DOI 10.20535/2411-1031.2024.12.1.306258
УДК 004.057

ВАЛЕРІЙ ЗАКУСІЛО,
НАТАЛІЯ КУЧИНСЬКА,
СЕРГІЙ КОНЮШОК

ПОШУК ВИСОКОЙМОВІРНІСНИХ РІЗНИЦЕВИХ ХАРАКТЕРИСТИК ЛЕГКОВАГОВОГО БЛОКОВОГО АЛГОРИТМУ PRESENT ІЗ НЕСТАНДАРТНИМИ БЛОКАМИ ЗАМІНИ

Розвиток Інтернету речей та велика різноманітність пристроїв пов’язаних з ним, стали причинами необхідності розроблення та подальшого впровадження стандартів шифрування інформації, з метою забезпечення безпеки передачі даних, що відповідають основним принципам шифрування, при використанні в пристроях з обмеженими обчислювальними ресурсами. На вирішення цих питань виникла нова галузь в криптографії – легковагова криптографія. Блоковий алгоритм шифрування PRESENT є одним з представників легковагових алгоритмів шифрування, який розроблявся саме з метою його використання в пристроях з обмеженими обчислювальними ресурсами, у зв’язку з цим він потребує всебічного і постійного аналізу на вразливості, як до вже відомих так і до нових методів криптоаналізу. Дана робота детально досліджує сам блоковий алгоритм шифрування PRESENT, його складові частини, принцип функціонування та алгоритм формування раундових ключів. В роботі проаналізовано відомі дослідження алгоритму щодо популярних на сьогодні методів криптоаналізу. З огляду на ці дослідження для даної роботи був обраний різницевий криптоаналіз, як один із ефективних методів. Оглянуто вимоги до побудови S-блоків, які висувають розробники даного алгоритму. За допомогою вимог до побудови S-блоків сформовано та представлено два альтернативні S-блоки для алгоритму. Висвітлено методику пошуку високоймовірнісних різницевих характеристик для алгориму PRESENT, з використанням відмінного від запропонованого розробниками блоку заміни. В роботі викладені результати дослідження алгоритму шифрування PRESENT з використанням альтернативних блоків заміни, щодо стійкості алгоритму до різницевого криптоаналізу. Наведено результати застосування представленої в роботі методики пошуку різницевих характеристик для представлених у роботі блоків заміни алгоритму PRESENT. Результати для алгоритму PRESENT з альтернативними блоками заміни, що отримані завдяки методиці пошуку різницевих характеристик, порівняно з відомими результатами для даного алгоритму.

Ключові слова: кібербезпека, кіберзахист, легковагова криптографія, різницевий криптоаналіз, блоковий алгоритм шифрування, блоки заміни.

Постановка проблеми. З розвитком Інтернету речей та розумних пристроїв, забезпечення безпеки даних на пристроях з обмеженим обчислювальним ресурсом стало однією з найбільш актуальних задач. Для вирішення цього завдання виникла нова галузь в криптографії, яка отримала назву – легковагова криптографія.

При виготовленні, наприклад, smart-карток, RFID-міток, SIM-карт, виробники вирішують завдання з оптимізації елементної бази для ефективного використання з точки зору обчислювальних ресурсів, пам'яті та енергії затраченої на обробку інформації. Фактично, легковагова криптографія зосереджена на досягненні компромісу між вимогами стійкості алгоритмів шифрування та наявними обчислювальними ресурсами.

У зв’язку з вищеперерахованими обмеженнями, використання в Інтернеті речей таких алгоритмів шифрування як AES не є можливим, так як він потребує суттєвих обчислювальних ресурсів.

Аналіз останніх досліджень і публікацій. Втіленням досягнень сучасної криптографічної науки та найкращих світових практик побудови шифрів, що відносяться до легковагової криптографії є міжнародний стандарт ISO/IEC 29192-2:2012, гармонізований в Україні як ДСТУ ISO/IEC 29192-2:2016 [1]. Одним із алгоритмів шифрування затверджених в ДСТУ ISO/IEC 29192-2:2016 є алгоритм PRESENT.

