УДК 621.3.06

М.Ю. РОДІНКО, Р.В. ОЛІЙНИКОВ, д-р техн. наук

ПОСТКВАНТОВИЙ МАЛОРЕСУРСНИЙ СИМЕТРИЧНИЙ БЛОКОВИЙ ШИФР«КИПАРИС»

Вступ

Поширення таких технологій як Інтернет речей (англ. Internet of Things), смарт-лічильники, системи безпеки для автомобілів та ін. висуває нові вимоги до криптографічних примітивів. Існуючі симетричні блокові шифри з високим рівнем криптографічної стійкості (такі, як AES [1] або «Калина» [2]) можуть не задовольняти вимогам компактної реалізації для застосування у пристроях з обмеженою кількістю споживання енергії. Для таких цілей існує цілий ряд малоресурсних блокових шифрів (PRESENT [3], XTEA [4], SPECK [5] та ін.). Однак більшість з них не підтримують довжину ключа, достатню для забезпечення високого рівня безпеки, тим більше, у постквантовий період. В Україні також не має власного постквантового малоресурсного блокового шифру. Таким чином, актуальною є задача створення шифру, який водночас має високий рівень криптографічної стійкості та високу швидкодію перетворень на різних платформах.

Серед підходів до побудування малоресурсних примітивів наряду з уже відомими SPN-структурою та мережею Фейстеля поширення набуває так зване ARX (Add-Rotate-XOR)-перетворення (SPECK, ChaCha [6]). Це обумовлено тим, що додавання за модулем та циклічний зсув є швидкими та простими у реалізації операціями.

У роботі пропонується постквантовий малоресурсний блоковий шифр «Кипарис», який заснований на мережі Фейстеля, а в якості циклової функції використовує ARX перетворення. Запропонований шифр має оптимізацію як під 32-бітові, так і під 64-бітові платформи та забезпечує високу швидкодію перетворень (у декілька разів вищу за AES).

1. Вимоги до перспективного малоресурсного блокового шифру

Виходячи з поставленої задачі, до перспективного малоресурсного симетричного блокового шифру були сформульовані наступні основні вимоги.

– Високий рівень криптографічної стійкості проти перебірних атак, що обумовлює необхідність підтримки ключів довжиною 256 та 512 біт.

– Застосування «сильної» схеми розгортання ключів (СРК) з метою захисту від криптоаналітичних атак на СРК.

– Висока швидкодія на різних програмно-апаратних платформах (в тому числі, мобільних).

– Компактна програмна реалізація як для стаціонарних систем (робочі станції, сервери), так і для мобільних платформ (смартфони, планшети).

– Наявність варіантів алгоритму, оптимізованих як під 64-бітові, так і під 32-бітові системи.

– Мінімальний об’єм пам’яті для швидкодіючої реалізації (компактний код та відсутність таблиць передобчислень).

– Постійний час шифрування блока на сучасних процесорах незалежно від параметрів, що обробляються, для захисту від атак по побічних каналах.

2. Опис алгоритму шифрування

2.1. Загальні параметри

Алгоритм шифрування «Кипарис» виконує перетворення блоків даних розміром l біт, із використанням ключа шифрування довжиною k біт, $l,k \in \{256,512\}$, $l = k$. Операції виконуються над s-бітними словами, $s \in \{32,64\}$. Основні загальні параметри шифру наведені в табл. 1.

Таблиця 1

Загальні параметри шифру «Кипарис»

	Кипарис-256	Кипарис-512
Розмір блока (l), біт	256	512
Довжина ключа (k), біт	256	512
Довжина слова (s), біт	32	64
Кількість ітерацій перетворення (t)	10	14

Варто відмітити, що «Кипарис-256» орієнтований на використання на 32-бітних платформах, «Кипарис-512» – на 64-бітних платформах, в т.ч. із вимогами до компактної реалізації та обмеженого енергоспоживання.

2.2. Процедура зашифрування/розшифрування

Загальна схема процедури зашифрування представлена на рис. 1.

