою є визначення відхилень від очікуваного числа відвідувань різних станів при довільному обході. Цей тест складається з 18 тестів, що проводяться для кожного стану:  $-9, -8, \dots, -1$  та  $+1, +2, \dots, +9$ .

Проходження кожного з тестів є важливим критерієм оцінки псевдовипадкового генератора [20]. Тому не відповідність за одним чи більше критеріями означає, що ключовий потік не може на високому рівні протистояти криптоаналізу. Якщо, з іншого боку, генератор проходить всі тести, це зовсім не означає захищеність генератора, оскільки такі тести не враховують особливостей реальної конструкції генератора.

Більшість сучасних криптоалгоритмів мають значення  $P_j$  перевищують порогове значення і як результат тестування використовують лише число пройдених тестів, тобто число ймовірностей  $P_j \geq 0.99$  з множини  $P = \{P_1, P_2, \dots, P_n\}$ . Позначимо число пройдених тестів для конкретної  $i$ -ї вибірки символом  $X_i$ ,  $0 \leq X_i \leq n$ ,  $i=1, \dots, N$ , де  $N$  – кількість протестованих вихідних послідовностей



криптоалгоритму. Слід зазначити, що значення  $X_i$ , так само як і значення з множини  $P = \{P_1, P_2, \dots, P_n\}$ , що характеризують статистичну безпеку досліджуваного криптоалгоритму, мають стохастичну природу. Ці значення безпосередньо залежать як від властивостей досліджуваного генератора, так і від початкових даних під час проведення експериментальних досліджень. Іншими словами, значення елементів  $P_j$  визначаються для конкретної  $i$ -ї вибірки,  $i = 1, \dots, N$ , тобто для конкретної вихідної послідовності криптоалгоритму заданої довжини. Різні початкові дані (різні вихідні послідовності заданої довжини в  $i$ -му експерименті) можуть давати і різні значення елементів  $P_j$ , при цьому відмінності у власних значеннях можуть бути істотними.

Таким чином, кількість пройдених тестів досліджуваного генератором, безпосередньо залежить від обраної вихідної послідовності криптоалгоритму. Для забезпечення заданої достовірності результатів статистичного тестування в роботах [20, 21, 27] запропоновано оцінити математичне сподівання числа пройдених тестів  $X_i$  досліджуваного генератором (криптоалгоритмом), розглядаючи при цьому кожне  $i$ -те тестування як одне спостереження, тобто як конкретну реалізацію деякої випадкової величини  $X$ . Саме цю методику було застосовано під час проведення експериментальних досліджень, отримані результати мають високу точність та достовірність статистичного тестування.

### 3. РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ

Відповідно до методики статистичного тестування були проведені експериментальні дослідження криптографічних властивостей поточкового шифру «Струмок» (були протестовані усі чотири версії алгоритму).

Для порівняння показників статистичної безпеки обрано всесвітньовідомі криптоалгоритми, які стандартизовані на міжнародному або національному рівні та, які на сьогоднішній день мають найбільшу довіру та розповсюдження. Зокрема, були протестовані ключові потоки сучасних поточкових шифрів [6 – 16, 25]: «Enocoro», «HC-128», «HC-256», «Grain», «MICKEY 2», «MUGI», «Rabbit», «Salsa20», «SNOW 2.0», «Sosemanuk», «Trivium», та вихідні послідовності блокового симетричного шифру «AES» із довжиною ключа 128 та 256 бітів (у режимі зворотного зв'язку за виходом цей шифр можна використовувати як поточковий). Наведемо стислі відомості щодо досліджених криптографічних алгоритмів.

**Потоковий симетричний шифр «SNOW 2.0»** є генератором ключових потоків [7], який використовує як вхідні дані 128 або 256-бітовий секретний ключ  $K$  і 128-бітовий вектор ініціалізації  $IV$ . Шифр є слово-

орієнтованим. Автори алгоритму – Томас Йохансон та Патрік Екдаль. Алгоритм було стандартизовано у ISO/IEC 18033-4. Для «SNOW 2.0» максимально рекомендовану кількість біт ключового потоку, виробленого на одній парі  $(K, IV)$ , дорівнює  $23 \cdot 2^{50}$  біт. Це обмеження виправдане з точки зору забезпечення стійкості алгоритму проти криптоаналітичних атак.

**Потоковий симетричний шифр «Sosemanuk»** – це синхронний програмно-орієнтований поточковий шифр, який відповідає першому профілю конкурсу eCRYPT [14]. Його довжина ключа може бути обрана між 128 і 256 бітами. Шифр працює з 128 бітовим початковим значенням, при цьому, як стверджується розробниками алгоритму, будь-яка довжина ключа досягає 128-бітного захисту. Алгоритм Sosemanuk використовує деякі основні принципи поточкового шифру «SNOW 2.0» і деякі перетворення, отримані з блокового шифру SERPENT.

**Потоковий симетричний шифр «Trivium»** – це симетричний апаратно-орієнтований паралельний поточковий шифр. Авторами шифру є Крістоф Де Канн'єр і Барт Пренел [15]. Trivium найбільш простий шифр проекту eSTREAM (другий профіль), який демонструє відмінні результати криптостійкості. За специфікацією алгоритм Trivium – це паралельний поточковий шифр, призначений для генерації  $2^{64}$  біт ключового потоку з 80 біт секретного ключа і 80 біт вектора ініціалізації. Шифр є біт-орієнтованим.

**Потоковий симетричний шифр «Enocoro»** – апаратно-орієнтований криптоалгоритм, який описано у [25]. Це байт-орієнтований шифр із довжиною ключа 128 біти та вектору ініціалізації 64 біти. Незважаючи на те, що «Enocoro» є апаратно-орієнтованим шифром, він також має і ефективну програмну реалізацію. Для досягнення різних вимог, використовуються байтові операції.

**Потоковий симетричний шифр «HC-256»**, який було розроблено у 2004 році [9]. HC-256 простий, безпечний, програмно-орієнтований шифр з ефективною реалізацією і може вільно використовуватися. Спрощену версію HC-128 було представлено на eSTREAM у першому профілі. Для ініціалізації використовується 256-бітний ключ та вектор ініціалізації довжиною 256 біт. Рекомендована максимальна довжина ключової послідовності –  $2^{128}$ .