PRESENT є блоковим алгоритмом шифрування, який має простий дизайн та реалізацію, що робить його ефективним для використання в пристроях з обмеженими ресурсами, пам'яттю та енергоспоживанням.

Робота [2], в якій було представлений алгоритм PRESENT, містить оцінку його стійкості до криптоаналізу, в тому числі і до різницевого. Ця стаття надала перші важливі відомості про стійкість алгоритму PRESENT і його здатність протистояти різницевому криптоаналізу, який є одним із сучасних статистичних методів криптоаналізу. Різницевий криптоаналіз – це метод, який аналізує вплив певних відмінностей у парах відкритого тексту на відмінності результуючих пар зашифрованого тексту. Ці відмінності можна використовувати, щоб визначити ймовірності можливим ключам і знайти найбільш ймовірний ключ [6].

В роботі [3] наведено результати детального аналізу стійкості PRESENT до методів різницевого та лінійного криптоаналізу, представлено альтернативний варіант S-блоку, який є менш вразливим до вказаних методів криптоаналізу. Дослідження [4] поширює аналіз стійкості до різницевого криптоаналізу на шифри, що побудовані за схемою алгоритму PRESENT, але зі зменшеною кількістю раундів. У цьому дослідженні представлено результати пошуку різницевих характеристик з двома активними S-блоками на алгоритм PRESENT зі зменшеною кількістю раундів до 5 та 14.

Варто зазначити, що наукові праці [3], [4], [5], досліджують різницеві характеристики пов'язані зі стандартизованим S-блоком.

Метою статті є запропонувати методику пошуку високоймовірнісних різницевих характеристик для блокового алгоритму PRESENT.

Виклад основного матеріалу дослідження. Блоковий алгоритм PRESENT [2] побудований на основі SP-мережі, з розміром блоку шифрування – 64 біти, довжиною ключа на вибір 80 або 128 біт та 32-ма раундами. Раундова функція містить чотири основні перетворення: generateRoundKeys(), addRoundKey(), sBoxLayer() та pLayer().

Функція addRoundKey() за допомогою операції XOR поєднує блок, що шифрується, та раундовий ключ.

Функція sBoxLayer() розбиває блок, що зашифровується, на 16 блоків, по 4 біти, і відповідно до вхідного значення повертає вихідне, відповідно до значень наведених в таблиці 1.

Таблиця 1 – S-блок алгоритму PRESENT [2]

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[x]	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Функція pLayer() є перестановкою виходу-функції sBoxLayer() (див. табл. 2).

Функція generateRoundKeys() формує масив із 32-х раундових ключів, розміром по 64 біти. Раундовий ключ, з ключа шифрування довжиною 80 біт, формується наступним чином:

$$K_i = k_{63}k_{62}...k_0 = k_{79}k_{78}...k_{16} \quad (1)$$

Таблиця 2 – pLayer алгоритму PRESENT [2]

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(i)	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
P(i)	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
P(i)	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
P(i)	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Після формування раундового ключа значення ключа оновлюється за наступною схемою:

1. $\left[k_{79}k_{78}...k_1k_0\right]=\left[k_{18}k_{17}...k_{20}k_{19}\right]$ – зсув ключа вліво по регістру на 61;
2. $\left[k_{79}k_{78}k_{77}k_{76}\right]=S\left[k_{79}k_{78}k_{77}k_{76}\right]$ – після зсуву чотири старші біти основного ключа перетворюються за допомогою S-блока;
3. $\left[k_{19}k_{18}k_{17}k_{16}k_{15}\right]=\left[k_{19}k_{18}k_{17}k_{16}k_{15}\right]\oplus round_{counter}$ – біти з 19 по 15, за допомогою операції XOR, додаються до значення раунду перетворення.

