УДК 004.056.55

О.О. КУЗНЕЦОВ, д-р техн. наук, Д.В. ІВАНЕНКО, канд. техн. наук, М.С. ЛУЦЕНКО, В.А. ТИМЧЕНКО, О.М. МЕЛКОЗЕРОВА, канд. техн. наук, М.О. ОСАДЧУК, Є.В. ОСТРЯНСЬКА

ПОРІВНЯЛЬНІ ДОСЛІДЖЕННЯ АЛГОРИТМІВ ПОТОКОВОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

Вступ

Потокові алгоритми криптографічного перетворення знайшли широке застосування та впровадження для захисту важливих інформаційних ресурсів, зокрема, таємної інформації, що є власністю держави, персональних даних, комерційної таємниці та інших відомостей, захист яких передбачено діючим законодавством [1, 2]. Основними перевагами потокового криптоперетворення є підвищена безпека та швидкодія [1 – 4], і це робить їх застосування найбільш доцільним для захисту каналів управління та зв'язку у військовій сфері, державному управлінні, банківському секторі та ін. Отже розробка, дослідження, впровадження та експлуатація засобів потокового шифрування є надзвичайно важливою та актуальною проблемою загальнодержавного значення з розбудови національної інформаційної інфраструктури та створення передових інформаційних технологій. Стандартизований на національному та/або міжнародному рівнях криптоалгоритм повинен забезпечувати високій рівень стійкості (в тому числі і в умовах можливого застосування квантового криптоаналізу), мати високу швидкодію та ефективно функціонувати на різних обчислювальних платформах [5 – 9].

В цій роботі викладаються основні результати порівняльних досліджень алгоритмів потокового криптографічного перетворення, зокрема стандартизованих на міжнародному рівні у ISO/IEC 18033-4 [6] та ISO/IEC 29192-3 [7], представлених у якості переможців міжнародного проекту eSTREAM з виявлення нових поточних шифрів придатних для широкого застосування у Європейському Союзі [8], та з проекту CRYPTREC (Cryptography Research and Evaluation Committees), заснованому японським урядом для оцінки і рекомендації шифрувальних методів для урядового і індустріального використання [9]. Перелік досліджуваних алгоритмів потокового криптоперетворення наведено у табл. 1, де вказано короткі відомості про шифри та належність до відповідних стандартів чи проектів. До порівняння долучено також алгоритми потокового симетричного шифрування (ПСШ) «Струмок» (STRUMOK) [10, 11] та RC4 [12 – 14], а також всесвітньовідомий блоковий симетричний шифр AES, що стандартизований на національному рівні в США (FIPS-197) [15] та на міжнародному рівні у ISO/IEC 18033-3 [16]. У певних режимах блоковий алгоритм AES може функціонувати як генератор ключових потоків.

Таблиця 1

Перелік досліджуваних алгоритмів потокового криптографічного перетворення

Назва шифру	Специфіковано	Розмір стану, біт	Розмір ключа, біт	Розмір IV, біт
AES-128	FIPS-197 [15], ISO/IEC 18033-3 [16], CRYPTREC [9]	128	128	128
AES-256		256	256	256
HC-128	eSTREAM [8]	128	128	128
HC-256		256	256	256
MICKEY-128	eSTREAM [8]	160	128	128
RABBIT	ISO/IEC 18033-4 [6], eSTREAM [8]	513	128	64
SALSA-20	eSTREAM [8]	512	128	64
SNOW2.0-128	ISO/IEC 18033-4 [6]	512	128	128
SNOW2.0-256	ISO/IEC 18033-4 [6]	512	256	256

SOSEMANUK	eSTREAM [8]	512	128	128
STRUMOK 256	[10, 11]	1024	256	256
STRUMOK 512	[10, 11]	1024	512	512
TRIVIUM	eSTREAM [8]	288	80	80
CRYPTMT3	eSTREAM [8]	128	128	64
DECIM-128	ISO/IEC 18033-4 [6], eSTREAM [8]	288	128	128
RC4	[12 – 14]	256	256	–
KCIPHER-2	ISO/IEC 18033-4 [6], CRYPTREC [9]	640	128	128
GRAIN	eSTREAM [8]	128	128	96
MUGI	ISO/IEC 18033-4 [6]	128	128	128

Порівняльні дослідження алгоритмів з табл. 1 проводилися за двома напрямками. По-перше, досліджувалася статистична безпека шляхом тестування вихідних послідовностей (генерованих ключових потоків). Для цього застосовано методики статистичного тестування NIST Statistical Test Suite (NIST STS) [17 – 19] та DIEHARD [20, 21]. По-друге, досліджувалася швидкодія відповідних генераторів у певних режимах (за методикою тестування, яку було запропоновано при проведенні конкурсу eSTREAM [8]). Отримані результати досліджуються з метою визначення перспективного напрямку подальших розробок та обґрунтування нового потокового шифру в Україні.

Порівняльні дослідження статистичної безпеки алгоритмів потокового шифрування

Для проведення експериментальних досліджень криптографічних властивостей потокового симетричного криптоперетворення в цій роботі використано статистичне тестування вихідних послідовностей (ключового потоку або гами шифрувальної). До найбільш відомих наборів статистичних тестів належать [17 – 21]:

– DIEHARD. Найбільш ранній і відомий набір тестів. Він містить 12 статистичних тестів;

– NIST Statistical Test Suite (NIST STS) розроблений Національним інститутом стандартів і технологій США. До його складу входять 15 статистичних тестів.

Пакет статистичного тестування NIST STS був розроблений в ході проведення конкурсу AES для дослідження генераторів випадкових або псевдовипадкових послідовностей (ПВП) і є найбільш поширеним інструментом оцінки статистичної безпеки криптографічних примітивів.

Порядок тестування окремої двійкової послідовності S має наступний вид [18]:

– висувається нульова гіпотеза H_0 – припущення про те, що дана двійкова послідовність S є випадковою;

– за послідовністю S розраховується статистика тесту $c(S)$;

– з використанням спеціальної функції та статистики тесту розраховується значення ймовірності $P = f(c(S))$;

– значення ймовірності P порівнюється з пороговим значенням $\alpha \in [0{,}96; 0{,}99]$. Якщо $P \geq \alpha$, то гіпотеза H_0 приймається. В іншому випадку приймається альтернативна гіпотеза.

Пакет містить 15 статистичних тестів:

1) *Частотний побітовий тест*. 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.

3) *Тест на послідовність однакових бітів*. В даному тесті необхідно з'ясувати, чи дійсно кількість неперервних послідовностей однакових бітів відповідає їх кількості у випадковій послідовності.

4) *Тест на найдовшу послідовність одиниць в блоці*. В даному тесті визначається найдовший рядок одиниць всередині блоку довжиною m бітів, перевіряється відповідність очікуваній довжини найдовшого рядку одиниць у випадковій послідовності.

5) *Тест рангів бінарних матриць*. Метою цього тесту є перевірка на лінійну залежність підрядків фіксованої довжини, що складають початкову послідовність. Даний тест також є в пакеті DIEHARD [20, 21].

6) *Спектральний тест*. Суть тесту полягає в оцінці висоти піків дискретного перетворення Фур'є початкової послідовності. Метою є виявлення періодичних властивостей вхідної послідовності.

7) *Тест на співпадіння шаблонів, що не перекриваються*. В даному тесті підраховується кількість заздалегідь визначених шаблонів, які знайдені в початковій послідовності. Необхідно виявити генератори випадкових або псевдовипадкових чисел, що формують занадто часто задані неперіодичні шаблони.

8) *Тест на співпадіння шаблонів, що перекриваються*. Суть даного тесту полягає в підрахунку кількості заздалегідь визначених шаблонів, які знайдені в початковій послідовності.

9) *Універсальний статистичний тест Маурера*. Тут визначається число бітів між однаковими шаблонами в початковій послідовності (міра, що має безпосереднє відношення до довжини стиснутої послідовності).

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 вважатися випадковою.

11) *Тест на періодичність*. Даний тест полягає в підрахунку частоти всіх можливих перекривань шаблонів довжини m бітів протягом початкової послідовності бітів.

12) *Тест приблизної ентропії*. Акцент робиться на підрахунку частоти всіх можливих перекривань шаблонів довжини m бітів протягом початкової послідовності бітів.

13) *Тест кумулятивних сум*. Необхідно визначити, чи є кумулятивна сума часткових послідовностей, що виникають у вхідний послідовності, занадто великою або занадто маленькою у порівнянні з очікуваною поведінкою такої суми для 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. Мета тесту полягає у визначенні того, чи відрізняється число відвідувань певного стану всередині циклу від аналогічного числа в разі випадкової вхідної послідовності.

15) *Інший тест на довільні відхилення*. У цьому тесті підраховується загальна кількість відвідувань певного стану при довільному обході кумулятивної суми.

Проходження кожного з 15 статистичних тестів є важливим критерієм оцінки псевдовипадкового генератору. Тому навіть 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 говорить про захищеність генератору, оскільки такі тести не враховують особливостей реальної конструкції генератору.

За методикою NIST STS для 15 наведених вище тестів в залежності від вхідних параметрів обчислюються 188 значень ймовірності P. Таким чином, в результаті тестування двійкової послідовності формується вектор $P=\{P_1,P_2...P_{188}\}$ значень ймовірностей. Аналіз складових P_j цього вектору дозволяють вказати на конкретні дефекти випадковості протестованої послідовності.

Відповідно до методики статистичного тестування [19] були проведені експериментальні дослідження криптографічних властивостей різних ПСШ. В роботі були протестовані ключові потоки сучасних потокових шифрів AES, CryptMT, DECIM, Enocoro, Grain, HC, KCipher, Mickey2, MUGI, Rabbit, RC4, Salsa20, Snow 2, Sosemanuk, Trivium та запропонованого в [10, 11] шифру «Струмок». Для статистичного тестування парою випадковий ключ K/випадковий вектор ініціалізації IV було згенеровано 100 послідовностей завдовжки 10^6 біт. Оцінювалося математичне сподівання числа пройдених тестів досліджуваним генератором. Результати випробувань наведені в табл. 2.

