УДК 621.3.06

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ НЕІН'ЄКТИВНИХ СХЕМ РОЗГОРТАННЯ КЛЮЧІВ СИМЕТРИЧНИХ БЛОКОВИХ ШИФРІВ

Марія Родінко, Роман Олійников

Харківський національний університет імені В. Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
m.rodinko@gmail.com, roliynykov@gmail.com

Рецензент: Олександр Кузнецов, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
kuznetsov@karazin.ua

Надійшло квітень 2017

Анотація. *Розглядаються неін'єктивні схеми розгортання циклових ключів, що застосовуються у багатьох відомих блокових шифрах («Калина», FOX, Twofish та ін.). Оцінюється ймовірність співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною схемою розгортання ключів (СРК), і множини ключів шифрування, формулюється та доводиться теорема, що визначає таку ймовірність. Показується, що для повномасштабного шифру з неін'єктивною СРК ймовірність співпадіння потужностей множини послідовностей циклових ключів і множини ключів шифрування практично дорівнює 1. Таким чином, доводиться, що складність атак переборного типу на неін'єктивні СРК практично дорівнює складності атак на ін'єктивні схеми (складність перебірних атак не знижується), при цьому неін'єктивні СРК забезпечують додаткову стійкість до атак на реалізацію та деяких інших криптоаналітичних атак.*

Ключові слова: *симетричний блоковий шифр, схема розгортання ключів, еквівалентні ключі шифрування, блоковий шифр «Калина», ДСТУ 7624:2014.*

1 Вступ

Схема розгортання циклових ключів є одним із основних компонентів симетричного блокового шифру. Схема розгортання ключів (СРК) – це алгоритм, що розширює відносно короткий майстер-ключ (як правило, довжиною від 128-512 біт) до відносно великого розширеного ключа (як, правило декілька сотень чи тисяч бітів) для подальшого застосування в алгоритмах зашифрування/розшифрування [1].

Часто в основу СРК покладено деяке бієктивне перетворення, що дозволяє відобразити ключ шифрування у послідовність циклових ключів. Перші СРК були дуже простими і включали, наприклад, просту перестановку бітів ключа шифрування (DES, IDEA) або пряме чи рекурсивне лінійне перетворення з майстер-ключа [2]. Із розвитком технологій криптоаналізу розробники почали додавати до СРК нелінійні операції (наприклад, підстановки) з метою уникнення атак на зв'язаних ключах.

Використання простої бієктивної функції дозволяє забезпечити компактну реалізацію, відносно високу швидкодію та відсутність еквівалентних ключів шифрування. При цьому, суттєвим недоліком подібних СРК є відсутність властивості односпрямованості, тобто складність відновлення ключа шифрування при знанні одного або декількох підключів є не вищою за поліноміальну. Це робить шифр більш уразливим до атак на реалізацію.

СРК шифру «Калина» (ДСТУ 7624:2014 [3]) розроблялася з урахуванням необхідності захисту від атак на реалізацію та атаки на зв'язаних ключах [4]. З цією метою була розроблена односпрямована СРК, що забезпечує неможливість відновлення циклового ключа при знанні ключа шифрування або інших підключів. Особливістю односпрямованих СРК є те, що вони є неін'єктивними, тобто теоретично припускається існування еквівалентних ключів (таких, що формують однакову послідовність циклових ключів). Односпрямовані СРК застосовуються в таких відомих блокових шифрах, як FOX [5], Twofish [6] та ін. Оцінка ймовірності співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування дозволила б додатково обґрунтувати стійкість односпрямованих СРК та доцільність їх використання у блокових шифрах.

2 Вимоги до схем розгортання ключів

Станом на сьогоднішній день не досягнуто консенсусу щодо необхідних та достатніх умов, яким повинна задовольняти СРК. Розробники приділяють більше уваги основному шифруючому перетворенню, ніж СРК [2]. Багато з існуючих правил проектування СРК є далекими від практичного застосування. Деякі з них є занадто слабкими з точки зору безпеки, деякі фокусуються лише на певних типах атак і є однобічними, інші є емпіричними і не мають достатнього обґрунтування [2].

Загальними принципами побудування СРК є відсутність слабких, напівслабких та еквівалентних ключів. Застосування циклових констант необхідно для попередження симетрії шифру, яка призводить до можливості реалізації слайд-атак [4].