**Потоковий симетричний шифр «Grain»**, який було представлено Мартіном Хеллом, Томасом Юханссоном та Віллі Мейєром у 2004 на міжнародному конкурсі eSTREAM за другим профілем (апаратно орієнтовані шифри) [10]. Симетричний алгоритм синхронного поточного шифрування, який орієнтований на використання на обчислювальних машинах з обмеженою кількістю вентилів (gate), невеликими потужністю та обсягом пам'яті. Залежно від апаратної реалізації шифр Grain може бути біт-орієнтованим або слово-орієнтованим.

В Grain v1 на вхід подається ключ довжиною 80 біт та вектор ініціалізації довжиною 64 біти. В основі конструкції алгоритму лежать 2 регістри зсуву – з лінійним та нелінійним зворотним зв'язком та вихідна функція. Рекомендована довжина ключового потоку, який може бути вироблений на одній парі ключ/вектор –  $2^{44}$  біт.

**Потоковий симетричний шифр «Mickey»**, вдосконалену версію 2.0 якого було представлено у 2005 році Стивом Беббіджем та Метью Доддом [11] (розшифровується як Mutual Irregular Clocking KEYstream generator – генератор ключового потоку із взаємно нерівномірним рухом). Його призначено для апаратних платформ з обмеженими ресурсами, тобто потоковий шифр MICKEY був розроблений за другим профілем, як апаратно-орієнтований шифр. Для ініціалізації початкового стану використовуються ключ довжиною 80 біт та вектор ініціалізації довжиною до 80 біт. Максимально можлива довжина ключового потоку дорівнює  $2^{40}$  біт на одному ключі, але з використанням різних векторів ініціалізації однієї довжини. Алгоритм шифрування MICKEY має просту апаратну реалізацію, але при цьому забезпечує високий рівень безпеки. Завдяки використанню нерегулярного руху регістрів зсуву, а також нових методів, забезпечується висока стійкість до певних криптоаналітичних атак.

**Потоковий симетричний шифр «MUGI»** є генератором ключових потоків, який було рекомендовано проектом CRYPTREC для використання у 2003 році урядом Японії [7]. Алгоритм було стандартизовано у ISO/IEC 18033-4. Як початкові дані MUGI використовує 128-бітовий секретний ключ, 128-бітовий вектор ініціалізації. MUGI використовує нелінійні блоки підстановки та лінійні трансформації з використанням MDS матриці алгоритму AES. Основні конструкції шифру подібні до конструкцій шифру Rapaata. Шифр MUGI є слово-орієнтованим.

**Потоковий симетричний шифр «Rabbit»**, розробниками алгоритму є Мартін Боегсгаард, Метте Вестерагер, Томас Педерсен, Йеспер Крістіансен та Ове Скавіньєс [12]. У травні 2005р., цей шифр був представлений на конкурсі eStream у першому профілі – програмно-орієнтовані алгоритми. Алгоритм використовує 128-бітний ключ і 64-бітний вектор ініціалізації. На одній парі ключ/вектор може бути вироблено до  $2^{67}$  бітів ключового потоку.

**Потоковий симетричний шифр «Salsa 20»**, який було розроблено Даніелем Бернштейном [13]. Алгоритм став переможцем конкурсу eSTREAM в першому профілі (програмно-орієнтовані алгоритми). Для ініціалізації внутрішнього стану використовується ключ довжиною 256 біт, 64-бітний попсе та 64-бітна позиція блоку ключового потоку. Максимальна довжина псевдовипадкової ключової послідовності дорівнює  $2^{70}$  біт.

**Блоковий симетричний шифр «AES»**, який стандартизовано в США як FIPS-197 [5]. На міжнародному рівні стандартизовано у ISO/IEC 18033-3 [6]. Використовує ключ довжиною 128, 192 або 256 біт. Залежно від довжини ключа відбувається 10, 12 або 14 раундів шифрування. AES базується на принципі, відомому як мережа заміни-перестановок та, завдяки цьому, має швидку апаратну та програмну реалізацію. У режимі зворотного зв'язку за виходом цей шифр можна використовувати як потоковий.

Для усіх протестованих шифрів було складено статистичні портрети, які наведено на рис. 3 – 18. Під статистичним портретом мають на увазі гістограму, на якій на осі ординат знаходяться вірогідності проходження j-го тесту, а на осі абсцис – номер j-го тесту.

