

**ДОСЛІДЖЕННЯ КРОСПЛАТФОРМНИХ РЕАЛІЗАЦІЙ
ПОТОКОВИХ СИМЕТРИЧНИХ ШИФРІВ****Вступ**

На сьогоднішній день інформаційні технології використовуються майже у всіх сферах нашого життя. Дуже широке розповсюдження отримав Інтернет речей (Internet of Things, IoT), майже у кожної людини є персональний мобільний пристрій. У зв'язку з цим з'явилося декілька проблем. По-перше, потрібно забезпечити роботу програмних засобів на всіх пристроях, тобто забезпечити кросплатформність реалізації відповідних сервісів та інформаційних служб. По-друге, необхідно забезпечити безпеку мобільних пристроїв та вирішити питання їх недостатньої потужності. Тому, актуальним завданням є дослідження різних криптографічних механізмів захисту інформації з можливістю кросплатформної реалізації, оцінка швидкодії в умовах обмежених обчислювальних ресурсів при портуванні на різні мобільні пристрої та операційні системи.

Мета роботи – аналіз та порівняльні дослідження сучасних симетричних потокових криптоперетворень, зокрема тестування їх швидкодії при кросплатформній реалізації мовою програмування Java. Тестування проводилися на операційних системах Windows 10 (x64), Debian (Kali), Android (x64) на різних обчислювальних системах.

Досліджувані симетричні шифри та умови тестування

При проведенні експериментальних досліджень були розглянуті сучасні потокові симетричні шифри Ecnosgo [1 – 3], Decim [1, 4, 5], Grain [6], HC [6], MUGI [1], Mickey [6], Rabbit [1, 6], RC-4 [7, 8], Salsa20 [6], SNOW2.0 [1], Sosemanuk [6], Strumok [9, 10], Trivium [2, 6], а також алгоритм блокового шифрування AES [11, 12], який може застосовуватися у потокових режимах шифрування. Метою досліджень є визначення швидкості шифрування на різних обчислювальних платформах при кросплатформній реалізації мовою програмування Java.

Потоковий симетричний шифр Ecnosgo – апаратно-орієнтований криптоалгоритм, який описано у [1 – 3]. Це байт-орієнтований шифр із довжиною ключа 128 біти та вектору ініціалізації 64 біти. Незважаючи на те, що Ecnosgo є апаратно орієнтованим шифром, він також має і ефективну програмну реалізацію. Для досягнення різних вимог, використовуються байтові операції.

Потоковий симетричний шифр Decim – спеціалізований для апаратного застосування алгоритм був розроблений Комом Бербаїном, Олівером Біллетом, Анн Канту, Николя Куртуа, Бландіном Дебре, Генрі Гільбертом, Луї Губином, Аліном Гуже, Луї Гранбуланом, Седериком Ларду, Марином Мінье, Томасом Порніним та Ервом Сібе [4]. Це апаратно орієнтований потоковий шифр з 80-бітним ключем та 64-бітним вектором ініціалізації (IV), який було подано до проекту потокового шифрування eSTREAM (не пройшов далі третього етапу конкурсу). Конструкція Decim заснована на нелінійному фільтрі регістру зсуву з лінійними зворотними зв'язками (РЗЛЗЗ, англ. LFSR) та нерегулярному механізмі розрідження псевдовипадкових послідовностей, який називають ABSG. Як наслідок, Decim має низьку апаратну складність. Після виявлення певних недоліків в [5] цей алгоритм було вдосконалено в новій версії Decim, що названо Decim^{v2}, виглядає більш безпечною, крім того, має меншу складність апаратної реалізації, ніж попередня версія Decim [1].

Потоковий симетричний шифр Grain, який було представлено Мартіном Хеллом, Томасом Юханссоном та Віллі Мейером у 2004 на міжнародному конкурсі eSTREAM за другим профілем (апаратно орієнтовані шифри) [6]. Симетричний алгоритм синхронного поточного шифрування, який орієнтований на використання на обчислювальних машинах з обмеженою

кількістю вентилів (gate), невеликими потужністю та обсягом пам'яті. В залежності 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 два регістри зсуву – з лінійним та нелінійним зворотним зв'язком та вихідна функція. Рекомендована довжина ключового потоку, який може бути вироблено на одній парі ключ/вектор, – 2^{44} біт.

Потоковий симетричний шифр HC-256, який було розроблено у 2004 році [6]. 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 MUGI є генератором ключових потоків, який було рекомендовано проектом CRYPTREC для використання у 2003 році урядом Японії. Алгоритм стандартизовано у ISO/IEC 18033-4 [1]. У якості початкових даних 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 Panama. Шифр MUGI є слово-орієнтованим.