Метою побудування сильної СРК є усунення будь-якої слабкості, яка гіпотетично або практично може бути використана для атаки на блоковий шифр [7]. Як і при проектуванні блокових шифрів, при розробці СРК часто застосовуються методи досягнення перемішування та розсіювання.

У роботі [8] показано, що шифри зі складними СРК є більш стійкими до атак диференціального та лінійного криптоаналізу, ніж шифри з більш простими СРК. Показано, що деякі ітеративні шифри з дуже простими СРК навіть при повному наборі циклів не досягають рівномірного розподілу ймовірностей диференціалів та лінійних корпусів. Водночас показано, що добре спроектовані шифри зі складними СРК досягають рівномірного розподілу швидше, ніж шифри з поганими СРК.

У роботі [9] Л. Кнудсен вважає, що сильна СРК повинна мати наступні загальні властивості, які можуть бути досягнуті водночас:

а) односпрямована функція, стійка до колізій (функція, яку неможливо інвертувати);
б) мінімальна взаємна інформація (між всіма бітами підключа та бітами майстер-ключа);
в) ефективна реалізація.

При розробці шифру «Калина» до СРК перспективного шифру були висунуті наступні вимоги [4]:

а) нелінійна залежність кожного біта кожного циклового ключа від кожного біта ключа шифрування;
б) циклові ключі суттєво відрізняються і мають складну нелінійну залежність;
в) захист від відомих криптоаналітичних атак, що орієнтовані на схему розгортання ключів;
г) відсутність слабких ключів, при яких погіршуються криптографічні властивості або знижується стійкість перетворення;
д) обчислювальна складність формування всіх циклових ключів не перевищує складності зашифрування трьох блоків;
е) простота програмної, програмно-апаратної і апаратної реалізації.

Як додаткові вимоги, розглядалися наступні [4]:

а) неможливість отримання ключа шифрування по одному або декільком цикловим ключам, що є доступними для криптоаналітика;
б) можливість формування циклових ключів у довільному порядку (однакова обчислювальна і просторова складність для зашифрування і розшифрування).

3 Атаки на схеми розгортання ключів

Слайд-атака. Слайд-атака вперше описана А. Бірюковим та Д. Вагнером у 1999 р. та є криптографічною атакою на основі підібраного відкритого тексту. При цьому, у більшості випадків атака дозволяє проводити криптоаналіз багатоциклових шифрів незалежно від числа циклів. Слайд-атака [10] експлуатує степінь самоподоби блокового шифру та в основному застосовується до ітеративних блокових шифрів з періодичною СРК.

Шифр розглядається як результат застосування ідентичних перетворень $F(x,k)$, де k є секретним ключем (при цьому F може складатися більше, ніж з одного циклу шифру) [10].

Ідея атаки полягає у зсуві однієї копії процесу зашифрування відносно іншої копії процесу зашифрування таким чином, що два процеси є зсунутими на один цикл. Це дає можливість легко отримати ключ шифрування після однієї ітерації F. Згідно парадоксу про день народження для здійснення атаки необхідно набрати $2^{n/2}$ пар (M_i, C_i) [10].

*Атака на зв'язаних ключах***.** Атака цього типу [11] припускає, що криптоаналітику відоме деяке математичне співвідношення, що зв'язує між собою ключі. Наприклад, співвідношення може бути простим значенням XOR з відомою константою $K_1 = K_2 \oplus C$ або більш складним зв'язком. Атака вперше була запропонована Е. Біхамом та нагадує слайд-атаку.

Атаки типу «зустріч посередині». Атаки цього типу [1] виникають, коли перша половина циклів шифру та друга половина циклів шифру залежать від різних наборів ключових бітів. Це дозволяє зловмиснику атакувати дві частини незалежно одна від одної і протидіє подвійному шифруванню з блоковим шифром та двома різними ключами.

Слабкі ключі [1]. Слабким вважається ключ K, для якого зашифрування є ідентичною функцією до розшифрування. Напівслабкими вважається пара ключів K та K', для яких зашифрування за допомогою K ідентичне розшифруванню за допомогою K' і навпаки. Якщо число слабких ключів відносно мале, вони можуть не представляти загрози для шифру, якщо той використовується для забезпечення конфіденційності. Однак в деяких режимах гешування (при використанні блокових шифрів), зловмисник може обрати вхідне значення ключа при спробі пошуку колізії. В таких режимах блоковий шифр не повинен мати слабких та напівслабких ключів.