Таблиця 2

Результати статистичного тестування для шифрів AES, CryptMT, DECIM, Enocoro, Grain, HC, KCipher, Mickey2, MUGI, Rabbit, RC4, Salsa20, Snow 2, Sosemanuk, Strumok, Trivium

Назва алгоритму	M099	D099	S099	P099	M096	D096	S096	P096	MIN
AES-128	127,07	20,456	4,438	1.00	186,63	0,3191	0,554	1.00	185
CRYPTMT	130,89	52,988	7,279	1.00	158,56	5,284	2,299	1.00	181
DECIM	132,44	19,358	4,399	1.00	186,44	0,9136	0,956	1.00	185
ENOCORO	132,92	51,22	7,157	1.00	187,17	0,79	0,89	1.00	185
GRAIN	132,36	57,32	7,571	1,00	186,92	1,414	1,185	1.00	182
HC-256	133,75	36,44	6,04	1,00	186,66	1,93	1,381	1.00	182
KCIPHER	131,29	11,061	3,3258	1.00	186,71	0,489	0,699	1,00	186
MICKEY_2	133,53	61,65	7,85	1,00	186,6	2,302	1,51	1,00	179
MUGI	132,23	53,721	7,329	1.00	186,5	0,978	0,989	1.00	185
RABBIT	132,65	16,87	4,017	1,00	187,22	0,451	0,657	1,00	185
RC4	133,7	67,01	8,186	1,00	186,3	1,61	1,269	1,00	184
SALSA20	134,16	28,055	5,27	1,00	187,001	1,01	0,99	1,00	183
SNOW2.0	132.78	23.93	4.89	1.00	186.79	0.43	0.656	1.00	183
SOSEMANUK	131,73	49,36	6,991	1,00	186,8	2,240	1,49	1,00	184
STRUMOK_256	130,01	23,6	4,86	1.00	186,45	1,4555	1,206	1.00	184
STRUMOK 512	132,83	56,516	7,518	1.00	186,90	0,802	0,896	1.00	185
TRIVIUM	130,24	99,683	9,935	1,00	187,15	1,49	1,214	1,00	182

В табл. 2 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 дисперсії (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 шифрів підтверджують їх високі криптографічні властивості. Зокрема, всі досліджувані криптоперетворення показали високе число успішно пройдених тестів: 130 – 134 за критерієм $P_j \geq 0{,}99$ та 186 – 187 за критерієм $P_j \geq 0{,}96$ (окрім CryptMT, який отримав результат 158). Ці оцінки отримано з дуже високою достовірністю, наприклад, $P_o = 0{,}99$ для критерію $P_j \geq 0{,}99$ та $P_o \approx 1$ для критерію $P_j \geq 0{,}96$. Мінімальні

значення числа пройдених статистичних тестів коливаються від 179 до 186 тестів. Найбільше число пройдених тестів показав KCipher.

Слід відмітити високі показники статистичної безпеки алгоритму ПСШ «Струмок», який виявив певні властивості генератору випадкових бітів. Зокрема за результатами даних табл. 2 видно, що формовані ПВП за своїми властивостями не поступаються ПВП, які сформовано всесвітньо відомими потоковими криптографічними алгоритмами, зокрема шифрами HC-256 та SNOW 2.0. Крім того, для ПСШ «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 алгоритму.

Набір статистичних тестів DIEHARD запропоновано у 1995 році Джорджем Марсальгія [21]. DIEHARD розглядаються як набір тестів з найбільш суворими критеріями до властивостей послідовності. Тести DIEHARD мають на меті характеризувати випадковість (або її відсутність) в послідовності цілих чисел, сформованих певним генератором псевдовипадкових послідовностей.

Специфічною властивістю системи DIEHARD є практична спрямованість тестів, тобто в основі деяких тестів лежать не теоретичні розрахунки оцінки статистичної безпеки, а оцінка результатів на основі проведених раніше автором практичних випробувань. Завдяки специфічній побудові цей пакет відрізняється тим, що для нього важко сформувати погану послідовність, яка не задовольняє вимогам випадковості, проте успішно б пройшла усі тести.

До складу DIEHARD входить 12 алгоритмів тестування:

1) *Дні народження (Birthday Spacings).* Обираються випадкові точки на великому інтервалі. Відстані між точками повинні бути асимптотично розподілені за Пуассоном. Назву цей тест отримав на основі парадоксу днів народження.

2) *Перестановки, що пересікаються (Overlapping Permutations).* Аналізуються послідовності п'яти послідовних випадкових чисел. 120 можливих перестановок повинні зустрічатися зі статистично еквівалентної ймовірністю.

3) *Тести бітового потоку (Monkey Tests, Bitstream test).* Послідовності з деякої кількості біт інтерпретуються як слова. Вважаються слова, що пересікаються, в потоці. Кількість «слів», які не з'являються, повинні задовольняти відомому розподілу. Назву цей тест отримав на основі теореми про нескінченну кількість мавп.

4) *Ранги матриць (Ranks of matrices).* Обираються кілька біт з деякої кількості випадкових чисел для формування матриці над {0,1}, потім визначається ранг матриці.

5) *Підрахунок одиниць (Count the 1's).* Підраховуються поодинокі біти в кожному з наступних або обраних байт.

6) *Тест на парковку (Parking Lot Test).* Одиничні окружності випадково розміщуються в квадраті 100 × 100. Якщо окружність перетинає вже існуючу, робиться спроба повторного розміщення окружності. Після 12 000 спроб, кількість успішно «припаркованих» кіл повинна бути нормально розподілена.

7) *Тест на мінімальну відстань (Minimum Distance Test).* 8000 точок випадково розміщуються в квадраті 10 000 × 10 000, потім знаходиться мінімальна відстань між будь-якими парами. Квадрат цієї відстані повинен бути експоненційно розподілений з деякою медіаною.

8) *Тест випадкових сфер (Random Spheres Test).* Випадково вибираються 4000 точок в кубі з ребром 1000. У кожній точці поміщається сфера, чий радіус є мінімальною відстанню до іншої точки. Мінімальний об`єм сфери повинен бути експоненційно розподілений з деякою медіаною.

9) *Тест стиснення (The Squeeze Test).* 2^{31} множиться на випадкові дійсні числа в діапазоні [0,1) до тих пір, доки не вийде 1. Повторюється 100 000 раз. Кількість дійсних чисел необхідних для досягнення 1 повинна бути розподілена певним чином.

10) *Тест сум, що пересікаються (Overlapping Sums Test).* Генерується довга послідовність дійсних чисел з інтервалу [0,1). У ній підсумовуються кожні 100 послідовних чисел. Суми повинні бути нормально розподілені з характерними середнім і дисперсією.

11) *Тест послідовностей (Runs Test).* Генерується довга послідовність на інтервалі [0,1). Підраховуються висхідні і низхідні послідовності. Числа повинні задовольняти деякого розподілу.

12) *Тест гри в кості (The Craps Test).* Граються 200 000 ігор в кістки, підраховуються перемоги і кількість кидків в кожній грі. Кожне отримане число має задовольняти деякому розподілу.

До складу програмної реалізації DIEHARD в залежності від вхідних даних загалом входить 215 тестів. Для оцінки результатів їх проходження використовують сукупну оцінку ймовірності з використанням критерію Колмогорова – Смирнова (KS), тобто значення декількох P_j згортаються на остаточну оцінку, використовуючи KS-тести. Критерій KS може використовуватися в тому випадку, коли результати випробувань становлять нескінчену множину. Його сутність полягає в наступному. Нехай у результаті n випробувань були отримані значення $X_i, i=\overline{1,n}$. Побудуємо емпіричну функцію розподілу

$$F_n(x)=\frac{1}{n}\sum_{i=1}^{n} X_i \le x .$$

Критерій KS визначає, наскільки емпірична функція розподілу $F_n(x)$ відрізняється від функції розподілу $F(x)$, яка визначає ймовірність того, що випадкова величина X матиме значення, менше або рівне x для заданого розподілу. Однак розрахунки цього критерію досить трудомісткі, тому замість критерію KS у математичній статистиці використовується критерій Андерсона – Дарлінга.

За критерієм Андерсона – Дарлінга приймається, що було проведено n випробувань й отримано статистики $X_i, i=\overline{1,n}$. В тесті DIEHARD результатом проведення тесту є ймовірність P_j. Якщо розташувати ці величини за зростанням, отримаємо

$$P_1 \le P_2 \le P_3 \le \ldots \le P_n .$$

В такому випадку тестова статистика приймає значення

$$A^2 = -n - \sum_{j=1}^{n} \frac{2j-1}{n}\left[\ln P_j + \ln P_{n+1-j}\right].$$

Остаточна оцінка ймовірності визначається як

$$P_{jKS}=\begin{cases} 0, & A^2 < \alpha \\ 2e^{-\frac{1.2337}{A^2}}\left(1+\frac{A^2}{2^3}-\frac{0.04958\left(A^2\right)^2}{1.325+A^2}\right), & \alpha \le A^2 < 2 \\ 1-0.6621361\cdot e^{-1.091638\cdot A^2}-0.95095\cdot e^{-2.005138\cdot A^2}, & 2 \le A^2 < 4 \\ 1-0.4938691\cdot e^{-1.050321\cdot A^2}-0.5946336\cdot e^{-1.527198\cdot A^2} & A^2 \ge 4 \end{cases},$$

де α – рівень значущості.

Таким чином, для оцінки проходження певного *j*-тесту використовуються значення ймовірності P_j або ймовірність отримана за критерієм Андерсона – Дарлінга P_{jKS}.

Відомо, що при тестуванні статистичних властивостей дійсно випадкової послідовності характерною властивістю є рівномірний розподіл отриманих ймовірностей проходження тестів. Тобто, серед усіх отриманих значень ймовірностей P_j їх розподіл має бути рівномірним на одиничному інтервалі. Відхилення від рівномірного розподілу вказують на те, що деякі з тестів DIEHARD виявили впорядковані шаблони у послідовності, що тестується. Якщо отримані 215 значень ймовірностей P_j, впорядковані за зростанням, представити у вигляді графіку, можна наочно визначити будь-які, навіть незначні, відхилення від рівномірного розподілу. Приклад результатів тестування «поганої», в статистичному сенсі, послідовності наведено на рис. 1. Ця послідовність була сформована стандартним генератором випадкових чисел для мови C++. З розподілу зрозуміло, що відповідний генератор не може використовуватися в якості частини реалізації криптографічного алгоритму шифрування.

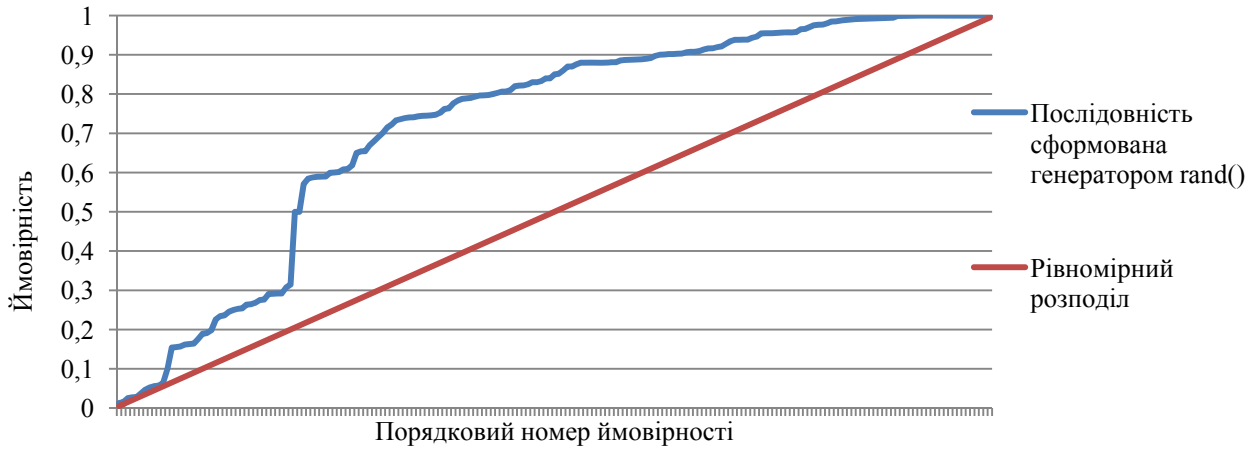

Рис. 1. Розподіли ймовірностей «поганої» послідовності

Результати статистичного тестування пакетом DIEHARD для симетричних шифрів AES, CryptMT, DECIM, Enocoro, Grain, HC, KCipher, Mickey2, MUGI, Rabbit, RC4, Salsa20, Snow 2, Sosemanuk, Trivium та ПСШ «Струмок» у вигляді розподілів ймовірностей на одиничному інтервалі наведено на рис. 2 – 19. На рис. 20 – 37 зображено статистичні портрети результатів тестування пакетом DIEHARD для симетричних шифрів.