Потоковий симетричний шифр Miquey, вдосконалену версію 2.0 якого було представлено у 2005 році Стивом Беббіджем та Метью Доддом [6] (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 одної 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 Rabbit, розробниками алгоритму є Мартін Боегсгаард, Метте Вестерагер, Томас Педерсен, Йеспер Крістіансен та Ове Скавіньюс [6]. У травні 2005 року, 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. Стандартизовано у ISO/IEC 18033-4 [1].

Потоковий симетричний шифр RC-4 був створений Рональдом Рівестом, співробітником компанії «RSA Security», в 1987 році. Скорочення «RC4» офіційно позначає «Rivest cipher 4» або «шифр Рівеста» («4» – номер версії) [7]. Протягом семи років шифр був комерційною таємницею, і точний опис алгоритму надавався тільки після підписання угоди про нерозголошення, але у вересні 1994 року його опис було анонімно відправлено в список розсилки «Cipherpunks» [8]. Володарі легальних копій вихідного коду RC4 підтвердили ідентичність алгоритмів при розбіжностях в позначеннях і структури програми.

Потоковий симетричний шифр Salsa 20, який було розроблено Даніелем Бернштейном [6]. Алгоритм став переможцем конкурсу eSTREAM в першому профілі (програмно-орієнтовані алгоритми). Для ініціалізації внутрішнього стану використовується ключ довжиною 256 біт, 64-бітний nonce та 64-бітна позиція блоку ключового потоку. Максимальна довжина псевдовипадкової ключової послідовності дорівнює 2^{70} біт.

Потоковий симетричний шифр SNOW 2.0 є генератором ключових потоків [1], 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 реко-

мендовану 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 [6]. 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 Strumok вперше представлений в [9, 10]. В основі алгоритму лежить класична схема підсумовуючого генератора [1, 6], подібна генератору SNOW-2.0, який визначено в ISO/IEC 18033-4:2011 [1]. В останній редакції алгоритм Струмок використовує 256-бітний вектор ініціалізації IV та 256-бітний або 512-бітний секретний ключ K і забезпечує високий та надвисокий рівень стійкості із врахуванням можливого застосування квантового криптографічного аналізу. Криптоалгоритм орієнтований на 64-розрядні обчислювальні системи, отже розмір слова визначено рівним 64 бітам.

Потоковий симетричний шифр Trivium – це симетричний апаратно-орієнтований паралельний поточковий шифр. Авторами шифру є Крістоф Де Канн'єр і Барт Пренел [6]. 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 вектору ініціалізації. Шифр є біт-орієнтованим.

Блоковий симетричний шифр AES, який стандартизовано в США як FIPS-197 [11]. На міжнародному рівні стандартизовано у ISO/IEC 18033-3 [12]. Використовує ключ довжиною 128, 192 або 256 біт. В залежності від довжини ключа відбувається 10, 12 або 14 раундів шифрування. AES базується на принципі, відомому як мережа замін-перестановок та, завдяки цьому, має швидку апаратну та програмну реалізацію. У режимі зворотного зв'язку за виходом цей шифр можна використовувати як поточковий.

Перелік досліджуваних алгоритмів наведено у табл. 1, де вказано короткі відомості про шифри та належність до відповідних стандартів чи дослідницьких проектів.

Таблиця 1

Криптоалгоритми, обрані для порівняння

Назва шифру	Джерело специфікації	Розмір стану, біт	Розмір ключа, біт	Розмір IV , біт
AES	FIPS-197, CRYPTREC, ISO/IEC 18033-4	128	128, 256	256
Enocoro	ISO/IEC 29192-3	272	80, 128	64
DECIMv2	ISO/IEC 18033-4, eSTREAM	288	128	128
GRAIN	eSTREAM	128	128	96
HC	eSTREAM	128, 256	128, 256	128, 256
MUGI	ISO/IEC 18033-4	128	128	128
MICKEY	eSTREAM	160	128	128
Rabbit	ISO/IEC 18033-4, eSTREAM	513	128	64
RC4	Список розсилки Cypherpunks	256	256	–
SALSA-20	eSTREAM	512	128	64
SNOW2.0	ISO/IEC 18033-4	512	128, 256	128, 56
SOSEMANUK	eSTREAM	512	128	128
Струмок-256	Цей документ	1024	256	256
Струмок-512		1024	512	512
TRIVIUM	eSTREAM, ISO/IEC 29192-3	288	80	80

В потокових алгоритмах інформація подається та обробляється у вигляді байт послідовності, де шифрується кожен символ відкритого тексту незалежно від інших символів [2]. Отже, важливими показниками потокових симетричних шифрів, які вимірюються за обраною методикою, є наступні:

- швидкість шифрування довгих потоків;
- швидкість шифрування коротких пакетів;
- швидкість ініціалізації ключових параметрів.

