DOI: 10.46972/2076-1546.2026.30.02

УДК 004.056.55:004.312.2

В. М. Рудницький, д-р техн. наук, проф.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки
https://orcid.org/0000-0003-3473-7433

В. В. Ларін, канд. техн. наук, доц.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки
https://orcid.org/0000-0003-0771-2660

С. А. Тристан
EPAM Systems, Inc.
https://orcid.org/0009-0004-5496-1517

П. М. Піонтківський, канд. техн. наук, ст. наук. співроб.
Житомирський військовий інститут імені С. П. Корольова
https://orcid.org/0000-0002-9103-5393

ПОБУДОВА ТА ДОСЛІДЖЕННЯ ОПЕРАЦІЙ РОЗШИРЕНОГО МАТРИЧНОГО КРИПТОПЕРЕТВОРЕННЯ НА ОСНОВІ ДИСКРЕТНО-КАЗУАЛЬНОЇ ЛОГІКИ

У статті розглянуто можливість побудови моделей СЕТ-операцій розширеного матричного криптографічного перетворення. Відповідність прямих та обернених операцій перевірено на основі взаємозв'язків між ними.

Проведено дослідження операцій розширеного матричного криптоперетворення із застосуванням дискретно-казуальної логіки. Побудовано множини двохоперандних трирозрядних СЕТ-операцій криптоперетворення шляхом поєднання одноопераднних дворозрядних СЕТ-операцій.

Виявлено, що дискретно-казуальне моделювання належить до апарату моделювання, який дозволяє описувати на його основі всі елементарні функції та СЕТ-операції, за допомогою яких будуються криптографічні системи потокового шифрування.

Розроблено моделі, які підтверджують гіпотезу, що СЕТ-операції розширеного матричного криптографічного перетворення можна розглядати як операції нелінійного перетворення. Встановлено, що отримана дискретно-казуальна модель розширеного матричного криптографічного перетворення реалізує чотири вироджені матриці, які вибираються залежно від значень вхідних змінних.

Доведено, що СЕТ-операції розширеного матричного криптографічного перетворення керовані інформацією. Акцентовано на тому, що застосування дискретно-казуального моделювання дозволяє однотипно описувати всі елементарні функції, на основі яких будуються СЕТ-операції. Крім того, з'ясовано, що дискретно-казуальне моделювання дозволяє розширити можливості дослідження елементарних функцій і СЕТ-операцій.

Сферою використання отриманих результатів дослідження можуть бути мобільні та стаціонарні системи малоресурсного криптографічного захисту конфіденційної інформації, шифросистеми, криптографічні протоколи тощо.

Ключові слова: *дискретно-казуальна модель; потокове шифрування; СЕТ-шифрування; СЕТ-операції; двохоперандні трирозрядні операції; одноопераднідні операції.*

Постановка проблеми в загальному вигляді. У сучасних умовах використання безпілотних авіаційних комплексів (БпАК) і робототехніки стало звичайною нормою. За їх допомогою вирішуються завдання з організації та забезпечення безпеки інформаційного ресурсу, а також питання в дослідницькій, охоронній та інших галузях.

У боротьбі з військовим агресором це новітнє озброєння та військова техніка стають усе більш ефективними й регулярно застосовуваними. Водночас і противник усе активніше задіює БпАК в своїй деструктивній діяльності. Саме тому дослідження питань про застосування БпАК та протидію їм необхідно вести паралельно.

Поява великої кількості розробників і виробників БпАК має низку причин. Зазначені комплекси, як правило, набагато дешевші за пілотовані літаки й вертольоти. Підготовка оператора безпілотної системи менш дороговартісна, ніж льотчика. Крім того, відсутність пілота дозволяє зменшити масу та габарити БпАК, збільшити діапазон допустимих перевантажень тощо.

