тів і зв'язків. Вузли цього короткого графа відповідають групам в максимумі (A, R), сумісні з угрупуваннями. А ребра цього короткого графа є групові відносини виведені з вузла відносин в R.

Висновки. Представлена операція агрегації УГОУВ заснована на угрупування графа. Цей метод дозволяє користувачам вільно вибирати атрибути вузлів і відносини, які становлять інтерес, і виробляють угрупування на основі певних функцій.

В рамках майбутньої роботи можна запропонувати організувати розробку формальної моделі графа даних і мови запитів, що дозволяє включення до УГОУВ, поряд з цілим рядом інших додаткових поширених і корисних методів графа відповідності.

Список використаних джерел:

1. Newman M. E. J. [Text]. The structure and function of complex networks. SIAM Review. 2003. P.167–256.
2. Leskovec J., Faloutsos C. [Text]. Sampling from large graphs. Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2006. C. 631–636.
3. Koby Crammer, OferDekel, Joseph Keshet, Shai Shalev-Shwartz, Yoram Singer. [Text]. Online Passive-Aggressive Algorithms. JMLR, 7(Mar): P. 551–585. 2006.

The mathematical model of data aggregation via social networks generalization graph was presented, that can be used in the field of internet marketing and create the necessary packet data for users of social networks.

Key words: *data aggregation, social network platform aggregation, generalization graph, media data.*

Одержано 16.02.2017

УДК 621.3.06

М. Ю. Родінко, аспірантка

ПАТ «Інститут інформаційних технологій», м. Харків

МАЛОРЕСУРСНИЙ СИМЕТРИЧНИЙ БЛОКОВИЙ ШИФР «КИПАРИС» — СУТНІСТЬ ТА ОСНОВНІ ВЛАСТИВОСТІ

Наведений опис та результати аналізу основних властивостей перспективного малоресурсного симетричного блокового шифру «Кипарис».

Ключові слова: *симетричний блоковий шифр, малоресурсна криптографія, мережа Фейстеля.*

Вступ. У зв’язку із поширенням Інтернету речей, до криптографічних алгоритмів, у тому числі й симетричних, висуваються нові вимоги. Такі блокові шифри, як «Калина» (ДСТУ 7624-2014 [1]), AES

[2] забезпечують високий рівень криптографічної стійкості та швидкодії на сучасних платформах, проте мають обмеження для застосування у малоресурсній криптографії (lightweight cryptography) для пристроїв із обмеженою кількістю споживання енергії. Для таких цілей необхідний блоковий шифр, який не тільки має достатній запас стійкості, але й забезпечує компактну реалізацію і високу швидкодію на різних програмно-апаратних платформах.

На сьогоднішній день існує достатньо багато малоресурсних блокових шифрів (PRESENT [3], XTEA [4], CLEFIA [5] та ін.), проте вони не забезпечують високого рівня криптографічної стійкості. Таким чином, актуальною задачею є розробка малоресурсного блокового шифру, в якому висока криптографічна стійкість (за умовами постквантової криптографії) поєднується з високими показниками швидкодії. В даній роботі пропонується саме такий перспективний малоресурсний алгоритм симетричного блокового перетворення «Кипарис». Далі наведений опис алгоритму.

Загальні параметри шифру. Алгоритм шифрування «Кипарис» виконує перетворення блоків даних розміром $l = 256$ (або 512) біт із використанням ключа шифрування довжиною $k = 256$ (512) біт. Довжина ключа співпадає з розміром блока. Усі операції в шифрі «Кипарис» виконуються над s-бітними словами, де $s = 32$ (64) біт в залежності від розміру блока/довжини ключа. Основні загальні параметри шифру наведені в табл. 1.

Отже, «Кипарис-256» орієнтований на використання на 32-бітних платформах, «Кипарис-512» — на 64-бітних платформах, в тому числі із вимогами до компактної реалізації та обмеженого енергоспоживання.

Таблиця 1

Загальні параметри алгоритму «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

До вхідних даних алгоритму «Кипарис» належать відкритий текст та ключ шифрування. Відкритий текст P складається з восьми s-бітних слів $P[0] \| P[1] \| ... \| P[7]$. Ключ шифрування також складається з восьми s-бітних слів $K[0] \| K[1] \| ... \| K[7]$.

До вихідних даних алгоритму належить шифртекст $C[0] \| C[1] \| ... \| C[7]$.

Процедура зашифрування. На вхід процедури зашифрування подається блок відкритого тексту $P = (P[0], P[1], ..., P[7])$ та циклові ключі RK_0, RK_1, …, RK_{t-1}, де кожен ключ $RK_i = (RK[0], RK[1], ..., RK[7])$.