Вимоги до побудови S-блоків.

В алгоритмі PRESENT використовується один 4-бітний S-блок $S:F_2^4\to F_2^4$. Реалізація такого S-блоку, є набагато компактнішою, ніж у випадку 8-бітного S-блоку. Але щоб зменшити вразливість до відомих атак на S-блоки такого розміру, розробниками алгоритму введено додаткові умови для S-блоків. Зокрема, S-блок для PRESENT відповідає наступним умовам:

$$S_b^W\left(a\right)=\sum_{x\in F_2^4}\left(-1\right)^{\langle b,S(x)\rangle+\langle a,x\rangle} \tag{2}$$

де S це коефіцієнт Фур'є.

1. Для будь-якої фіксованої відмінної від нуля вхідної різниці $\Delta_I\in F_2^4$ та будь-якої фіксованої відмінної від нуля вихідної різниці $\Delta_0\in F_2^4$, вимагається, щоб

$$\left\{x\in F_2^4\vee S\left(x\right)+S\left(x+\Delta_I\right)=\Delta_0\right\}\le 4, \tag{3}$$

2. Для будь-якої фіксованої відмінної від нуля вхідної різниці $\Delta_I\in F_2^4$ та будь-якої фіксованої відмінної від нуля вихідної різниці $\Delta_0\in F_2^4$, таких, що $wt\left(\Delta_I\right)=wt\left(\Delta_0\right)=1$,

$$\left\{x\in F_2^4\vee S\left(x\right)+S\left(x+\Delta_I\right)=\Delta_0\right\}=\varnothing, \tag{4}$$

3. Для всіх ненульових $a\in F_2^4$ та всіх ненульових $b\in F_4$ виконується $\left|S_b^W\left(a\right)\right|\le 8$.
4. Для всіх $a\in F_2^4$ та всіх ненульових $b\in F_4$ таких, що $wt\left(a\right)=wt\left(b\right)=1$, виконується $S_b^w\left(a\right)=\pm 4$.

Ці умови, за словами розробників, забезпечують стійкість алгоритму PRESENT до різницевих та лінійних атак. За допомогою аналізу всіх 4-бітних S-блоків, які відповідають вищезазначеним вимогам, розробниками був вибраний S-блок, який, крім всього, підходить для ефективної апаратної реалізації [2].

Стандартний S-блок при різницевому криптоаналізі 14 раундового алгоритму PRESENT має вихідну різницю з ймовірністю 2^{-62}, що є досить малою ймовірністю. Проте за

допомогою вимог до побудови S-блоків можливо знайти S-блок з меншою ймовірністю різницевих характеристик.

Методика побудови високоймовірнісних різницевих характеристик, із використанням двох активних S-блоків, легковагового алгоритму PRESENT.

У дослідженні [5] використовується властивість алгоритму, що дозволяє на кожному раунді перетворень різницевих характеристик використовувати лише два активні S-блоки. Відповідно до структури алгоритму виявлено, що при пошуку різницевих характеристик та виборі певних значень з розподільчої таблиці в кожному наступному раунді, не нульові значення поступають лише на два S-блоки [5].

На основі алгоритму представленого в роботі [5], можливо сформулювати методику для пошуку різницевих характеристик з двома активними S-блоками у кожному раунді перетворення.

Методика складається з 3 етапів: попередній, основний та заключний. Попередній етап – це підготовка вихідних даних для їх подальшого використання в основному етапі. Основний етап – побудова різницевих характеристик з двома активними S-блоками для кожного раунду перетворення (кількість раундів може бути довільною). Заключний етап – це обчислення ймовірності кожної характеристики, що була побудована для певної кількості раундів.

Розглянемо детально кожен з етапів.

Попередній етап:

1. Побудова різницевої розподільчої таблиці для відповідного S-блоку, що використовується в алгоритмі.

