ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

DOI
УДК 004.056.5:629.7.052

Л.В. Ковальчук, д-р техн. наук,
e-mail: lusi.kovalchuk@gmail.com; orcid.org/0000-0003-2874-7950
С.Я. Гільгурт, д-р техн. наук,
e-mail: hilgurt@ukr.net; orcid.org/0000-0003-1647-1790
А.М. Давиденко, д-р техн. наук,
e-mail: davidenkoan@gmail.com; orcid.org/0000-0001-6466-1690
Т.М. Клименко
e-mail: klimenko-t@ukr.net; orcid.org/0009-0003-4675-6428
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
Україна, 03164, Київ, вул. Олега Мудрака, 15

Аналіз стійкості алгоритму блокового шифрування DONATION до структурних та алгебраїчних атак

Робота продовжує серію досліджень стійкості малоресурсного блокового шифру DONATION, призначеного для шифрування відеопотоків з БпЛА. Проведено попередній аналіз його стійкості до структурних та алгебраїчних атак. Проаналізовано вплив бітової перестановки на байтову структуру стану та можливість застосування інтегральних атак і атак типу «вузького місця». Показано, що перестановка після нелінійного перетворення повністю руйнує байтову структуру, тому розглянуті атаки безпосередньо на DONATION не переносяться. Для восьми повних раундів система, що описує шифр, містить 2496 квадратичних рівнянь, 1024 змінні для входів і виходів блоків підстановки та 576 змінних для бітів раундових ключів (без урахування лінійних рівнянь). Очевидного алгебраїчного спрощення, яке давало б змогу практично розв'язати цю систему, не виявлено.

Ключові слова: малоресурсний блоковий шифр, структурний криптоаналіз, алгебраїчний криптоаналіз, інтегральна атака, квадратичні булеві рівняння.

Захист відеопотоків, що передаються з безпілотних літальних апаратів у реальному часі, потребує поєднання одночасного виконання вимог щодо малої часової затримки передачі, малоресурсності та достатнього рівня тимчасової стійкості (тобто стійкості протягом часу виконання місії або часу цінності отриманої інформації). У роботі [1] було запропоновано відповідний підхід на основі концепції тимчасової криптографічної стійкос-

Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

ті. На його основі розроблено малоресурсний блоковий шифр DONATION, повний опис якого, а також оцінки стійкості до різницевого і лінійного криптоаналізу наведено у прийнятій до публікації роботі [2]. DONATION є SPN-шифром (substitution-permutation network) типу PRESENT [3] з 64-бітовим блоком, вісьмома 8-бітовими блоками підстановки, бітовою перестановкою та вісьмома повними раундами. При цьому мала кількість раундів запропонованого алгоритму має певні потенційні ризики, що робить особливо важливою перевірку інших, крім розглянутих у [2], можливих напрямків криптоаналізу, зокрема, таких як структурні та алгебраїчні атаки.

Структурні атаки використовують особливості структури шифру, наприклад, байтову структуру, як в AES; або якісь зв'язки між бітами, які можна відслідкувати навіть після виконання кількох раундів шифрування. До таких атак зокрема належать «класичний» інтегральний криптоаналіз [4] та його версія — інтегральний криптоаналіз, що базується на бітових шаблонах [5]. Саме цю версію було вперше застосовано до скорочених версій алгоритму PRESENT. Сучасні методи автоматизованого пошуку інтегральних атак, атак неможливих диференціалів та атак нульової кореляції, які також були застосовані до алгоритму PRESENT, наведено у [6]. Важливість дослідження стійкості до структурних атак також підтверджують нові результати 2025 р.: у [7] побудовано інтегральну атаку на повну 20-раундову версію малоресурсного шифру LBC, а в [8] — на повний 10-раундовий шифр FUTURE.

Інший тип атак, який також необхідно враховувати при розробці алгоритму шифрування, — це так звані алгебраїчні атаки, для виконання яких перетворення шифру подається системою поліноміальних рівнянь над полем F_2, а відновлення ключа зводиться до розв'язання цієї системи [9]. Аналіз стійкості до таких атак також було виконано для скорочених версій PRESENT у роботі [10]. У роботі [11] попередню алгебраїчну обробку поєднано з булевими розв'язувачами й апробовано на скорочених версіях PRESENT і SIMON. Система BONC [12] за кодом раундового шифру формує бітову модель для диференціального, лінійного та інтегрального аналізу.

Тому аналіз стійкості алгоритму DONATION до структурних та алгебраїчних атак також є необхідною частиною його досліджень. Так, для використання цього алгоритму необхідно як мінімум переконатись, що у ньому відсутні структурні або алгебраїчні особливості, що сприяють практичній реалізації цих атак за обмежений час. Тому метою цієї роботи є проведення попереднього аналізу стійкості алгоритму шифрування DONATION до цих двох класів атак.

У роботі показано, що бітова перестановка, яка виконується після нелінійного перетворення у кожному раунді, руйнує байтову структуру, яка

зберігається після ключового суматора та блоків підстановки. Тому класичні інтегральні атаки й атаки типу «вузького місця» для AES-подібних шифрів не переносяться безпосередньо на DONATION. За результатами проведеного попереднього аналізу очевидних структурних або алгебраїчних вразливостей алгоритму DONATION не виявлено.

Опис алгоритму DONATION. Алгоритм блокового шифрування DONATION є SPN-шифром та має такі параметри:

• довжина блока дорівнює 64 біти;

• довжина раундового ключа теж 64 біти;

• кількість раундів шифрування дорівнює 8 (без урахування неповного 9-го раунду, в якому єдина операція — забілювання, тобто побітове додавання за модулем 2 з ключем), але може змінюватися залежно від бажаної стійкості до основних атак;

• нелінійний шар раунду складається з восьми 8-бітових блоків підстановки;

• лінійне перетворення є бітовою перестановкою.