Для тестування було використано різні обчислювальні системи:

- переносний персональний комп'ютер з процесором Intel Pentium 3550m 2.3ГГц, операційна система Windows 10 (x64) та Debian (kali), оперативна пам'ять 4Гб (1600МГц);
- смартфон Samsung Galaxy S7 із функціональністю кишенькового персонального комп'ютера з процесором Samsung Exynos 8890 2.4ГГц, операційна система Android (x64), оперативна пам'ять 4Гб.

За першими двома показниками вимірюється час шифрування та швидкість шифрування за співвідношенням байтів/мікросекунду. При вимірюванні швидкості шифрування для довгих потоків ми повинні вважати на те, що саме цей показник має найбільшу потенційну перевагу над блоковими шифрами, тому, ймовірно, ця цифра буде найважливішим критерієм у більшості додатків [6]. Цікаво визначити, на якій довжині пакетів потоковий шифр почне програвати за швидкістю блоковим шифрам. Отже в дослідженні ми застосовували декілька довжин блоків.

Результати досліджень кросплатформних реалізацій потокових шифрів

Переносний персональний комп'ютер. У табл. 2 - 6 наводяться показники швидкодії різних шифрів при проведенні досліджень на переносному персональному комп'ютері.

За першим критерієм вимірювався час, витрачений на шифрування довгих потоків (1Гбайт). Як видно з табл. 2, найбільшу швидкість при шифруванні довгих пакетів (1Гбайт даних) показують алгоритми Sosemanuk, Strumok та SNOW2.0, найгірші показники отримали шифри Mickey, Decim та Grain.

За другим критерієм вимірюється швидкість шифрування коротких пакетів різної довжини. Для забезпечення репрезентативності досліджень було обрано різні довжини пакетів телекомунікаційного трафіку. Дослідження проводилися шляхом шифрування: 50 пакетів по 1500 байтів; 350 пакетів по 40 байтів; 120 пакетів по 576 байтів. Отримані результати зведено у табл. 3 – 5.

Таблиця 2

Шифрування довгих потоків, Windows 10 (x64)

Назва алгоритму	Час, msec	Швидкість,	
		Bytes/ μ sec	Мбіт/с
AES-128	93398	11.4965	87.7053
AES-256	87819	12.2266	93.2765
Enocofo	57102	18.8033	143.4653
Decim	3276232	0.3277	2.4576
Grain	1638008	0.6555	4.9152
HC-128	14341	74.8725	571.1825
HC-256	33624	31.9333	243.6037
MUGI	35816	29.9796	228.3547
Mickey	54237364	0.1979	0.0486
Rabbit	19664	54.6036	416.5857
RC-4	320659	3.34855	25.4974
Salsa20	45737	23.4768	179.0923
SNOW2.0-128	23379	45.9274	350.3137
SNOW2.0-256	22071	48.6497	371.0926
Sosemanuk	12096	88.7684	677.1766
Strumok-256	20845	51.5108	392.9043
Strumok-512	21469	50.0134	381.5454
Trivium	1048576	1.0241	7.8028

Таблиця 3

Шифрування коротких пакетів (50 пакетів по 1500 байтів), Windows 10 (x64)

Назва алгоритму	Час, μsec	Швидкість,		
		Bytes/ μsec	Мбіт/с	Packets/ μsec
AES-128	3952	0.3795	2.8672	0.0126
AES-256	5476	0.2739	2.0480	0.0091
Enocoro	3676	0.4080	3.0720	0.0136
Decim	23534	0.0063	0.0409	0.0002
Grain	14775	0.0101	0.0716	0.0033
HC-128	3087	0.4850	3.6864	0.0160
HC-256	9453	0.1580	1.1264	0.0052
MUGI	29673	0.0505	0.3788	0.0016
Mickey	4474571	0.0003	0.0204	10^{-5}
Rabbit	354	4.2372	32.2564	0.1412
RC-4	6661	0.2251	1.7100	0.0075
Salsa20	33767	0.0444	0.3379	0.0014
SNOW2.0-128	4061	0.3693	2.8164	0.0123
SNOW2.0-256	3894	0.3852	2.9286	0.0128
Sosemanuk	7573	0.1980	1.4336	0.0066
Strumok-256	1434	1.0457	7.8848	0.0348
Strumok-512	1450	1.0344	7.5848	0.0344
Trivium	80356	0.0186	0.1331	0.0006

Таблиця 4

Шифрування коротких пакетів (120 пакетів по 576 байтів), Windows 10 (x64)

