УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.08**

В.І. РУЖЕНЦЕВ, д-р техн. наук

ПОРІВНЯЛЬНИЙ АНАЛІЗ ARX СХЕМ ШИФРУВАННЯ

Вступ

Базовим елементом для багатьох сучасних систем захисту інформації є блоковий симетричний шифр (БСШ). З 2000 р. по теперішній час найбільш розповсюдженим в світі БСШ може вважатися AES (FIPS-197). Відомо, що цей алгоритм орієнтований на використання у 32-бітних платформах. Приблизно з 2005 р. зрозумілою стала актуальність розроблення шифру, який би був більш швидким та потребував би значно менших ресурсів на широкому спектрі сучасних обчислювальних систем, – так званого малоресурсного шифру (lightweight cryptography). На думку багатьох вчених, саме такі шифри мають використовуватися у системах Internet of Things (IoT).

В якості базових перетворень до малоресурсного БСШ перспективними сьогодні вважаються перетворення групи ARX – addition, rotation, xor. З використанням лише цих трьох типів перетворень за останній час було створено багато алгоритмів шифрування. До таких алгоритмів можна віднести шифри сімейства RC. Початком сучасного етапу розвитку ARX криптоагоритмів можна вважати роботи [1, 2], в яких запропоновано клас ARX потокових включно з алгоритмами Salsa та Chacha. Фіналісти конкурса SHA-3 Skein [3] та Blake [4] також є ARX алгоритмами. Пізніше запропоновані алгоритми шифрування Chaskey-cipher [5], Sparx [8], LAX [8], Американським агентством безпеки (American National Security Agency) запропоновано шифр Speck [6], південно-корейські вчені розробили lea [7].

ARX перетворення швидкі, ефективно реалізуються багатьма сучасними процесорами, легко масштабуються. Головна проблема пов’язана із доведенням криптографічних властивостей таких алгоритмів.

Найбільш ефективними криптоаналітичними атаками на ARX алгоритми вважаються диференційний та лінійний криптоаналіз [9 – 12], алгебраїчні атаки, атака «зсуву»(rotational cryptanalysis), атака зустріч у середині» (meet-in-the-middle) [9, 13], інтегральний криптоаналіз [14] та його варіант, що отримав назву «division» криптоаналіз [15, 16], атака нездійснених диференціалів [17] та інші.

Оцінювання стійкості до відомих криптоаналітичних атак є одним з найбільш важливих і, разом з тим, складних етапів створення сучасного блокового симетричного шифру. Існує декілька пояснень складності цього етапу. По-перше, існує багато видів криптоаналітичних атак, які постійно вдосконалюються, також з’являються нові види атак. По-друге, складність прямої перевірки стійкості шифру до багатьох атак є занадто великою для того, щоб здійснити таку перевірку за прийнятний час навіть з використанням дуже потужних обчислювальних систем. По-третє, багато з існуючих методів оцінювання стійкості не надають гарантій того, що шифр буде захищеним від даної атаки. По-четверте, розмір блока симетричних шифрів постійно збільшується і, якщо деякий метод оцінювання стійкості пов’язаний з вирішенням задач переборного типу для частини блока або ключа, то він може виявитись занадто складним для роботи з шифрами зі збільшеним блоком. Важливо також, що недостатня точність методів оцінювання стійкості може привести або до вразливостей криптографічного алгоритму, або до його низької швидкості.

При цьому відомо, що однією з переваг ARX структур є можливість їх масштабування. Тому можна розраховувати, що зменшена модель таких перетворень збереже криптографічні властивості повномасштабного прообразу. Підхід з аналізом зменшених моделей використовувався і в інших наших роботах [18].

Загальною метою роботи є обрання або запропонування найкращої з точки зору ефективність-стійкість структури ARX-перетворення.

Для досягнення мети на початковому етапі дослідження на прикладі аналізу опису відомих ARX-криптоалгоритмів планується виділити декілька найбільш вдалих рішень. Для обраних варіантів розробити зменшені програмні моделі (моделі зі значно зменшеним розміром блоку та ключа, для яких можливо, застосувавши «силові» методи, оцінити криптоаналітичні властивості), за допомогою яких проаналізувати такі властивості, як швидкість та ефективність реалізації, стійкість до найбільш потужних криптоаналітичних атак, серед яких диференційний та лінійний криптоаналіз, алгебраїчні атаки та інші.