Зауваження. Зазначимо, що при таких параметрах сумарна довжина всіх раундових ключів дорівнює $64 \cdot 9 = 576$ біт. З метою збільшення швидкості роботи алгоритму, раундові ключі можна зберігати у пам'яті протягом усього сеансу, замість того щоб виробляти їх у процесі шифрування з ключа шифрування згідно з ключовим розкладом. Тому найпростішим варіантом вироблення ключа шифрування є генерація ключа довжиною 576 біт для кожного сеансу, хоча така довжина ключа є надлишковою порівняно з отриманими нижче оцінками стійкості до атак.

Перейдемо до формалізованого опису алгоритму. Нехай $n, l, m \in N$ та $n = lm.$ Тут і далі ми переважно розглядаємо випадок, коли $n = 64 = 8 \times 8,$ $l = m = 8.$ Позначимо $V_n = \{0,1\}^n.$

Згідно з [2] раундова функція алгоритму, параметризована раундовим ключем $k \in V_{64},$ має вигляд:

$$f_k : V_{64} \to V_{64}.$$

Ця функція при фіксованому $k \in V_n$ є бієктивним відображенням, яке визначається за наступним правилом:

$$\forall x \in V_n,\ x = (x_1, ..., x_m),\ x_i \in V_l,\ i \in [m]:\ f_k(x) = L\,(S\,(x \oplus k)),$$

де $S(x) = (s_1(x_1),...,s_m(x_m)),\ s_i : V_l \to V_l,\ i \in [m]$ — бієктивні відображення.

В цих позначеннях процедура зашифрування може бути описана як

$$E_K(x) = k_9 \oplus f_{k_8}(f_{k_7}(...(f_{k_1}(x)))),$$

де $K = (k_1, ..., k_9) \in (V_{64})^9$ — ключ шифрування, $x \in V_{64}$ — блок відкритого тексту.

З метою досягнення необхідного рівня тимчасової стійкості при збереженні малоресурсності алгоритму, для побудови нелінійного блоку підстановки та лінійного оператора використовуються функції L та S зі спеціальними криптографічними властивостями. Ці властивості певною мірою подібні до властивостей відповідних перетворень в алгоритмі PRESENT [3] та забезпечують достатній рівень тимчасової стійкості побудованого шифру до основних атак, зокрема до різницевого та лінійного криптоаналізу, навіть за малої кількості раундів. Нижче ми наведемо ці функції та їх властивості.

Бітова перестановка L. Функція L є перестановкою, подібною до перестановки PRESENT, на множині $\{0, 1, ..., 63\}$, і визначена у табл. 1 для випадку $n = 64 = 8 \times 8$.

У табл. 1 змінна i означає номер позиції біту у вході в функцію L, де вхідний вектор задається як $x = (x_0, ..., x_{63})$, тобто i приймає значення від 0 до 63. Величина L_i визначає номер позиції біту x_i у вихідному векторі $L(x)$, на яку переходить біт x_i вхідного вектора: рівність $L_i = j$ означає, що у векторі $L(x)$ біт x_i знаходиться на позиції з номером j.

Величина L_i може бути обчислена аналітично за формулою:

$$L_i = \left\lfloor \frac{i}{8} \right\rfloor + 8\,(i \bmod 8),$$

У двійковому вигляді це перетворення можна визначити так: якщо $i = (a_2 a_1 a_0 b_2 b_1 b_0)$, то $L_i = (b_2 b_1 b_0 a_2 a_1 a_0)$, тобто величина L_i отримана перестановкою першої і другої половини вектора $i = (a_2 a_1 a_0 b_2 b_1 b_0)$. Звідси зокрема випливає, що L є інволюцією, тобто $L\,(L\,(i)) = i$.

Таблиця 1. **Перестановка L алгоритму DONATION**

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

Нелінійне перетворення (блок підстановки) s (x). Алгоритм використовує нелінійне перетворення

$$S\ (x) = (s\ (x_0, ..., x_7), ...,\ s\ (x_{56}, ..., x_{63})),$$

де всі *s*-блоки задані однаково. Функція, що задає окремий *s*-блок, визначена в табл. 2.

Наприклад, згідно з табл. 2, *s* (00) = 00, *s* (01) = 2C, *s* (02) = 43, *s* (*FF*) = 63.

Запропонований 8-бітовий блок підстановки був побудований як відображення, що є афінно-еквівалентним до відображення інверсії у полі F_{2^8}:

$$s\ (x) = A\ ((Bx)^{-1}), \qquad (1)$$

де A та B є лінійними оборотними перетвореннями над F_{2^8} (тобто невиродженими матрицями), а під інверсією розуміється обчислення оберненого