На вхід процедури зашифрування подається блок відкритого тексту $P = (P_0, P_1, ..., P_7)$ та циклові ключі $RK^{(0)}, RK^{(1)}, \ldots, RK^{(t-1)}$. Кожний ключ $RK^{(i)} = (RK_0^{(i)}, RK_1^{(i)}, RK_2^{(i)}, RK_3^{(i)})$ складається з чотирьох s-бітних слів. Циклові ключі формуються за допомогою СРК на основі ключа шифрування $K = (K_0, K_1, ..., K_7)$.

Блок відкритого тексту P ділиться на два підблока: $L_0 = (P_0, P_1, P_2, P_3)$, $R_0 = (P_4, P_5, P_6, P_7)$. Вихід i-ї ітерації перетворення обчислюється як

$$L_i = R_{i-1} \oplus F\left(L_{i-1}, RK^{(i-1)}\right),$$

$$R_i = L_{i-1}.$$

Циклова функція F представляє собою додавання підблока L_{i-1} з ключем $RK^{(i-1)}$ за модулем 2 та двократне повторення функції $h(P_0', P_1', P_2', P_3')$, на вхід якої подається чотири s-бітних слова. Вихідне значення функції h обчислюється як

$$P_0' = ADD(P_0', P_1'),\ P_3' = XOR(P_3', P_0'),\ P_3' = ROTL(P_3', r1),$$
$$P_2' = ADD(P_2', P_3'),\ P_1' = XOR(P_1', P_2'),\ P_1' = ROTL(P_1', r2),$$
$$P_0' = ADD(P_0', P_1'),\ P_3' = XOR(P_3', P_0'),\ P_3' = ROTL(P_3', r3),$$
$$P_2' = ADD(P_2', P_3'),\ P_1' = XOR(P_1', P_2'),\ P_1' = ROTL(P_1', r4),$$

де $ADD(x, y)$ – додавання за модулем s двох s-бітних слів;

$XOR(x, y)$ – XOR двох s-бітних слів;

$ROTL(x, r)$ – циклічний зсув s-бітного слова вліво на r біт.

Значення циклічних зсувів (r_0, r_1, r_2, r_3) залежать від довжини блока і дорівнюють:

- для шифру «Кипарис-256» $(r_0, r_1, r_2, r_3) = (16, 12, 8, 7)$.
- для шифру «Кипарис-512» $(r_0, r_1, r_2, r_3) = (32, 24, 16, 15)$.

Процедура розшифрування є ідентичною до процедури зашифрування, лише циклові ключі подаються у зворотному порядку.

2.3. Схема розгортання ключів шифру «Кипарис»

Циклові ключі формуються за допомогою неін'єктивної СРК, в основі якої лежить структура СРК шифру «Калина». У [7] показано, що складність перебірних атак на неін'єктивні СРК у порівнянні з ін'єктивними схемами не знижується, при цьому

неін’єктивні схеми забезпечують додатковий захист від атак на реалізацію та інших криптоаналітичних атак.