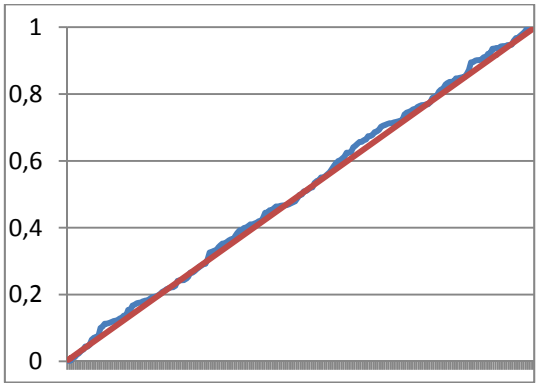

Рис. 2. AES-128

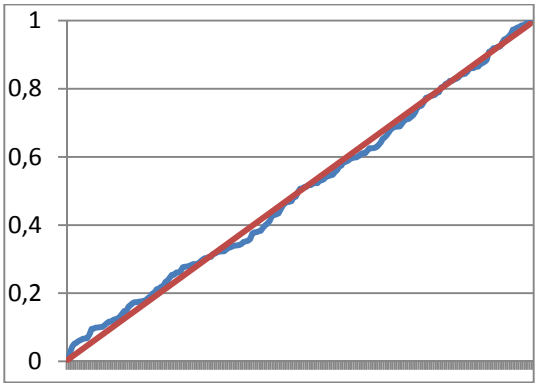

Рис. 3. AES-256

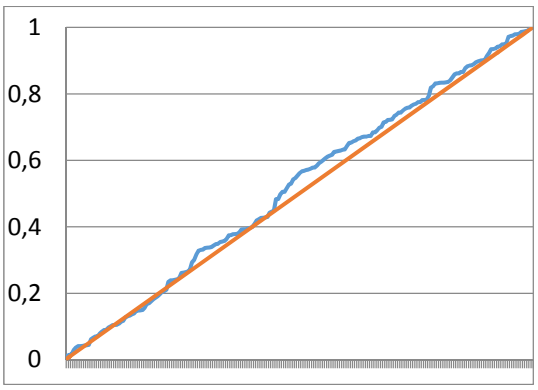

Рис. 4. CryptMT

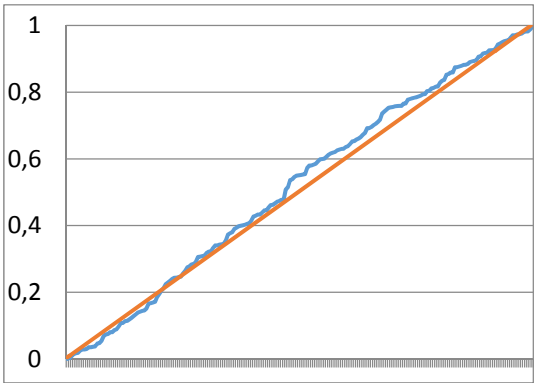

Рис. 5. DECIM

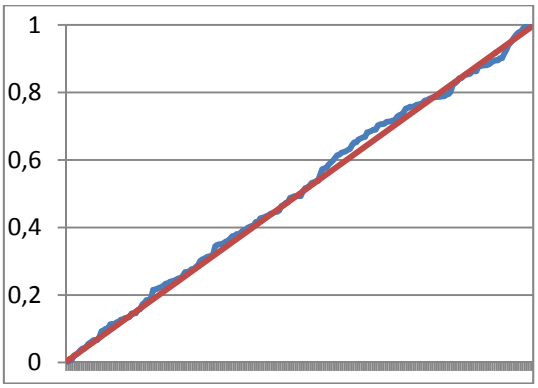

Рис. 6. Enocoro

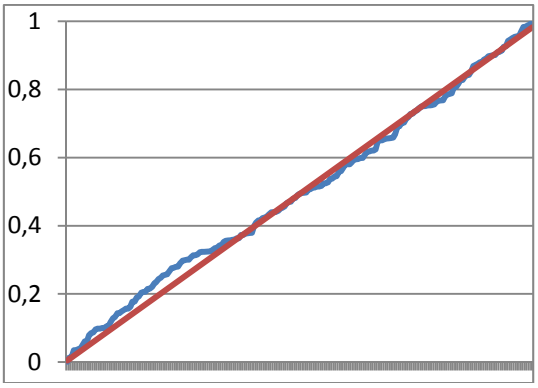

Рис. 7. Grain

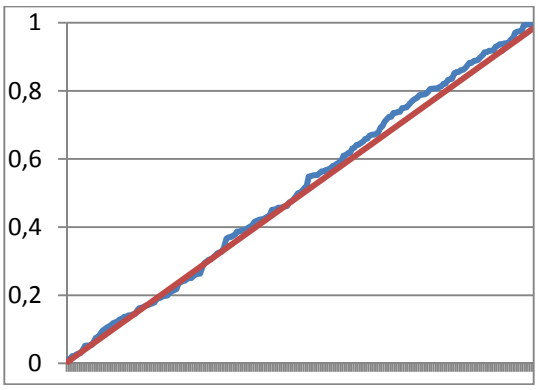

Рис. 8. HC-128

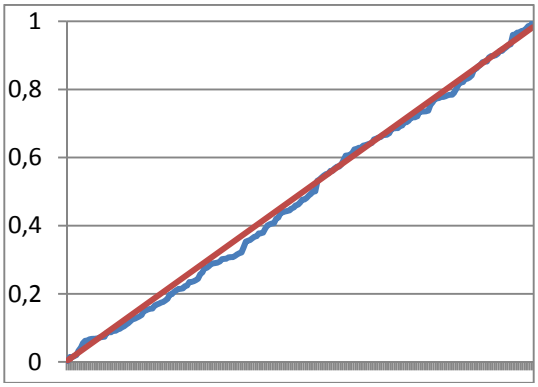

Рис. 9. HC-256

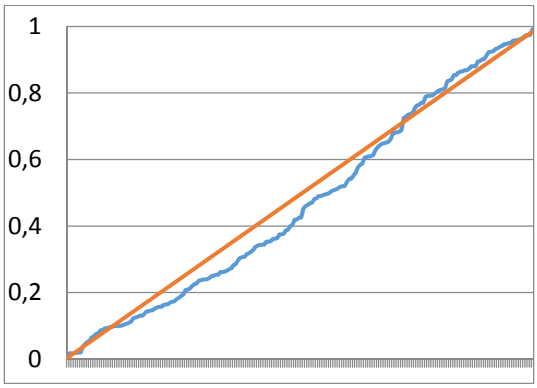

Рис. 10. KCipher

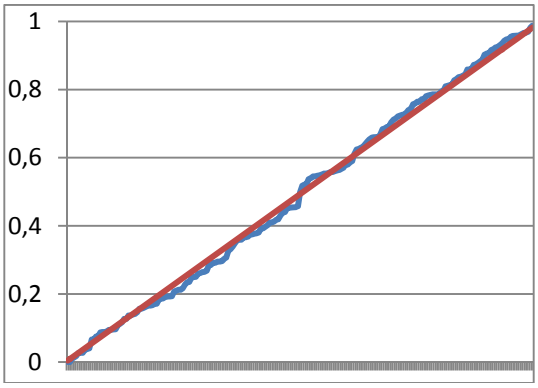

Рис. 11. Mickey2

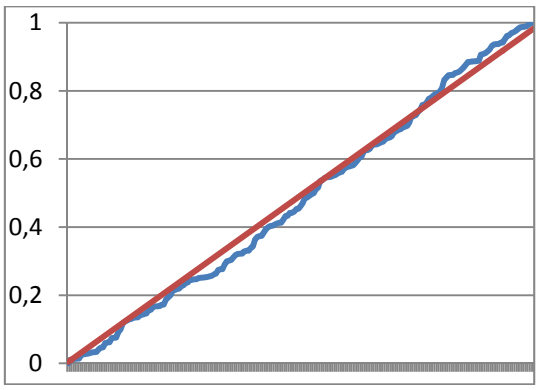

Рис. 12. MUGI

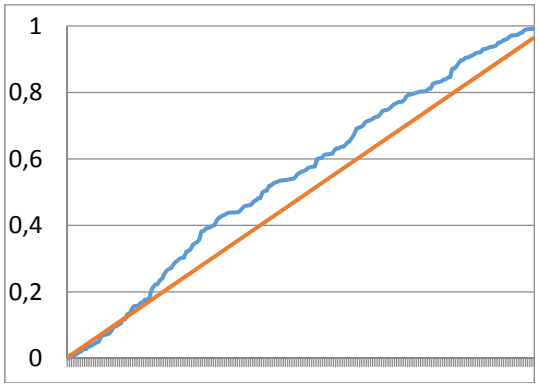

Рис. 13. RC4

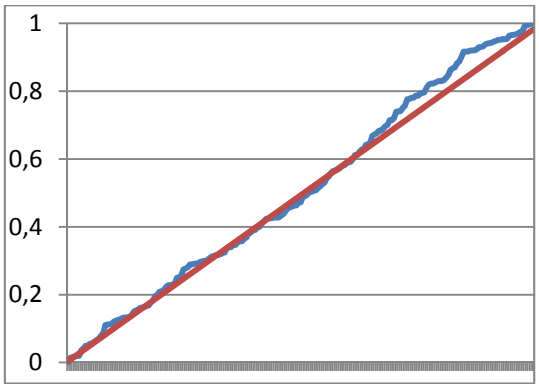

Рис. 14. Salsa20

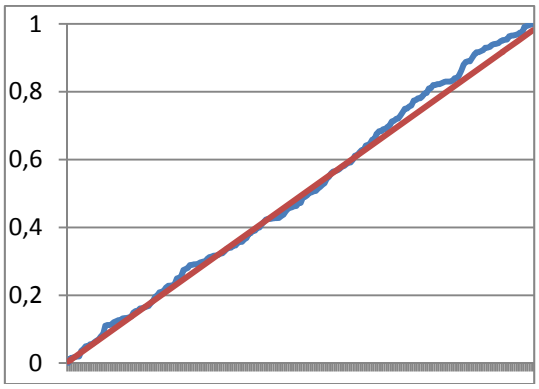

Рис. 15. Snow 2

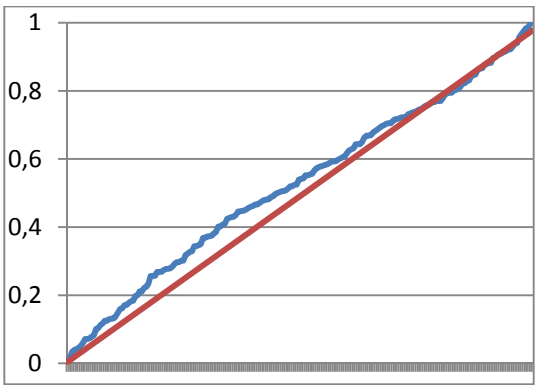

Рис. 16. Sosemanuk

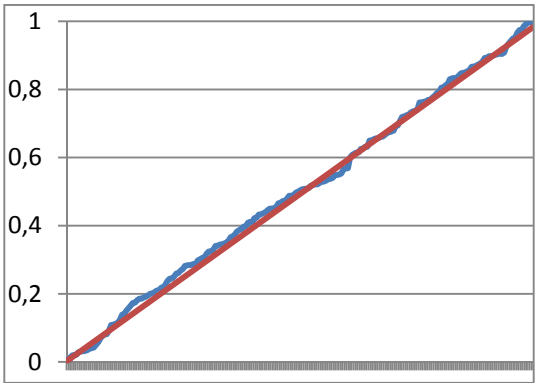

Рис. 17. «Струмок-256»

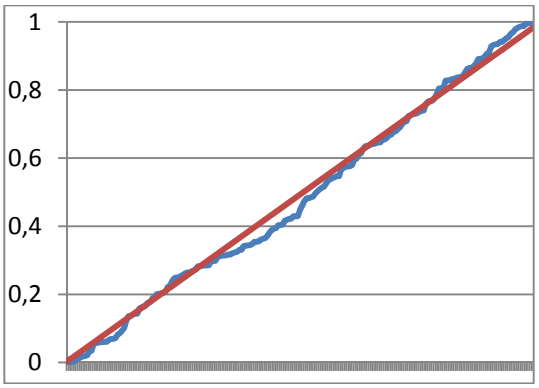

Рис. 18. «Струмок-512»