Значущим є і фактор безпеки: втрата безпілотних апаратів не призводить до загибелі пілотів. Однак під час використання безпілотної авіації виникає ціла низка проблем, адже доступ до каналів передачі інформації можуть отримати і неавторизовані користувачі для задоволення своїх власних потреб. Як і проводові мережі, БпАК потрапляють під вплив різних атак. Актуальність застосування шифрування каналів управління та передачі спеціальної інформації БпАК зумовлена високою ймовірністю перехоплення команд управління, підміни телеметричних даних та несанкціонованого доступу до службової інформації противником. Удосконалення криптографічних методів захисту дозволить забезпечити конфіденційність, цілісність і автентичність переданих даних. Крім того, шифрування каналів зв’язку підвищує стійкість БпАК до впливу противника, що є критично важливим під час виконання бойових та спеціальних завдань.

Аналіз останніх досліджень і публікацій. У [1–4, 24] наведено основні вимоги до кодування обладнання БпАК, а також варіант побудови системи криптографії та передавання даних. У [6–9] розглянуто порівняльні характеристики та можливості різних стандартів захисту інформації в каналах управління та зв’язку, основні параметри, яким мають відповідати канал безпекового зв’язку й окремі елементи бортового обладнання БпАК.

Одним із провідних напрямів захисту інформації був і залишається криптографічний [9]. За останні десятиріччя системи криптографічного захисту набули значного розвитку [10–11]. Передові наукові дослідження в галузі криптографії провадяться в контексті квантових та постквантових технологій, малоресурсності, криптографічного кодування [12–16]. У [17, 22] запропоновано використовувати дискретно-казуальне подання моделей елементарних функцій і СЕТ-операцій, зокрема й СЕТ-операцій, керованих інформацією.

Проте можливість моделювання операції розширеного матричного криптографічного перетворення на сьогоднішній день не досліджувалася.

Формулювання завдання дослідження. Метою статті є дослідження можливості дискретно-казуального моделювання операції розширеного матричного криптографічного перетворення для збільшення можливостей і уніфікації побудови, а також вивчення криптографічних систем потокового СЕТ-шифрування, множин двохоперандних трирозрядних СЕТ-операцій криптоперетворення, отриманих за допомогою поєднання одноопераднних дворозрядних СЕТ-операцій.

Виклад основного матеріалу. З-поміж СЕТ-операцій особливе місце займають операції розширеного матричного криптографічного перетворення, які прийнято вважати нелінійними, хоча на сьогодні це не доведено.

СЕТ-операції розширеного матричного криптографічного перетворення будуються на основі елементарних функцій розширеного матричного криптографічного перетворення [18], наведених у табл. 1 [19, 23, 24].

Таблиця 1

Елементарні функції розширеного матричного криптографічного перетворення

Пряма елементарна операція			Обернена елементарна операція		
Код		Опис	Код		Опис
0001 1110	30	$f_{30} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$	1110 0001	225	$f_{225} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3$
0011 0110	54	$f_{54} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3$	1100 1001	201	$f_{201} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
0011 1001	57	$f_{57} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	1100 0110	198	$f_{198} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
0100 1011	75	$f_{75} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	1011 0100	180	$f_{180} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
0101 0110	86	$f_{86} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$	1010 1001	169	$f_{169} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3$
0101 1001	89	$f_{89} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	1010 0110	166	$f_{166} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3$
0110 0011	99	$f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	1001 1100	156	$f_{156} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$
0110 0101	101	$f_{101} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	1001 1010	154	$f_{154} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$
0110 1010	106	$f_{106} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	1001 0101	149	$f_{149} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
0110 1100	108	$f_{108} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	1001 0011	147	$f_{147} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
0111 1000	120	$f_{120} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	1000 0111	135	$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
0010 1101	45	$f_{45} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	1101 0010	210	$f_{210} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$

Моделювання СЕТ-операцій проводилося на основі дискретного або дискретно-модульного подання елементарних функцій [20, 21]. Дані моделювання елементарних функцій розширеного матричного криптографічного перетворення наведено в табл. 2.