1.1. Всі різницеві характеристики S-блоку, $(\Delta X, \Delta Y)$ визначені, а ймовірність появи різниці ΔY, що залежить від ΔX, отримана шляхом розгляду вхідних пар (X', X'') такими, що $X' \oplus X'' = \Delta x$. Для S-блоку, потрібно розглянути всі 16 значень для X', а потім значення ΔX, що включає значення X'', яке визначається формулою:

$$X'' = X' \oplus \Delta x, \tag{5}$$

1.2. Отримані дані, записуємо до різницевої розподільчої таблиці ΔY для кожної вхідної пари $(X', X'' = X' \oplus \Delta x)$. В результаті отримано різницеву розподільчу таблицю.

2. Вхідну різницю представимо у вигляді:

$$A_i = \{a_{i0} a_{i1} \dots a_{i15}\}, \tag{6}$$

де A_i – 64 бітна раундова вхідна різниця, а a_{ij} – 4 біти інформації в 16-ти річному представленні, що потрапляє на окремий S-блок, при чому лише два значення $a_{ij} \neq 0$, а решта 14 $a_{ij} = 0$.

Основний етап:

1. A_i поступає на вхід 16-ти S-блоків.

2. Відповідно до різницевої розподільчої таблиці a_{ij} замінюється на значення, яке має найбільшу ймовірність, але при цьому не дорівнює таким значенням – 7, 11, 12, 13, 14, 15, так як ці значення при проходженні перетворення pLayer у наступному раунді не виконається умова описана в пункті 2 попереднього етапу. В результаті отримано $B_i = \{b_{i0} b_{i1} \dots b_{i15}\}$.

3. Обчислити ймовірність появи B_i шляхом добутку ймовірностей появи двох b_{ij}, які $\neq 0$. Ймовірність появи b_{ij} обчислюється в залежності від значення в різницевій розподільчій таблиці поділене на 16.

4. Виконати перетворення pLayer над B_i. В результаті отримаємо $C_i = \{c_{i0}c_{i1}\dots c_{i15}\}$.

4.1. Якщо після проходження pLayer, вихідна послідовність на наступному раунді буде застосовувати більше ніж 2 S-блоки, слід повернутись до пункту 2 основного етапу, з вибором наступної найбільш ймовірної різницевої характеристики з різницевої розподільчої таблиці.

5. $C_i = A_{i+1}$. Повертаємось до виконання пункту 1 основного етапу ту кількість разів, в залежності від характеристику якої кількості раундів необхідно отримати.

Заключний етап:

1. C_i – високоймовірнісна різницева характеристика необхідної кількості раундів.

2. Обчислюється ймовірність вихідної різниці.

Результатом роботи методики є високоймовірнісна різницева характеристика для легковагового блокового алгоритму PRESENT.

Високоймовірністною характеристикою ми вважаємо через те, що у пункті 2 основного етапу з різницевої розподільчої таблиці вибирається різницева характеристика, що має найбільше значення, тобто найбільшу ймовірність.

Аналіз результатів отриманих за допомогою запропонованої методики.

Побудова різницевих характеристик на 14-раундовому алгоритмі PRESENT з двома активними S-блокам в кожному раунді перетворень показала, що максимальна ймовірність таких характеристик дорівнює 2^{-62}, а мінімальна – 2^{-70} [4]. Далі в статті, з метою порівняння з уже відомими результатами в дослідженні [4], представлені результати побудови різницевих характеристик для 14-раундового алгоритму PRESENT.

Таблиця 3 – Кількість різницевих характеристик згрупованих по їх ймовірностях для стандартного S-блоку алгоритму PRESENT [4]

Ймовірність	2^{-62}	2^{-63}	2^{-64}	2^{-65}	2^{-66}	2^{-67}	2^{-68}	2^{-70}
Кількість знайдених характеристик	141	120	737	144	647	24	193	22

Різницевих характеристик, що використовують лише два S-блоки було знайдено у кількості 2028 [4]. У таблиці 3 представлено відповідно до ймовірності – кількість знайдених різницевих характеристик.