На наступному етапі, використовуючи зменшені моделі, планується проаналізувати вплив таких параметрів шифруючого перетворення, як кількість та розмір підблоків, кількість окремих базових перетворень (модульне додавання, зсув, XOR-додавання), на стійкість цього перетворення до основних криптоаналітичних атак. Зробити спробу формалізувати залежність стійкості кінцевого перетворення від властивостей та кількості базових перетворень. Якщо така залежність буде знайдена, то вона може бути використана і для визначення стійкості повнорозмірного ARX-перетворення.

1. Зменшені ARX моделі

Перша ARX-схема QR – це quarter-round потокового алгоритму Chacha 2 [1] зі зменшеним розміром підблоків. 16-бітовий блок схеми QR складається з чотирьох 4-бітових підблоків (рис. 1).

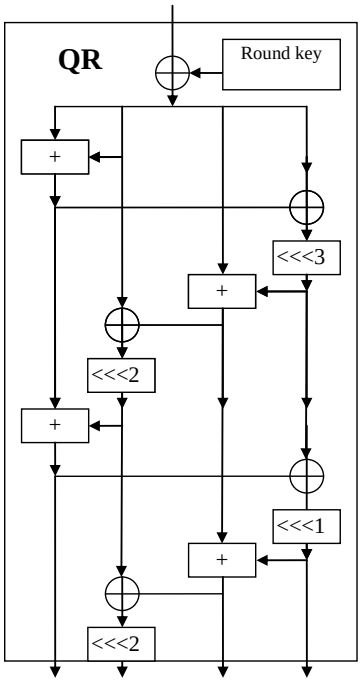


Рис. 1. QR схема

Подібна схема перетворень використовується і в блоковому алгоритмі шифрування Cypress [19].

Друга ARX-схема HR – це спрощена схема алгоритму Speckey. Спрощення полягає у відсутності двох операцій циклічного зсуву, які в оригінальному варіанті передували операціям модульного додавання. 16-бітовий блок схеми HR складається з двох 8-бітових підблоків (рис. 2).

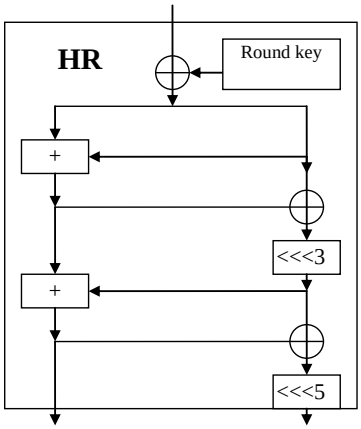


Рис.2. HR схема

Зменшена модель циклу алгоритму Simon представлена на рис. 3.

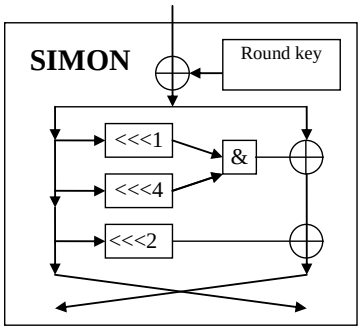
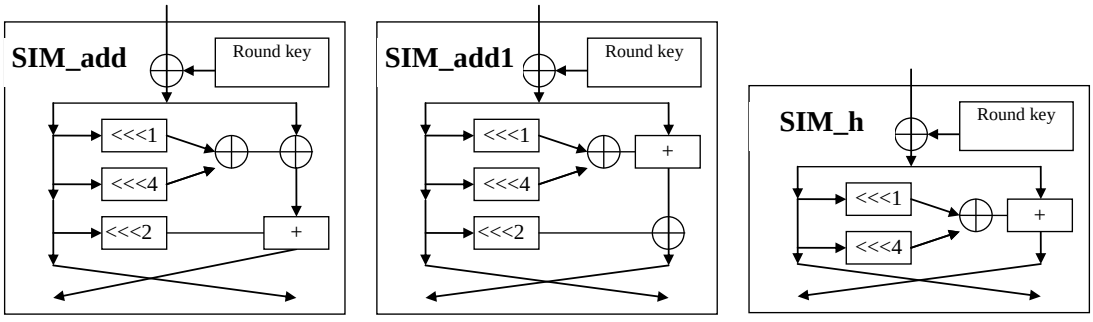