Таблиця 2

Моделі елементарних функцій СЕТ-операцій розширеного матричного криптографічного перетворення

Моделі елементарних функцій			Моделі елементарних функцій		
00011110	30	$f_{30} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$	11100001	225	$f_{225} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3$
		$f_{30} = x_1 \oplus (x_2 \cdot x_3)$			$f_{225} = \bar{x}_1 \oplus (x_2 \cdot x_3)$
00101101	45	$f_{45} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	11010010	210	$f_{210} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
		$f_{45} = x_1 \oplus (x_2 \cdot \bar{x}_3)$			$f_{210} = \bar{x}_1 \oplus (x_2 \cdot \bar{x}_3)$
00110110	54	$f_{54} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3$	11001001	201	$f_{201} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
		$f_{54} = x_2 \oplus (x_1 \cdot x_3)$			$f_{201} = \bar{x}_2 \oplus (x_1 \cdot x_3)$
00111001	57	$f_{57} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	11000110	198	$f_{198} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
		$f_{57} = x_2 \oplus (x_1 \cdot \bar{x}_3)$			$f_{198} = \bar{x}_2 \oplus (x_1 \cdot \bar{x}_3)$
01001011	75	$f_{75} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10110100	180	$f_{180} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
		$f_{75} = x_1 \oplus (\bar{x}_2 \cdot x_3)$			$f_{180} = \bar{x}_1 \oplus (\bar{x}_2 \cdot x_3)$
01010110	86	$f_{86} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$	10101001	169	$f_{169} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3$
		$f_{86} = x_3 \oplus (x_1 \cdot x_2)$			$f_{169} = \bar{x}_3 \oplus (x_1 \cdot x_2)$
01011001	89	$f_{89} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	10100110	166	$f_{166} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3$
		$f_{89} = x_3 \oplus (x_1 \cdot \bar{x}_2)$			$f_{166} = \bar{x}_3 \oplus (x_1 \cdot \bar{x}_2)$
01100011	99	$f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10011100	156	$f_{156} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$
		$f_{99} = x_2 \oplus (\bar{x}_1 \cdot x_3)$			$f_{156} = \bar{x}_2 \oplus (\bar{x}_1 \cdot x_3)$
01100101	101	$f_{101} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	10011010	154	$f_{154} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$
		$f_{101} = x_3 \oplus (\bar{x}_1 \cdot x_2)$			$f_{154} = \bar{x}_3 \oplus (\bar{x}_1 \cdot x_2)$
01101010	106	$f_{106} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10010101	149	$f_{149} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
		$f_{106} = \bar{x}_3 \oplus (\bar{x}_1 \cdot \bar{x}_2)$			$f_{149} = x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2)$
01101100	108	$f_{108} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	10010011	147	$f_{147} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
		$f_{108} = \bar{x}_2 \oplus (\bar{x}_1 \cdot \bar{x}_3)$			$f_{147} = x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3)$
01111000	120	$f_{120} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	10000111	135	$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
		$f_{120} = \bar{x}_1 \oplus (\bar{x}_2 \cdot \bar{x}_3)$			$f_{135} = x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3)$

Базисом забезпечення гарантованого захисту інформаційного ресурсу, який циркулює в інформаційно-телекомунікаційних системах у режимі реального часу, є криптографічні методи та засоби захисту інформації.

Обмеженнями в ході дослідження є операції криптографічного перетворення, побудовані на основі додавання за модулем два.

Однооперандні операції розширеного матричного криптографічного перетворення [1, 20, 24] описані виразами (1)–(3).

$$C_{30,57,149}(x) = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}; \qquad C_{45,54,149}(x) = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}; \qquad (1)$$

$$C_{75,57,101}(x) = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix}; \qquad C^{/}_{75,57,101}(x) = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix}; \qquad (2)$$

$$C_{135,54,101}(x) = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix}; \qquad C^{/}_{135,99,101}(x) = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix}. \qquad (3)$$

Проте цей математичний апарат моделювання не сумісний з апаратом моделювання інших груп СЕТ-операцій, наприклад, матричних; операцій переставлянь, керованих інформацією; операцій на основі елементарних функцій; операцій, керованих інформацією. Зазначені групи операцій відповідно до [1, 7–12] були реалізовані на основі дискретно-казуального моделювання.

Дослідимо на основі таблиць істинності елементарних функцій розширеного матричного криптографічного перетворення дискретно-казуальні моделі.

Дискретно-казуальна модель (4) є казуальним поєднанням трьох дискретних функцій [19–24]:

$$f(x) = (f_1(x))(f_2(x))(f_3(x)), \qquad (4)$$

де $f_2(x)$ – функція керування;

$f_1(x)$ і $f_3(x)$ – перша і друга функції перетворення.