Класи ключів, що виявляються [1]. Одним зі способів зменшення ефективного ключового простору є його поділ на класи і подальший пошук атаки, які показують, до якого класу належить ключ. У деяких випадках об'єм роботи із визначення приналежності ключа до певного класу дуже малий. Подібні ключі іноді називають слабкими [1]. Наприклад, певні ключі в алгоритмі Blowfish призводять до однакових входів у S-блок і можуть бути виявлені у зменшених за кількістю циклів варіантах шифру. Шифр IDEA має декілька класів ключів, що виявляються, лише за допомогою двох зашифрувань обраних відкритих текстів [1].

Прості зв'язки та еквівалентні ключі [1]. Простий зв'язок виникає між двома різними ключами і проявляється як співвідношення між відкритими текстами та шифртекстами. Блокові шифри DES та LOKI мають простий зв'язок, який виражається в наступному: якщо K зашифровує P у C, тоді побітове доповнення K зашифровує побітове доповнення P у побітове доповнення C. Це зменшує ефективний ключовий простір на один біт. Алгоритми DES та LOKI мають пари ключів, для яких простий зв'язок існує, щонайменше, для частини всіх відкритих текстів [1]. Два ключа є еквівалентними, якщо вони зашифровують усі відкриті тексти ідентично. Це може розглядатися як спеціальний вид простого зв'язку.

Атаки на СРК, що не є односпрямованими [1]. СРК не є односпрямованою, якщо маючи декілька циклових підключів, зловмисник може отримати інформацію про ключ шифрування або інші невідомі підключі. Так, відновлення декількох циклових підключів дозволяє відновити більшу частину майстер-ключа в СРК DES. Е. Біхам та А. Шамір використали це для оптимізації їхньої диференціальної атаки на DES. Крім того, це може зробити простішим пошук слабких та зв'язаних ключів для СРК, що не є односпрямованими.

4 Неін'єктивна схема розгортання ключів шифру «Калина»

Розглянемо приклад неін'єктивної СРК (шифр «Калина»). СРК шифру передбачає обчислення допоміжного ключа K_t, на основі якого формуються циклові ключі. Схематично алгоритм формування K_t наведений на рис. 1.

Застосування допоміжного ключа необхідне для забезпечення односпрямованості СРК та руйнування симетрії шифру [4]. Призначення початкового вектора *iv* полягає у забезпеченні унікальних послідовностей циклових ключів для кожної комбінації розміру блока та клю-

ча [4] (наприклад, для режима 128/128 і 128/256 циклові ключі будуть формувати унікальні псевдовипадкові послідовності, навіть якщо 256-бітовий ключ складається зі співпадаючих 128-бітових підблоків, які дорівнюють ключу режиму 128/128).

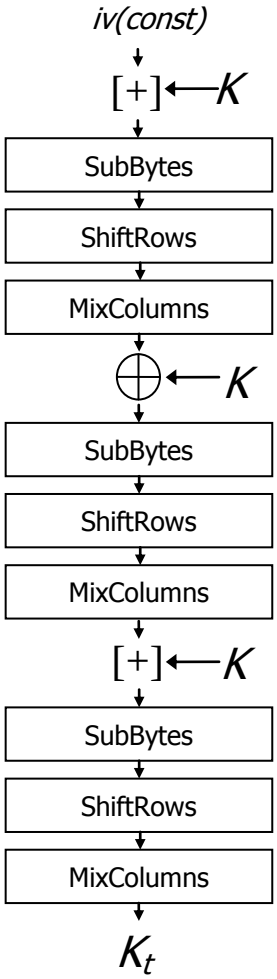

Рис. 1 – Формування допоміжного ключа K_t

Застосування двох ключів та константи забезпечує односпрямованість, унікальність кожного сформованого значення і додатково покращує криптографічні властивості як схеми розгортання, так і всього шифру для забезпечення стійкості до атак, що використовують нерухомі точки циклового перетворення [4]. Циклові ключі з парними індексами формуються на основі ключа шифрування, допоміжного ключа та константи *tmv* (див. Рис. 2), яка залежить від номеру циклу [4]. Циклові ключі з непарними індексами формуються шляхом циклічного зсуву парних. Цей підхід забезпечує як необхідний рівень запасу криптографічної стійкості, так і достатню швидкодію перетворення [4].