Таблиця 2. **Нелінійний блок підстановки *s* (*x*)**

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	2C	43	CC	5D	4E	8F	70	32	D6	0D	E7	FD	EC	18	35
1	72	C6	C1	9F	D2	AA	39	3A	29	4A	6A	40	98	4F	A1	53
2	1D	B4	F5	D3	A6	C7	D8	5E	34	F3	BA	69	EB	DC	E5	47
3	38	88	2B	7F	F6	52	56	FA	B3	EE	3F	7C	DA	04	0B	85
4	03	45	37	A7	A2	66	78	E1	E9	D1	28	7E	8D	07	02	73
5	BF	71	CD	33	AD	83	F0	8A	DF	19	65	5F	1B	8C	10	E8
6	55	FF	41	DE	05	8E	DB	13	5C	89	5B	4D	24	12	3D	AB
7	F8	0E	8B	A0	C8	FB	97	14	6E	B7	95	77	3C	BD	C3	6D
8	6C	B8	A3	A5	9C	68	20	9E	91	C4	75	AE	F1	81	B5	99
9	0C	E3	58	CA	CB	4C	80	B1	D7	92	86	67	61	B9	F2	EF
A	FC	9A	50	F7	25	D0	3B	9D	2E	49	96	2F	36	6F	7A	1E
B	C5	C0	60	21	57	9B	E6	A8	06	11	17	AC	BB	A4	D4	2D
C	09	B6	74	84	E0	1A	0A	82	4B	FE	44	D5	7D	16	5A	CE
D	3E	30	1C	08	42	7B	AF	DD	EA	F4	B0	F9	54	1F	E4	BE
E	ED	C2	27	48	CF	B2	51	15	90	6B	D9	79	E2	23	46	94
F	BC	C9	93	62	22	01	0F	76	87	2A	64	A9	59	26	31	63

елемента в мультиплікативній групі поля $F_{2^8} = F_2(\alpha)$, де α є коренем незвідного над F_2 полінома $m(t) = t^8 + t^4 + t^3 + t + 1 \in F_2[X]$; при цьому, за домовленістю, вважаємо що $0^{-1} = 0$.

Лінійні оператори A та B у формулі (1) зручно задавати стовпчиками, тобто образами стандартних базисних векторів e_i, $i \in \{0, 1, ..., 7\}$, при дії на них цих операторів:

$$A = (2C, 1A, 93, F4, C3, 19, 97, 08);$$
$$B = (01, 02, 04, 69, 08, 49, 5A, D2).$$

Тут кожне двоцифрове шістнадцяткове число інтерпретується як 8-бітовий вектор-стовпчик.

Отже, побудований блок підстановки належить до класу інверсійних 8-бітових перестановок, але відрізняється від «чистої» інверсії застосуванням пари невироджених матриць. Ці матриці були обрані таким чином, щоб забезпечити побудованому блоку підстановки певні різницеві та лінійні властивості, які ми опишемо нижче.

У цих позначеннях процедура розшифрування, з урахуванням інволютивності функції L, відбувається аналогічно до зашифрування, але раундові ключі вводяться у зворотному порядку. Відповідно операція забілювання з раундовим ключем виконується на початку розшифрування, а в нелінійному перетворенні використовуються s-блоки s^{-1}, тобто блоки підстановки, що задають перетворення, обернені до визначеного в табл. 2.

Визначений у (4) блок підстановки має такі різницеві властивості (D1 та D2), аналогічні до тих, що визначені для 4-бітових блоків підстановки у шифрі PRESENT.

D1. Максимальна імовірність диференціалу для вибраного блока підстановки не перевищує $1/64$. Тобто для $\forall \alpha, \beta \in V_8 \setminus \{\overline{0}\}$ виконується нерівність:

$$DP^s(\alpha, \beta) := \frac{1}{2^8} \sum_{x \in V_8} \delta\left(s(x \oplus \alpha) \oplus s(x), \beta\right) \le \frac{4}{256} = 2^{-6},$$

де $\delta(x, y) = \begin{cases} 1, \text{ якщо } x = y, \\ 0, \text{ інакше,} \end{cases}$ — символ Кронекера. Іншими словами, блок підстановки є різницево 4-рівномірним.

D2. Жодна 1-бітова вхідна різниця не переходить в однобітову вихідну. Позначимо $e_i = 2^i$, $i \in \{0, 1, ..., 7\}$, вектори, у яких вага Хеммінга дорів-

нює 1. Тоді ця властивість може бути записана так: $DP^s(e_i, e_j) = 0$ для всіх $i, j \in \{0, 1, ..., 7\}$. Іншими словами, якщо вхідна різниця має вагу Хеммінга 1, то вага Хеммінга вихідної різниці не менша за 2.

Також слід зазначити, що властивість D2 є «симетричною» в тому сенсі, що якщо вона виконується для деякого перетворення s, то вона буде виконуватись і для оберненого перетворення.

Визначений у табл. 2 блок підстановки також має такі лінійні властивості (L1 та L2), які не є повним аналогом лінійних властивостей для 4-бітового блока підстановки алгоритму PRESENT, але сформульовані з аналогічною метою. Тобто ми адаптували відповідні лінійні властивості, сформульовані в [3] для 4-бітового блока підстановки, до визначеного вище 8-бітового блока підстановки, з метою забезпечення достатньої (хоч і тимчасової) стійкості алгоритму DONATION.

Нехай

$$W_s(\alpha, \beta) = \sum_{x \in V_8} (-1)^{\alpha x \oplus \beta s(x)}$$

є коефіцієнтом Уолша для блока підстановки s, де $\alpha, \beta \in V_8$, множення «$\cdot$» визначає скалярний добуток 8-бітових векторів над полем F_2, а додавання «$\oplus$» є побітовим додаванням за модулем 2.

Визначимо відповідно кореляцію та квадратичну кореляцію для блока підстановки s як

$$C_s(\alpha, \beta) = \frac{W_s(\alpha, \beta)}{2^8} \text{ та } LP_s(\alpha, \beta) = C_s(\alpha, \beta)^2.$$

Величину $LP_s(\alpha, \beta)$ також інколи називають імовірністю лінійної апроксимації, але при цьому слід пам'ятати, що ця величина не є безпосередньо імовірністю виконання відповідної лінійної рівності.

Відповідні лінійні властивості (L1 та L2) для блока підстановки s можна сформулювати так.