Назва алгоритму	Час, μsec	Швидкість,		
		Bytes/ μsec	Мбіт/с	Packets/ μsec
AES-128	1245	0.4626	3.4816	0.0960
AES-256	7432	0.0775	0.5120	0.0160
Enocoro	6102	0.0943	0.7168	0.0190
Decim	224623	0.0025	0.0204	0.0005
Grain	15835	0.0363	0.2764	0.0075
HC-128	9345	0.0616	0.4608	0.0128
HC-256	25721	0.0223	0.1638	0.0046
MUGI	27349	0.0210	0.1536	0.0043
Mickey	4511735	0.0001	0.0009	$26 \cdot 10^{-5}$
Rabbit	338	1.7041	12.9024	0.3550
RC-4	7238	0.0795	0.6041	0.0016
Salsa20	36527	0.0157	0.1126	0.0032
SNOW2.0-128	5534	0.1040	0.7884	0.0220
SNOW2.0-256	5462	0.1052	0.7987	0.0219
Sosemanuk	3846	0.1497	1.1366	0.0312
Strumok-256	1318	0.4368	3.2768	0.0910
Strumok-512	1335	0.4312	3.2870	0.0898
Trivium	73037	0.0078	0.0512	0.0016

Таблиця 5

Шифрування коротких пакетів (350 пакетів по 40 байтів), Windows 10 (x64)

Назва алгоритму	Час, μsec	Швидкість,		
		Bytes/ μsec	Мбіт/с	Packets/ μsec
AES-128	765	0.4575	3.4816	0.0522
AES-256	768	0.4557	3.3792	0.0523
Encoro	1954	0.0020	0.0102	0.0179
Decim	48257	0.0008	0.0061	0.0072
Grain	4753	0.0084	0.0614	0.0735
HC-128	7256	0.0055	0.0409	0.0482
HC-256	15324	0.0026	0.0204	0.0228
MUGI	9571	0.0041	0.0307	0.0365
Mickey	1303412	$3 \cdot 10^{-5}$	0.0003	0.0002
Rabbit	131	0.3053	2.3244	2.6717
RC-4	1037	0.0385	0.2048	0.0241
Salsa20	97234	0.0004	0.0030	0.0035
SNOW2.0-128	1256	0.0318	0.2355	0.2786
SNOW2.0-256	1187	0.0336	0.2560	0.2948
Sosemanuk	2564	0.0156	0.1126	0.1365
Strumok-256	274	0.1456	1.1059	1.2742
Strumok-512	320	0.1250	0.9523	1.0937
Trivium	15176	0.0026	0.0204	0.0164

Таблиця 6

Ініціалізація ключових параметрів, Windows 10 (x64)

Назва алгоритму	Встановлення ключів		Встановлення векторів ініціалізації	
	Час, sec	Кільк. / μs	Час, sec	Кільк. / μs
AES-128	0.0072	0.9715	$1.16 \cdot 10^{-4}$	4.3105
AES-256	0.0086	0.8108	$1.25 \cdot 10^{-4}$	4
Encoro	0.0075	0.9270	$7.1 \cdot 10^{-5}$	7.0423
Decim	0.0001	53.435	$5.9 \cdot 10^{-5}$	8.4745
Grain	0.0010	6.9582	$7.6 \cdot 10^{-5}$	6.5784
HC-128	1.1679	0.0059	$6.3 \cdot 10^{-5}$	7.9362
HC-256	4.2364	0.0016	$7.8 \cdot 10^{-5}$	6.4105
MUGI	0.0246	0.2839	$5.4 \cdot 10^{-5}$	9.2594
Mickey	10.695	0.0006	0.3347	0.0013
Rabbit	0.0017	3.9230	0.0001	4.1332
RC-4	0.0175	0.3997	-	-
Salsa20	-	-	-	-
SNOW2.0-128	0.0056	1.2289	$4.2 \cdot 10^{-5}$	11.9041
SNOW2.0-256	0.0018	3.7981	$6.3 \cdot 10^{-5}$	7.9365
Sosemanuk	0.0053	1.2991	$1.77 \cdot 10^{-4}$	2.8248
Strumok-256	0.0045	1.5527	$1.1 \cdot 10^{-5}$	45.4546
Strumok-512	0.0020	3.4163	$4 \cdot 10^{-6}$	125
Trivium	1.4926	0.0046	$1.52 \cdot 10^{-4}$	3

Як видно із табл. 3 – 5, при великій довжині пакетів вигреш мають потокові шифри Rabbit, Strumok, SNOW2.0 та Encoro. Але при зменшенні довжини пакетів (до декілька десятків байт) перевагу має, як і очікувалося, блоковий шифр AES.

Швидкість ініціалізації ключових параметрів є найменш критичним параметром для відображення швидкості шифрування. Ці часові витрати зневажливо малі в порівнянні з процесом генерації ключового потоку. При дослідженнях проводилося 7000 ключових установок та 500 установок векторів ініціалізації. Отримані результати тестування показано в табл. 6, вони свідчать про перевагу алгоритмів Decim та Grain. Далі йдуть шифри Rabbit, SNOW2.0, Sosemanuk та Strumok.

У табл. 7 – 11 наводяться показники швидкості шифрів на ОС Debian (kali) за тією ж методикою, що і для ОС Windows 10 (x64).