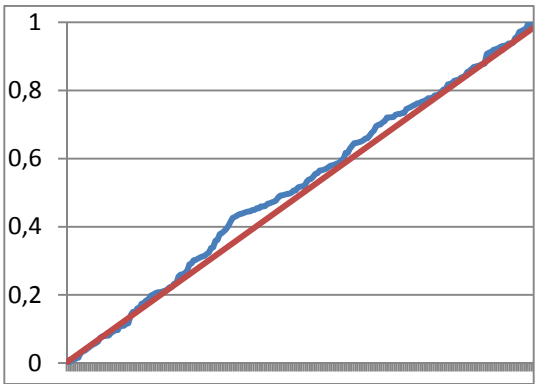

Рис. 19. Trivium

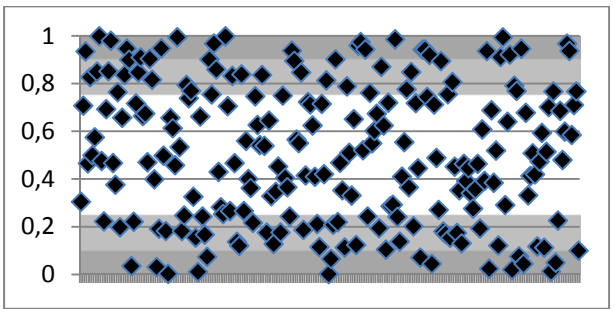

Рис. 20. AES-128

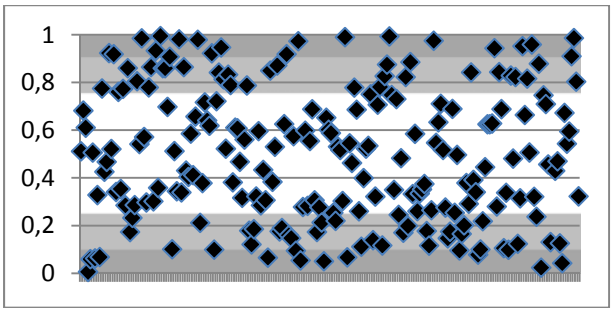

Рис. 21. AES-256

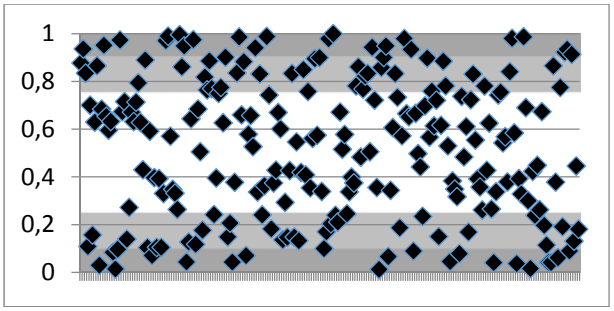

Рис. 22. CryptMT

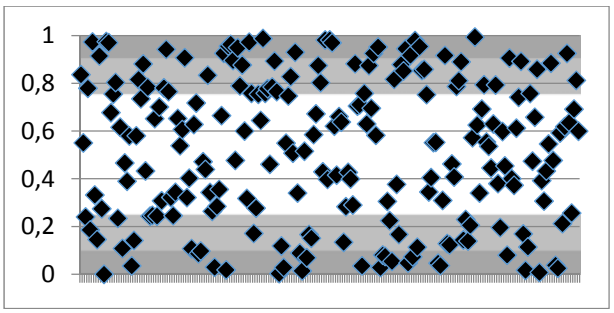

Рис. 23. DECIM

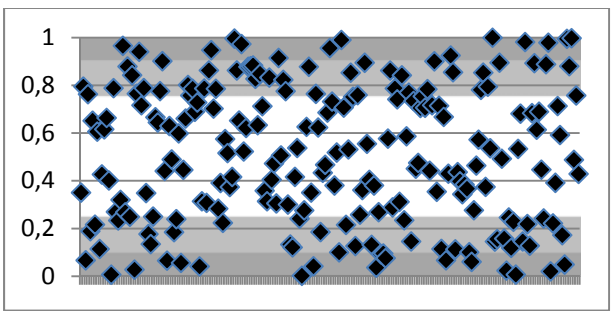

Рис. 24. Enocoro

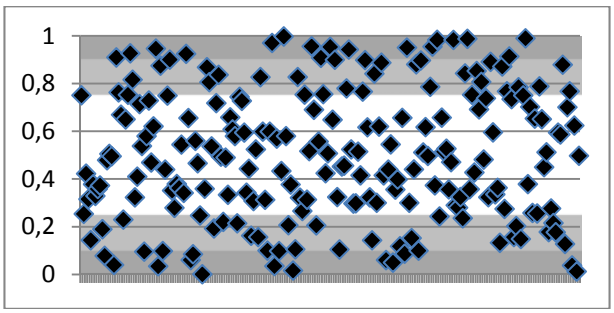

Рис. 25. Grain

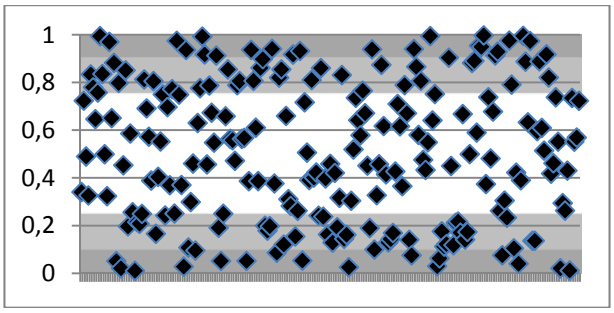

Рис. 26. HC-128

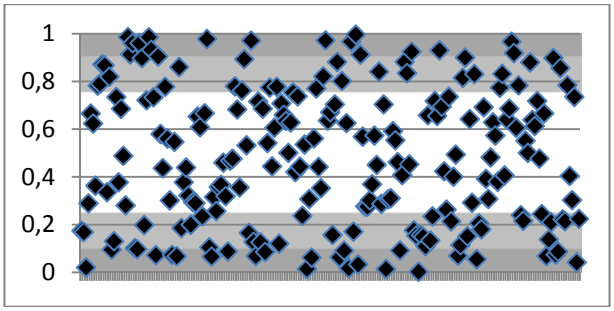

Рис. 27. HC-256

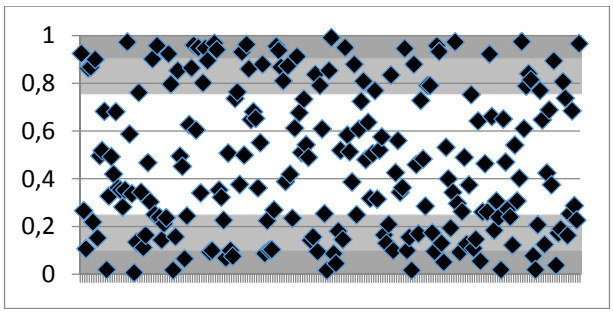

Рис. 28. KCipher

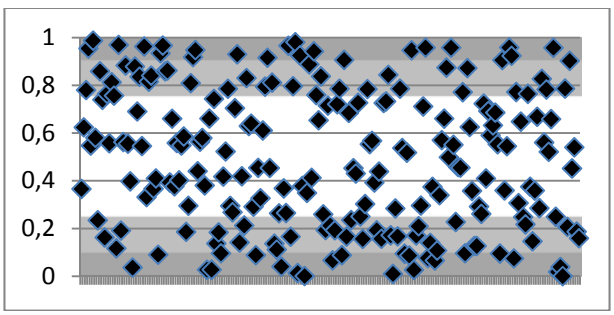

Рис. 29. Mickey2

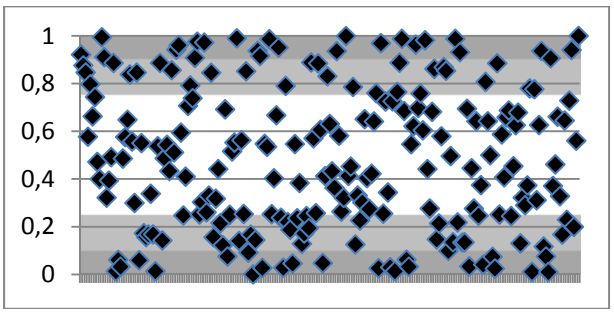

Рис. 30. MUGI

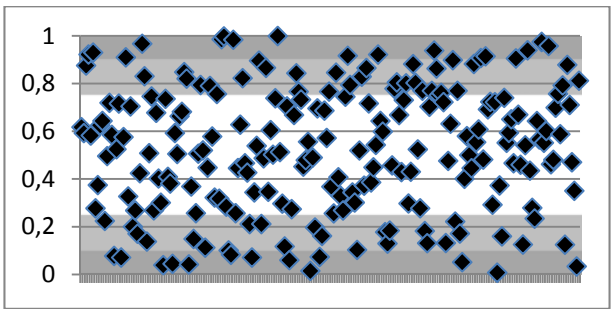

Рис. 34. Sosemanuk

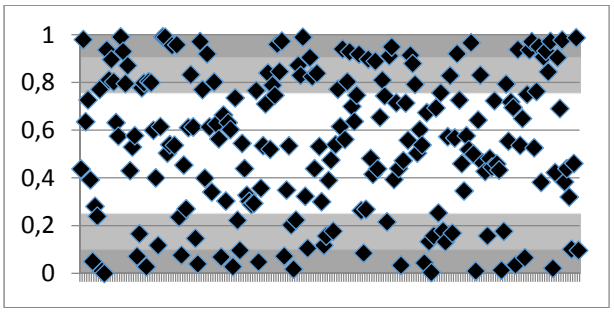

Рис. 31. RC4

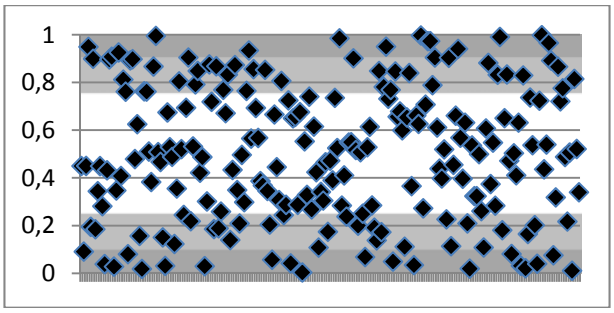

Рис. 35. «Струмок-256»

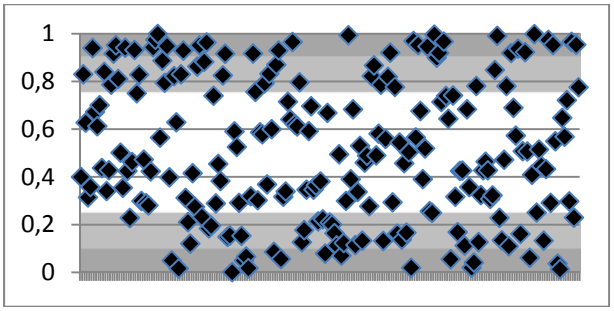

Рис. 32. Salsa20

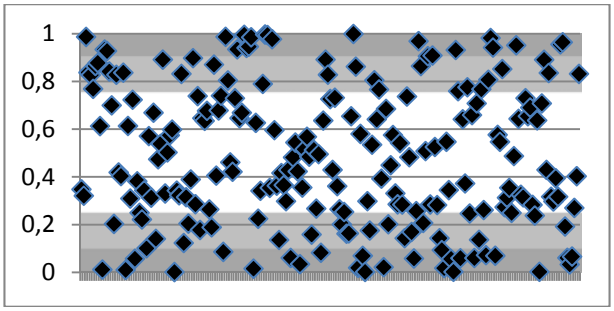

Рис. 36. «Струмок-512»

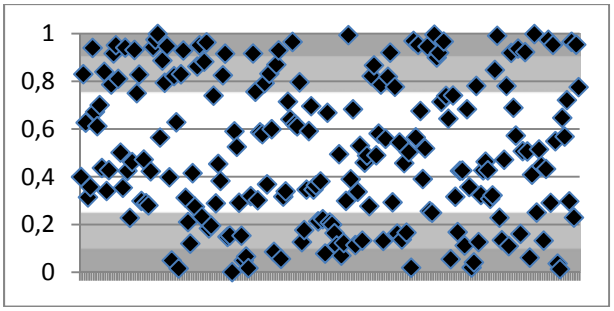

Рис. 33. Snow 2

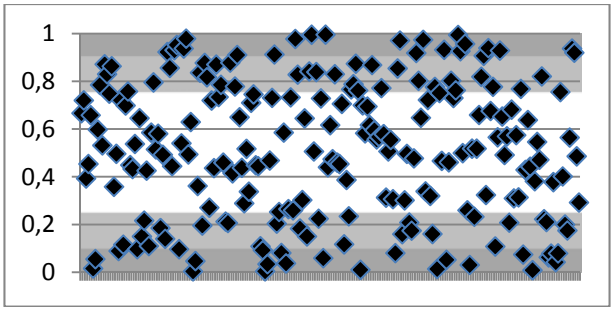

Рис. 37. Trivium

Розподіл ймовірностей на одиничному інтервалі дає можливість приблизно оцінити випадковість послідовності, що була протестована, на відповідність до розподілу дійсно випадкової послідовності. Можна побачити, що розподіл ймовірностей для більшості шифрів відповідає рівномірному розподілу з невеликими флуктуаціями.

Для оцінки статистичних властивостей за результатами проходження тестів в [22] використовується дещо інший підхід. Умовно розділимо одиничний відрізок на декілька підінтервалів. Якщо ймовірність належить певному інтервалу це характеризує проходження j-го тесту як:

1) провал тесту, при ймовірності $P_j \le 0.1$ або $P_j > 0.9$
2) результати тесту сумнівні, якщо ймовірність належить до одного із під інтервалів $0.1 < P_j \le 0.25$ або $0.75 < P_j \le 0.9$;
3) тест пройдено, якщо ймовірність приймає значення $0.25 < P_j \le 0.75$.

Очевидно, що у випадку, коли більшість результатів належить інтервалу (0.25,0.75] можна вважати, що послідовність має достатні статистичні властивості у порівнянні з дійсно випадковою. Якщо переважна більшість результатів належить інтервалам (0,0.25) та [0.9,1) послідовність, що тестується можна вважати поганою в статистичному сенсі.

Підрахована кількість ймовірностей проходження тестів для кожного з зазначених шифрів зведена до табл. 3.

Таблиця 3

Кількість результатів проходження тестів розподілених за п'ятьма інтервалами