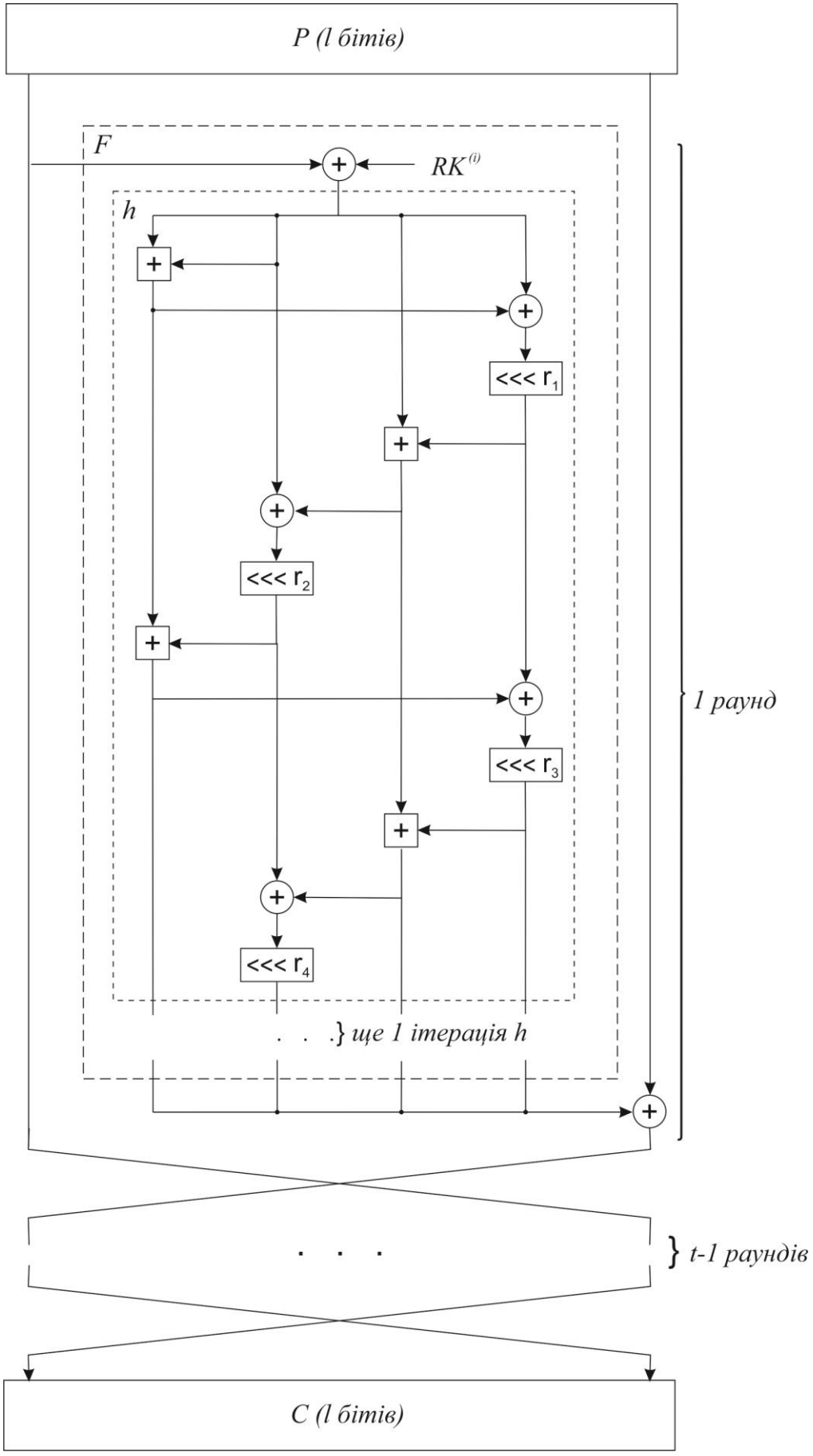


Рис. 1. Процедура зашифрування шифру «Кипарис»

При шифруванні використовується t циклових ключів довжиною $4\times s$ біт.

Спочатку формується проміжний ключ K_σ довжиною $4\times s$ біт. Формування ключа здійснюється із використанням ключа шифрування $K=(K_0,K_1,...,K_7)$ наступним чином:

$$K_l=(K_0,K_1,K_2,K_3), K_r=(K_4,K_5,K_6,K_7),$$
$$st=XOR(0x1,K_l), st=h(h(st)),$$
$$st=ADD(st,K_r), st=h(h(st)),$$
$$st=XOR(st,K_l), K_\sigma=st.$$

Циклові ключі формуються на основі ключа шифрування K, проміжного ключа K_σ та константи tmv = (0x000F000F, 0x000F000F, 0x000F000F, 0x000F000F) наступним чином:

$$st=(K_0,K_1,K_2,K_3), K_t=ADD(K_\sigma,tmv),$$
$$st=ADD(st,K_t), st=h(h(st)),$$
$$st=XOR(st,K_t), st=h(h(st)),$$
$$st=ADD(st,K_t), RK_{2i}=st,$$
$$tmv=ShiftLeft(tmv,0x1),$$
$$st=(K_4,K_5,K_6,K_7), K_t=ADD(K_\sigma,tmv),$$
$$st=ADD(st,K_t), st=h(h(st)),$$
$$st=XOR(st,K_t), st=h(h(st)),$$
$$st=ADD(st,K_t), RK_{2i+1}=st,$$

де функція *ShiftLeft* передбачає зсув кожного s-бітного слова вліво на один біт.