Рис. 3. Схема циклової функції шифру Simon

Як виявилося пізніше, в такому вигляді алгоритм навіть при великій кількості циклів не виходить на показники випадкової підстановки, отже в роботі також розглядалися модифікації Sim_add, Sim_add1, Sim_h, які представлено на рис. 4, *а – в* та які замість операції AND та деяких операцій XOR використовують модульне додавання.



а *б* *в*

Рис. 4. Модифікації циклової функції шифру Simon

Наступна ARX-схема – це зменшена схема алгоритму Chaskey. 16-бітовий блок схеми Chaskey складається з чотирьох 4-бітових підблоків (рис. 5).

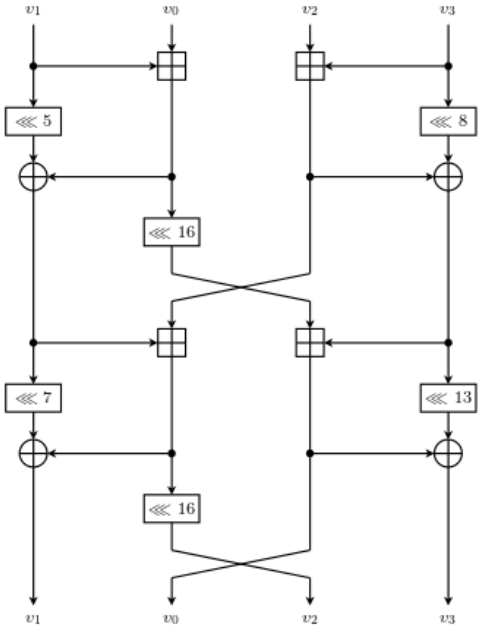


Рис. 5. Схема циклової функції шифру Chaskey

У табл. 1 представлені кількість і формат операцій для розглянутих вище схем.

Таблиця 1

Кількість та формат операцій в одному циклі шифруючих перетворень (без додавання ключа)

Шифруючі схеми	Модульне додавання (Addition)	Циклічний зсув (Rotation)	XOR
HR	2*8 bit	2*8 bit	2*8 bit
QR	4*4 bit	4*4 bit	4*4 bit
Simon	1*8 bit	3*8 bit	1*8 bit +1 AND
Sim_add	1*8 bit	3*8 bit	2*8 bit
Sim_add1	1*8 bit	3*8 bit	2*8 bit
Sim_h	1*8 bit	2*8 bit	1*8 bit
Chaskey	4*4 bit	4*4 bit	4*4 bit

Серед схем, які обрано для аналізу, є такі, що працюють з 4-бітними блоками (QR та Chaskey), та такі, що працюють з 8-бітними блоками (HR та варіанти алгоритму Simon). Кожна операція додавання (модульна або XOR), що працює з 8-бітними блоками, майже еквівалентна двом 4-бітним ідентичним операціям. Виконання 8-бітного циклічного зсуву потребує більших ресурсів ніж дві ідентичні 4-бітові операції. Але все одно, при порівнянні 4-бітних та 8-бітних схем можна вважати, що кожна 8-бітна операція еквівалентна двом таким 4-бітним операціям. Наприклад, схема HR містить у два рази менше операцій, чим QR, але формат операцій у два рази більше, ніж у схемі QR. Тому з погляду на швидкість або продуктивність ці схеми можна вважати еквівалентними при реалізації на 4-бітному процесорі, але на 8-бітному процесорі HR буде майже удвічі швидшою.