L1. Для всіх лінійних апроксимацій $(\alpha, \beta) \in V_8 \setminus \{0\} \times V_8 \setminus \{0\}$, абсолютна величина коефіцієнта Уолша задовольняє нерівності $|W_s(\alpha, \beta)| \le 32$, що еквівалентно нерівності $LP_s(\alpha, \beta) \le 2^{-6}$.

L2. Для однобітових вхідних та вихідних масок, коефіцієнт Уолша є ще меншим: для $e_i = 2^i$ та $e_j = 2^j$, $i, j \in \{0, 1, ..., 7\}$, які мають вагу Хеммінга 1, виконується нерівність $|W_s(e_i, e_j)| \le 24$, тобто

$$LP_s(e_i, e_j) \le \frac{9}{10^{24}} = 2^{-6{,}830074998} \approx 2^{-6{,}83}.$$

Властивість L2 не є повним аналогом відповідної лінійної властивості для 4-бітового блока підстановки алгоритму PRESENT, сформульованої в [3] для коефіцієнта Уолша однобітових масок. Але ця властивість додатково покращує цей коефіцієнт для таких масок і, відповідно, покращує верхні оцінки імовірності лінійних характеристик, які ми оцінюємо через кількість активних блоків підстановки.

Стійкість алгоритму DONATION до структурних та алгебраїчних атак. Оцінки стійкості алгоритму DONATION до різницевого та лінійного криптоаналізу були отримані у роботі [2]. У цій роботі для 8-раундової версії DONATION отримано верхні оцінки ймовірностей різницевих та лінійних характеристик, які показують достатній рівень захисту від відповідних класичних методів криптоаналізу в моделі тимчасової стійкості.

Нижче розглянемо ще два класи атак, які зазвичай враховують при аналізі SPN-шифрів: структурні атаки та алгебраїчні атаки. Наведений аналіз дає змогу визначити, чи має конструкція DONATION очевидні структурні або алгебраїчні властивості, які могли б призвести до атаки, істотно кращої за різницеві та лінійні атаки.

Структурні атаки. До структурних атак на блокові шифри належать, зокрема, інтегральні атаки, атаки типу «вузького місця», деякі варіанти атак усічених диференціалів та інші методи, які використовують не лише ймовірності окремих різницевих або лінійних характеристик, а й регулярну будову всього перетворення. Історично інтегральний криптоаналіз розвинувся з так званої квадратної атаки, запропонованої для шифру Square у 1997 р. [9]. У 2002 р. Кнудсен і Вагнер узагальнили цей підхід як інтегральний криптоаналіз [10]. Атаку типу «вузького місця» на скорочений Rijndael запропонували Жильбер і Міньє у 2000 р. [11]; відповідні властивості AES пізніше додатково досліджено в роботі Міньє [12]. Для біторієнтованих та малоресурсних шифрів важливою є також інтегральна атака на основі бітових шаблонів, запропонована З'аба, Раддумом, Генріксеном і Доусоном у 2008 р. та застосована, зокрема, до скорочених версій PRESENT [5].

Такі атаки особливо природні для AES-подібних шифрів, у яких стан має чітко виражену байтову структуру або структуру на рівні слів, а лінійне перетворення діє на байти або слова так, що певні структурні властивості можуть простежуватися протягом кількох раундів. Саме тому в аналізі PRESENT автори окремо розглядали структурні атаки і зазначали, що такі атаки добре пристосовані до AES-подібних шифрів, але значно гірше переносяться на PRESENT через переважно бітову структуру його перетворень.

Алгоритм DONATION, на відміну від PRESENT, використовує 8-бітові блоки підстановки, тобто на рівні нелінійного шару він має байтову

структуру. Проте ця байтова структура руйнується при застосуванні лінійного перетворення L. Перетворення L в алгоритмі DONATION є бітовою перестановкою, яка не зберігає вхідні байти — навпаки, всі біти кожного вхідного байта будуть розосереджені між вісьмома різними байтами вихідного вектора. Це означає, що якщо вихід одного блока підстановки містить вісім бітів, то після застосування перетворення L ці вісім бітів потрапляють не в один наступний блок підстановки, а розподіляються по одному біту між усіма вісьмома блоками підстановки наступного раунду.

Звідси випливає, що DONATION не має сталої AES-подібної байтової структури, на якій базуються класичні інтегральні атаки та атаки типу «вузького місця». Після одного раунду байтовий вихід кожного активного блока підстановки розсіюється між усіма байтовими позиціями наступного раунду, а після наступного нелінійного шару ці біти взаємодіють із бітами інших вхідних байтів, тому проста байтова структура не зберігається. Це ускладнює збереження простих структур типу «активний байт — константні байти» або «збалансована сума по байту» протягом багатьох раундів.

Таким чином, стандартні структурні атаки, розроблені для AES-подібних шифрів із чітко збереженою байтовою структурою, не можуть бути безпосередньо перенесені на шифр DONATION. Сама по собі регулярність перестановки L не дає можливості побудувати структурний розрізнювач, оскільки між двома застосуваннями цієї перестановки виконується нелінійне перетворення, а біти з виходу кожного блока підстановки надходять до восьми різних блоків підстановки наступного раунду. Водночас мала кількість раундів DONATION не виключає існування спеціально побудованих структур для атак усічених диференціалів, інтегральних атак, інтегральних атак на основі бітових шаблонів або атак неможливих диференціалів, які не випливають безпосередньо з байтової організації стану. За результатами проведеного аналізу в конструкції DONATION не виявлено очевидної AES-подібної структури на рівні слів, яка безпосередньо приводила б до стандартної структурної атаки.