5 Оцінка властивостей неін'єктивних схем розгортання ключів

Розв'язання задачі оцінки потужності множини послідовностей циклових ключів було започатковано у [12]. Запропонуємо новий підхід до її вирішення, який дозволяє отримати більш точні оцінки та довести, що для неін'єктивних схем розгортання циклових ключів потужність множини циклових ключів не зменшується у порівнянні з ін'єктивними схемами. Введемо математичну модель оцінки ймовірності співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування. Математична модель використовує припущення, що схема розгортання ключів представляє собою випадкове відображення, що випливає із конструкції та підтверджується результатами статистичного тестування. Тоді справедливою є наступна теорема.

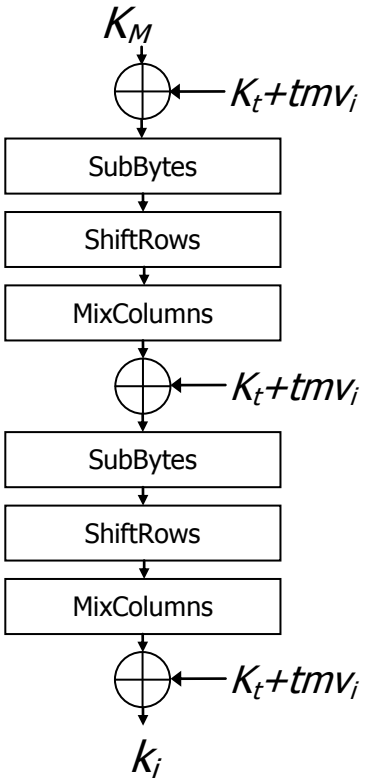

Рис. 2 – Формування циклових ключів з парними індексами

Теорема 1 (про ймовірність співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування).

Нехай τ – неін'єктивна схема розгортання ключів, що реалізує випадкове відображення та має наступні параметри:

k – довжина ключа шифрування в бітах;

l – довжина циклового ключа в бітах;

t – кількість циклових ключів;

$K = 2^k$ – потужність множини ключів шифрування;

$L = 2^{tl}$ – потужність множини послідовностей циклових ключів.

Тоді ймовірність співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування для τ обчислюється через наступне співвідношення:

$$P_\theta = \left(\frac{L}{L-K}\right)^{L-K+\frac{1}{2}} \cdot e^{(-K)}. \quad (1)$$

Доведення.

Нехай задано множину ключів шифрування $\Psi = \left\{K^{(i)} \mid i = 0,1,...,2^k - 1\right\}$ з потужністю $K = |\Psi|$ та множину послідовностей циклових ключів $\Lambda = \left\{L^{(i)} | i = 0,1,...,2^{tl} - 1\right\}$ з потужністю $L = |\Lambda|$.

Послідовність циклових ключів, що формується СРК, має вигляд $L^{(i)} = (L_0^{(i)}, L_1^{(i)}, ..., L_{t-1}^{(i)})$.

Генерація кожної послідовності ключів $L^{(i)}$ виконується за допомогою випадкової функції $f : \Psi \to \Lambda$.

Для кожного ключа шифрування $K^{(i)}$ формується послідовність циклових ключів, тобто всього з множини Λ обирається K послідовностей. Першу послідовність $L^{(0)} = (L_0^{(0)}, L_1^{(0)}, ..., L_{t-1}^{(0)})$ можна обрати L способами, другу $L^{(1)} = (L_0^{(1)}, L_1^{(1)}, ..., L_{t-1}^{(1)})$ *(так, щоб вона*

не співпадала з 1-ю) – $(L-1)$ способами, останню $L^{(K)}=(L_0^{(K)},L_1^{(K)},...,L_{t-1}^{(K)})$ – $(L-(K-1))$ способами. Таким чином, загальна кількість варіантів K послідовностей, що не повторюються,

$$L\cdot(L-1)\cdot...\cdot(L-(K-1))=\frac{L!}{(L-K)!}.$$

Число всіх можливих варіантів послідовностей циклових ключів дорівнює L^K. Тоді ймовірність співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування визначається як

$$P_\theta=\frac{L!}{(L-K)!L^K}.$$

Згідно з формулою Стирлінга, наближене значення факторіала обчислюється як

$$n!\approx\sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

Таким чином, отримуємо:

$$P_\theta=\frac{L!}{(L-K)!\cdot L^K}=\frac{\sqrt{2\pi L}\cdot\left(\frac{L}{e}\right)^L}{\sqrt{2\pi(L-K)}\cdot\left(\frac{L-K}{e}\right)^{L-K}\cdot L^K}=\sqrt{\frac{L}{L-K}}\cdot\frac{e^{-L}\cdot L^L}{e^{-L+K}\cdot(L-K)^{L-K}\cdot L^K}=$$

$$=\sqrt{\frac{L}{L-K}}\cdot e^{-K}\cdot(L-K)^{K-L}\cdot L^{L-K}=\sqrt{\frac{L}{L-K}}\cdot e^{-K}\cdot\left(\frac{L}{L-K}\right)^{L-K}=\left(\frac{L}{L-K}\right)^{L-K+\frac{1}{2}}\cdot e^{-K}.$$

Доведення закінчено.

В таблиці 1 представлені результати розрахунків за формулою (1).

Таблиця 1 – Результати розрахунків

k, біт	l, біт	t	P_θ
4	4	2	0,6197211
		3	0,9710922
		4	0,9981705
		5	0,9998856
		6	0,9999928
		7	0,9999996
		8	0,99999997
		9	0,999999998
		10	0,99999999989
8	8	2	0,6073225
		3	0,9980564
		4	0,9999924
		5	0,99999997
		6	0,99999999988
16	16	2	0,6065337
		3	0,9999924

Як слід з таблиці вже при $K = 2^4$ та $L = 2^{40}$ ймовірність співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування дорівнює 0,99999999989. Зі зростанням довжин ключа шифрування та циклового ключа значення P_θ зростає. Для повномасштабного шифру практично $P_\theta \approx 1$. Цей факт

означає, що складність атак переборного типу на неін'єктивні СРК, практично дорівнює складності атак на ін'єктивні СРК.

6 Висновки

Застосування сильних схем розгортання ключів шифрування дозволяє усунути вразливості, які теоретично і практично можуть бути використані для атаки на шифр. Також, використання сильних СРК покращує характеристики шифру, зокрема диференціальні та лінійні.

До основних вимог, яким повинна задовольняти сильна СРК відносяться односпрямованість, нелінійна залежність між всіма бітами циклових ключів та ключа шифрування і ефективна реалізація.

Більшість відомих атак на схеми розгортання ключів не представляють практичної небезпеки, проте вони демонструють теоретичну слабкість, що може бути використана за певних обставин. При цьому найбільш небезпечними слід вважати атаку на зв'язаних ключах та атаки на СРК, що не є односпрямованими.

Запропонована математична модель оцінки ймовірності співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування. Зокрема, отримано співвідношення, що дозволяє обчислити цю ймовірність. Доведено, що складність атак переборного типу на неін'єктивні схеми розгортання ключів практично дорівнює складності атак на ін'єктивні схеми (*складність перебірних атак не знижується*). При цьому, неін'єктивні СРК забезпечують додаткову стійкість до атак на реалізацію та інших криптоаналітичних атак. Таким чином, при побудуванні перспективного симетричного блокового шифру доцільно використовувати саме неін'єктивну схему розгортання циклових ключів.

Посилання

[1] Kelsey J. Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES / J. Kelsey, B. Schneier, D. Wagner // Advances in Cryptology – CRYPTO'96. – Berlin; Heidelberg : Springer, 1996. – P. 237–251.

[2] Huang J. Revisiting Key Schedule's Diffusion In Relation With Round Function's Diffusion / J. Huang, X. Lai // Designs, codes and cryptography. – 2014. – Vol.73. – №1. – P. 85–103.

[3] Informacijni tehnologii'. Kryptografichnyj zahyst informacii'. Algorytm symetrychnogo blokovogo peretvorennja: DSTU 7624:2014. – [Chynnyj vid 2015–01–07]. – Kyi'v: Minekonomrozvytku Ukrai'ny, 2015. – 48 s.

[4] Olijnykov R. Pryncypy pobudovy i osnovni vlastyvosti novogo nacional'nogo standartu blokovogo shyfruvannja Ukrai'ny / R. Olijnykov, I. Gorbenko, O. Kazymyrov, V. Ruzhencev, Ju. Gorbenko // Zahyst informacii'. – 2015. – T. 17. – №2. – S. 142–157.

[5] Junod P. FOX: a new family of block ciphers / P. Junod, S. Vaudenay // Selected Areas in Cryptography. – Berlin; Heidelberg: Springer, 2005. – P. 114–129.