За умови $f_2(x) = 0$ буде виконуватися перша функція перетворення ($f_1(x)$), інакше – друга функція перетворення ($f_3(x)$).

Елементарну функцію переставляння, керовану інформацією, відповідно до (4) можна описати моделлю

$$f(x) = (x_1)(x_2)(x_3). \qquad (5)$$

Для вдосконалення методів синтезу елементарних функцій і СЕТ-операцій переставлянь, керованих інформацією, необхідні такі властивості дискретно-казуальної моделі (4):

1) інверсія результату реалізації функції керування зумовить переставляння місцями функцій перетворення: $f(x) = (f_1(x))(f_2(x))(f_3(x)) = (f_3(x))(\overline{f_2(x)})(f_1(x)$;

2) інверсія результатів реалізації функцій перетворення спричинить інверсію реалізації моделі: $(\overline{f_1(x)})(f_2(x))(\overline{f_3(x)}) = \overline{f(x)}$.

Елементарні функції переставлянь, які керуються інформацією (дискретно-казуальні моделі), наведено в табл. 3.

Таблиця 3

Елементарні функції переставлянь, які керуються інформацією (дискретно-казуальні моделі)

№ функції	Результат виконання	Дискретна модель	№ функції	Результат виконання	Дискретна модель
83	01010011	$f(x) = (x_3)(x_1)(x_2)$	197	11000101	$f(x) = (\bar{x}_2)(x_1)(x_3)$
163	10100011	$f(x) = (\bar{x}_3)(x_1)(x_2)$	202	11001010	$f(x) = (\bar{x}_2)(x_1)(\bar{x}_3)$
46	00101110	$f(x) = (x_1)(x_2)(\overline{x_3})$	209	11010001	$f(x) = (\overline{x_1})(x_2)(x_3)$
71	01000111	$f(x) = (x_3)(x_2)(x_1)$	226	11100010	$f(x) = (\overline{x_1})(x_2)(\overline{x_3})$
…	…	….	….	….	…..

Одноопераднi операції переставлянь, керовані інформацією, описано виразами (6)–(7):

$$C_{39,58,116}(x) = \begin{bmatrix}(x_2)(x_3)(x_1)\\(x_2)(x_1)(\bar{x}_3)\\(x_3)(x_2)(\bar{x}_1)\end{bmatrix}; \qquad C'_{39,58,116}(x) = C_{46,27,92}(x) = \begin{bmatrix}(x_1)(x_2)(\bar{x}_3)\\(x_1)(x_3)(x_2)\\(x_3)(x_1)(\bar{x}_2)\end{bmatrix}; \qquad (6)$$

$$C_{39,85,27}(x) = \begin{bmatrix}(x_2)(x_3)(x_1)\\(x_3)(x_1)(x_3)\\(x_1)(x_3)(x_2)\end{bmatrix}; \qquad C'_{39,85,27}(x) = C_{71,29,51}(x) = \begin{bmatrix}(x_3)(x_2)(\bar{x}_1)\\(x_1)(x_2)(x_3)\\(x_2)(x_1)(x_2)\end{bmatrix}. \qquad (7)$$

Тоді подамо групу елементарних функцій операцій, керованих інформацією, у табл. 4.

Таблиця 4

Група елементарних функцій операцій, керованих інформацією

Елементарна функція	Результат реалізації	Елементарна функція	Результат реалізації
$f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3$	00010111	$f_{232} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$	11101000
$f_{43} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$	00101011	$f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$	11010100
$f_{77} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$	01001101	$f_{178} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$	10110010
$f_{113} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3$	01110001	$f_{142} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$	10001110

Дискретно-казуальні моделі елементарних функцій операцій, керованих інформацією, наведено в табл. 5.