Алгебраїчні атаки. Для виконання алгебраїчної атаки на алгоритм шифрування потрібно подати перетворення, яке виконується при шифруванні, у вигляді системи поліноміальних рівнянь над полем F_2, де змінними є біти відкритого тексту, шифртексту, проміжних станів та ключів. Для SPN-шифрів така система будується як суперпозиція відповідних рівнянь для блоків підстановки (нелінійні рівняння) та рівнянь, що відповідають лінійним перетворенням, таким як додавання раундового ключа та перестановка L (лінійні рівняння). Після цього задача відновлення ключа зводиться до розв'язання великої системи булевих поліноміальних рівнянь.

Важливим етапом розвитку алгебраїчного криптоаналізу стала поява XL-алгоритму для розв'язання перевизначених систем поліноміальних рівнянь, запропонованого Куртуа, Клімов, Патарен і Шамір у 2000 р. [13]. У 2002 р. Куртуа і Пепшик запропонували застосовувати XSL-підхід до блокових шифрів, зокрема до AES-подібних конструкцій [14]. Для практичного розв'язання таких систем застосовують методи обчислення базисів Гребнера; одним із найвідоміших є алгоритм F4, запропонований Ж.-К. Фожером у 1999 р. [15]. Слід зазначити, що автори алгоритму PRESENT також досліджували стійкість запропонованого ними алгоритму до алгебраїчних атак, зокрема оцінили кількість змінних і квадратичних рівнянь у системі, що описує повну версію PRESENT [3].

В алгоритмі DONATION лінійне перетворення L, операції додавання за модулем 2 з раундовими ключами, а також фінальне забілювання задаються лінійними рівняннями над полем F_2. Єдиними нелінійними перетвореннями є 8-бітові блоки підстановки. Оскільки блок підстановки алгоритму DONATION є афінно-еквівалентним до інверсії у полі F_{2^8}, його координатні булеві функції мають алгебраїчний степінь 7.

Для алгебраїчного подання блока підстановки будувались співвідношення найменшого можливого нелінійного степеня, тобто другого степеня. Використання таких співвідношень дає змогу описати залежності між вхідними та вихідними бітами блока підстановки рівняннями другого степеня замість безпосереднього використання координатних функцій степеня 7. Для розв'язування квадратичних булевих систем рівнянь застосовують алгоритми XL і XSL [13, 14], методи обчислення базисів Гребнера [15—17], а також розв'язувачі задачі булевої виконуваності [18].

Для одержання цих співвідношень позначимо $\Gamma_s = \{(x, s(x)) : x \in F_{2^8}\} \subset$ $\subset F_{2^8} \times F_{2^8}$ — графік-блоку $s : F_{2^8} \to F_{2^8}$, тобто множину всіх 256 пар «вхід-вихід». Для кожної пари $(x, s(x))$ введемо вектор $z = (z_1, ..., z_{16}) =$ $= (x \| s(x))$ — вектор, утворений послідовним записом восьми координат вектора x та восьми координат вектора $s(x)$. Для пошуку поліноміальних співвідношень, степінь яких не вище 2, розглядалися всі мультилінійні мономи відповідного степеня. Оскільки для бітових змінних виконується рівність $z_i^2 = z_i$, то до цього набору входять такі мономи: сталий моном 1; 16 лінійних мономів z_i; 120 попарних добутків $z_i z_j$, $1 \le i < j \le 16$ — тобто усього 137 мономів.

На всіх 256 точках графіка було обчислено значення цих 137 мономів і сформовано матрицю $M_{256\times137}$ над полем F_2. Її рядки відповідають парам

$(x, s(x))$, а стовпці — мономам: елемент на перетині певного рядка і стовпця дорівнює значенню відповідного монома у точці $(x, s(x))$. Якщо $\overline{c}$ — вектор, що складається із 137 коефіцієнтів деякого многочлена від 16 змінних, степінь якого не вище 2, то справедливе наступне твердження: цей многочлен дорівнює нулю на всіх парах «вхід–вихід» (тобто є тотожнім нулем) тоді й лише тоді, коли $M\overline{c} = \overline{0}$. Ядро матриці M було обчислено методом Гауса над полем F_2: спочатку матрицю приведено до скороченого східчастого вигляду за допомогою перестановки рядків і їх додавання за модулем 2, після чого за вільними змінними було побудовано базис простору розв'язків системи $M\overline{c} = \overline{0}$. Розмірність ядра дорівнює 39, тому його базис задає 39 лінійно незалежних квадратичних співвідношень між вхідними та вихідними бітами блока підстановки.

Блоковий шифр DONATION у кожному раунді використовує вісім блоків підстановки, тобто у восьми раундах шифрування (скорочений дев'ятий раунд не містить блоків підстановки) всього задіяно $8 \cdot 8 = 64$ блоки підстановки. Якщо кожен блок підстановки описувати 39 незалежними квадратичними рівняннями, то нелінійна частина загальної системи, що відповідає восьми раундам, складатиметься з $64 \cdot 39 = 2496$ квадратичних рівнянь. Для 64 блоків підстановки це відповідає $64 \cdot 16 = 1024$ бітовим змінним, оскільки для кожного блока підстановки буде вісім змінних, що відповідають восьми бітам його входу, і відповідно вісім змінних, що відповідають бітам виходу. Якщо явно вводити також біти незалежних раундових ключів, то для восьми повних раундів і фінального забілювання потрібно ще $9 \cdot 64 = 576$ бітових змінних, що відповідають бітам раундових ключів. Тобто при поданні дев'яти раундового шифру DONATION у вигляді системи квадратичних рівнянь отримаємо систему, яка складається з близько 2496 квадратичних рівнянь та містить 1024 змінних, що відповідають входам/виходам блоків підстановки, і 576 додаткових змінних, що відповідають бітам раундових ключів — і це все не рахуючи лінійних рівнянь, що задають зв'язки між раундами.