Після формування кожної пари парний/непарний ключ значення tmv та K модифікуються наступним чином:

$$tmv=ShiftLeft(tmv,1),$$
$$K=ROTLKey(K,1),$$

де $ROTLKey(K,1)$ – циклічний зсув масиву s-бітних слів ключа вліво.

4. Дослідження швидкодії шифру «Кипарис»

У ході досліджень на різних програмно-апаратних платформах була оцінена швидкодія алгоритмів «Кипарис-256» та «Кипарис-512» та порівняна зі швидкодією шифру AES.

Вимірювання швидкодії блокових шифрів здійснювалося на наступних платформах:

– Intel Core i3 / Windows 7 x32 з компілятором Visual C++ 2010;
– Intel Core i3 / Windows 7 x64 з компілятором Visual C++ 2010;
– Intel Core i5 / Linux (64 bit) з компілятором g++ версії 4.8;
– ARM Cortex-A7 / Android 4.2.2 Jelly Bean (32 bits).

Результати вимірювання швидкодії шифрів на різних платформах наведені в таблиці 2.

Таблиця 2

Швидкодія шифрів «Кипарис» та AES, Мбіт/с

Платформа	Кипарис-256	Кипарис-512	AES-256
Intel Core i3 / Windows 7 x32	1796,86	786,24	711,13
Intel Core i3 / Windows 7 x64	1878,5	2617,74	858,77
Intel Core i5 / Linux (64 bit)	3954,55	5395,81	1969,65

ARM Cortex-A7 / Android 4.2.2 (32 bit)	122	136	43

Як видно з табл. 2, блоковий шифр «Кипарис» за швидкістю перевершує алгоритм AES на всіх обраних платформах. На платформі x86 з 32-бітовою архітектурою шифр «Кипарис-256» у 2,5 рази швидший, ніж AES-256. На платформі x86 з 64-бітовою архітектурою шифр «Кипарис-512» приблизно у 3 рази швидший, ніж AES-256. На платформі ARM Cortex-A7 «Кипарис-256» та «Кипарис-512» приблизно у 3 рази швидші, ніж AES-256.

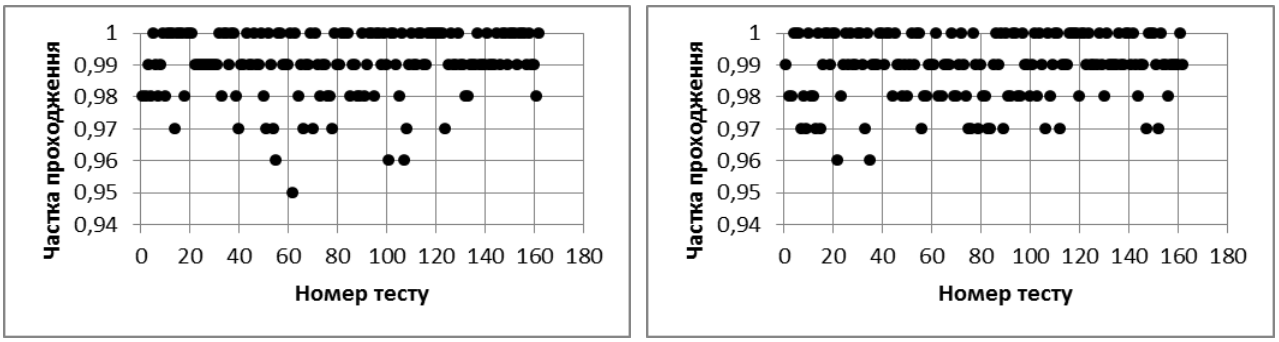
5. Основні властивості шифру

5.1. Статистичні властивості шифру «Кипарис»

Статистичні властивості шифруючого перетворення та СРК оцінювалися згідно з методикою NIST STS [8]. Для оцінки статистичних властивостей були обрані вхідні послідовності, що мають максимальну збитковість.