Таблиця 5

Дискретно-казуальні моделі елементарних функцій операцій, керованих інформацією

Моделі прямих елементарних функцій	Моделі обернених елементарних функцій
$f_{23} = (x_2 \cdot x_3)(x_1)(x_2 \vee x_3)$	$f_{232} = (\bar{x}_2 \vee \bar{x}_3)(x_1)(\bar{x}_2 \cdot \bar{x}_3)$
$f_{23} = (x_1 \cdot x_3)(x_2)(x_1 \vee x_3)$	$f_{232} = (\bar{x}_1 \vee \bar{x}_3)(x_2)(\bar{x}_1 \cdot \bar{x}_3)$
$f_{23} = (x_1 \cdot x_2)(x_3)(x_1 \vee x_2)$	$f_{232} = (\bar{x}_1 \vee \bar{x}_2)(x_3)(\bar{x}_1 \cdot \bar{x}_2)$
$f_{43} = (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3)$	$f_{212} = (\bar{x}_2 \vee x_3)(x_1)(\bar{x}_2 \cdot x_3)$
$f_{43} = (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3)$	$f_{212} = (\bar{x}_1 \vee x_3)(x_2)(\bar{x}_1 \cdot x_3)$
$f_{43} = (x_1 \vee x_2)(x_3)(x_1 \cdot x_2)$	$f_{212} = (\bar{x}_1 \cdot \bar{x}_2)(x_3)(\bar{x}_1 \vee \bar{x}_2)$
$f_{77} = (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3)$	$f_{178} = (x_2 \vee \bar{x}_3)(x_1)(x_2 \cdot \bar{x}_3)$
$f_{77} = (x_1 \vee x_3)(x_2)(x_1 \cdot x_3)$	$f_{178} = (\bar{x}_1 \cdot \bar{x}_3)(x_2)(\bar{x}_1 \vee \bar{x}_3)$
$f_{77} = (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2)$	$f_{178} = (\bar{x}_1 \vee x_2)(x_3)(\bar{x}_1 \cdot x_2)$
$f_{113} = (x_2 \vee x_3)(x_1)(x_2 \cdot x_3)$	$f_{142} = (\bar{x}_2 \cdot \bar{x}_3)(x_1)(\bar{x}_2 \vee \bar{x}_3)$
$f_{113} = (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3)$	$f_{142} = (x_1 \vee \bar{x}_3)(x_2)(x_1 \cdot \bar{x}_3)$
$f_{113} = (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2)$	$f_{142} = (x_1 \vee \bar{x}_2)(x_3)(x_1 \cdot \bar{x}_2)$

Одноопернадні операції на основі елементарних функцій операцій, керованих інформацією, описано виразами (8)–(9):

дискретно-казуальна модель прямої СЕТ-операції –

$$C(x) = \begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3) \\ (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \end{bmatrix}; \quad (8)$$

дискретно-казуальна модель оберненої СЕТ-операції –

$$C^{/}(x) = \begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \end{bmatrix}. \quad (9)$$

Операції розширеного матричного криптографічного перетворення не розглядалися так, як операції, керовані інформацією.

Побудуємо дискретно-казуальні моделі елементарних функцій СЕТ-операцій розширеного матричного криптографічного перетворення. Результати, описані дискретно-казуальними моделями операцій розширеного матричного криптографічного перетворення, наведено в табл. 6.

Отримані результати побудови та взаємоперетворення дискретно-казуальних моделей елементарних функцій СЕТ-операцій розширеного матричного криптографічного перетворення наведено в табл. 7.

Таблиця 6

Дискретно-казуальні моделі елементарних функцій СЕТ-операцій розширеного матричного криптографічного перетворення