Таблиця 7

Шифрування довгих потоків, Debian (kali)

Назва алгоритму	Час, msec	Швидкість,	
		Bytes/ μ sec	Мбіт/с
AES-128	92919	11.7471	11.1616
AES-256	85848	12.9264	12.3187
Enocoro	54865	19.5728	18.6654
Decim	3465528	0.3098	0.2949
Grain	1905016	0.5365	0.51097
HC-128	13438	79.9036	76.1958
HC-256	31326	34.2764	32.6860
MUGI	31257	34.3526	32.7577
Mickey	4861480	0.2200	0.02099
Rabbit	7888	136.1284	1038.43
RC-4	117824	9.1130	8.6906
Salsa20	43850	24.6373	23.4496
SNOW2.0-128	29442	36.4464	34.7545
SNOW2.0-256	29170	36.8092	35.1027
Sosemanuk	18443	58.2197	55.5212
Strumok-256	25414	42.2504	40.2841
Strumok-512	27554	38.9682	37.1609
Trivium	1076536	1.0762	1.0260

Таблиця 8

Шифрування коротких пакетів (50 пакетів по 1500 байтів), Debian (kali)

Назва алгоритму	Час, μ sec	Швидкість,		
		Bytes/ μ sec	Мбіт/с	Packets/ μ sec
AES-128	2752	0.4995	3.7888	0.0319
AES-256	6275	0.2939	2.1504	0.0097
Enocoro	3176	0.4270	0.3072	0.0147
Decim	440000	0.0034	3.1744	0.0001
Grain	164306	0.0090	0.0061	0.0003
HC-128	2147	0.5340	3.9936	0.0210
HC-256	5253	0.2990	2.2528	0.0112
MUGI	21673	0.1125	0.8192	0.0023
Mickey	3367000	0.0004	0.0030	10 ⁻⁴
Rabbit	347	0.1440	32.972	4.3227
RC-4	74616	0.0201	0.1024	0.0006
Salsa20	34567	0.0432	0.3072	0.0012
SNOW2.0-128	3242	0.4623	3.4816	0.0154
SNOW2.0-256	6212	0.2762	2.0480	0.0098
Sosemanuk	4367	0.3430	2.5600	0.0114
Strumok-256	1869	0.8024	6.0416	0.0267
Strumok-512	1801	0.8325	6.3488	0.0277
Trivium	93863	0.0159	0.1024	0.0005

Таблиця 9

Шифрування коротких пакетів (120 пакетів по 576 байтів), Debian (kali)

Назва алгоритму	Час, μsec	Швидкість,		
		Bytes/ μsec	Мбіт/с	Packets/ μsec
AES-128	2105	0.4726	3.6044	0.1695
AES-256	8272	0.0795	0.6041	0.0435
Eneoro	5722	0.1143	0.8704	0.0233
Decim	466436	0.0012	0.0092	0.0002
Grain	144000	0.0034	0.0204	0.0008
HC-128	7215	0.0726	0.5529	0.0173
HC-256	17721	0.0632	0.4812	0.0116
MUGI	25349	0.0240	0.1740	0.0049
Mickey	3522000	0.0001	0.0010	$3 \cdot 10^{-5}$
Rabbit	334	1.7245	13.1077	0.3592
RC-4	66432	0.0086	0.0614	0.0018
Salsa20	32527	0.0187	0.1331	0.0072
SNOW2.0-128	1234	0.4540	3.4611	0.0970
SNOW2.0-256	3262	0.1762	1.3414	0.0335
Sosemanuk	7264	0.0756	0.5734	0.0162
Strumok-256	1802	0.3195	2.4371	0.0665
Strumok-512	1680	0.3427	2.6112	0.0714
Trivium	85924	0.0067	0.0409	0.0013

Таблиця 10

Шифрування коротких пакетів (350 пакетів по 40 байтів), Debian (kali)

Назва алгоритму	Час, μsec	Швидкість,		
		Bytes/ μsec	Мбіт/с	Packets/ μsec
AES-128	785	0.4565	3.4816	0.0532
AES-256	798	0.4587	3.4806	0.0510
Eneoro	1134	0.0060	0.0409	0.0259
Decim	121023	0.0003	0.0020	0.0028
Grain	48210	0.0008	0.0061	0.0072
HC-128	9256	0.0047	0.0307	0.0323
HC-256	13324	0.0031	0.0204	0.0288
MUGI	7531	0.0091	0.0614	0.0645
Mickey	1069000	$3 \cdot 10^{-5}$	0.0002	0.0003
Rabbit	138	0.2898	2.1504	2.5362
RC-4	9466	0.0042	0.0307	0.0264
Salsa20	93164	0.0004	0.0020	0.0032
SNOW2.0-128	843	0.0468	0.3481	0.4786
SNOW2.0-256	2237	0.0176	0.1331	0.1578
Sosemanuk	2763	0.0144	0.1024	0.1265
Strumok-256	404	0.0989	0.7475	0.8656
Strumok-512	361	0.1108	0.8396	0.9695
Trivium	17577	0.0022	0.0102	0.0199