2. Аналіз криптографічної стійкості

Найбільш вагомими криптографічними показниками шифруючої функції є:

- максимальна імовірність проходження різниці (визначає стійкість шифру до атак диференціального криптоаналіза);

- максимальна імовірність лінійної апроксимації (визначає стійкість шифру до атак лінійного криптоаналіза);

- нелінійний порядок (визначає стійкість шифру до атак інтерполяційного, алгебраїчного криптоаналіза).

Для зменшених моделей шифруючих функцій є можливість визначити ці показники. Подібний підхід використовувався, наприклад, в роботі [18].

2.1. Стійкість до диференційних атак

Для обчислення максимальної імовірності проходження різниці через *n*-бітну функцію необхідно попередньо побудувати таблицю різниці, що складається зі значень

$$e_s(a, b) = \#\{x \in GF(2^n) \mid S(x \oplus a) \oplus S(x) = b\}$$

для всіх варіантів вхідної та вихідної різниць $a, b \in GF(2^n)$.

Максимальна імовірність проходження різниці через функцію $p_{D\ \max}$ визначається як усереднене для всіх ключів значення

$$p_{D\max} = \frac{\max\limits_{a\neq 0; b} e_s(a,b)}{2^n}.$$

Відомо, що для випадкової підстановки 16 в 16 бітів $p_{D\max} = 20/2^{-16} = 2^{-11,7}$.

З використанням вичерпного перебору вхідних різниць було здійснено пошук диференціалів, що володіють максимальною імовірністю, для розглянутих ARX схем. В ході пошуку використовувалися 64 випадково обраних ключі. Результати наведено у табл. 2.

Таблиця 2

Ймовірності диференціалів (для 64 випадкових ключів)

Шифруючі схеми	Кількість циклів							
	1	2	3	4	5	6	7	8
HR	1	2^{-2}	$2^{-4,6}$	$2^{-9,1}$	$2^{-11,7}$	$2^{-11,7}$	$2^{-11,7}$	$2^{-11,7}$
QR	1	2^{-2}	2^{-5}	$2^{-10,2}$	$2^{-11,7}$	$2^{-11,7}$	$2^{-11,7}$	$2^{-11,7}$
Simon	-	-	-	2^{-3}	-	$2^{-6,6}$	-	$2^{-7,9}$
Sim_add	1	$2^{-0,8}$	$2^{-1,7}$	2^{-4}	$2^{-5,9}$	$2^{-9,8}$	$2^{-11,5}$	$2^{-11,5}$
Sim_add1	1	2^{-2}	$2^{-3,8}$	$2^{-5,8}$	$2^{-8,9}$	$2^{-11,8}$	$2^{-11,8}$	$2^{-11,8}$
Sim_h	1	2^{-2}	$2^{-2,5}$	$2^{-4,4}$	2^{-6}	$2^{-8,3}$	2^{-10}	$2^{-11,7}$
Chaskey	1	2^{-3}	$2^{-8,7}$	$2^{-11,1}$	$2^{-11,8}$	$2^{-11,8}$	$2^{-11,8}$	$2^{-11,7}$

Отримані результати демонструють, що моделі приходять до стабільного значення $2^{-11,7}$ при використанні деякої кількості циклів. HR, QR та Chaskey потребують для цього п’ять циклів, Sim_add – 7 циклів, Sim_add1 – 6 циклів, Sim_h – вісім циклів.

Алгоритм Simon, навпаки, не виходить на показники випадкової підстановки при будь-якій кількості циклів. При однаковій кількості операцій в циклі алгоритм Sim_add1 демонструє кращі показники стійкості ніж Sim_add. З подальшого аналізу виключено алгоритми Simon та Sim_add.

2.2. Стійкість до лінійних атак

Для обчислення максимальної імовірності лінійної апроксимації функції необхідно попередньо побудувати таблицю лінійних апроксимацій, що складається зі значень

$$c_s(a,b) = \#\{x \in GF(2^n) \mid (W(x \,\&\, a) + W(S(x) \,\&\, b)) \bmod 2 = 0\} - 2^{n-1}$$

для всіх варіантів $a, b \in GF(2^n)$, де & – побітова кон’юнкція, $W(x)$ – вага Хемінга вектора x (кількість одиничних бітів у цьому векторі), mod 2 – операція взяття по модулю 2.