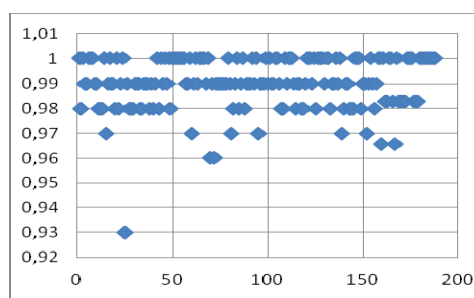


Рис. 3. Статистичний портрет шифру AES-128

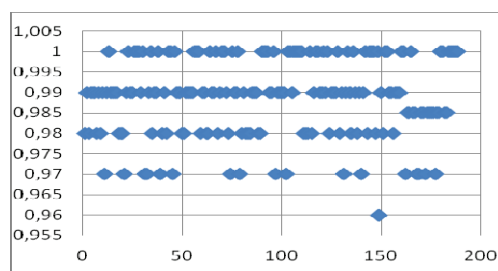


Рис. 4. Статистичний портрет шифру AES-256

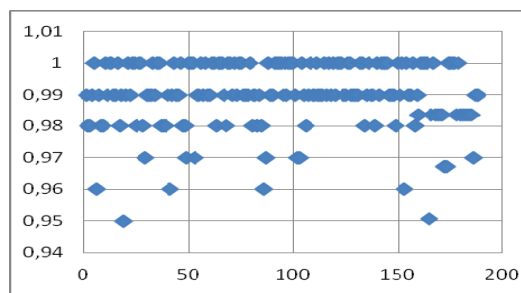


Рис. 5. Статистичний портрет шифру Епосого

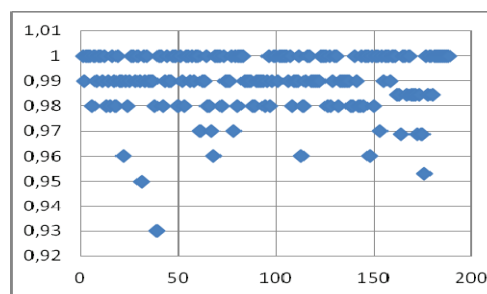


Рис. 6. Статистичний портрет шифру Grain

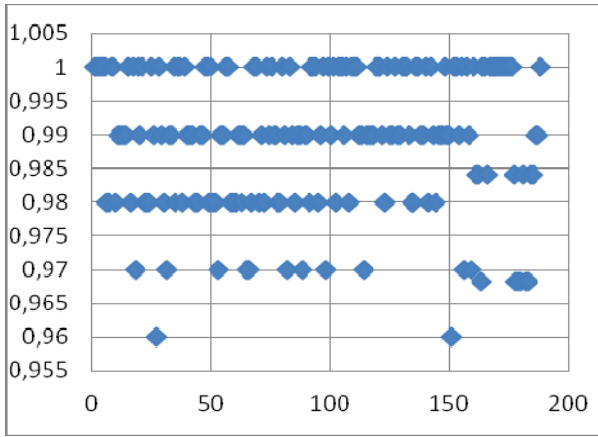


Рис. 7. Статистичний портрет шифру HC-128

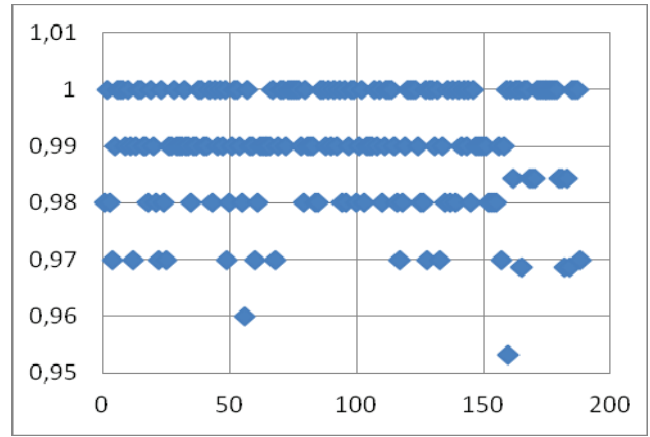


Рис. 11. Статистичний портрет шифру Rabbit

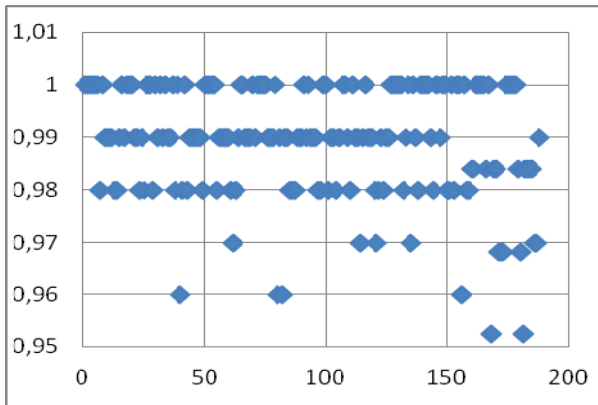


Рис. 8. Статистичний портрет шифру HC-256

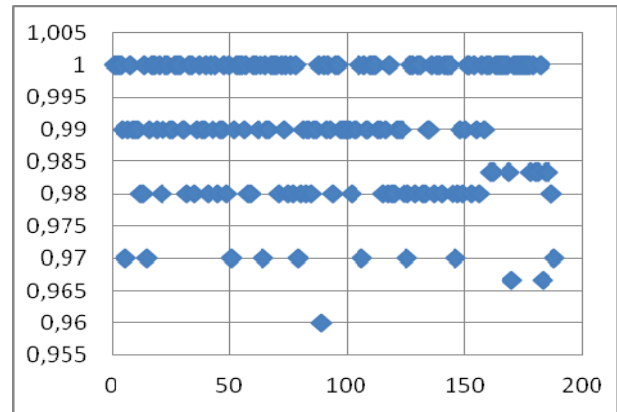


Рис. 12. Статистичний портрет шифру Salsa20

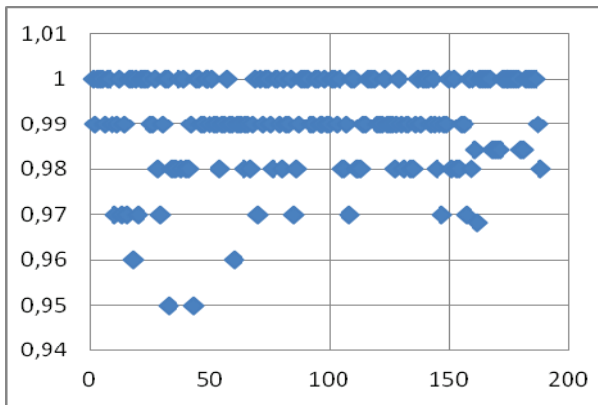