Для тестування шифруючого перетворення була обрана послідовність відкритих текстів $m_0 = 0$, $m_1 = 1$, …, $m_i = i$, $m_n = 100000$ (з максимальною збитковістю). Вихідна послідовність шифртекстів (отримана в режимі електронної кодової книги) тестувалася згідно з NIST STS.

Статистичні профілі вихідних послідовностей для розміру блока 256 та 512 біт наведені на рис. 2, *а* та *б* відповідно.

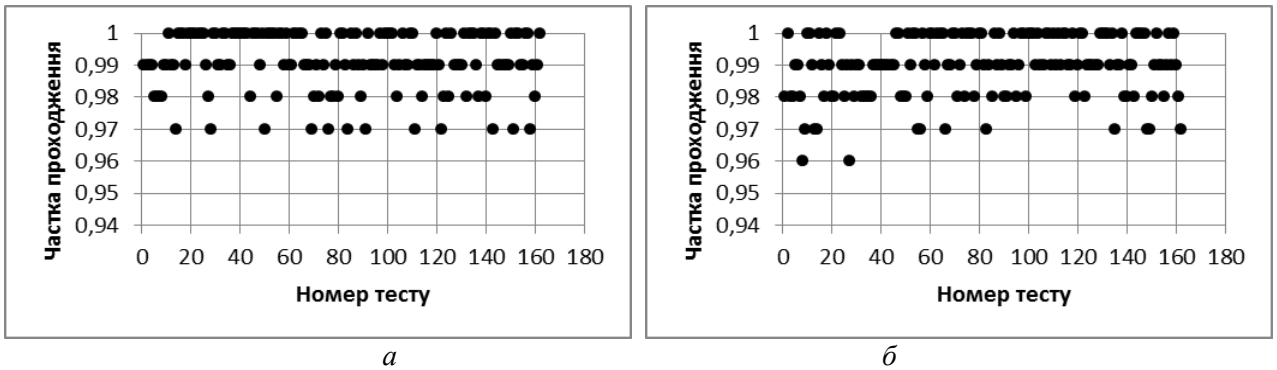


а *б*

Рис. 2. Статистичні профілі вихідних послідовностей для розміру блока 256 та 512 біт

Для тестування схеми розгортання ключів була обрана послідовність ключів шифрування $K_0 = 0$, $K_1 = 1$, …, $K_i = i$, $K_n = 100000$ (з максимальною збитковістю). Отримані циклові ключі формували вихідну послідовність, що тестувалася згідно з NIST STS.

Статистичні профілі вихідних послідовностей циклових ключів для довжини ключа 256 та 512 біт наведені на рис. 3, *а* та *б* відповідно.



а *б*

Рис. 3. Статистичні профілі вихідних послідовностей для розміру блока 256 та 512 біт

6.2. Лавинні показники шифру «Кипарис»

Лавинний ефект [9] є властивістю шифру, яка означає, що зміна малої кількості бітів у відкритому тексті призведе до «лавинної» зміни значень бітів шифртексту. Якщо блоковий шифр не володіє достатнім лавинним ефектом, криптоаналітик може зробити припущення щодо вхідної інформації, спираючись на вихідну інформацію, тому досягнення лавинного ефекту є важливою метою при розробці блокового шифру.

Вважається, що алгоритм задовольняє лавинному критерію, якщо зміна одного біта відкритого тексту призводить до зміни не менше половини бітів шифртексту.

Для оцінки лавинного ефекту шифру «Кипарис» були обчислені наступні показники:

1) мінімум математичного сподівання (МС) кількості вихідних бітів, що змінилися при зміні одного вхідного біта для N блоків даних;
2) максимум математичного сподівання кількості вихідних бітів, що змінилися при зміні одного вхідного біта для N блоків даних;
3) мінімум середньоквадратичного відхилення (СКВ) кількості вихідних бітів, що змінилися при зміні одного вхідного біта для N блоків даних;
4) максимум середньоквадратичного відхилення кількості вихідних бітів, що змінилися при зміні одного вхідного біта для N блоків даних.