Більше ніж четверта частина, а саме 540, знайдених різницевих характеристик на виході мають однакове значення – 00000900_x || 00000900_x [4].

Результати побудови різницевих характеристик для S-блоку, значення якого зображено в таблиці 4 та згенерованого відповідно до вимог, приведено нижче.

Таблиця 4 – Таблиця значень S-блоку згенерованого відповідно до вимог

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[x]	5	0	1	2	3	4	6	8	C	9	F	E	7	A	D	B

Різницева розподільча таблиця для даного S-блоку представлена в таблиці 5.

Таблиця 5 – Різницева розподільна таблиця S-блоку представленого в таблиці 4

		Вихідні різниці															
Вхідні різниці		0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
	0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1_x	0	2	0	2	0	4	2	2	0	0	0	0	0	2	2	0
	2_x	0	2	2	2	2	2	0	2	0	0	2	0	2	0	0	0
	3_x	0	2	4	0	0	0	2	4	0	0	0	2	2	0	0	0
	4_x	0	0	2	2	2	2	2	2	0	0	2	2	0	0	0	0
	5_x	0	2	0	4	4	0	2	0	0	2	0	0	0	0	2	0
	6_x	0	2	4	2	2	0	2	0	4	0	0	0	0	0	0	0
	7_x	0	2	0	0	2	4	2	2	0	2	0	0	0	2	0	0
	8_x	0	0	0	2	2	0	0	0	0	4	0	2	2	0	4	0
	9_x	0	0	0	2	0	2	0	0	0	2	0	0	4	4	0	2
	A_x	0	2	2	0	0	0	0	0	0	0	2	2	0	2	4	2
	B_x	0	0	0	0	0	0	0	0	4	2	0	2	2	0	2	4
	C_x	0	0	2	0	0	0	2	0	0	4	2	0	2	2	0	2
	D_x	0	0	0	0	0	0	0	4	4	0	4	0	0	0	0	4
	E_x	0	2	0	0	0	0	2	0	4	0	4	2	2	0	0	0
	F_x	0	0	0	0	2	2	0	0	0	0	0	4	0	4	2	2

Таблиця 6 – Вхідні різниці з однаковими різницевими характеристиками

$P = 2^{-66}$		$P = 2^{-67}$	
0000000000001010	0000000000000770	0000000000000150	00000000000000a7
0000000000000110	0000000000000707	0000000000002010	0000000000b00030
0000000000000101	0000000000000077	0000000000000201	00000000000b0003
0000000000000011	000000000000d0d0	0000000000000021	0000000000b00060
0000000000001070	0000000000000dd0	0000000000002070	00000000000b0006
0000000000000170	0000000000000d0d	0000000000000207	0000000000d00030
0000000000000107	00000000000000dd	0000000000000027	00000000000d0003
0000000000000017	000000000000d0e0	0000000000003090	0000000000d00060
0000000000005010	0000000000000de0	0000000000000309	00000000000d0006
0000000000000501	0000000000000d0e	0000000000000039	0000000000e00030
0000000000000051	00000000000000de	0000000000006090	00000000000e0003
0000000000005070	000000000000e0d0	0000000000000609	0000000000e00060
0000000000000507	0000000000000ed0	0000000000000069	00000000000e0006
0000000000000057	0000000000000e0d	0000000000000750	000000000000f010
0000000000007010	00000000000000ed	000000000000a010	0000000000000f01
0000000000000710	000000000000e0e0	0000000000000a01	00000000000000f1
0000000000000701	0000000000000ee0	00000000000000a1	000000000000f070
0000000000000071	0000000000000e0e	000000000000a070	0000000000000f07
0000000000007070	00000000000000ee	0000000000000a07	00000000000000f7

Якщо ж для S-блоку представленого в таблиці 7, який також згенерованого відповідно до вимог, за допомогою методики побудувати різницеві характеристики отримано наступні результати.