Максимальна імовірність лінійної апроксимації функції $p_{L\max}$ визначається як усереднене для всіх ключів значення

$$p_{L\max} = \frac{\left| \max\limits_{a\neq 0, b\neq 0} c_S(a,b) \right|}{2^{n-1}}.$$

Для випадкової підстановки 16 в 16 бітів $p_{L\max} = 2^{-6,4}$.

Для аналізу стійкості розглянутих ARX моделей виконувався пошук лінійної апроксимації, що володіє максимальною імовірністю, для перших п'яти варіантів вхідної маски і для випадково обраних п’яти ключів. Результати представлено в табл. 3.

Таблиця 3

Ймовірності лінійних апроксимацій (для 5 випадкових ключів)

Шифруючі схеми	Кількість циклів							
	1	2	3	4	5	6	7	8
HR	-	$2^{-3,6}$	2^{-6}	$2^{-6,3}$	$2^{-5,9}$	$2^{-8,1}$	$2^{-6,4}$	$2^{-6,4}$
QR	-	2^{-4}	$2^{-4,3}$	2^{-5}	$2^{-5,8}$	$2^{-6,5}$	$2^{-6,6}$	$2^{-8,1}$
Sim_add1	-	$2^{-2,7}$	$2^{-3,7}$	$2^{-5,6}$	$2^{-6,6}$	$2^{-6,5}$	$2^{-6,6}$	$2^{-6,6}$
Sim_h	-	2^{-2}	$2^{-3,7}$	$2^{-5,2}$	$2^{-5,4}$	$2^{-5,4}$	2^{-7}	$2^{-6,6}$
Chaskey	$2^{-0,7}$	$2^{-5,3}$	$2^{-5,2}$	$2^{-5,7}$	$2^{-6,6}$	$2^{-6,6}$	$2^{-8,1}$	$2^{-6,6}$

Отримані результати демонструють, що моделі приходять до стабільного значення $2^{-6,4}$ при збільшенні кількості циклів. Відхилення від цього значення пов'язано з розглядом сильно обмеженої безлічі вхідних масок (5 з 65536).

2.3. Стійкість до алгебраїчних атак

Для оцінки нелінійного порядку n-бітної функції $GF(2^n)\rightarrow GF(2^n)$ варто представити підстановку у вигляді n булевих функцій s_i, $0 \le i \le n-1$, кожна з яких задає відображення $GF(2)^n\rightarrow GF(2)$. Кожна з цих булевих функцій може бути представлена у вигляді суми над $GF(2)$ добутків її аргументів ступеня не вище n-1. Таке представлення булевої функції має назву алгебраїчна нормальна форма. Ступінь нелінійності булевої функції – це максимальний ступінь доданка в алгебраїчній нормальній формі цієї функції. Ступінь нелінійності (чи нелінійний порядок) усієї підстановки – це мінімальний ступінь нелінійності серед усіх складових її булевих функцій s_i, $0 \le i \le n-1$.

Нелінійний порядок для випадкової підстановки 16 в 16 бітів дорівнює 15. При аналізі зменшених моделей використовувався метод [20]. Усі моделі приходять до цього значення при використанні трьох та більше циклів.

3. Порівняльний аналіз ARX схем

Маючи для кожної з розглянутих схем показники стійкості (табл. 2, 3), можна визначити скільки операцій додавання та зсуву потрібно для забезпечення показників випадкової підстановки. У табл. 4, 5 наведена кількість операцій, відповідно, для 8-бітних та 4-бітних схем, яка потрібна для забезпечення показників випадкової підстановки.