Рис. 9. Статистичний портрет шифру Mickey 2

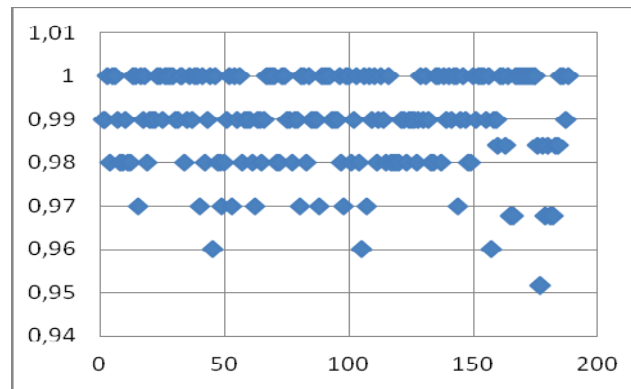


Рис. 13. Статистичний портрет шифру Sosemanuk

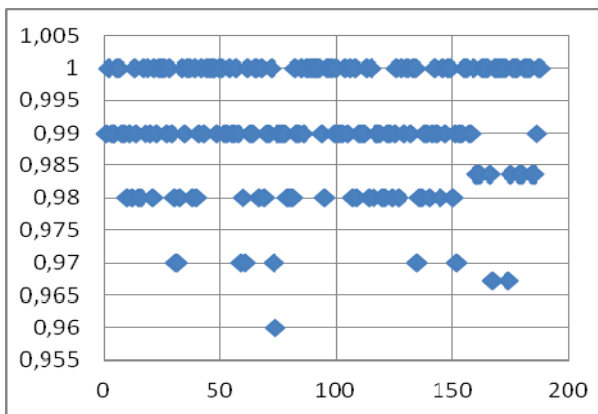


Рис. 10. Статистичний портрет шифру MUGI

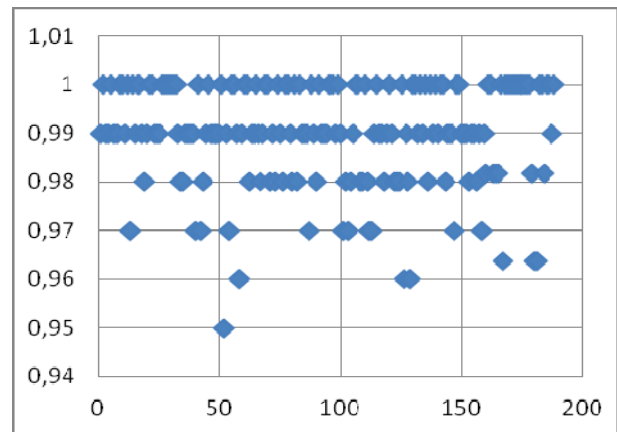


Рис. 14. Статистичний портрет шифру Trivium

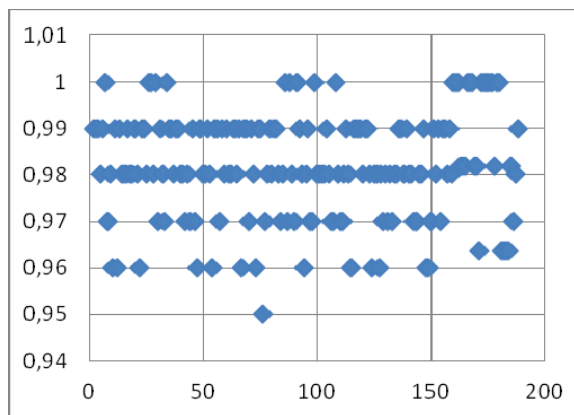


Рис. 15. Статистический портрет шифру SNOW2.0

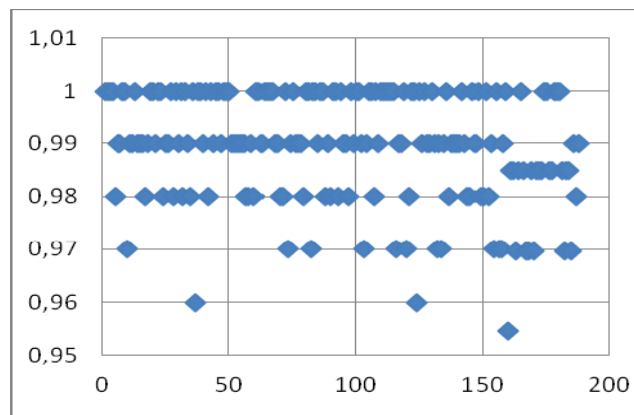


Рис. 19. Статистический портрет шифру «Струмок»

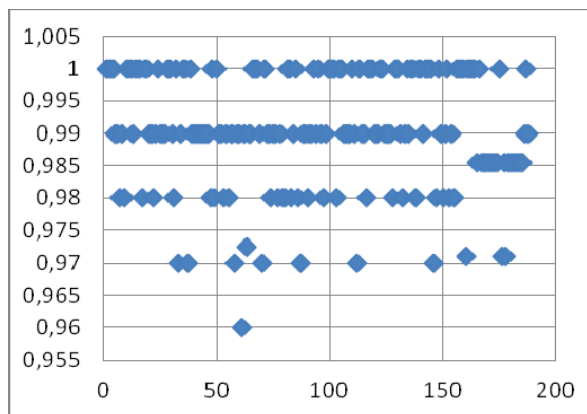


Рис. 16. Статистический портрет шифру «Струмок»

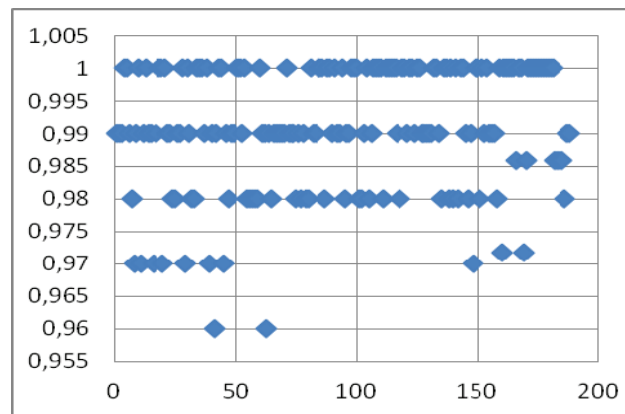


Рис. 20. Статистический портрет шифру «Струмок»

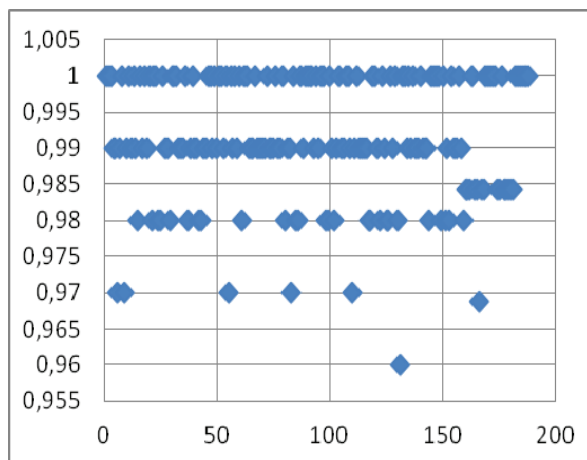


Рис. 17. Статистический портрет шифру «Струмок»