[6] Schneier B. Twofish: A 128-Bit Block Cipher / B. Schneier, et al. // AES algorithm submission. – June 15, 1998. – 68 p.

[7] May L. Strengthening the Key Schedule of the AES / L. May, M. Henricksen // Information Security and Privacy. – Berlin; Heidelberg: Springer, 2002. – P. 226–240.

[8] Knudsen R. Lars. On the Role of Key Schedules in Attacks on Iterated Ciphers / Lars R. Knudsen, John E. Mathiassen // Computer Security–ESORICS 2004. – Berlin; Heidelberg: Springer, 2004. – P. 322–334.

[9] Knudsen L. R. Practically secure Feistel ciphers / L. R. Knudsen // Fast Software Encryption. – Berlin; Heidelberg: Springer, 1993. – P. 211 – 221.

[10] Biryukov A. Slide attacks / A. Biryukov, D. Wagner // In Fast Software Encryption. – Berlin; Heidelberg: Springer, 1999. – P. 245–259.

[11] Biham Eli. New types of cryptanalytic attacks using related keys / Eli Biham // Journal of Cryptology. – Berlin; Heidelberg: Springer – Verlag, 1994. – Vol. 7. – №4 – P. 229–246.

[12] Olijnykov R.V. Metody analizu i syntezu perspektyvnyh symetrychnyh kryptografichnyh peretvoren': Dys. na zdobuttja nauk. st. doktora tehn. nauk po special'nosti 05.13.05 – Komp'juterni systemy ta komponenty. KhNURE / R.V. Olijnykov. – Kharkiv, 2014. – 423 s.

Reviewer: Alexandr Kuznetsov Dr., Full Professor, V.N. Karazin Kharkiv National University, Kharkov, Ukraine
E-mail: kuznetsov@karazin.ua

Received: April 2017

Authors:
M. Rodinko, PhD student, Department of Information Systems and Technologies Security, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: m.rodinko@gmail.com

R. Oliynykov, Doctor of Sciences (Engineering), Ph.D. (Engineering), Full Prof., Department of Information Systems and Technologies Security, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: roliynykov@gmail.com

The research of block ciphers non-injective key schedules properties.

Abstract. The considers non-injective key schedules used in many known block ciphers ("Kalyna", FOX, Twofish, etc.). It is estimated the probability of matching of round keys (formed by non-injective key schedule) set and encryption keys set cardinalities; a theorem which determines such a probability is formulated and proved. It is shown that for a full cipher with a non-injective key schedule, the probability of matching of round keys set and encryption keys set cardinalities is practically equal to 1. Thus, it is proved that the exhaustive search attacks complexity on non-injective key schedules is almost equal to injective ones (the exhaustive search attacks complexity does not decrease). At the same time, non-injective key schedules provide additional strength to attacks on the implementation and other attacks.

Key words: block cipher, key schedule, equivalent keys, block cipher "Kalyna", DSTU 7624: 2014.

Рецензент: Олександр Кузнецов, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: kuznetsov@karazin.ua

Поступила: Апрель 2017.

Авторы:
Мария Родинко, аспирантка, каф. «Безопасности информационных систем и технологий», Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: m.rodinko@gmail.com
Роман Олейников, д.т.н., проф., каф. «Безопасности информационных систем и технологий», Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: roliynykov@gmail.com

Исследование свойств неинъективных схем разворачивания ключей симметричных блочных шифров.

Аннотация. Рассматриваются неинъективные схемы разворачивания цикловых ключей, применяемые во многих известных блочных шифрах («Калина», FOX, Twofish и др.). Оценивается вероятность совпадения мощностей множества последовательностей цикловых ключей, которые формируются неинъективной схемой разворачивания ключей (СРК), и множества ключей шифрования; формулируется и доказывается теорема, которая определяет такую вероятность. Показывается, что для полномасштабного шифра с неинъективной СРК вероятность совпадения мощностей множества последовательностей цикловых ключей и множества ключей шифрования практически равна 1. Таким образом, доказывается, что сложность атак переборного типа на неинъективные СРК практически равна сложности атак на инъективные схемы (сложность переборных атак не снижается), при этом неинъективные СРК обеспечивают дополнительную стойкость к атакам на реализацию и другим криптоаналитическим атакам.

Ключевые слова: симметричный блочный шифр, схема разворачивания ключей, эквивалентные ключи шифрования, блочный шифр «Калина», ДСТУ 7624: 2014.