Різницева розподільча таблиця для даного S-блоку представлена в таблиці 8.

Таблиця 7 – Таблиця значень S-блоку згенерованого відповідно до вимог

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[x]	0	3	F	E	D	6	C	9	B	1	A	7	4	8	5	2

Таблиця 8 – Різницева розподільна таблиця S-блоку представленого в таблиці 7

		Вихідні різниці															
Вхідні різниці		0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
	0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1_x	0	2	0	2	0	2	0	2	0	0	2	2	2	2	0	0
	2_x	0	6	0	0	0	0	2	0	0	0	2	0	0	2	0	4
	3_x	0	0	0	0	2	0	2	0	0	0	2	2	4	2	2	0
	4_x	0	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4
	5_x	0	0	4	2	0	2	4	0	2	0	0	0	0	0	2	0
	6_x	0	0	2	2	0	0	0	0	2	0	2	0	2	0	4	2
	7_x	0	0	2	4	2	0	0	0	0	6	0	0	0	0	0	2
	8_x	0	0	2	0	0	2	0	0	0	6	0	4	0	0	2	0
	9_x	0	2	2	0	2	2	0	0	4	0	0	0	2	0	2	0
	A_x	0	2	0	0	6	0	0	0	4	0	2	0	0	0	0	2
	B_x	0	0	0	2	2	2	0	2	0	2	0	0	0	2	2	2
	C_x	0	0	0	0	2	0	4	2	0	0	2	2	2	0	2	0
	D_x	0	0	0	2	0	0	0	2	2	0	0	4	2	4	0	0
	E_x	0	4	0	0	0	2	2	4	2	0	0	2	0	0	0	0
	F_x	0	0	4	0	0	0	2	2	0	0	4	0	2	2	0	0

Таблиця 9 демонструє статистику розподілу кількості різницевих характеристик, для S-блоку (таблиця 7), до їх ймовірностей.

Таблиця 9 – Кількість різницевих характеристик згрупованих по їх ймовірностях для запропонованого S-блоку

Ймовірність	2^{-70}	2^{-71}	2^{-72}	2^{-73}	2^{-74}
Кількість знайдених характеристик	16	16	204	14	235
Ймовірність	2^{-75}	2^{-76}	2^{-77}	2^{-78}	2^{-79}
Кількість знайдених характеристик	132	324	98	192	100
Ймовірність	2^{-80}	2^{-81}	2^{-82}	2^{-83}	2^{-84}
Кількість знайдених характеристик	119	28	31	14	11

За допомогою методики побудови високоймовірнісних різницевих характеристик, для S-блоку представленого в таблиці 7, перевірено 27 000 різницевих характеристик, з яких виявилося лише 1534 таких, що за 14 раундів використовують лише два S-блоки. Найбільша ймовірність знайдених характеристик – 2^{-70}, що в свою чергу у 2^8 разів менше ніж при використанні стандартного S-блоку. В свою чергу найменша ймовірність різницевої характеристики дорівнює 2^{-84}, що також є меншою від аналогічної при застосуванні стандартного S-блоку.

Висновки. Розвиток методів криптоаналізу не залишає в спокої та сприяє постійному дослідженню вже існуючих алгоритмів шифрування. Як нові так і вже відомі алгоритми шифрування повинні постійно досліджуватись на виявлення вразливостей, як до вже відомих методів криптоаналізу так і до нових.

У даному дослідженні представлено два нових S-блоки, що володіють покращеними властивостями в контексті різницевого криптоаналізу при їх використанні в алгоритмі PRESENT. Результати різницевого криптоаналізу алгоритму PRESENT, який був скорочений за кількістю раундів та використовував S-блоки, відмінні від стандартних, свідчать про те, що обрані S-блоки проявляють різницеві характеристики з меншими ймовірностями порівняно зі стандартним S-блоком.