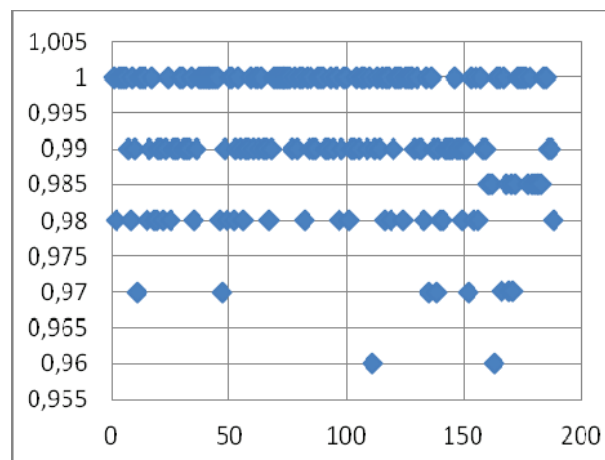


Рис. 21. Статистический портрет шифру «Струмок»

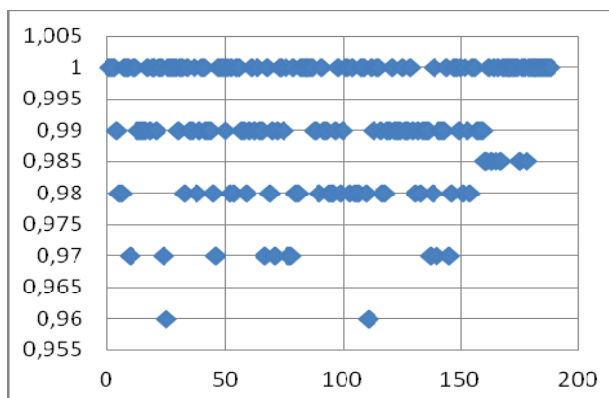


Рис. 18. Статистический портрет шифру «Струмок»

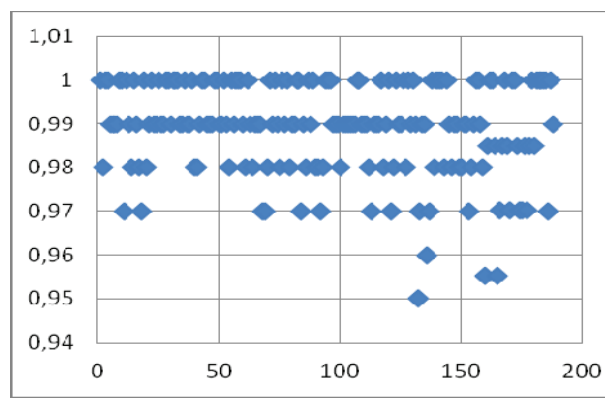


Рис. 22. Статистический портрет шифру «Струмок»



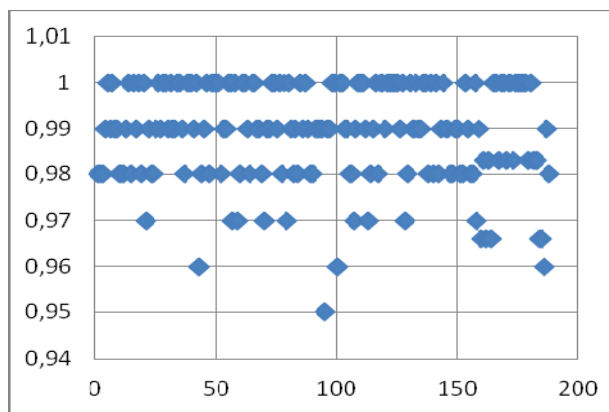


Рис. 23. Статистичний портрет шифру «Струмок»

На рис. 16 – 23 наведено статистичний портрет шифру «Струмок» із параметрами:

- рис. 16, 17 – ключ 512 та 1024 бітів, поліном  $g(z)$  за першим варіантом;
- рис. 18, 19 – ключ 512 та 1024 бітів, поліном  $g(z)$  за другим варіантом;
- рис. 20, 21 – ключ 512 та 1024 бітів, поліном  $g(z)$  за третім варіантом;
- рис. 22, 23 – ключ 512 та 1024 бітів, поліном  $g(z)$  за четвертим варіантом.

Нижче у таблиці 1 наведено результати статистичного тестування послідовності, яку було згенеровано парою випадковий ключ  $K$  / випадковий вектор ініціалізації  $IV$ , для всіх чотирьох варіантів обрання поліному  $g(z)$  з довжиною ключа 512 і 1024 біта. Кожна послідовність завдовжки  $10^6$  біт.

Аналіз даних таблиці 1 показує, що наведені результати тестування приблизно однакові. Але для першого варіанта обрання поліному  $g(z)$  показники виявилися дещо вищими, саме цю версію реалізації алгоритму і обрано для подальшого порівняльного аналізу з іншими криптоалгоритмами.

Результати порівняльного аналізу наведено у таблицях 2, 3 з такими позначеннями:

- «IV\_const» – послідовності для тестування сформовані парою випадковий ключ  $K$  / вектор ініціалізації  $IV$ ;

- «K\_const» – послідовності для тестування сформовані парою ключ  $K$  / випадковий вектор ініціалізації  $IV$ ;

- «K\_IV» – послідовності для тестування сформовані парою випадковий ключ  $K$  / випадковий вектор ініціалізації  $IV$ .

В таблицях 1 – 4 наведено такі дані:

- «M096» та «M099» – оцінки математичного сподівання (вибіркові середні) числа пройдених статистичних тестів за критерієм  $P_j \geq 0.96$  та за критерієм  $P_j \geq 0.99$ , відповідно;

- «D096» та «D099» («S096» та «S099») – оцінки дисперсій (середньоквадратичних відхилень) результатів тестування числа пройдених статистичних тестів за критеріями  $P_j \geq 0.96$  та  $P_j \geq 0.99$ , відповідно;

- «P099» – значення довірчої ймовірності для числа пройдених статистичних тестів за критерієм  $P_j \geq 0.99$  та при точності  $\varepsilon = 2$ ;

- «P096» – значення довірчої ймовірності для числа пройдених статистичних тестів за критерієм  $P_j \geq 0.96$  та при точності  $\varepsilon = 1$ ;

- «Min096» – мінімальні значення числа пройдених статистичних тестів за критерієм  $P_j \geq 0.96$ .