Ініціалізація ключових параметрів, Debian (kali)

Назва алгоритму	Встановлення ключів		Встановлення векторів ініціалізації	
	Час, sec	Кількість / μ s	Час, sec	Кількість / μ s
AES-128	0.0070	0.9940	$1.33 \cdot 10^{-4}$	3.759
AES-256	0.0102	0.6830	$1.52 \cdot 10^{-4}$	3.289
Enocoro	0.0093	0.7470	$8.6 \cdot 10^{-5}$	5.813
Decim	0.0008	8.0275	$1.37 \cdot 10^{-4}$	3.649
Grain	0.0011	5.8873	$9.2 \cdot 10^{-5}$	5.434
HC-128	1.2589	0.0055	$1.28 \cdot 10^{-4}$	3.906
HC-256	4.4324	0.0015	$1.62 \cdot 10^{-4}$	3.086
MUGI	0.0291	0.2405	$7.9 \cdot 10^{-5}$	6.329
Mickey	11.069	0.0006	0.3377	0.001
Rabbit	0.0015	4.5425	0.0001	4.901
RC-4	0.0162	0.4297	-	-
Salsa20	-	-	-	-
SNOW2.0-128	0.0069	1.0060	$6.1 \cdot 10^{-5}$	8.196
SNOW2.0-256	0.0016	4.2296	$5.6 \cdot 10^{-5}$	8.928
Sosemanuk	0.0036	1.9283	$1.65 \cdot 10^{-4}$	3.030
Strumok-256	0.0047	1.4858	$2.5 \cdot 10^{-5}$	20.00
Strumok-512	0.0025	2.7821	$2 \cdot 10^{-5}$	25.00
Trivium	1.0863	0.0064	$1.73 \cdot 10^{-5}$	2.890

Як можна побачити з отриманих результатів, при тестуванні на ОС Debian (kali) більшість шифрів погіршили свої результати. Однак співвідношення швидкодії між окремими шифрами за різними показниками майже такі самі. Слід відмітити, що алгоритм Струмोक, який забезпечує високі показники криптографічного захисту, достатні для застосування у постквантовий період (довжина ключа 256 та 512 бітів, довжина вектору ініціалізації 256 бітів, довжина внутрішнього стану 1024 біти), за більшістю показників швидкодії також має певну перевагу, зокрема в більшості випадків він не поступається найкращим світовим аналогам.

Смартфон із функціональністю персонального комп'ютера. Результати досліджень швидкодії потокових шифрів при застосуванні їх на смартфоні із функціональністю персонального комп'ютера наведено у табл. 12 – 16.

Як бачимо із даних табл. 12, за критерієм шифрування довгих пакетів найбільшу швидкість показують алгоритми HC, Rabbit, Salsa20 і Strumok, найгірші показники отримали шифри MUGI, Mickey та Trivium.

За критерієм шифрування коротких пакетів перевагу має шифр Rabbit, далі йдуть шифри AES, Strumok, SNOW2.0 та інші. Найгірші показники мають шифри Decim, Grain, Mickey та Trivium. Але слід відмітити, що загальної тенденції не спостерігається, бо окремі шифри дають нестабільні результати. Можливо, на швидкість шифрування дуже впливає рівень завантаженості обчислювальної системи іншими процесами.

За останнім показником (час ініціалізації ключових даних) перевагу мають шифри Grain і Trivium. Далі йдуть шифри Strumok, Rabbit, SNOW2.0 та інші.

Таблиця 12

Шифрування довгих потоків, Android (x64)

Назва алгоритму	Час, msec	Швидкість,	
		Bytes/ μ sec	Мбіт/с
AES-128	2185096	0.4913	3.7483
AES-256	920464	1.1665	8.8996
Enocoro	887846	1.2094	9.2269
Decim	$2 \cdot 10^{-7}$	0.0361	0.2755
Grain	$1.6 \cdot 10^{-7}$	0.0644	0.4914
HC-128	23146	46.4825	354.64
HC-256	27157	39.6214	302.28
MUGI	138013696	0.0077	0.0592
Mickey	$3.5 \cdot 10^{-8}$	0.0030	0.0229
Rabbit	38496	27.8924	212.81
RC-4	1081352	0.9929	7.5752
Salsa20	110243	9.7397	74.309
SNOW2.0-128	397753	2.7040	20.629
SNOW2.0-256	457926	2.3447	17.888
Sosemanuk	342231	3.1374	23.937
Strumok-256	186653	5.7526	43.889
Strumok-512	184243	5.8278	44.463
Trivium	$4.9 \cdot 10^{-8}$	0.0021	0.0165