Таблиця 4

Кількість 8-бітних операцій для забезпечення стійкості
проти диференційних, лінійних та алгебраїчних атак

Шифруючі схеми	Мінімальна кількість циклів	Кількість 8-бітних операцій			
		Addition	Rotation	Xor	Всього
HR	6	12	12	12	36
Sim_add1	6	6	18	12	36
Sim_h	8	8	16	8	32

Таблиця 5

Кількість 4-бітних операцій для забезпечення стійкості проти диференційних, лінійних та алгебраїчних атак

Шифруючі схеми	Мінімальна кількість циклів	Кількість 4-бітних операцій			
		Addition	Rotation	Xor	Всього
QR	6	24	24	24	72
Chaskey	5	20	20	20	60

Представлені у табл. 4, 5 результати демонструють, що найбільш ефективною 4-бітовою конструкцією можна вважати Chaskey, а найбільш ефективною 8-бітовою – схему Sim_h.

Стосовно схеми Sim_h важливим є те, що операція додавання підблоків (див. рис. 4, *в*) є відмінною від операції введення секретності (додавання з ключем). Якщо в цій схеми поміняти місцями операцію модульного додавання та XOR, то схема не виходить на диференційні показники випадкової підстановки навіть при великій кількості циклів.

Висновки

1. Проведено аналіз показників криптографічної стійкості зменшених моделей (16 бітний блок та ключ) відомих сьогодні ARX алгоритмів шифрування: Salsa, Chacha, Cypress, Speckey, Simon, Chaskey та їх модифікації. Продемонстровано, що для більшості з них можливо отримати показники випадкової підстановки при використанні певної кількості циклів. Виявлено, що схема алгоритму Simon не дозволяє отримати ці показники навіть при великій кількості циклів, що, на наш погляд, свідчить про вразливості цього алгоритму.

2. Показано, що потенційно ARX схеми з більшим форматом операцій є більш гнучкими та ефективними, оскільки, за нашими результатами, потребують приблизно вдвічі меншої кількості операцій для забезпечення криптографічних показників випадкової підстановки. З огляду на це, можливо більш ефективно було б запропонувати ARX схему, яка б працювала з 16-бітними блоками та виходила на показники випадкової підстановки, але поки що цього не вдалось зробити. Можливо це буде метою подальших досліджень.

3. За результатами табл. 4, 5 найбільш ефективною 4-бітовою конструкцією є зменшена модель Chaskey, а найбільш ефективною 8-бітовою – запропонована в роботі схема Sim_h (рис. 4, *в*). При цьому реалізація на 8-бітному процесорі Sim_h потребує майже вдвічі меншої кількості операції ніж Chaskey.

Список літератури:

1. Daniel J. Bernstein. Chacha, a variant of Salsa20. SASC 2008 –the State of the Art in Stream Ciphers. See also https://cr.yp.to/chacha.html, 2008.

2. Daniel J. Bernstein. The salsa20 family of stream ciphers. In Matthew Robshaw and Olivier Billet, editors, New Stream Cipher Designs: The eSTREAM Finalists, volume 4986 of Lecture Notes in Computer Science, pages 84–97, Berlin, Heidelberg, 2008.

3. Ferguson Niels, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein hash function family. Submission to NIST, (round 3), 2010.

4. Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and Raphael C.-W. Phan.SHA-3 proposal BLAKE: Submission to NIST (Round 3). http: //ehash.iaik.tugraz.at/wiki/BLAKE, 2010.

5. Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede. Chaskey: An effcient MAC algorithm for 32-bit microcontrollers. In Antoine Joux and Amr M. Youssef, editors, SAC 2014: 21st Annual International Workshop on Selected Areas in Cryptography, volume 8781 of Lecture Notes in Computer Science, pages 306–323. Springer, Heidelberg, August 2014. Doi:10.1007/978-3-319-13051-4_19

6. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/404.

7. Deukjo Hong, Jung-Keun Lee, Dong-Chan Kim, Daesung Kwon, Kwon Ho Ryu, and Dong-Geon Lee. LEA: A 128-bit block cipher for fast encryption on common processors. In Yongdae Kim, Heejo Lee, and Adrian Perrig, editors, WISA 13: 14th International Workshop on Information Security Applications, volume 8267 of Lecture Notes in Computer Science, pages 3–27. Springer, Heidelberg, August 2014. Doi:10.1007/978-3-319-05149-9_1

8. Daniel Dinu, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, Johann Großschädl, and Alex Biryukov. Design strategies for ARX with provable bounds: Sparx and LAX. In Jung Hee Cheon and Tsuyoshi Takagi, editors,