Ймовірність / Шифр	$P_j \le 0.1$	$0.1 < P_j \le 0.25$	$0.25 < P_j \le 0.75$	$0.75 < P_j \le 0.9$	$P_j > 0.9$
AES-128	16	37	109	28	25
AES-256	15	33	115	31	21
CRYPTMT	21	34	99	36	25
DECIM	25	29	93	42	26
ENOCORO	18	36	102	43	16
GRAIN	17	26	122	31	19
HC-128	17	37	103	36	22
HC-256	25	33	109	30	18
KCIPHER-2	25	41	90	39	20
MICKEY2	21	35	104	32	23
MUGI	25	33	107	27	23
RC4	23	21	104	35	32
SASLA20	17	33	106	27	32
SNOW 2.0	21	31	112	33	18
SOSEMANUK	13	25	126	34	17
STRUMOK 256	20	29	113	35	18
STRUMOK 512	26	26	113	28	22
TRIVIUM	24	27	107	35	22

Усі шифри показали достатній рівень статистичної безпеки. Для наочності кількість тестів, які пройдено, тобто у яких результат належить до інтервалу $0.25 < P_j \le 0.75$, зведено до гістограми на рис. 38.

Не дивлячись на те, що шифр Sosemanuk за результатами відповідності розподілу ймовірностей до рівномірного показав незначні, але дещо більші на відміну від інших шифрів, відхилення від рівномірного розподілу, за результатами останнього тесту займає провідну позицію. Також слід відмітити, що за кількістю пройдених статистичних тестів пакету NIST STS шифр KCipher займав першу позицію, але у тестуванні DIEHARD він на останньому місці.

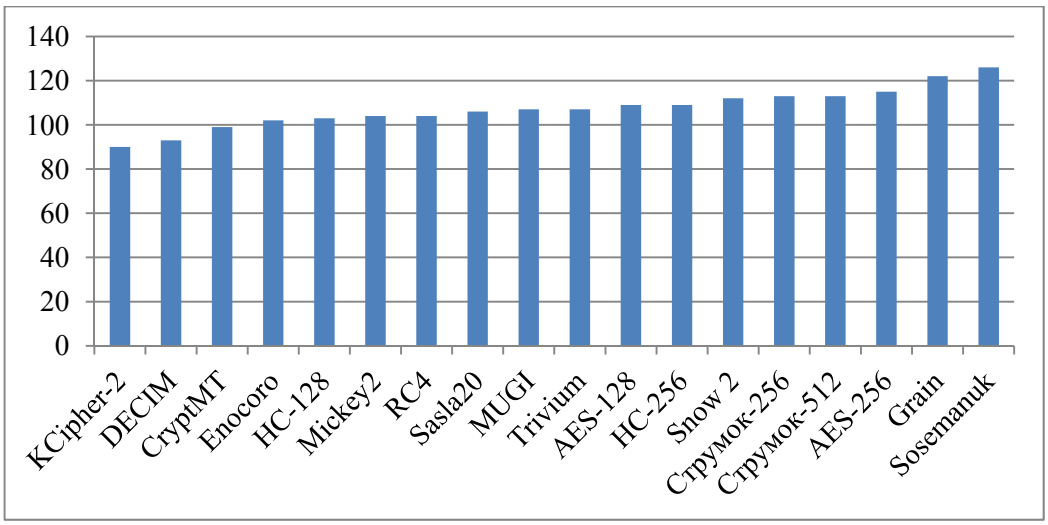

Рис. 38. Кількість успішно пройдених статистичних тестів DIEHARD

Порівняльні дослідження швидкодії алгоритмів потокового шифрування

Важливою характеристикою сучасних криптографічних засобів захисту інформації є показники швидкодії, які характеризують здатність криптосистеми обробляти великі обсяги даних за встановлений час. В цьому розумінні важливим є дослідження швидкісних характеристик потокових шифрів, їх порівняння за різними критеріями, які відображають здатність криптопримітивів до швидкої обробки різних за обсягами масивів даних [1 – 5, 11].

В цій роботі аналіз швидкодії потокових шифрів проводиться за методикою, яка була запропонована на всесвітньовідомому конкурсі eSTREAM [8]. Ця методика полягає у тестуванні за різними реальними ситуаціями, які можуть виникати у каналах передачі інформації, передбачено наступні критерії:

1. Критерій зашифрування довгих потоків. Поточні шифри мають найбільш потенційну перевагу над блочними шифрами при зашифруванні довгих потоків;
2. Критерій зашифрування коротких потоків. Цей показник відображає швидкість зашифрування пакетів різної (зазвичай, невеликої) довжини;
3. Критерій ініціалізації/генерації ключових параметрів. Ця характеристика окремо відображає ефективність встановлення ключа та вектору ініціалізації.