Додатково, в результаті проведених досліджень була сформульована методика побудови різницевих характеристик легковагового алгоритму PRESENT. Ця методика, представлена в роботі, сприяє пришвидшенню пошуку різницевих характеристик для алгоритму PRESENT, що в свою чергу полегшує проведення додаткових досліджень стійкості алгоритму PRESENT до різницевого криптоаналізу та може бути корисним, як в контексті застосування алгоритму, так і для загального розвитку криптографічних методів.

Дослідження стійкості алгоритму PRESENT до різних методів криптоаналізу не потрібно припиняти. Навіть у випадку, коли PRESENT вже пройшов значний аналіз і виявив стійкість до різницевого криптоаналізу, додаткові дослідження можуть вирішити кілька важливих аспектів:

підтвердити або підкріпити вже встановлену стійкість PRESENT до різницевого криптоаналізу. Це може сприяти підтвердженню незалежними дослідниками та підвищити довіру до алгоритму;

допомогти виявити можливі різницеві характеристики алгоритму, які не були розглянуті раніше. Це може бути важливим для забезпечення майбутньої стійкості алгоритму перед можливими атаками;

результати досліджень можуть послужити основою для подальших вдосконалень PRESENT або розробки нових варіантів, які будуть володіти ще більшою стійкістю до різницевого криптоаналізу.

У перспективах подальших досліджень для додаткового поглиблення досліджень, планується використання методики пошуку високоймовірнісних характеристик для знаходження блоків заміни з меншими ймовірностями для блокового алгоритму PRESENT. Це може визначити нові шляхи для покращення стійкості алгоритму та його застосування в умовах зростаючих вимог до криптографічних алгоритмів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1]. *ДСТУ ISO/IEC 29192-2:2016. Інформаційні технології. Методи захисту. Легковагова криптографія. Частина 2. Блокові шифри (ISO/IEC 29192-2:2012, IDT).* [На заміну ДСТУ ISO/IEC 29192-2:2015; чинний від 2018-01-01]. Вид. офіц. Київ: Технічний комітет зі стандартизації "Інформаційні технології" (ТК 20), 2018.

[2]. A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher", in *Proc. Cryptographic Hardware and Embedded Systems – CHES 2007*, Vienna, Austria, pp. 450-466, 2007, doi: https://doi.org/10.1007/978-3-540-74735-2_31.

[3]. M. Siji, “Analysis and Implementation of the Ultra-Lightweight Block Cipher: PRESENT”, *Journal of VLSI Design and its Advancement*, vol. 3, no. 1, pp. 1-8, 2020.
[4]. M. Wang, “Differential Cryptanalysis of PRESENT”, in *Proc. Progress in Cryptology – AFRICACRYPT 2008*, Casablanca, Morocco, pp. 40-49, doi: https://doi.org/10.1007/978-3-540-68164-9_4.
[5]. M. Wang, Y. Sun, E. Tischhauser, and B. Preneel, “A Model for Structure Attacks, with Applications to PRESENT and Serpent”, *Fast Software Encryption*, 2012, pp. 49-68, doi: https://doi.org/10.1007/978-3-642-34047-5_4.
[6]. E. Biham, and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems”, *Journal of Cryptology*, vol. 4, 1990, pp. 3-72, doi: https://doi.org/10.1007/3-540-38424-3_1.

Стаття надійшла до редакції 14.05.2024.