Тут важливим є той факт, що в алгоритмі DONATION раундові ключі не породжуються під час шифрування відповідно до ключового розкладу, а зберігаються як незалежний ключовий матеріал для однієї сесії. З одного боку, це зменшує кількість нелінійних рівнянь, які були б пов'язані з ключовим розкладом. З іншого боку, це не створює додаткових алгебраїчних залежностей між раундовими ключами, які зловмисник міг би використати в атаці. Тому атаки, що використовують особливості ключового розкладу алгоритму, у такій постановці не можуть бути застосовані до алгоритму DONATION.

Порівняно з повнораундовим алгоритмом PRESENT, система квадратичних рівнянь для алгоритму DONATION є значно меншою через меншу кількість раундів. Тому ми не можемо стверджувати, що алгебраїчна атака на алгоритм DONATION має таку ж складність, як і аналогічна атака на повнораундовий алгоритм PRESENT. Але побудована система є достатньо великою, розрідженою, нелінійною і містить співвідношення, які описують 8-бітові інверсійні блоки підстановки. У наведеній системі не виявлено очевидного алгебраїчного спрощення, яке випливало б зі структури раундових перетворень або зі зв'язків між раундовими ключами.

Таким чином, проведений попередній аналіз не виявив очевидних алгебраїчних залежностей низького степеня, які безпосередньо давали б змогу побудувати ефективну алгебраїчну атаку на повну 8-раундову версію DONATION. Практичну складність розв'язання відповідних систем можна оцінювати за допомогою програмних засобів обчислення базисів Гребнера [16] або розв'язувачів задачі булевої виконуваності (SAT) [18].

Висновки

У роботі проведено попередній аналіз стійкості алгоритму DONATION до структурних та алгебраїчних атак. Оскільки бітова перестановка L у цьому алгоритмі порушує байтову структуру стану, то стандартні інтегральні атаки й атаки типу «вузького місця» не переносяться безпосередньо на алгоритм. Для блока підстановки визначено 39 незалежних квадратичних співвідношень та оцінено розмір системи рівнянь повної 8-раундової версії. Очевидних властивостей, які приводили б до атаки, ефективнішої за різницеві та лінійні, не виявлено. За результатами аналізу зроблено висновок, що в DONATION не виявлено структурних або алгебраїчних властивостей, які безпосередньо приводили б до ефективних атак.

Подальші дослідження доцільно спрямувати на аналіз кожного окремого класу структурних атак. Для інтегральних атак потрібно визначити, чи існують для скорочених версій DONATION множини відкритих текстів із заданою структурою входу (частина байтів фіксована, а один або кілька байтів перебирають усі можливі значення), для яких після кількох раундів побітова сума за модулем 2 вибраних компонент стану має передбачуване значення. Окремо слід розглянути інтегральні атаки на основі бітових шаблонів, у яких такі властивості задаються та відстежуються для окремих бітів, а не цілих байтів стану. Для атак усічених та неможливих диференціалів потрібно простежити, як класи різниць поширюються через послідовні раунди, визначити переходи, що не можуть відбутися, та най-

більшу кількість раундів, для яких виконуються відповідні характеристики. Ще одним напрямом досліджень є обчислювальні експерименти з булевими системами із застосуванням базисів Гребнера та розв'язувачів задачі булевої виконуваності для оцінювання практичної складності алгебраїчних атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kovalchuk L., Davydenko A., Klymenko T., Nedashkivska, A., Hilgurt S. Development of an algorithm with temporary cryptographic security for encrypting video stream from an unmanned aerial vehicle. *Eastern-European Journal of Enterprise Technologies.* 2025, vol. 5, no. 9 (137). P. 41—53. URL: https://doi.org/10.15587/1729-4061.2025.340917
2. Kovalchuk L., Hilgurt S., Davydenko A., Klymenko T. The Lightweight Block Cipher DONATION and Estimates of Its Security against Differential and Linear Cryptanalysis. *Cybernetics and Systems Analysis*, 2026, v. 62, no. 6, pp. 60—72. DOI and stable URL have not yet been assigned.
3. Bogdanov A., Knudsen L.R., Leander G., Paa, C., Poschmann A., Robshaw M.J.B., Seurin Y., Vikkelsoe C. PRESENT: An Ultra-Lightweight Block Cipher. In Cryptographic Hardware and Embedded Systems — CHES 2007. *LNCS 4727; Springer: Berlin, Heidelberg*, 2007. P. 450—466. URL: https://doi.org/10.1007/978-3-540-74735-2_31
4. Knudsen L.R., Wagner D. Integral Cryptanalysis. In Fast Software Encryption - FSE 2002. *LNCS 2365; Springer: Berlin, Heidelberg.* 2002. P. 112—127. URL: https://doi.org/10.1007/3-540-45661-9_9
5. Z'aba M.R., Raddum H., Henricksen M., Dawson E. Bit-Pattern Based Integral Attack. In Fast Software Encryption - FSE 2008. *LNCS 5086; Springer: Berlin, Heidelberg.* 2008. P. 363—381. URL: https://doi.org/10.1007/978-3-540-71039-4_23
6. Hadipour H., Gerhalte, S., Sadeghi S., Eichlseder M. Improved Search for Integral, Impossible-Differential and Zero-Correlation Attacks: Application to Ascon, ForkSKINNY, SKINNY, MANTIS, PRESENT and QARMAv2. IACR *Transactions on Symmetric Cryptology 2024,* 2024(1). P. 234—325. URL: https://doi.org/10.46586/tosc.v2024.i1.234-325
7. Shibayama N., Igarashi Y. Integral Attack with Bit-Based Division Property on the Lightweight Block Cipher LBC. In Information Security Applications - WISA 2024. Revised Selected Papers. *LNCS 15499; Springer Nature: Singapore.* 2025. P. 16—28. URL: https://doi.org/10.1007/978-981-96-1624-4_2
8. Xu Z., Cui J., Hu K., Wang M. Integral Attack on the Full FUTURE Block Cipher. *Tsinghua Science and Technology.* 2025. 30(1), p. 161—170. URL: https://doi.org/10.26599/TST.2024.9010007
9. Daemen J., Knudsen L.R., Rijmen V. The block cipher Square. In Fast Software Encryption — FSE 1997. *LNCS 1267; Springer: Berlin, Heidelberg*, 1997. P. 149—165. URL: https://doi.org/10.1007/BFb0052343
10. Knudsen L.R., Wagner D. Integral Cryptanalysis. In Fas tSoftware Encryption — FSE 2002. *LNCS 2365; Springer: Berlin, Heidelberg*. 2002. P. 112—127. URL: https://doi.org/10.1007/ 3-540-45661-9_9
11. Gilbert H., Minier M. A Collision Attack on 7 Rounds of Rijndael. In Proceedings of the Third Advanced Encryption Standard Candidate Conference. *NIST: NewYork, NY, USA.* 2000. P. 230—241. URL: https://crypto.orange-labs.fr/acg/publication/infoPublication.php?id=39 (accessedon 19 August 2026).