Наведені результати тестування різних поточкових криптоперетворень підтверджують їхні високі криптографічні показники. Досліджувані шифри показали високе число успішно пройдених тестів: 130 – 133 за критерієм  $P_j \geq 0.99$  та 186-187 за критерієм  $P_j \geq 0.96$ . Ці оцінки отримані з високою достовірністю ( $P_o = 0,99$  для  $P_j \geq 0.99$  та  $P_o \approx 1$  для  $P_j \geq 0.96$ ).

Таблиця 1

Результати статистичного тестування різних версій алгоритму «Струмок»

Назва алгоритму	M099	D099	S099	P099	M096	D096	S096	P096	MIN
Strumok_1_512	130,01	23,6	4,86	1.00	186,45	1,4555	1,206	1.00	184
Strumok_2_512	132,58	50,20	7,086	1.00	186,63	2,054	1,433	1.00	184
Strumok_3_512	133,75	36,44	6,037	1.00	186,66	1,907	1,381	1.00	182
Strumok_4_512	131,38	55,702	7,463	1.00	186,71	1,452	1,205	1.00	184
Strumok_1_1024	132,83	56,516	7,518	1.00	186,90	0,802	0,896	1.00	185
Strumok_2_1024	132,125	66,22	8,1376	1.00	186,792	1,0162	1,0081	1.00	185
Strumok_3_1024	131,204	29,443	5,4261	1.00	186,122	0,5156	0,7181	1.00	184
Strumok_4_1024	134,14	34,932	5,9102	1.00	186,4	2,516	1,586	1.00	183

Таблица 2

Результати статистичного тестування алгоритму «Струмок»

	M099	D099	S099	P099	M096	D096	S096	P096	MIN
Strumok-512_K	133,475	77,62	8,81	1,00	186,96	1,6222	1,274	1,00	185
Strumok-512_IV	133,34	35,71	5,9757	1,00	186,921	1,4195	1,191	1,00	184
Strumok-512_K_IV	130,01	23,614	4,8594	1,00	186,455	1,416	1,1901	1,00	184
Strumok-1024_K	130,158	32,866	5,733	1,00	187,099	1,099108	1,0484	1,00	184
Strumok-1024_IV	132,1	45,967	6,7799	1,00	186,911	1,289089	1,1354	1,00	184
Strumok-1024_K_IV	132,56	56,06	7,4873	1,00	186,891	0,791	0,889	1,00	185

Таблица 3

Результати статистичного тестування сучасних поточкових шифрів

	M099	D099	S099	P099	M096	D096	S096	P096	MIN
AES-128_K_IV	127,07	20,456	4,438	1,00	186,63	0,3191	0,554	1,00	185
Enocoro_K_IV	132,92	51,22	7,157	1,00	187,17	0,79	0,89	1,00	185
HC_256_K_IV	133,75	36,44	6,04	1,00	186,66	1,93	1,381	1,00	182
Snow2.0_K_IV	132,78	23,93	4,89	1,00	186,79	0,43	0,656	1,00	183
Strumok-512_K_IV	130,01	23,6	4,86	1,00	186,45	1,4555	1,206	1,00	184
Strumok-1024_K_IV	132,83	56,516	7,518	1,00	186,90	0,802	0,896	1,00	185
Grain_K_IV	132,36	57,32	7,571	1,00	186,921	1,414	1,185	1,00	182
Mickey_2_K_IV	133,53	61,65	7,85	1,00	186,6	2,302	1,51	1,00	179
MUGI_K_IV	132,227	56,279	7,3295	1,00	186,5	1,0238	0,9886	1,00	185
Rabbit_K_IV	132,65	16,87	4,017	1,00	187,22	0,451	0,657	1,00	185
Salsa20_K_IV	134,16	28,055	5,27	1,00	187,001	1,01	0,99	1,00	183
Sosemanuk_K_IV	131,73	49,36	6,991	1,00	186,8	2,240	1,49	1,00	184
Trivium_K_IV	130,24	99,683	9,935	1,00	187,15	1,49	1,214	1,00	182

Таблица 4

Результати статистичного тестування алгоритму «Струмок» з різною кількістю початкових тактувань

Кількість тактувань	M099	D099	S099	P099	M096	D096	S096	P096	MIN
0	130,381	20,141	4,488	1,00	186,905	1,5147	1,2307	1,00	183
16	133,095	87,5147	9,355	1,00	186,714	0,966	0,9828	1,00	185
32	132,238	24,753	4,975	1,00	187,143	0,6939	0,833	1,00	185
64	135	35,333	5,9442	1,00	187,095	1,0386	1,019	1,00	184
128	133,905	73,4195	8,5685	1,00	186,762	0,84807	0,921	1,00	185

Слід відмітити високі показники статистичної безпеки алгоритму шифрування «Струмок», який виявив певні властивості генератора випадкових бітів. Зокрема за результатами даних таблиці видно, що формовані послідовності за своїми властивостями не поступаються всесвітньо відомим поточковим криптографічним алгоритмам, зокрема шифрами HC-256, Salsa20, Mickey та SNOW 2.0. Крім того, для шифру «Струмок» мінімальні значення числа пройдених статистичних тестів за критерієм  $P_j \geq 0.96$  є вищі, ніж у цих алгоритмах, що свідчить про незначну перевагу показників статистичної безпеки дослідженого алгоритму.

Процес ініціалізації алгоритму «Струмок» включає в себе окремі етапи: встановлення ключа і уста-

новку вектора ініціалізації, початкове тактування. Для того, щоб генератор вийшов в робочий стан необхідно зробити 64 ініціюючих такти без генерації ключового потоку, тобто 4 повних циклів. Тому перед початком генерації ключового потоку необхідно зробити 64 зсуви вмісту комірок без генерації потоку, вихід з кінцевого автомата братиме участь у формуванні вмісту комірок регістра, а не ключового потоку. Вибір саме такої кількості початкових тактувань виходить в тому числі із міркувань поліпшення статистичних властивостей послідовності, яку буде згодом згенеровано. Для перевірки доцільності такої кількості тактувань було проведено тестування послідовності довжиною  $10^6$  бітів після різної кількості початкових тактувань. Отримані результати наведені в таблиці 4, які свідчать

про те, що після 64 тактувань забезпечуються високі статистичні властивості формованої послідовності.