00011110 30 000 0 001 0 010 0 011 1 100 1 101 1 110 1 111 0	00011110 30 000 0 001 0 100 1 101 1 010 0 011 1 110 1 111 0	00011110 30 000 0 001 0 010 0 011 1 100 1 101 1 110 1 111 0	00011110 30 000 0 010 0 100 1 110 1 001 0 011 1 101 1 111 0
$f_{30}(x) = (x_1)(x_2)(x_1 \oplus x_3)$		$f_{30}(x) = (x_1)(x_3)(x_1 \oplus x_2)$	
$f_{30} = x_1 \oplus (x_2 \cdot x_3) = (x_1)(x_2)(x_1 \oplus x_3) = (x_1)(x_3)(x_1 \oplus x_2)$			
00101101 45 000 0 001 0 010 1 011 0 100 1 101 1 110 0 111 1	00101101 45 000 0 001 0 100 1 101 1 010 1 011 0 110 0 111 1	00101101 45 000 0 001 0 010 1 011 0 100 1 101 1 110 0 111 1	00101101 45 000 0 010 1 100 1 110 0 001 0 011 0 101 1 111 1
$f_{45}(x) = (x_1)(x_2)(x_1 \equiv x_3)$ $f_{45}(x) = (x_1)(x_2)(x_1 \equiv x_3)$ $= (x_1)(x_2)(x_1 \oplus \bar{x}_3)$		$f_{45}(x) = (x_1 \oplus x_2)(x_3)(x_1)$ $f_{45}(x) = (x_1 \oplus x_2)(x_3)(x_1)$ $= (x_1)(\bar{x}_3)(x_1 \oplus x_2)$	
$f_{45} = x_1 \oplus (x_2 \cdot \bar{x}_3)$ $f_{45} = x_1 \oplus (x_2 \cdot \bar{x}_3) = (x_1)(x_2)(x_1 \oplus \bar{x}_3) = (x_1)(\bar{x}_3)(x_1 \oplus x_2)$			
01001011 75 000 0 001 1 010 0 011 0 100 1 101 0 110 1 111 1	01001011 75 000 0 001 1 100 1 101 0 010 0 011 0 110 1 111 1	01001011 75 000 0 001 1 010 0 011 0 100 1 101 0 110 1 111 1	01001011 75 000 0 010 0 100 1 110 1 001 1 011 0 101 0 111 1
$f_{75}(x) = (x_1 \oplus x_3)(x_2)(x_1)$ $= (x_1)(\bar{x}_2)(x_1 \oplus x_3)$		$f_{75}(x) = (x_1)(x_3)(x_1 \equiv x_2)$ $= (x_1)(x_3)(x_1 \oplus \bar{x}_2)$	
$f_{75} = x_1 \oplus (\bar{x}_2 \cdot x_3)$ $f_{75} = x_1 \oplus (\bar{x}_2 \cdot x_3) = (x_1)(\bar{x}_2)(x_1 \oplus x_3) = (x_1)(x_3)(x_1 \oplus \bar{x}_2)$			
. . . . .			

Таблиця 7

Результати побудови та взаємоперетворення дискретно-казуальних моделей елементарних функцій СЕТ-операцій розширеного матричного криптографічного перетворення