Усі шифри були реалізовані за допомогою ЕОМ з процесором Intel(R) Pentium(R) CPU P6200 @ 2.13GHz, 2128, RAM: 2 по 2 ГБ(з частотою 1333МГц), КЕШ: 1-го рівня (128 Кб); 2-го рівня (512 Кб); 3-го рівня (3072 Кб) в операційній системі Windows 8.1 Професійна 64bit, на компіляторі Microsoft Visual Studio 2012 32bit версії 11.00.50727.1.

Після реалізації обраних шифрів усі шифри були запущені на різних за потужністю/продуктивністю процесорах, на різних платформах, реалізованих на різних мовах програмування та компіляторах. Результати тестування представлено нижче.

Тестування за критерієм швидкості зашифрування довгих потоків. Однією з областей, де можуть використовуватися поточні шифри, є шифрування довгих потоків. Ця задача виникає при шифруванні даних об’ємних носіїв інформації, зокрема жорсткого диску [8]. Наприклад, для забезпечення конфіденційності особистих даних користувачі можуть шифрувати носії інформації, але платою за це є зниження швидкості роботи операційної системи.

Для визначення показників швидкості сучасних шифрів проведено експериментальні дослідження, в яких використано програмне забезпечення VeraCrypt та TrueCrypt для шифрування дискового простору [23, 24]; виконано стандартні тести перевірки швидкості шифрування для усіх можливих реалізованих алгоритмів. Експеримент проводився у наступних умовах: згенерували об’єм даних у розмірі 1 Гб та шифри: AES, Twofish, AES-

Twofish, SERPENT, SERPENT-AES, AES-Twofish-SERPENT, SERPENT-Twofish-AES, Twofish-SERPENT, зашифровували та розшифровували дані. Отримані експериментальні результати продемонстровано на рис. 39 та 40.

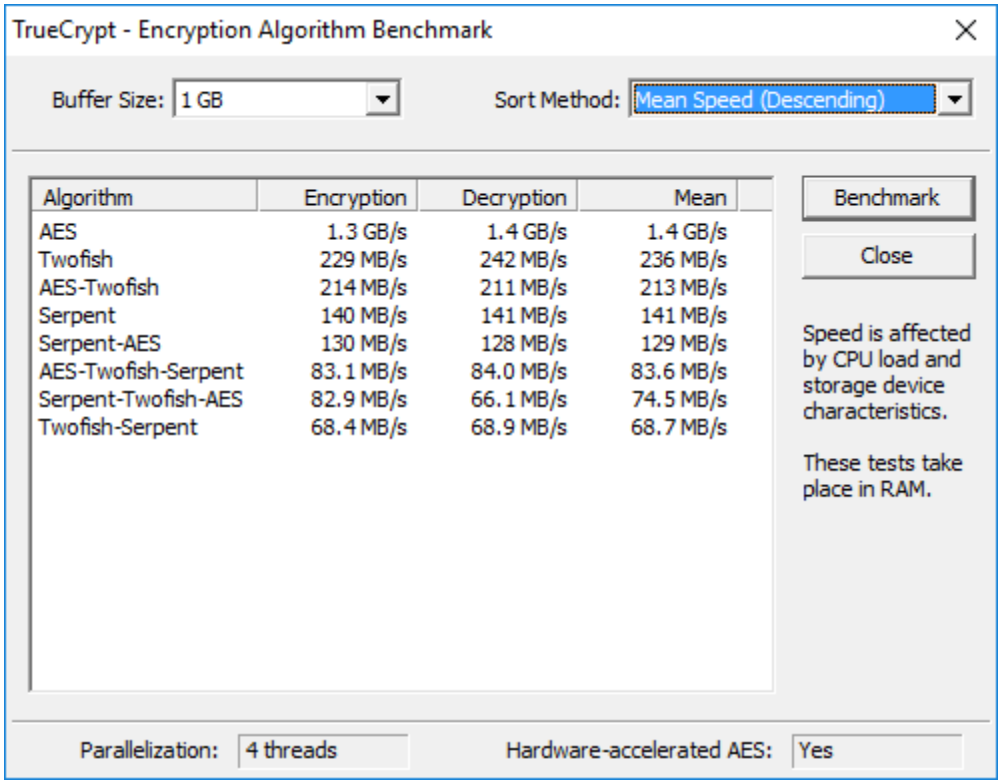

Рис. 39. Результати експериментальних досліджень за допомогою TrueCrypt

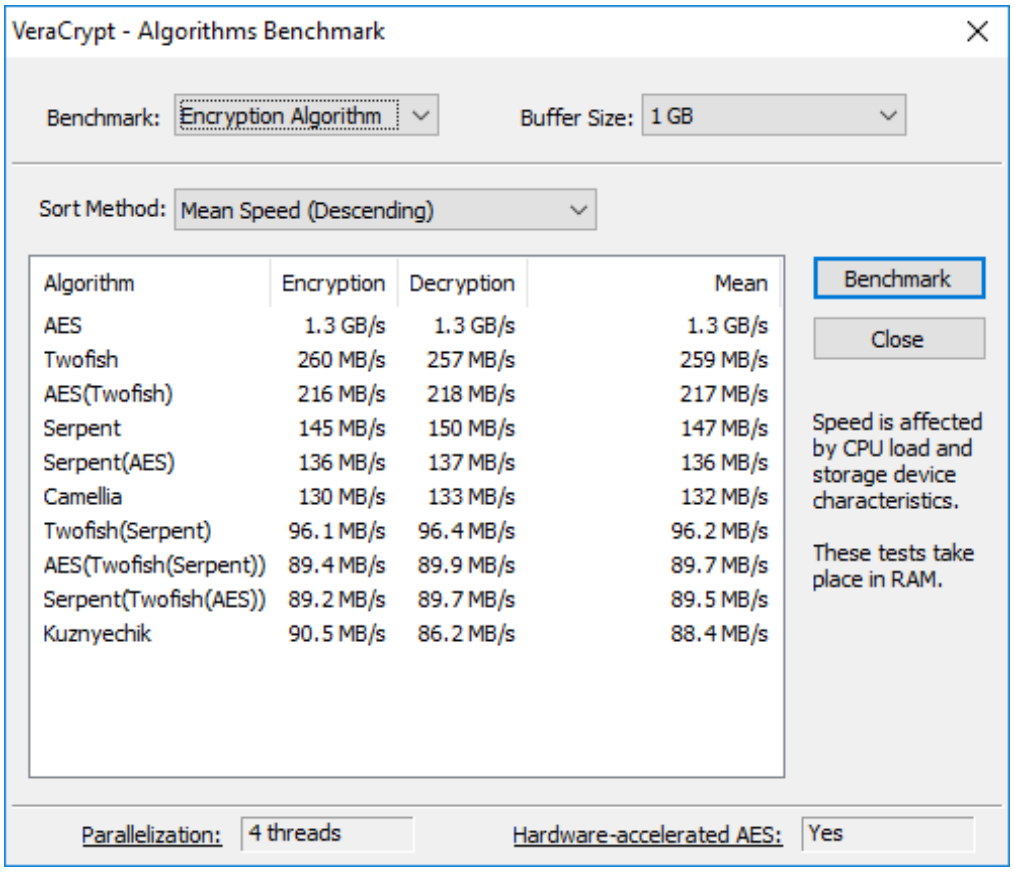

Рис. 40. Результати експериментальних досліджень за допомогою VeraCrypt

Критерій шифрування довгих потоків характерний саме для потокових шифрів, тому увага до цих показників приділяється в першу чергу. За методикою дослідження випадковим чином генеруються дані об'ємом у 1 Гб, потім випадково генерується один ключ та за допомогою вектору ініціалізації встановлюється випадковий стан регістрів. Наступним кроком відбувається безпосередньо шифрування 1 Гб даних, та вимірюється час протікання процесу шифрування і пропускна здатність алгоритму (кількість байт, зашифрованих за одну мікросекунду). Результати зібрані у табл. 4. Найкращі показники за критерієм шифрування довгих повідомлень показали «Струмок», HC-128 та "SNOW 2.0".

Таблиця 4

Результати експериментальних досліджень швидкісних характеристик шифрів на різних за потужністю процесорах

Назва шифру	Зашифрування 1GB (Intel Core i7-6820HQ 2.7Gh)		Зашифрування 1GB (Intel Core i7-5500u 2.4Gh)		Зашифрування 1GB (Intel Pentium P6200 2.13Gh)	
	Час, ms	Швидкість, bytes / µs	Час, ms	Швидкість, bytes / µs	Час, ms	Швидкість, bytes / µs
AES-128	3229	332,51	4570	234,97	9787	109,72
AES-256	4819	236,83	6766	158,69	14133	75,98
HC-128	698	1537,65	1040	1032,25	2073	518,09
HC-256	1559	688,83	2061	521,08	4465	240,47
MICKEY-128	116786	9,19	164304	6,54	265471	4,05
RABBIT	2190	490,27	2893	371,22	5656	189,85
SALSA-20	2650	405,26	3885	276,40	8428	127,40
SNOW2.0-128	913	1176,19	1474	728,50	2924	367,18
SNOW2.0-256	917	1170,80	1445	742,87	2989	359,22
SOSEMANUK	1967	545,82	3124	343,69	4973	215,91
STRUMOK 256	601	1788,08	797	1347,06	3648	294,33
STRUMOK 512	584	1839,54	821	1308,01	3677	292,03
TRIVIUM	2058	521,72	2879	372,93	5016	214,05
CryptMT3	1351	794,83	1728	621.378370	1981	541,97
DECIM-128	703486	1,53	815187	1,32	994679	1,08
RC4	2232	481,07	2491	431,05	4786	224,35
KCIPHER-2	20253	53,02	20253	53,02	25986	41,32
GRAIN	1263313	0,85	1456900	0,74	1864210	0,58
MUGI	2207	486,45	2685	399,95	3098	346,57

Беручу до уваги результати експериментальних досліджень швидкісних характеристик шифрів на різних за потужністю процесорах, можна побачити, що на процесорах з невеликою частотою шифр «Струмок» програє у швидкості, але на більш потужних процесорах швидкість зростає. Цей програш, насамперед, обумовлений більшим розміром блоку ніж у інших алгоритмів, на який витрачається більше часу обчислення процесором математичних операцій.

Тестування за критерієм швидкості зашифрування коротких потоків. Швидкість зашифрування довгих потоків є основною характеристикою блокових шифрів, яка відображає спроможність криптопримітиву функціонувати за своїм цільовим призначенням. Тому при тестуванні потокових шифрів цей критерій досліджується для визначення

поведінки структури алгоритмів, визначення слабких сторін та виявлення переваг і недоліків певних шифрів.

Критерій зашифрування коротких потоків відповідно до методики дослідження відображає швидкість зашифрування пакетів різної довжини (40 байт, 576 байт та 1500 байт), які репрезентовано відображають трафік телекомунікаційного каналу передачі інформації. Тобто ці дослідження є певною імітацією функціонування потокового шифру при його використанні для шифрування трафіку сучасних телекомунікаційних систем із комутацією пакетів.