### ВИСНОВКИ

Алгоритм поточкового шифрування «Струмок» виконано за схемою 64-розрядного слово-орієнтованого синхронного поточного криптоалгоритму, що заснований на ідеї класичного сумуючого генератора. Він застосовує базову структуру алгоритму «SNOW2.0» та призначений для збільшення швидкості формування ключового потоку при збереженні високих криптографічних властивостей. Це досягається за рахунок застосування перетворень над 64-бітними словами, які розглядаються як елементи скінченного поля  $GF(2^{64})$ , із використанням РЗЛЗЗ над цим полем для формування послідовності максимального періоду. У сукупності із нелінійними перетвореннями над послідовністю станів генератору це забезпечує властивості випадковості та непередбачуваності формованих послідовностей.

Методика, яка розглянута в даній роботі, та отримані з її використання результати можуть розглядатися як первинний аналіз криптографічних властивостей генератора, оскільки такі статистичні тести не враховують власну структуру генератора.

За результатами експериментальних досліджень слід відмітити високі показники статистичної безпеки алгоритму шифрування «Струмок». Формовані послідовності за своїми властивостями не поступаються всесвітньо відомим поточковим криптографічним алгоритмам. Крім того, для шифру «Струмок» мінімальні значення числа пройдених статистичних тестів є вищі ніж у цих алгоритмах, що свідчить про незначну перевагу показників статистичної безпеки дослідженого алгоритму.

Статистичні дослідження вихідних послідовностей з різною кількістю початкових тактувань (на етапі ініціалізації шифру) показали, що після 64 ітерацій забезпечуються високі показники статистичної безпеки. Це опосередковано підтверджує правильність обрання кількості початкових тактувань в специфікації алгоритму поточкового шифрування.

Перспективним напрямком подальших досліджень є аналіз криптографічних властивостей алгоритму поточкового шифрування «Струмок», обґрунтування практичних рекомендацій з його застосування, в тому числі і на постквантовий період.

### Література

- [1] Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: Підручник для вищих навч. закладів. – Харків: Вид-во «Форт», 2013. – 880 с.
- [2] Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. – Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем / За заг. ред. д.т.н., професора І.Д. Горбенка / Ю.І. Горбенко // Харків, Видавництво «Форт», 2016. – 960 с.
- [3] Кузнецов О.О., Сватовський І.І. та ін., всього 13 осіб. Аналіз, розробка та дослідження постквантових криптографічних примітивів та обґрунтування умов їхнього застосування в Україні: звіт про НДР (проміжний). Том 1. – Аналіз та порівняльні дослідження симетричних криптографічних перетворень на постквантовий період / ХНУ ім. В.Н. Каразіна; кер. Кузнецов О.О.; вик.: Сватовський І.І. [та інш., всього 13 осіб]. Х.: ХНУ ім. В.Н. Каразіна. – 2016. – 119 с.
- [4] Кузнецов О.О., Сватовський І.І. та ін., всього 6 осіб. Аналіз, розробка та дослідження постквантових криптографічних примітивів та обґрунтування умов їхнього застосування в Україні: звіт про НДР (проміжний). Том 2. – Аналіз та порівняльні дослідження постквантових алгоритмів електронного цифрового підпису та направленої шифрування / ХНУ ім. В.Н. Каразіна; кер. Кузнецов О.О.; вик.: Сватовський І.І. [та інш., всього 6 осіб]. Х.: ХНУ ім. В.Н. Каразіна. – 2016. – 66 с.
- [5] FIPS-197: Advanced Encryption Standard (AES). National Institute of Standards and Technology. - 2001. [Електронний ресурс]. – Режим доступу: <http://csrc.nist.gov/publications/fips/fips197/fips197.pdf>.
- [6] Information technology – Security techniques – Encryption algorithms, Part 3: Block ciphers (ISO/IEC 18033-3) - 80 p.
- [7] ISO/IEC 18033-4:2011. Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers. [Електронний ресурс]. – Режим доступу: [http://www.iso.org/iso/home/store/catalogue\\_ics/catalogue\\_detail\\_ics.htm?csnumber=54532](http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54532)
- [8] ISO/IEC 29192-3:2012. Information technology – Security techniques – Lightweight cryptography – Part 3: Stream ciphers. [Електронний ресурс]. – Режим доступу: [http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=56426](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56426)
- [9] The eSTREAM Project - eSTREAM Phase 3. HC (Portfolio Profile 1). [Електронний ресурс]. – Режим доступу: <http://www.ecrypt.eu.org/stream/hcpf.html>
- [10] The eSTREAM Project - eSTREAM Phase 3. Grain (Portfolio Profile 2). [Електронний ресурс]. – Режим доступу: <http://www.ecrypt.eu.org/stream/grainpf.html>
- [11] The eSTREAM Project - eSTREAM Phase 3. MICKEY (Portfolio Profile 2). [Електронний ресурс]. – Режим доступу: <http://www.ecrypt.eu.org/stream/mickeypf.html>
- [12] The eSTREAM Project - eSTREAM Phase 3. Rabbit (Portfolio Profile 1). [Електронний ресурс]. – Режим доступу: <http://www.ecrypt.eu.org/stream/rabbitpf.html>
- [13] The eSTREAM Project - eSTREAM Phase 3. Salsa20 (Portfolio Profile 1). [Електронний ресурс]. – Режим доступу: <http://www.ecrypt.eu.org/stream/salsa20pf.html>
- [14] The eSTREAM Project - eSTREAM Phase 3. SOSEMANUK (Portfolio Profile 1). [Електронний ресурс]. – Режим доступу: <http://www.ecrypt.eu.org/stream/sosemanukpf.html>
- [15] The eSTREAM Project - eSTREAM Phase 3. Trivium (Portfolio Profile 2). [Електронний ресурс]. – Режим доступу: <http://www.ecrypt.eu.org/stream/triviumpf.html>
- [16] Горбенко Ю.І., Потий А.В., Избенко Ю.А., Орлова С.Ю. Анализ схем поточного шифрования, представленных на европейский конкурс NESSIE // Правове, нормативне та метрологічне забезпечення

системи захисту інформації в Україні: науково-технічний збірник. – 2002. – Вип. 5. – С. 92-110.