$f_{30}(x) = x_1 \oplus (x_2 \cdot x_3) = (x_1)(x_2)(x_1 \oplus x_3) = (x_1)(x_3)(x_1 \oplus x_2)$ $f_{54}(x) = x_2 \oplus (x_1 \cdot x_3) = (x_2)(x_1)(x_2 \oplus x_3) = (x_2)(x_3)(x_1 \oplus x_2)$ $f_{86}(x) = x_3 \oplus (x_1 \cdot x_2) = (x_3)(x_1)(x_2 \oplus x_3) = (x_3)(x_2)(x_1 \oplus x_3)$
$f_{45}(x) = x_1 \oplus (x_2 \cdot \bar{x}_3) = (x_1)(x_2)(x_1 \oplus \bar{x}_3) = (x_1)(\bar{x}_3)(x_1 \oplus x_2)$ $f_{57}(x) = x_2 \oplus (x_1 \cdot \bar{x}_3) = (x_2)(x_1)(x_2 \oplus \bar{x}_3) = (x_2)(\bar{x}_3)(x_1 \oplus x_2)$ $f_{89}(x) = x_3 \oplus (x_1 \cdot \bar{x}_2) = (x_3)(x_1)(\bar{x}_2 \oplus x_3) = (x_3)(\bar{x}_2)(x_1 \oplus x_3)$
$f_{75}(x) = x_1 \oplus (\bar{x}_2 \cdot x_3) = (x_1)(\bar{x}_2)(x_1 \oplus x_3) = (x_1)(x_3)(x_1 \oplus \bar{x}_2)$ $f_{99}(x) = x_2 \oplus (\bar{x}_1 \cdot x_3) = (x_2)(\bar{x}_1)(x_2 \oplus x_3) = (x_2)(x_3)(\bar{x}_1 \oplus x_2)$ $f_{101}(x) = x_3 \oplus (\bar{x}_1 \cdot x_2) = (x_3)(\bar{x}_1)(x_2 \oplus x_3) = (x_3)(x_2)(\bar{x}_1 \oplus x_3)$
$f_{135}(x) = x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) = (x_1)(\bar{x}_2)(x_1 \oplus \bar{x}_3) = (x_1)(\bar{x}_3)(x_1 \oplus \bar{x}_2)$ $f_{147}(x) = x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) = (x_2)(\bar{x}_1)(x_2 \oplus \bar{x}_3) = (x_2)(\bar{x}_3)(\bar{x}_1 \oplus x_2)$ $f_{149}(x) = x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) = (x_3)(\bar{x}_1)(\bar{x}_2 \oplus x_3) = (x_3)(\bar{x}_2)(\bar{x}_1 \oplus x_3)$
$f_{225}(x) = \bar{x}_1 \oplus (x_2 \cdot x_3) = (\bar{x}_1)(x_2)(\bar{x}_1 \oplus x_3) = (\bar{x}_1)(x_3)(\bar{x}_1 \oplus x_2)$ $f_{201}(x) = \bar{x}_2 \oplus (x_1 \cdot x_3) = (\bar{x}_2)(x_1)(\bar{x}_2 \oplus x_3) = (\bar{x}_2)(x_3)(x_1 \oplus \bar{x}_2)$ $f_{169}(x) = \bar{x}_3 \oplus (x_1 \cdot x_2) = (\bar{x}_3)(x_1)(x_2 \oplus \bar{x}_3) = (\bar{x}_3)(x_2)(x_1 \oplus \bar{x}_3)$
$f_{210}(x) = \bar{x}_1 \oplus (x_2 \cdot \bar{x}_3) = (\bar{x}_1)(x_2)(\bar{x}_1 \oplus \bar{x}_3) = (\bar{x}_1)(\bar{x}_3)(\bar{x}_1 \oplus x_2)$ $f_{198}(x) = \bar{x}_2 \oplus (x_1 \cdot \bar{x}_3) = (\bar{x}_2)(x_1)(\bar{x}_2 \oplus \bar{x}_3) = (\bar{x}_2)(\bar{x}_3)(x_1 \oplus \bar{x}_2)$ $f_{166}(x) = \bar{x}_3 \oplus (x_1 \cdot \bar{x}_2) = (\bar{x}_3)(x_1)(\bar{x}_2 \oplus \bar{x}_3) = (\bar{x}_3)(\bar{x}_2)(x_1 \oplus \bar{x}_3)$
$f_{180}(x) = \bar{x}_1 \oplus (\bar{x}_2 \cdot x_3) = (\bar{x}_1)(\bar{x}_2)(\bar{x}_1 \oplus x_3) = (\bar{x}_1)(x_3)(\bar{x}_1 \oplus \bar{x}_2)$ $f_{156}(x) = \bar{x}_2 \oplus (\bar{x}_1 \cdot x_3) = (\bar{x}_2)(\bar{x}_1)(\bar{x}_2 \oplus x_3) = (\bar{x}_2)(x_3)(\bar{x}_1 \oplus \bar{x}_2)$ $f_{154}(x) = \bar{x}_3 \oplus (\bar{x}_1 \cdot x_2) = (\bar{x}_3)(\bar{x}_1)(x_2 \oplus \bar{x}_3) = (\bar{x}_3)(x_2)(\bar{x}_1 \oplus \bar{x}_3)$
$f_{120}(x) = \bar{x}_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) = (\bar{x}_1)(\bar{x}_2)(\bar{x}_1 \oplus \bar{x}_3) = (\bar{x}_1)(\bar{x}_3)(\bar{x}_1 \oplus \bar{x}_2)$ $f_{108}(x) = \bar{x}_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) = (\bar{x}_2)(\bar{x}_1)(\bar{x}_2 \oplus \bar{x}_3) = (\bar{x}_2)(\bar{x}_3)(\bar{x}_1 \oplus \bar{x}_2)$ $f_{106}(x) = \bar{x}_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) = (\bar{x}_3)(\bar{x}_1)(\bar{x}_2 \oplus \bar{x}_3) = (\bar{x}_3)(\bar{x}_2)(\bar{x}_1 \oplus \bar{x}_3)$