В основі процедури шифрування лежить мережа Фейстеля. Блок відкритого тексту P ділиться на два підблоки: $L_0 = (P[0], P[1], P[2], P[3])$, $R_0 = (P[4], P[5], P[6], P[7])$. Вихід i-ої ітерації перетворення обчислюється як:

$$L_i = R_{i-1} \oplus f\left(L_{i-1}, RK_{i-1}\right),$$
$$R_i = L_{i-1}.$$

В основу циклової функції покладено ARX-перетворення. На вхід циклової функції подається чотири s-бітних слова $f = (P_0', P_1', P_2', P_3')$. Вихідне значення обчислюється як:

$$P_0' \boxplus = P_1',\ P_3' \oplus = P_0',\ ROL_{r1}(P_3');$$
$$P_2' \boxplus = P_3',\ P_1' \oplus = P_2',\ ROL_{r2}(P_1');$$
$$P_0' \boxplus = P_1',\ P_3' \oplus = P_0',\ \mathrm{ROL}_{r3}(P_3'),$$
$$P_2' \boxplus = P_3',\ P_1' \oplus = P_2',\ \mathrm{ROL}_{r4}(P_1');$$
$$P_0' \boxplus = P_1',\ P_3' \oplus = P_0',\ \mathrm{ROL}_{r1}(P_3');$$
$$P_2' \boxplus = P_3',\ P_1' \oplus = P_2',\ \mathrm{ROL}_{r2}(P_1');$$
$$P_0' \boxplus = P_1',\ P_3' \oplus = P_0',\ \mathrm{ROL}_{r3}(P_3');$$
$$P_2' \boxplus = P_3',\ P_1' \oplus = P_2',\ \mathrm{ROL}_{r4}(P_1'),$$

де $P_i' \boxplus = P_j'$ — додавання за модулем s двох s-бітних слів; $P_i' \oplus = P_j'$ — XOR двох s-бітних слів; $\mathrm{ROL}_{ri}(P_j')$ — циклічний зсув s-бітного слова вліво на ri біт.

Значення циклічних зсувів (r_0, r_1, r_2, r_3) залежать від довжини блока і практично 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. Циклові ключі слід подавати у зворотному порядку.

Циклові ключі формуються за допомогою неін'єктивної схеми розгортання ключів шифру «Калина».

Аналіз статистичних та лавинних показників шифру. Аналіз статистичних властивостей шифру показав, що шифр «Кипарис» та його схема розгортання ключів задовольняють вимогам зі статистичного тестування випадкових послідовностей NIST STS. Статистичні профілі вихідних послідовностей шифруючого перетворення для розміру блока 256 та 512 біт показані на рис. 1 та 2.

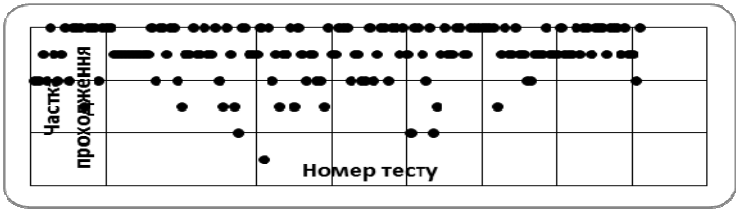

Рис. 1. *Статистичний профіль вихідної послідовності шифруючого перетворення для розміру блока 256 біт*

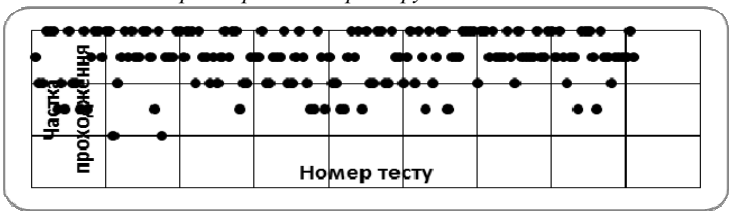

Рис. 2. *Статистичний профіль вихідної послідовності шифруючого перетворення для розміру блока 512 біт*

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

а) мінімум математичного сподівання кількості вихідних бітів, що змінилися при зміні одного вхідного біта для *N* блоків даних;
б) максимум математичного сподівання кількості вихідних бітів, що змінилися при зміні одного вхідного біта для *N* блоків даних;
в) мінімум середньоквадратичного відхилення кількості вихідних бітів, що змінилися при зміні одного вхідного біта для *N* блоків даних;
г) максимум середньоквадратичного відхилення кількості вихідних бітів, що змінилися при зміні одного вхідного біта для *N* блоків даних.