Відповідно до методики дані пакетів генеруються випадковим чином. При тестуванні вимірюється час шифрування пакетів, швидкість зашифрованих байт на мікросекунду та швидкість зашифрованих пакетів на мікросекунду.

Результати тестування за критерієм шифрування коротких повідомлень зведено у табл. 5 – 7.

За узагальненням цих даних можна зробити наступні висновки:

– найкращі показники за критерієм зашифрування коротких потоків отримано для шифрів «Струмок», «SNOW 2.0» та «SOSEMANUK» відповідно;

– отримані показники демонструють те, що шифри «SNOW 2.0» та «SOSEMANUK» показують кращі показники у випадку, коли пакетів багато але малих за розміром даних;

– щодо потокового шифру «Струмок» маємо зворотні результати: шифр демонструє кращі показники, коли пакетів мало, але вони великі за розміром.

Таблиця 5

Експериментальні результати дослідження за критерієм шифрування коротких повідомлень (Intel Core i7-6820HQ 2.7Gh)

Назва шифру	Зашифрування пакетів								
	50 пакетів по 1500 байт			120 пакетів по 576 байт			350 пакетів по 40 байт		
	Час, μs	Швидкість, bytes / μs	Швидкість, packets / μs	Час, μs	Швидкість, bytes / μs	Швидкість, packets / μs	Час, μs	Швидкість, bytes / μs	Швидкість, packets / μs
AES-128	230	326,09	0,2174	211	327,58	0,5687	60	233,33	5,8333
AES-256	323	232,20	0,1548	300	230,40	0,4000	81	172,84	4,3210
HC-128	257	291,83	0,1946	546	126,59	0,2198	1492	9,38	0,2346
HC-256	1420	52,82	0,0352	3413	20,25	0,0352	9605	1,46	0,0364
MICKEY-128	7819	9,59	0,0064	7542	9,16	0,0159	3532	3,96	0,0991
RABBIT	154	487,01	0,3247	158	437,47	0,7595	88	159,09	3,9773
SALSA-20	190	394,74	0,2632	175	394,97	0,6857	58	241,38	6,0345
SNOW2.0-128	70	1071,43	0,7143	71	973,52	1,6901	64	218,75	5,4688
SNOW2.0-256	71	1056,34	0,7042	71	973,52	1,6901	64	218,75	5,4688
SOSEMANUK	91	824,18	0,5495	102	677,65	1,1765	79	177,22	4,4304
STRUMOK 256	49	1530,61	1,0204	60	1152,00	2,0000	76	184,21	4,6053
STRUMOK 512	50	1500,00	1,0000	61	1133,11	1,9672	75	186,67	4,6667
TRIVIUM	153	490,20	0,3268	168	411,43	0,7143	128	109,38	2,7344
CryptMT3	120	625,00	0,4167	183	377,70	0,6557	227	61,67	1,5419
DECIM-128	50291	1,49	0,0010	46635	1,48	0,0026	13122	1,07	0,0267
RC4	155	483,87	0,3226	149	463,89	0,8054	38	368,42	9,2105
KCIPHER-2	680	110,29	0,0735	1063	65,02	0,1129	745	18,79	0,4698
GRAIN	108503	0,69	0,0005	1000586	0,07	0,0001	34241	0,41	0,0102
MUGI	177	423,73	0,2825	205	337,17	0,5854	212	66,04	1,6509

Таблиця 6

Експериментальні результати дослідження за критерієм шифрування коротких повідомлень (Intel Core i7-5500u 2.4Gh)

Назва шифру	Зашифрування пакетів								
	50 пакетів по 1500 байт			120 пакетів по 576 байт			350 пакетів по 40 байт		
	Час, µs	Швидкість, bytes / µs	Швидкість, packets / µs	Час, µs	Швидкість, bytes / µs	Швидкість, packets / µs	Час, µs	Швидкість, bytes / µs	Швидкість, packets / µs
AES-128	313	239,62	0,1597	291	237,53	0,4124	91	153,85	3,8462
AES-256	432	173,61	0,1157	406	170,25	0,2956	113	123,89	3,0973
HC-128	412	182,04	0,1214	844	81,90	0,1422	2241	6,25	0,1562
HC-256	2148	34,92	0,0233	4916	14,06	0,0244	14225	0,98	0,0246
MICKEY-128	10651	7,04	0,0047	10462	6,61	0,0115	4963	2,82	0,0705
RABBIT	210	357,14	0,2381	209	330,72	0,5742	105	133,33	3,3333
SALSA-20	262	286,26	0,1908	233	296,65	0,5150	77	181,82	4,5455
SNOW2.0-128	118	635,59	0,4237	117	590,77	1,0256	101	138,61	3,4653
SNOW2.0-256	110	681,82	0,4545	120	576,00	1,0000	103	135,92	3,3981
SOSEMANUK	150	500,00	0,3333	171	404,21	0,7018	122	114,75	2,8689
STRUMOK 256	66	1136,36	0,7576	82	842,93	1,4634	108	129,63	3,2407
STRUMOK 512	69	1086,96	0,7246	84	822,86	1,4286	126	111,11	2,7778
TRIVIUM	211	355,45	0,2370	238	290,42	0,5042	175	80,00	2,0000
CryptMT3	155	483,87	0,3226	229	301,83	0,5240	277	50,54	1,2635
DECIM-128	56987	1,32	0,0009	53800	1,28	0,0022	15067	0,93	0,0232
RC4	174	431,03	0,2874	172	401,86	0,6977	41	341,46	8,5366
KCIPHER-2	680	110,29	0,0735	1063	65,02	0,1129	745	18,79	0,4698
GRAIN	110360	0,68	0,0005	85329	0,81	0,0014	29499	0,47	0,0119
MUGI	225	333,33	0,2222	255	271,06	0,4706	248	56,45	1,4113

Таблиця 7

Експериментальні результати дослідження за критерієм шифрування коротких повідомлень (Intel Pentium P6200 2.13Gh)

Назва шифру	Зашифрування пакетів								
	50 пакетів по 1500 байт			120 пакетів по 576 байт			350 пакетів по 40 байт		
	Час, μs	Швидкість, bytes / μs	Швидкість, packets / μs	Час, μs	Швидкість, bytes / μs	Швидкість, packets / μs	Час, μs	Швидкість, bytes / μs	Швидкість, packets / μs
AES-128	383	195,82	0,1305	353	195,81	0,3399	100	140,00	3,5000
AES-256	538	139,41	0,0929	507	136,33	0,2367	141	99,29	2,4823
HC-128	452	165,93	0,1106	949	72,83	0,1264	2581	5,42	0,1356
HC-256	2530	29,64	0,0198	5769	11,98	0,0208	16320	0,86	0,0214
MICKEY-128	12803	5,86	0,0039	12625	5,47	0,0095	5923	2,36	0,0591
RABBIT	289	259,52	0,1730	284	243,38	0,4225	149	93,96	2,3490
SALSA-20	340	220,59	0,1471	313	220,83	0,3834	103	135,92	3,3981
SNOW2.0-128	124	604,84	0,4032	123	561,95	0,9756	117	119,66	2,9915
SNOW2.0-256	125	600,00	0,4000	141	490,21	0,8511	122	114,75	2,8689
SOSEMANUK	163	460,12	0,3067	183	377,70	0,6557	131	106,87	2,6718
STRUMOK 256	83	903,61	0,6024	103	671,07	1,1650	131	106,87	2,6718
STRUMOK 512	86	872,09	0,5814	104	664,62	1,1538	133	105,26	2,6316
TRIVIUM	275	272,73	0,1818	298	231,95	0,4027	227	61,67	1,5419
CryptMT3	180	416,67	0,2778	281	245,98	0,4270	369	37,94	0,9485
DECIM-128	71205	1,05	0,0007	67090	1,03	0,0018	19255	0,73	0,0182
RC4	333	225,23	0,1502	320	216,00	0,3750	78	179,49	4,4872
KCIPHER-2	971	77,24	0,0515	1409	49,06	0,0852	1028	13,62	0,3405
GRAIN	135271	0,55	0,0004	128127	0,54	0,0009	44250	0,32	0,0079
MUGI	253	296,44	0,1976	296	233,51	0,4054	317	44,16	1,1041

Тестування за критерієм швидкості ініціалізації/генерації ключових параметрів. Цей критерій окремо характеризує такий елемент структури шифрів, як встановлення ключа та вектору ініціалізації. Ці дві складові структури шифру є найменш критичні для відображання швидкості алгоритму, так як мало затрачується на встановлення ключа та вектору ініціалізації в порівнянні з процесом шифрування.

За методикою було визначено наступне: для оцінки схеми розгортання ключа потрібно зробити 7000 ключових установок, це 700 установок на один ключ (10 ключів на 700 установок). Для оцінки процесу ініціалізації початкового вектору визначено наступне: 500 ключових установок, це 50 установок на один вектор (10 векторів по 50 установок).

Для оцінки описаних параметрів буде фіксуватися загальний час виконання операції, кількість затрачених циклів на установку та кількість установок, яких можна зробити за одну секунду.

Отримані результати зведено у табл. 8 – 10.

Таблиця 8

Експериментальні результати дослідження шифрів за критерієм ініціалізація/генерація ключових параметрів (Intel Core i7-6820HQ 2.7Gh)

Назва шифру	Встановлення ключових параметрів			
	Ключ (7000 установок)		Вектор ініціалізації (500 установок)	
	Час, μs	Швидкість, кількість установок / μs	Час, μs	Швидкість, кількість установок / μs
AES-128	483	14,5	0,09	5555,6
AES-256	1075	6,5	0,06	8333,3
HC-128	22	318,2	2101,6	0,2
HC-256	339	20,6	13347,6	0,0
MICKEY-128	7	1000,0	2987,8	0,2
RABBIT	886	7,9	58,3	8,6
SALSA-20	25	280,0	0,09	5555,6
SNOW2.0-128	33	212,1	54,9	9,1
SNOW2.0-256	64	109,4	55,1	9,1
SOSEMANUK	1084	6,5	70,2	7,1
STRUMOK 256	33	212,1	62,4	8,0
STRUMOK 512	34	205,9	61,3	8,2
TRIVIUM	46	152,2	138	3,6
CryptMT3	223	31,4	281,4	1,8
DECIM-128	2	3500,0	7889	0,1
RC4	5793	1,2	-	-
KCIPHER-2	182	38,5	751	0,7
GRAIN	4	1750,0	18817,2	0,0
MUGI	1309	5,3	280,9	1,8

Таблиця 9

Експериментальні результати дослідження шифрів за критерієм ініціалізація/генерація ключових параметрів (Intel Core i7-5500u 2.4Gh)