- [17] Дослідження режимів застосування блокових симетричних шифрів: звіт про НДР (заключний). / ХНУ ім. В.Н. Каразіна; кер. Кузнецов О.О.; вик.: Шлокін В.М. [та ін., всього 4 особи]. Х.: ХНУ ім. В.Н. Каразіна. – 2014. – 89 с.
- [18] Розробка нового блокового симетричного шифру: звіт за перший етап НДР «Алгоритм» (проміжний) / АТ «ІТ»; кер. І.Д. Горбенко – Харків, 2014, Том 4. – 304 с.
- [19] Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К.: Мінекономрозвитку України, 2015. – 238 с.
- [20] Аналіз та порівняльні дослідження сучасних алгоритмів потокового криптоперетворення: звіт про НДР (проміжний). / ХНУ ім. В.Н. Каразіна; кер. Кузнецов О.О.; вик.: Малахов С.В. [та ін., всього 11 осіб]. Х.: ХНУ ім. В.Н. Каразіна. – 2015. – 254 с.
- [21] Розробка пропозицій до проекту алгоритму потокового симетричного шифрування та обґрунтування його властивостей: звіт про НДР (заключний). / ХНУ ім. В.Н. Каразіна; кер. Кузнецов О.О.; вик.: Малахов С.В. Х.: ХНУ ім. В.Н. Каразіна. – 2015. – 73с.
- [22] Кузнецов О.О., Іваненко Д.В., Белозерцев І.М., Андрушкевич А.В. Алгоритм потокового криптоперетворення «Струмок» // Труды научно-технической конференции с международным участием «Компьютерное моделирование в наукоемких технологиях», 26-31 мая 2016 г. – Х.: ХНУ имени В.Н. Каразина – 2016. – С. 187 – 190.
- [23] Kuznetsov O. O., Ivanenko D.V., Lutsenko M.S. Strumok stream cipher: specification and basic properties // Third International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PICS&T-2016). October 4 - 6, 2016 Ukraine, Kharkiv. – Kharkiv: Ministry of Education and Science of Ukraine, Kharkov National University of Radioelectronics. – 2016. – С. 15-28
- [24] Андрушкевич А.В., Іваненко Д.В., Луценко М.С., Кухар Ю.В. Аналіз властивостей перспективного потокового шифру «Струмок» // 71-ша науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів. м. Одеса 6-8 грудня 2016 р. – м. Одеса: ОНАЗ.
- [25] Pseudorandom number generator Enocho. [Електронний ресурс]. – Режим доступу: <http://www.hitachi.com/rd/yr/crypto/enochog/>
- [26] Special Publication 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. [Електронний ресурс]. Режим доступу: <http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf>
- [27] Кузнецов А.А., Мордвинов Р.И., Колованова Е.П., Самойлова А.В. Методика статистического тестирования криптографических алгоритмов // Спеціальні телекомунікаційні системи та захист інформації. – Київ – 2014. – №1(25). – С.54-61



**Кузнецов Олександр Олександрович**, доктор технічних наук, професор, професор кафедри БІСТ ХНУ імені В.Н. Каразіна. Область наукових інтересів: Криптографія та автентифікація, теорія передачі даних, стеганографічні методи захисту інформації.



**Луценко Марія Сергіївна**, студентка факультету комп'ютерних наук ХНУ імені В.Н. Каразіна. Область наукових інтересів: Криптографічні методи захисту інформації, потокові симетричні шифри.



**Андрушкевич Аліна Вадимівна**, молодший науковий співробітник кафедри БІСТ ХНУ імені В.Н. Каразіна. Область наукових інтересів: аналіз стійкості симетричних шифрів, криптографія і автентифікація.



**Мелкозерова Ольга Михайлівна**, кандидат технічних наук, магістрант факультету комп'ютерних наук ХНУ імені В.Н. Каразіна. Область наукових інтересів: Криптографічні методи захисту інформації, потокові симетричні шифри.



**Новікова Дарина Вікторівна**, студентка радіотехнічного факультету ХНУРЕ. Область наукових інтересів: Криптографічні методи захисту інформації, потокові симетричні шифри.



**Лобан Анна Володимирівна**, студентка радіотехнічного факультету ХНУРЕ. Область наукових інтересів: Криптографічні методи захисту інформації, потокові симетричні шифри.

УДК 004.056.55

**Статистические исследования современных потоковых шифров** / А.А. Кузнецов, М.С. Луценко, А.В. Андрушкевич, О.М. Мелкозерова, Д.В. Новикова, А.В. Лобан // Прикладная радиоэлектроника: науч.-техн. журнал. – 2016. – Том 15, № 3. – С. 167 – 178.

Рассматривается математическая структура нового потокового симметричного шифру «Струмок». Исследуется його криптографические свойства путем статистического тестирования выходных последовательностей (гаммы шифровальной). Проводится сравнительный анализ показателей статистической безопасности с известными мировыми потоковыми шифрами.

**Ключевые слова:** потоковый симметричный шифр, криптографические свойства, статистическое тестирование.

Табл.: 04. Ил.: 23. Библиогр.: 27 назв.

UDC 004.056.55

**Statistical studies of modern stream ciphers** / O.O. Kuznetsov, M.S. Lutsenko, A.V. Andrushkevych, O.M. Melkozherova, D.V. Novikova, A.V. Loban // Applied Radio Electronics: Sci. Journ. – 2016. – Vol. 15, № 3. – P. 167 – 178.

The paper considers the mathematical structure of the new stream symmetric cipher "Strumok". Its cryptographic properties are studied by statistical tests of initial sequences (gamma encryption). A comparative analysis of statistical indicators of security of the new cipher and those of known world stream ciphers has been performed.

**Keywords:** stream symmetric cipher, cryptographic properties, statistical testing.

Tab.: 04. Fig.: 23. Ref.: 27 items.