Advances in Cryptology – ASIACRYPT 2016, Part I, volume 10031 of Lecture Notes in Computer Science, pages 484–513. Springer, Heidelberg, December 2016. Doi:10.1007/978-3-662-53887-6_18

9. Alex Biryukov, Patrick Derbez, and Léo Perrin. Differential analysis and meet-in-the-middle attack against round-reduced TWINE. In Gregor Leander, editor, Fast Software Encryption – FSE 2015, volume 9054 of Lecture Notes in Computer Science, pages 3–27. Springer, Heidelberg, March 2015. Doi:10.1007/978-3-662-48116-5_1

10. Alex Biryukov, Vesselin Velichkov, and Yann Le Corre. Automatic Search for the Best Trails in ARX: Application to Block Cipher Speck. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 9783, 2016. P. 289-310. Doi:10.1007/978-3-662-52993-5_15

11. An Improved Automatic Search Method for Differential Trails in TEA Cipher. International Journal of Network Security, Vol.18, No.4, 2016. PP.644-649.

12. Alex Biryukov, Arnab Roy, and Vesselin Velichkov. Differential Analysis of Block Ciphers SIMON and SPECK. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 8540, 2015. P. 546-570. Doi:10.1007/978-3-662-46706-0_28

13. Patrick Derbez and Léo Perrin. Meet-in-the-middle attacks and structural analysis of round reduced PRINCE. In Gregor Leander, editor, Fast Software Encryption – FSE 2015, volume 9054 of Lecture Notes in Computer Science, pages 190–216. Springer, Heidelberg, March 2015. Doi:10.1007/978-3-662-48116-5_10

14. L. Wen and M. Wang. Integral zero-correlation distinguisher for ARX block cipher, with application to shacal-2," in Information Security and Privacy, pp. 454-461, Springer, 2014. Doi:10.1007/978-3-319-08344-5_32

15. Yosuke Todo. Structural evaluation by generalized integral property. In Elisabeth Oswald and Marc Fischlin, editors, Advances in Cryptology – EUROCRYPT 2015, Part I, volume 9056 of Lecture Notes in Computer Science, pages 287–314. Springer, Heidelberg, April 2015.

16. Christina Boura and Anne Canteaut. Another view of the division property. In Matthew Robshaw and Jonathan Katz, editors, Advances in Cryptology – CRYPTO 2016, Part I, volume 9814 of Lecture Notes in Computer Science, pages 654–682. Springer, Heidelberg, August 2016.

17. Xuexin Zheng and Keting Jia. Impossible differential attack on reduced-round TWINE. In Hyang-Sook Lee and Dong-Guk Han, editors, ICISC 13: 16th International Conference on Information Security and Cryptology, volume 8565 of Lecture Notes in Computer Science, pages 123–143. Springer, Heidelberg, November 2014.

18. Долгов В.И. Анализ циклических свойств блочных шифров / В.И. Долгов, И.В. Лисицкая, В.И. Руженцев // Прикладная радиоэлектроника. 2007. Т. 6, №2. С. 257-263.

19. Малоресурсний симетричний блоковий шифр "Кипарис" – сутність та основні властивості / М.Ю. Родінко // Математичне та комп'ютерне моделювання. Серія: Технічні науки : зб. наук. пр. Кам'янець-Подільський : Кам'янець-Подільськ. нац. ун-т, 2017. Вип. 15. С. 203-208.

20. Knudsen L. R. Truncated and Higher Order Differentials [Text] / L. R. Knudsen // Fast Software Encryption : proceedings of the Second International Workshop, Leuven, Belgium, December 14–16, 1994. Berlin ; Heidelberg : Springer-Verlag, 1995. P. 196–211. (Lecture Notes in Computer Science ; vol. 1008).

Надійшла до редколегії 04.09.2020

Відомості про авторів:

Руженцев Віктор Ігорович – д-р техн. наук, Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій, Україна, e-mail: viktor.ruzhentsev@nure.ua, ORCID: https://orcid.org/0000-0002-1007-6530