У табл. 3, 4 наведені результати обчислення лавинних показників для шифрів «Кипарис-256» та «Кипарис-512» відповідно.

Таблиця 3

Лавинні показники шифру «Кипарис-256»

Кількість циклів шифрування	Показник	Значення	Кількість циклів шифрування	Показник	Значення
1	Мінімум МС	1	6	Мінімум МС	127,941
	Максимум МС	65,0254		Максимум МС	128,078
	Мінімум СКВ	0		Мінімум СКВ	63,2596
	Максимум СКВ	49,8347		Максимум СКВ	64,7305
2	Мінімум МС	62,3417	7	Мінімум МС	127,94
	Максимум МС	128,016		Максимум МС	128,066
	Мінімум СКВ	32,1742		Мінімум СКВ	63,1499
	Максимум СКВ	81,6093		Максимум СКВ	64,7323
3	Мінімум МС	125,375	8	Мінімум МС	127,927
	Максимум МС	128,06		Максимум МС	128,064
	Мінімум СКВ	63,3573		Мінімум СКВ	63,2817
	Максимум СКВ	82,1095		Максимум СКВ	64,7861
4	Мінімум МС	127,929	9	Мінімум МС	127,924
	Максимум МС	128,079		Максимум МС	128,072
	Мінімум СКВ	63,2875		Мінімум СКВ	63,2531
	Максимум СКВ	64,6699		Максимум СКВ	64,7662
5	Мінімум МС	127,926	10	Мінімум МС	127,941
	Максимум МС	128,09		Максимум МС	128,075
	Мінімум СКВ	63,2186		Мінімум СКВ	63,2797
	Максимум СКВ	64,8311		Максимум СКВ	64,778

Таблиця 4

Лавинні показники шифру «Кипарис-512»

Кількість циклів шифрування	Показник	Значення	Кількість циклів шифрування	Показник	Значення
1	Мінімум МС	1	8	Мінімум МС	255,889
	Максимум МС	161,034		Максимум МС	256,096
	Мінімум СКВ	0		Мінімум СКВ	126,625
	Максимум СКВ	417,279		Максимум СКВ	129,672
2	Мінімум МС	98,0896	9	Мінімум МС	255,9
	Максимум МС	256,052		Максимум МС	256,078
	Мінімум СКВ	63,6531		Мінімум СКВ	126,646

	Максимум СКВ	481,193		Максимум СКВ	129,51
3	Мінімум МС	225,032	10	Мінімум МС	255,911

Продовження табл. 4

Кількість циклів шифрування	Показник	Значення	Кількість циклів шифрування	Показник	Значення
3	Максимум МС	256,081	10	Максимум МС	256,109
	Мінімум СКВ	126,813		Мінімум СКВ	126,321
	Максимум СКВ	482,083		Максимум СКВ	129,6
4	Мінімум МС	255,911	11	Мінімум МС	255,912
	Максимум МС	256,084		Максимум МС	256,1
	Мінімум СКВ	126,4		Мінімум СКВ	126,691
	Максимум СКВ	129,707		Максимум СКВ	129,297
5	Мінімум МС	255,915	12	Мінімум МС	255,909
	Максимум МС	256,1		Максимум МС	256,138
	Мінімум СКВ	125,956		Мінімум СКВ	126,219
	Максимум СКВ	129,338		Максимум СКВ	129,697
6	Мінімум МС	255,862	13	Мінімум МС	255,895
	Максимум МС	256,096		Максимум МС	256,103
	Мінімум СКВ	126,708		Мінімум СКВ	126,53
	Максимум СКВ	129,394		Максимум СКВ	129,524
7	Мінімум МС	255,915	14	Мінімум МС	255,89
	Максимум МС	256,102		Максимум МС	256,108
	Мінімум СКВ	126,838		Мінімум СКВ	126,607
	Максимум СКВ	129,639		Максимум СКВ	129,597

Як видно з табл. 3, 4, «Кипарис-256» та «Кипарис-512» задовольняють лавинному критерію вже після четвертого циклу.