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

У табл. 2 наведені результати обчислення лавинних показників для шифру «Кипарис-256». Як видно з таблиці, «Кипарис-256» відповідає вимогам щодо лавинного ефекту починаючи з чотирьох циклів шифрування («Кипарис-512» також задовольняє лавинному критерію вже після 4-го циклу).

Аналіз продуктивності шифру. 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:

а) Intel Core i3 / Windows 7 x32 з компілятором Visual C++ 2010;
б) Intel Core i3 / Windows 7 x64 з компілятором Visual C++ 2010;

в) Intel Core i5 / Linux (64 bit) з компілятором g++ версії 4.8;
г) ARM Cortex-A7 / Android 4.2.2 Jelly Bean (32 bits).

Таблиця 2

Лавинні показники шифру «Кипарис-256»

Кількість циклів шифрування	**Показник**	**Значення**
1	Мінімум мат. сподівання	1
	Максимум мат. сподівання	65,0254
	Мінімум середньокв. відхилення	0
	Максимум середньокв. відхилення	49,8347
2	Мінімум мат. сподівання	62,3417
	Максимум мат. сподівання	128,016
	Мінімум середньокв. відхилення	32,1742
	Максимум середньокв. відхилення	81,6093
3	Мінімум мат. сподівання	125,375
	Максимум мат. сподівання	128,06
	Мінімум середньокв. відхилення	63,3573
	Максимум середньокв. відхилення	82,1095
4	Мінімум мат. сподівання	127,929
	Максимум мат. сподівання	128,079
	Мінімум середньокв. відхилення	63,2875
	Максимум середньокв. відхилення	64,6699
5	Мінімум мат. сподівання	127,926
	Максимум мат. сподівання	128,09
	Мінімум середньокв. відхилення	63,2186
	Максимум середньокв. відхилення	64,8311
…	…	…
10	Мінімум мат. сподівання	127,941
	Максимум мат. сподівання	128,075
	Мінімум середньокв. відхилення	63,2797
	Максимум середньокв. відхилення	64,778

Результати порівняння швидкодії шифру «Кипарис» та AES-256 наведені у табл. 3.

Таблиця 3

Швидкодія шифрів «Кипарис» та AES, Мбіт/с

Платформа	**Блоковий шифр**		
	«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. 3, 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.

Висновки. Таким чином, запропонований симетричний блоковий шифр «Кипарис», що з точки зору продуктивності та зручності реалізації на різних програмно-апаратних платформах має наступні переваги:

а) два варіанти шифру («Кипарис-256» та «Кипарис-512») орієнтовані на 32-бітову та 64-бітову архітектури відповідно;
б) висока швидкодія перетворень незалежно від платформи:
   1) на платформі x86 з 32-бітною архітектурою шифр «Кипарис-256» у 2,5 рази швидший, ніж AES-256;
   2) на платформі x86 з 64-бітною архітектурою шифр «Кипарис-512» приблизно у 3рази швидший, ніж AES-256;
   3) на платформі ARM Cortex-A7 з 32-бітною архітектурою «Кипарис-256» та «Кипарис-512» приблизно у 3 рази швидші за AES-256;
в) компактна реалізація незалежно від платформи (робоча станція або мобільний пристрій);
г) мінімальний необхідний обсяг пам'яті для швидкодіючої реалізації, відсутність необхідності у таблицях передобчислень;
д) можливість організації ефективних захищених високошвидкісних каналів зв'язку між мобільними системами та серверами, у тому числі тими, що використовують апаратні прискорювачі.

Список використаних джерел:

1. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Текст]. Введ. 01–07–2015. К.: Мінекономрозвитку України, 2015. 119 с.
2. Standard, Advanced Encryption. «Federal Information Processing Standards Publication 197» [Text] / FIPS PUB, 46-3. 2001. 51 p.
3. Bogdanov A., Knudsen L.R., Leander G. et al. PRESENT: An Ultra-Lightweight Block Cipher [Text]: Springer Berlin Heidelberg, 2007. P. 450–466.
4. Needham Roger M., Wheeler D.J. Tea extensions [Text]. Report, Cambridge University, Cambridge, UK. 1997. 4 p.
5. Shirai T., Shibutani K., Akishita T. et al. The 128-bit blockcipher CLEFIA [Text]. Fast software encryption.: Springer Berlin Heidelberg, 2007. P. 181–195.

It is presented a description and the main results of analysis of the main properties of prospective lightweight block cipher «Cypress».

Key words: *block cipher, lightweight cryptography, Feistel network.*

Одержано 01.03.2017