Таблиця 13

Шифрування коротких пакетів (50 пакетів по 1500 байтів), Android (x64)

Назва алгоритму	Час, μ sec	Швидкість,		
		Bytes/ μ sec	Мбіт/с	Packets/ μ sec
AES-128	10376	0.0385	0.2941	0.3468
AES-256	11467	0.0034	0.0259	0.0925
Enocoro	12199	0.0032	0.0244	0.0286
Decim	725739	$5 \cdot 10^{-5}$	0.0004	0.0004
Grain	2562911	10^{-5}	0.0001	0.0001
HC-128	10341	0.0038	0.0289	0.0340
HC-256	25749	0.0015	0.0114	0.0135
MUGI	22673	0.0017	0.0129	0.0154
Mickey	3528571	10^{-5}	0.0001	$9 \cdot 10^{-5}$
Rabbit	841	0.0475	0.3623	0.4161
RC-4	72537	$5 \cdot 10^{-4}$	0.0042	0.0048
Salsa20	12354	0.0032	0.0244	0.0283
SNOW2.0-128	8573	0.0046	0.0350	0/0408
SNOW2.0-256	5690	0.0070	0.0535	0.0615
Sosemanuk	18573	0.0021	0.0160	0.0188
Strumok-256	6134	0.0065	0.0495	0.0570
Strumok-512	3496	0.0114	0.0869	0.1001
Trivium	5256627	$7 \cdot 10^{-6}$	$5 \cdot 10^{-5}$	$6 \cdot 10^{-5}$

Таблиця 14

Шифрування коротких пакетів (120 пакетів по 576 байтів), Android (x64)

Назва алгоритму	Час, μsec	Швидкість,		
		Bytes/ μsec	Мбіт/с	Packets/ μsec
AES-128	28453	0.0527	0.4020	0.0017
AES-256	28579	0.0524	0.3990	0.0017
Enocoro	8473	0.1770	1.3504	0.0059
Decim	1728461	$8 \cdot 10^{-4}$	0.0066	$2 \cdot 10^{-5}$
Grain	1264469	0.0011	0.0083	$3 \cdot 10^{-5}$
HC-128	17387	0.0862	0.6573	0.0028
HC-256	20457	0.0733	0.5592	0.0024
MUGI	88463	0.0169	0.1289	$5 \cdot 10^{-4}$
Mickey	$2.2 \cdot 10^{-5}$	$5 \cdot 10^{-5}$	0.0004	10^{-6}
Rabbit	3351	0.4476	3.4142	0.0149
RC-4	2016361	$7 \cdot 10^{-4}$	0.0056	$2 \cdot 10^{-5}$
Salsa20	70610	0.0212	0.1617	$7 \cdot 10^{-4}$
SNOW2.0-128	37261	0.0402	0.3067	0.00134
SNOW2.0-256	38377	0.0390	0.2975	0.0013
Sosemanuk	272471	0.0055	0.0419	10^{-4}
Strumok-256	11012	0.1362	1.0395	0.0045
Strumok-512	14936	0.1004	0.7659	0.0033
Trivium	$1.7 \cdot 10^{-8}$	$8 \cdot 10^{-6}$	$6 \cdot 10^{-5}$	$2 \cdot 10^{-7}$

Таблиця 15

Шифрування коротких пакетів (350 пакетів по 40 байтів), Android (x64)

Назва алгоритму	Час, μsec	Швидкість,		
		Bytes/ μsec	Мбіт/с	Packets/ μsec
AES-128	30434	0.0189	0.1443	0.0039
AES-256	31644	0.0182	0.1388	0.0037
Enocoro	58575	0.0098	0.0747	0.0020
Decim	1872478	$3 \cdot 10^{-4}$	0.0023	$6 \cdot 10^{-5}$
Grain	1104634	$5 \cdot 10^{-4}$	0.0039	10^{-4}
HC-128	20543	0.0280	0.2136	0.0058
HC-256	25721	0.0223	0.1701	0.0046
MUGI	88286	0.0065	0.0495	0.0013
Mickey	$2 \cdot 10^{-7}$	$2 \cdot 10^{-5}$	0.0001	$4 \cdot 10^{-6}$
Rabbit	2441	0.2359	1.7997	0.0491
RC-4	1224535	$4 \cdot 10^{-4}$	0.0035	$9 \cdot 10^{-5}$
Salsa20	45201	0.0127	0.0968	0.0026
SNOW2.0-128	26982	0.0213	0.1625	0.0044
SNOW2.0-256	27361	0.0210	0.1602	0.0043
Sosemanuk	18699	0.0308	0.2349	0.0064
Strumok-256	17189	0.0335	0.2555	0.0069
Strumok-512	18472	0.0311	0.2372	0.0064
Trivium	$2 \cdot 10^{-7}$	$2 \cdot 10^{-5}$	10^{-5}	$4 \cdot 10^{-5}$