Висновки

З урахуванням сучасних вимог до симетричних примітивів був розроблений постквантовий малоресурсний блоковий шифр «Кипарис», що заснований на мережі Фейстеля. Циклова функція шифру представляє собою ARX-перетворення, схема розгортання циклових ключів неін'єктивна та використовує принципи побудови СРК шифру «Калина». Алгоритм підтримує довжину блока (ключа) 256 та 512 бітів, що дозволяє забезпечити необхідний рівень криптографічної стійкості. «Кипарис-256» орієнтований на використання на 32-бітних платформах, «Кипарис-512» – на 64-бітних платформах.

Дослідження статистичних властивостей показали, що шифр «Кипарис» та його СРК задовольняють вимогам зі статистичного тестування випадкових послідовностей NIST STS.

Дослідження лавинних показників показали, що шифр «Кипарис-256» (число циклів дорівнює 10) та шифр «Кипарис-512» (число циклів дорівнює 14) відповідають вимогам щодо лавинного ефекту починаючи з чотирьох циклів шифрування.

Вимірювання швидкодії виконувалося на платформі x86 (x86_64) під управлінням ОС Windows та Linux і платформі ARM-v7 під управлінням ОС Android. На різних програмно-апаратних платформах шифр продемонстрував наступні показники швидкодії:

- на платформі x86 з 32-бітною архітектурою «Кипарис-256» у 2,5 рази швидший, ніж AES-256;
- на платформі x86 з 64-бітною архітектурою «Кипарис-512» приблизно у 3 рази швидший, ніж AES-256;
- на платформі ARM-v7 з 32-бітною архітектурою «Кипарис-256» та «Кипарис-512» приблизно у 3 рази швидші за AES-256.

Таким чином, у порівнянні з шифрами «Калина» та AES, блоковий шифр «Кипарис» має наступні переваги:

- висока швидкодія перетворень незалежно від використовуваної платформи;

– наявність варіантів алгоритму, оптимізованих як під 64-бітові, так і під 32-бітові системи;
– компактна реалізація як для стаціонарних систем, так і для мобільних платформ;
– швидкодіюча реалізація не потребує використання таблиць передобчислень, що забезпечує використання мінімального об'єму пам'яті;
– можливість організації ефективних захищених високошвидкісних каналів зв'язку між мобільними системами та серверами, у тому числі тими, що використовують апаратні прискорювачі;
– постійний час шифрування блока на сучасних процесорах незалежно від параметрів, що обробляються.

Список літератури: 1. *Standard, Advanced Encryption*. Federal Information Processing Standards Publication 197 / FIPS PUB, 46-3. – 2001. – 51 p. 2. *ДСТУ* 7624:2014. *Інформаційні* технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Введ. 01–07–2015. – К. : Мінекономрозвитку України, 2015. – 119 с. 3. *Bogdanov, A.* PRESENT: An Ultra-Lightweight Block Cipher / A. Bogdanov, L.R. Knudsen, G. Leander et al.: Springer Berlin Heidelberg, 2007. – pp. 450-466. 4. *Needham, Roger M.* Tea extensions] / Roger M. Needham, D. J. Wheeler // Report, Cambridge University, Cambridge, UK. – 1997 – 4 p. 5. *Beaulieu, Ray, et al.* The SIMON and SPECK lightweight block ciphers.Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015. 6. *Bernstein, Daniel J.* ChaCha, a variant of Salsa20. Workshop Record of SASC. Vol. 8. 2008. 7. *Родінко, М.Ю.* Математична модель оцінки властивостей неін'єктивних схем розгортання ключів симетричних блокових шифрів / М.Ю. Родінко, Р.В. Олійников // Прикладна радіоелектроніка. – 2016. – Т. 15. – № 3. – С. 179-183. 8. *Rukhin, Andrew, et al.* A statistical test suite for random and pseudorandom number generators for cryptographic applications. Booz-Allen and Hamilton Inc Mclean Va, 2001. 9. *Feistel, Horst.* Cryptography and Computer Privacy // Scientific American, Vol. 228, No. 5, 1973.

Харківський національний університет
імені В.Н. Каразіна

Надійшла до редколегії 14.04.2017