12. Minier M. A Three Rounds Propertyof the AES. In Advanced Encrypti on Standard — AES 2004. *LNCS 3373; Springer: Berlin, Heidelberg*. 2005. P. 16—26. URL: https://doi.org/10.1007/11506447_3
13. Courtois N., Klimov A., Patarin J., Shami, A. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In Advances in Cryptology - EUROCRYPT 2000. *LNCS 1807; Springer: Berlin, Heidelberg.* 2000. P. 392—407. URL: https://doi.org/10.1007/3-540-45539-6_27
14. Courtois N.T., Pieprzyk J. Cryptanalysis of Block Ciphers with Overdefined Systems of Equationss. In Advances in Cryptology - ASIACRYPT 2002. *LNCS 2501; Springer: Berlin, Heidelberg.* 2002. P. 267—287. URL: https://doi.org/10.1007/3-540-36178-2_17
15. Faugère J.-C. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra.* 1999. Vol. 139(1-3). P. 61—88. URL: https://doi.org/10.1016/S0022-4049(99)00005-5
16. Bard G.V. Algebraic Cryptanalysis. *Springer: NewYork, NY, USA*, 2009. URL: https://doi.org/10.1007/978-0-387-88757-9
17. Yeo S.L., Le D.-P., Khoo K. Improved algebraic attacks on lightweight block ciphers. *Journal of Cryptographic Engineering*. 2021. Vol. 11. P. 1—19. URL: https://doi.org/10.1007/s13389-020-00237-4
18. Massacci F., Marraro L. Logical Cryptanalysis as a SAT Problem. *Journal of Automated Reasoning*. 2000. Vol. 24 (1-2), P. 165—203. URL: https://doi.org/10.1023/ A:1006326723002

Стаття надійшла 3.09.2026

REFERENCES

1. Kovalchuk, L., Davydenko, A., Klymenko, T., Nedashkivska, A., Hilgurt, S. (2025). Development of an algorithm with temporary cryptographic security for encrypting video stream from an unmanned aerial vehicle. *Eastern-European Journal of Enterprise Technologies*, 5(9(137)), 41-53. https://doi.org/10.15587/1729-4061.2025.340917
2. Kovalchuk, L., Hilgurt, S., Davydenko, A., Klymenko, T. (2026). The Lightweight Block Cipher DONATION and Estimates of Its Security against Differential and Linear Cryptanalysis. *Cybernetics and Systems Analysis*, v. 62, no. 6, pp. 60—72. DOI and stable URL have not yet been assigned.
3. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C. (2007). PRESENT: An Ultra-Lightweight Block Cipher. In Cryptographic Hardware and Embedded Systems — CHES 2007. *LNCS 4727; Springer: Berlin, Heidelberg*, 450-466. https://doi.org/10.1007/978-3-540-74735-2_31
4. Knudsen, L.R., Wagner, D. (2002). Integral Cryptanalysis. In Fast Software Encryption — FSE 2002; *LNCS 2365; Springer: Berlin, Heidelberg,* 112-127. https://doi.org/10.1007/3-540-45661-9_9
5. Z'aba, M.R., Raddum, H., Henricksen, M., Dawson, E. (2008). Bit-Pattern Based Integral Attack. In Fast Software Encryption — FSE 2008. *LNCS 5086; Springer: Berlin, Heidelberg,* 363-381. https://doi.org/10.1007/978-3-540-71039-4_23
6. Hadipour, H., Gerhalter, S., Sadeghi, S., Eichlseder, M. (2024). Improved Search for Integral, Impossible-Differential and Zero-Correlation Attacks: Application to Ascon, Fork-SKINNY, SKINNY, MANTIS, PRESENT and QARMAv2. *IACR Transactions on Symmetric Cryptology*, 2024(1), 234-325. https://doi.org/10.46586/tosc.v2024.i1.234-325
7. Shibayama, N., Igarashi, Y. (2025). Integral Attack with Bit-Based Division Property on the Lightweight Block Cipher LBC. In Information Security Applications — WISA 2024, Revised Selected Papers*; LNCS 15499; Springer Nature: Singapore*, 16-28. https://doi.org/10.1007/978-981-96-1624-4_2