Ініціалізація ключових параметрів, Android (x64)

Назва алгоритму	Встановлення ключів		Встановлення векторів ініціалізації	
	Час, sec	Кількість / μ s	Час, sec	Кількість / μ s
AES-128	0.1554	0.0450	0.0042	0.1180
AES-256	0.2764	0.0253	0.0047	0.1040
Epoporo	0.5824	0.0120	0.0025	0.1970
Decim	0.0257	0.2720	0.0021	0.2367
Grain	0.0005	12.433	0.0001	4.6728
HC-128	0.5714	0.0122	0.0008	0.5590
HC-256	2.8776	0.0024	0.0010	0.4940
MUGI	0.1638	0.0427	0.0067	0.0740
Mickey	85.916	$8 \cdot 10^{-5}$	0.0027	0.1794
Rabbit	0.3347	0.0209	0.0004	1.1467
RC-4	0.0541	0.1292	-	-
Salsa20	-	-	-	-
SNOW2.0-128	0.1145	0.0611	0.0005	0.8880
SNOW2.0-256	0.1145	0.0610	0.0006	0.7418
Sosemanuk	0.2394	0.0292	0.0197	0.0253
Strumok-256	0.0679	0.1030	0.0004	1.0869
Strumok-512	0.0621	0.1125	0.0004	1.0822
Trivium	0.0066	1.0523	0.0008	0.6090

Висновки

Отримані результати експериментальних досліджень свідчать, що розроблені кросплатформні реалізації потокових шифрів дозволяють застосувати відповідні криптоперетворення на різних обчислювальних платформах. Для цього достатня наявність відповідного інтерпретатора, за допомогою якого вдається забезпечити роботу програмних засобів на різних пристроях, тобто забезпечити кросплатформність відповідних сервісів та інформаційних служб, в тому числі із врахуванням вимог недостатньої потужності та малоресурсності апаратної складової.

Слід відмітити, що кросплатформна реалізація криптоалгоритмів значно зменшує показники швидкодії як при шифруванні довгих потоків, так і при обробці окремих пакетів та ініціалізації ключових даних. Однак співвідношення по швидкодії між окремими шифрами час-то зберігаються. Певні зміни цих співвідношень пояснюються особливостями апаратної складової та відповідних обчислювальних алгоритмів, зокрема, окремі шифри орієнтовано на апаратну реалізацію, деякі – на програму із певною розрядністю операційної системи.

Отримані результати будуть корисними в подальшому обґрунтуванні пропозицій для практичного застосування алгоритмів потокового шифрування.

Список літератури:

1. ISO/IEC 18033-4:2011. Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers. [Електронний ресурс] URL: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54532 [Dec., 2012].
2. ISO/IEC 29192-3:2012. Information technology – Security techniques – Lightweight cryptography – Part 3: Stream ciphers. [Електронний ресурс] URL: <https://www.iso.org/standard/56426.html> 3. Pseudorandom Number Generator Epoporo. [Електронний ресурс] URL: http://www.cryptrec.go.jp/english/cryptrec_13_spec_cypherlist_files/PDF/23_00espec.pdf
4. C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, and H. Sibert. Decim – A new Stream Cipher for Hardware applications. In ECRYPT Stream Cipher Project Report 2005/004. [Електронний ресурс] URL: <http://www.ecrypt.eu.org/>

5. W.Hongjun and B.Preneel. Cryptanalysis of Stream Cipher Decim. [Електронний ресурс] URL: <http://www.ecrypt.eu.org/stream/>
6. The eSTREAM Project. [Електронний ресурс] URL: <http://www.ecrypt.eu.org/>
7. Frequently Asked Questions. [Електронний ресурс] URL: <http://people.csail.mit.edu/rivest/faq.html#Ron>
8. Thank you Bob Anderson. [Електронний ресурс] URL: <http://cypherpunks.venona.com/date/1994/09/msg00304.html>
9. Kuznetsov O., Lutsenko M. and Ivanenko D. Strumok stream cipher: Specification and basic properties // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 59-62.
10. Gorbenko I., Kuznetsov A., Lutsenko M. and Ivanenko D. The research of modern stream ciphers // 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 207-210.
11. FIPS-197: Advanced Encryption Standard (AES) / National Institute of Standards and Technology, 2001. [Електронний ресурс] URL: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
12. ISO/IEC 18033-3:2010. Information technology – Security techniques – Encryption algorithms. Part 3: Block ciphers. [Електронний ресурс] URL: <https://www.iso.org/standard/54531.html>

*Харківський національний
університет імені В.Н. Каразіна;
Харківський національний
університет радіоелектроніки*

Надійшла до редколегії 03.04.2018