REFERENCES

[1] *DSTU ISO/IEC 29192-2:2016. Information Technology. Protection methods. Lightweight cryptography. Part 2. Block ciphers (ISO/IEC 29192-2:2012, IDT).* [To replace DSTU ISO/IEC 29192-2:2015; valid from 2018-01-01]. Kyiv official publishing house: Technical Committee for Standardization “Information Technologies” (TK 20), 2018.
[2] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher”, in *Proc. Cryptographic Hardware and Embedded Systems – CHES 2007*, Vienna, Austria, pp. 450-466, 2007, doi: https://doi.org/10.1007/978-3-540-74735-2_31.
[3] M. Siji, “Analysis and Implementation of the Ultra-Lightweight Block Cipher: PRESENT”, *Journal of VLSI Design and its Advancement*, vol. 3, no. 1, pp. 1-8, 2020.
[4] M. Wang, “Differential Cryptanalysis of PRESENT”, in *Proc. Progress in Cryptology – AFRICACRYPT 2008*, Casablanca, Morocco, pp. 40-49, doi: https://doi.org/10.1007/978-3-540-68164-9_4.
[5] M. Wang, Y. Sun, E. Tischhauser, and B. Preneel, “A Model for Structure Attacks, with Applications to PRESENT and Serpent”, *Fast Software Encryption*, 2012, pp. 49-68, doi: https://doi.org/10.1007/978-3-642-34047-5_4.
[6] E. Biham, and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems”, *Journal of Cryptology*, vol. 4, 1990, pp. 3-72, doi: https://doi.org/10.1007/3-540-38424-3_1.

VALERII ZAKUSILO,
NATALIIA KUCHYNSKA,
SERHII KONIUSHOK

SEARCH FOR HIGH-PROBABILITY DIFFERENTIAL CHARACTERISTICS OF THE LIGHTWEIGHT BLOCK CIPHER ALGORITHM PRESENT WITH NON-STANDARD SUBSTITUTION BLOCKS

The development of the Internet of Things and the associated devices has made it necessary to establish and implement encryption standards to ensure secure data transmission. These standards need to be comply with fundamental encryption principles and cater to devices with limited

computational resources. As a result, lightweight cryptography has emerged as a distinct field within cryptography. The PRESENT block cipher algorithm is a lightweight encryption algorithm designed for deployment in resource-constrained devices. It requires comprehensive and ongoing vulnerability analysis against both known and novel cryptanalysis methods. This work extensively investigates the PRESENT block cipher algorithm, examining its components, operational principles, and key scheduling algorithm. This study analyses existing research on the algorithm with regards to contemporary cryptanalysis methods. Differential cryptanalysis was selected as the method of choice. The requirements for constructing S-boxes, as set forth by the algorithm developers, are reviewed. Two alternative S-boxes are formulated and presented based on these requirements. The paper presents a methodology for identifying high-probability differential characteristics for the PRESENT algorithm, using a substitute substitution block that differs from the one proposed by the developers. The research reports on the encryption algorithm PRESENT, using alternative substitution blocks, and evaluates its resistance to differential cryptanalysis. The text presents the results of applying the methodology for searching differential characteristics to the substituted blocks in the PRESENT algorithm. A comparative analysis is made between the results obtained through the differential characteristic search methodology for the PRESENT algorithm with alternative substitution blocks and the known results for this algorithm.

Keywords: cybersecurity, cyber defense, lightweight cryptography, differential cryptanalysis, encryption algorithm, substitution blocks.

Закусіло Валерій Олегович, аспірант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0001-6906-2742, zak.valera@gmail.com.

Кучинська Наталія Вікторівна, кандидат технічних наук, доцент, доцент кафедри математичних методів захисту інформації, Навчально-науковий фізико-технічний інститут Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-6457-7525, n.kuchinska@gmail.com.

Конюшок Сергій Миколайович, кандидат технічних наук, доцент, заступник начальника інституту (з наукової роботи), Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0003-4121-1464, 3tooth@gmail.com.

Zakusilo Valerii, postgraduate, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Kuchynska Nataliia, associate professor, candidate of technical sciences, associate professor Department of mathematical methods of information security, Institute of physics and technology of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Koniushok Serhii, associate professor, candidate of technical sciences, deputy head of the institute (for scientific work), Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.