8. Xu, Z., Cui, J., Hu, K., Wang, M. (2025). Integral Attack on the Full FUTURE Block Cipher. *Tsinghua Science and Technology,* 30(1), 161-170. https://doi.org/10.26599/TST.2024.9010007
9. Daemen, J., Knudsen, L.R., Rijmen, V. (1997). The block cipher Square. In Fast Software Encryption — FSE 199. *LNCS 1267; Springer: Berlin, Heidelberg.* 149-165. https://doi.org/10.1007/BFb0052343
10. Knudsen, L.R., Wagner, D. (2002). Integral Cryptanalysis. In Fast Software Encryption — FSE 2002. *LNCS 2365; Springer: Berlin, Heidelberg*, 112-127. https://doi.org/10.1007/3-540-45661-9_9
11. Gilbert, H., Minier, M. (2000). A Collision Attack on 7 Rounds of Rijndael. In Proceedings of the Third Advanced Encryption Standard Candidate Conference. *NIST: NewYork, NY, USA,* 230-241. https://crypto.orange-labs.fr/acg/publication/infoPublication.php?id=39 (accessedon 19 August 2026).
12. Minier, M. (2005). A Three Rounds Propertyof the AES. In Advanced Encrypti on Standard — AES 2004. *LNCS 3373; Springer: Berlin, Heidelberg*, 16-26. https://doi.org/10.1007/11506447_3
13. Courtois, N., Klimov, A., Patarin, J., Shamir, A. (2000). Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In Advances in Cryptology - EUROCRYPT 2000. *LNCS 1807; Springer: Berlin, Heidelberg,* 392-407. https://doi.org/10.1007/3-540-45539-6_27
14. Courtois, N.T., Pieprzyk, J. (2002). Cryptanalysis of Block Ciphers with Overdefined Systems of Equationss. In Advances in Cryptology ASIACRYPT 2002. *LNCS 2501; Springer: Berlin, Heidelberg*, 267-287. https://doi.org/10.1007/3-540-36178-2_17
15. Faugère, J.-C. (1999). A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra,* 139(1-3), 61-88. https://doi.org/10.1016/S0022-4049(99)00005-5
16. Bard, G.V. (2009). Algebraic Cryptanalysis; *Springer: NewYork, NY, USA*, https://doi.org/10.1007/978-0-387-88757-9
17. Yeo, S.L., Le, D.-P., Khoo, K. (2021). Improved algebraic attacks on lightweight block ciphers. *Journal of Cryptographic Engineering*, 11, 1-19. https://doi.org/10.1007/s13389-020-00237-4
18. Massacci, F., Marraro, L. (2000). Logical Cryptanalysis as a SAT Problem. *Journal of AutomatedReasoning,* 24(1-2), 165-203. https://doi.org/10.1023/A:1006326723002

Article received 3.09.2026

L.V. Kovalchuk, S.Ya. Hilhurt, A.M. Davydenko, T.M. Klymenko

ANALYSIS OF THE SECURITY OF THE DONATION BLOCK CIPHER ALGORITHM AGAINST STRUCTURAL AND ALGEBRAIC ATTACKS

This paper continues a series of studies on the security of the resource-efficient block cipher DONATION, designed for encrypting video streams from UAVs. A preliminary analysis of its resistance to structural and algebraic attacks has been conducted. The impact of bit permutation on the byte structure of the state and the possibility of applying integral attacks and “bottleneck” attacks are analyzed. It is shown that permutation following a nonlinear transformation completely destroys the byte structure; therefore, the attacks considered do not directly apply to DONATION. For eight full rounds, the system describing the cipher contains 2,496 quadratic equations, 1,024 variables for the inputs and outputs of the substitution blocks, and 576 variables for the bits of the round keys (excluding linear equations). No obvious algebraic simplification has been found that would allow this system to be solved in practice.

K e y w o r d s: lightweight block cipher, structural cryptanalysis, algebraic cryptanalysis, integral attack, quadratic Boolean equations.

КОВАЛЬЧУК Людмила Василівна, д-р техн. наук, професор, пров. наук. співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 1989 р. закінчила Київський державний університет ім. Т.Г. Шевченко. Область наукових досліджень — теорія імовірності, математична статистика, абстрактна алгебра, теорія чисел, скінченні поля, криптологія, технології блокчейн, доведення без розголошення, децентралізовані фінансові системи на блокчейні.

ГІЛЬГУРТ Сергій Якович, д-р техн. наук, зав. відділу математичного та економетричного моделювання Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. В 1986 р. закінчив Київський інститут інженерів цивільної авіації. Область наукових досліджень — високопродуктивні та розподілені обчислювальні середовища, реконфігуровні обчислення на базі ПЛІС, сигнатурні засоби захисту інформації в кіберфізичних системах та на об'єктах критичної інфраструктури.

ДАВИДЕНКО Анатолій Миколайович д-р техн. наук, професор, пров. наук. співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України; професор кафедри комп'ютерної інженерії Державного університету інформаційно-комунікаційних технологій. У 1986 р. закінчив Київський інститут інженерів цивільної авіації. Область наукових досліджень — моделювання систем захисту інформації на об'єктах критичної інфраструктури та в розподілених і високопродуктивних обчислювальних середовищах, використання методів штучного інтелекту при побудові засобів захисту інформації.

КЛИМЕНКО Тетяна Михайлівна, зав. науково-організаційним відділом Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 1984 р. закінчила Київський політехнічний інститут. Область наукових досліджень — менеджмент наукових проєктів, оптимізація планування робіт.