Назва шифру	Встановлення ключових параметрів			
	Ключ (7000 установок)		Вектор ініціалізації (500 установок)	
	Час, μs	Швидкість, кількість установок / μs	Час, μs	Швидкість, кількість установок / μs
AES-128	657	10,7	0.08	6250,0
AES-256	1436	4,9	0.09	5555,6
HC-128	29	241,4	2982.80	0,2
HC-256	441	15,9	22889.10	0,0
MICKEY-128	9	777,8	4257.90	0,1
RABBIT	1215	5,8	80.80	6,2
SALSA-20	36	194,4	0.12	4166,7
SNOW2.0-128	50	140,0	91.70	5,5
SNOW2.0-256	100	70,0	90.30	5,5
SOSEMANUK	1550	4,5	101.60	4,9
STRUMOK 256	44	159,1	84.30	5,9
STRUMOK 512	44	159,1	105	4,8
TRIVIUM	66	106,1	219.90	2,3
CryptMT3	231	30,3	330,1	1,5
DECIM-128	2	3500,0	7889,9	0,1
RC4	6091	1,1	-	-
KCIPHER-2	182	38,5	751	0,7
GRAIN	5	1400,0	22713,3	0,0
MUGI	1609	4,4	326,7	1,5

Таблиця 10

Експериментальні результати дослідження шифрів за критерієм ініціалізація/генерація ключових параметрів (Intel Pentium P6200 2.13Gh)

Назва шифру	Встановлення ключових параметрів			
	Ключ (7000 установок)		Вектор ініціалізації (500 установок)	
	Час, μs	Швидкість, кількість установок / μs	Час, μs	Швидкість, кількість установок / μs
AES-128	944	7,4	0,1	5000,0
AES-256	2109	3,3	0,11	4545,5
HC-128	36	194,4	3648	0,1
HC-256	484	14,5	23303,2	0,0
MICKEY-128	13	538,5	5106,7	0,1
RABBIT	1804	3,9	115,6	4,3
SALSA-20	42	166,7	0,15	3333,3
SNOW2.0-128	58	120,7	107,8	4,6
SNOW2.0-256	114	61,4	109,4	4,6

SOSEMANUK	1878	3,7	121,9	4,1
STRUMOK 256	58	120,7	106,3	4,7
STRUMOK 512	58	120,7	104,7	4,8
TRIVIUM	78	89,7	256,3	2,0
CryptMT3	238	29,4	430,2	1,2
DECIM-128	2	3500,0	10634,2	0,0
RC4	10294	0,7	-	-
KCIPHER-2	235	29,8	1042,6	0,5
GRAIN	5	1400,0	27690	0,0
MUGI	2042	3,4	431,5	1,2

За отриманими показниками швидкості ініціалізації/генерації ключових параметрів можна зробити висновки, що найгірші значення у шифрів HC-128, HC-256, MICKEY-128. Це пояснює погані показники у HC-128 та HC-256 за критерієм шифрування коротких повідомлень – у алгоритмі багато часу витрачається на оновлення нових ключових параметрів. Найкращі показники мають AES-128, AES-256 та SALSA-20.

Висновки

Досліджені алгоритми ПСШ забезпечують високі криптографічні показники. Зокрема, виконуються вимоги статистичної безпеки, тобто послідовність, що сформована генераторами, не відрізняється за своїми статистичними властивостями від дійсно випадкової послідовності. Методики статистичних досліджень, які розглянуті в даній роботі, та отримані результати можуть розглядатися як первинний аналіз криптографічних властивостей генераторів, оскільки такі статистичні тести не враховують власну структуру генератора.

Наведені результати тестування різних потокових криптоперетворень підтверджують їхні високі криптографічні показники. Всі досліджувані шифри показали високе число успішно пройдених тестів: 130 – 134 за критерієм $P_j \geq 0{,}99$ та 186 – 187 за критерієм $P_j \geq 0{,}96$. Слід відмітити високі показники статистичної безпеки алгоритму ПСШ «Струмок», який виявив певні властивості генератору випадкових бітів. Зокрема, за своїми характеристиками сформовані послідовності не поступаються ПВП, які сформовано всесвітньо відомими потоковими криптографічними алгоритмами, зокрема шифрами HC-256 та SNOW 2.0. Крім того, для ПСШ «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 алгоритму «Струмок».

Результати статистичного тестування пакетом DIEHARD для симетричних шифрів AES, Enocoro, Grain, HC, MICKEY, MUGI, Salsa20, Sosemanuk, Trivium та ПСШ «Струмок» показують, що за більшістю показників всі потокові криптоалгоритмів мають порівняні показники статистичної безпеки. Для ПСШ «Струмок» додатково були проведені тести DIEHARD щодо розподілу ймовірностей, за результатами яких встановлено, що розподіл ймовірності відповідає рівномірному закону з невеликими флуктуаціями. Це додатково свідчить на користь висновку щодо високих показників статистичної безпеки цього алгоритму.

Результати тестування швидкодії показали, що за критерієм шифрування довгих повідомлень найкращі показники отримали «Струмок», HC-128 та SNOW 2.0. Причому, алгоритм «Струмок» дає кращі результати, ніж HC-128 на 30 %, та кращі за SNOW 2.0 майже удвічі. Експериментальні результати за критерієм шифрування коротких повідомлень

продемонстрували, що найкращі показники дає шифр «Струмок», SNOW 2.0 та SOSEMANUK відповідно. Шифри SNOW 2.0 та SOSEMANUK мають кращі показники в тому випадку, коли пакетів багато але малих за розміром. У потоковому шифрі «Струмок» результати зворотні: шифр демонструє кращі показники, коли пакети великі за розміром. За показниками критерію ініціалізація/генерація ключових параметрів найгірші показники у шифрів HC-128, HC-256, MICKEY-128. Це пояснює погані показники у HC-128 та HC-256 за критерієм шифрування коротких повідомлень – у алгоритмі багато часу витрачається на оновлення нових ключових параметрів. Найкращі ж показники мають AES-128, AES-256 та SALSA-20.

Таким чином, за результатами досліджень швидкодії встановлено, що в порівнянні з кращими світовими аналогами (потоковими криптоалгоритмами Grain, HC-128, HC-256, MICKEY, Rabbit, Salsa20, SNOW 2.0, Sosemanuk, Trivium) криптоалгоритм «Струмок» забезпечує найвищі (після HC-128 та HC-256) показники швидкості. Отже, алгоритм «Струмок» здатний забезпечувати високі показники швидкодії та ефективно функціонувати на різних обчислювальних платформах. Зазначимо, що ці оцінки не є граничними, тобто перспективним напрямком подальшої розробки є оптимізація програмної реалізації для збільшення пропускної здатності, наприклад за рахунок розпаралелювання або прискорення за рахунок залучення додаткових апаратних засобів.

Результати експериментальних досліджень статистичної безпеки та швидкісних характеристик потокових шифрів свідчать, що алгоритм «Струмок» є найбільш виваженим рішенням, він спроможний забезпечувати властивості генератора випадкових послідовностей та видавати величезні показники за швидкістю шифрування. Практично доведено, що швидкість шифрування алгоритмом «Струмок» на сучасних обчислювальних системах може досягати 10 – 15 Гбіт/с.

Список літератури: 1. *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія. – Харків : ХНУРЕ; Форт, 2012. – 868 с. 2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія : підручник. – Харків : ХНУРЕ; Форт, 2012. – 878 с. 3. *Есин В.І., Кузнецов О.О., Сорока Л.С.* Безпека інформаційних систем і технологій. – Харків : ХНУ ім. В.Н. Каразіна, 2013. – 632 с. 4. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – М. : Триумф, 2002. – 797 с. 5. *Розробка* нового блокового симетричного шифру: звіт за перший етап НДР «Алгоритм» (проміжний) / АТ «ІІТ» ; кер. І.Д. Горбенко – Харків, 2014. – Т. 4. – 304 с. 6. *ISO/IEC* 18033-4. 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. 7. *ISO/IEC* 29192-3. 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 8.*The eSTREAM* Project. [Електронний ресурс]. – Режим доступу: http://www.ecrypt.eu.org 9. *Cryptography* Research and Evaluation Committees. [Електронний ресурс]. – Режим доступу: http://www.cryptrec.go.jp/english/about.html 10. *Kuznetsov O. O., Ivanenko D.V., Lutsenko M.S.* Strumok stream cipher: spesification and basic properties // 2016 Third International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PICS&T-2016). October 4 – 6, 2016 Ukraine, Kharkiv. – Kharkiv : IEEE, 2016. C. 59-62. 11. *Дослідження* потокових симетричних шифрів та потокових режимів блокових симетричних шифрів: звіт про НДР (заключний), шифр «Струмок». Т. 2. – Розробка пропозицій до проекту алгоритму потокового симетричного шифрування та обґрунтування його властивостей / ХНУ ім. В.Н. Каразіна ; кер. Кузнецов О.О. ; вик.: Малахов С.В. [та інш., всього 13 осіб]. – Харків : ХНУ ім. В.Н. Каразіна. – 2015. – 73 с. 12. *Thank* you Bob Anderson. Список рассылки Cypherpunks (9 сентября 1994). [Електронний ресурс]. – Режим доступу: http://cypherpunks.venona.com/date/1994/09/msg00304.html 13. *Bruce Schneier*. Applied cryptography. Second edition. John Wiley & Sons. 1996 14. *Andreas Klein*. Attacks on the RC4 stream cipher. [Електронний ресурс]. – Режим доступу: http://www.networklife.net/images/wep-rc4/RC4.pdf. 15.*FIPS-197*: Advanced Encryption Standard (AES). National Institute of Standards and Technology. – 2001. [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. 16. *ISO/IEC* 18033-3. Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers. [Електронний ресурс]. – Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec:18033:-3:ed-2:v1:en 17. *NIST* 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 18. *Потий А.В, Орлова С.Ю, Гриненко Т.А*. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS // Правове, нормативне та

метрологічне забезпечення захисту інформації в Україні. Вип.2, 2001. – С. 206 – 213. 19. *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. 20. *Diehard*er: A Random Number Test Suite. [Електронний ресурс]. – Режим доступу: http://www.phy.duke.edu/~rgb/General/dieharder.php 21.*The Marsaglia* Random Number CDROM including the Diehard Battery of Tests of Randomness. [Електронний ресурс]. – Режим доступу: http://stat.fsu.edu/pub/diehard/ 22. *Gjorgjievski, Sashe* (et al.). Relation Between Statistical Tests for Pseudo-Random Number Generators and Diaphony as a Measure of Uniform Distribution of Sequences. In: Stojanov, Georgi, Kulakov, Andrea (Eds.), ICT Innovations 2016. Cognitive Functions and Next Generation ICT Systems. Springer International Publishing, pp. 80-92. 23. *VeraCrypt*. [Електронний ресурс]. – Режим доступу: https://veracrypt.codeplex.com/ 24. *TrueCrypt*. [Електронний ресурс]. – Режим доступу: http://truecrypt.sourceforge.net/

Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 15.09.2017