Дослідження дискретно-казуальних моделей СЕТ-операцій розширеного матричного криптографічного перетворення

Побудову і аналіз дискретно-казуальних моделей СЕТ-операцій розширеного матричного криптографічного перетворення розглянемо на прикладі (10):

$$C_{30,57,149}(x) = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}; \qquad C'_{30,57,149}(x) = C_{45,54,149}(x) = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}. \qquad (10)$$

Дискретно-казуальну модель прямої СЕТ-операції розширеного матричного криптографічного перетворення описано виразом (11):

$$C_{30,57,149}(x)=\begin{bmatrix}(x_1)(x_3)(x_1\oplus x_2)\\(x_2)(\bar{x}_3)(x_1\oplus x_2)\\(x_3)(\bar{x}_2)(\bar{x}_1\oplus x_3)\end{bmatrix}=\begin{cases}\begin{bmatrix}x_1\\x_1\\\bar{x}_1\end{bmatrix}, & \text{якщо } x_2=0;\ x_3=0;\\ \begin{bmatrix}x_1\\x_1\\\bar{x}_1\end{bmatrix}, & \text{якщо } x_2=0;\ x_3=1;\\ \begin{bmatrix}x_1\\x_1\oplus 1\\0\end{bmatrix}, & \text{якщо } x_2=1;\ x_3=0;\\ \begin{bmatrix}x_1\oplus 1\\x_1\\0\end{bmatrix}, & \text{якщо } x_2=1;\ x_3=1.\end{cases} \tag{11}$$

Дискретно-казуальна модель оберненої СЕТ-операції розширеного матричного криптографічного перетворення описана виразом (12):

$$C'_{30,57,149}(x)=C_{45,54,149}(x)=\begin{bmatrix}(x_1)(\bar{x}_3)(x_1\oplus x_2)\\(x_2)(x_3)(x_1\oplus x_2)\\(x_3)(\bar{x}_2)(\bar{x}_1\oplus x_3)\end{bmatrix}=$$

$$=\begin{cases}\begin{bmatrix}x_1\\0\\x_1\oplus 1\end{bmatrix}, & \text{якщо } x_2=0;\ x_3=0;\\ \begin{bmatrix}x_1\\x_1\\x_1\end{bmatrix}, & \text{якщо } x_2=0;\ x_3=1;\\ \begin{bmatrix}x_1\oplus 1\\1\\0\end{bmatrix}, & \text{якщо } x_2=1;\ x_3=0;\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\\1\end{bmatrix}, & \text{якщо } x_2=1;\ x_3=1.\end{cases} \tag{12}$$

Отже, описані дискретно-казуальні моделі прямої й оберненої СЕТ-операцій розширеного матричного криптографічного перетворення дозволяють зробити такі висновки:

1. Наведену дискретно-казуальну модель розширеного матричного криптографічного перетворення $C_{30,57,149}(x)$ можна розглядати як модель, яка реалізує чотири вироджені матриці, що вибираються залежно від значень вхідних змінних x_2 і x_3.

2. Оскільки операція $C_{30,57,149}(x)$ несиметрична, то й реалізовані нею матриці будуть виродженими.

3. Для несиметричної операції $C_{30,57,149}(x)$ є обернена операція $C'_{30,57,149}(x)=C_{45,54,149}(x)$, яка також несиметрична.

4. Обернена операція $C'_{30,57,149}(x)=C_{45,54,149}(x)$ реалізує також чотири вироджені матриці.

Застосування дискретно-казуального моделювання дозволяє реалізувати однотипний опис усіх елементарних функцій, на основі яких будуються СЕТ-операції. Крім того, як

показали отримані результати, дискретно-казуальне моделювання дозволяє розширити можливості дослідження елементарних функцій і СЕТ-операцій.

Висновки. У роботі досліджено можливості застосування апарату дискретно-казуального моделювання для побудови та аналізу СЕТ-операцій розширеного матричного криптографічного перетворення. На основі аналізу таблиць істинності елементарних функцій розширеного матричного криптографічного перетворення побудовано відповідні дискретно-казуальні моделі, які забезпечують формалізований опис прямих і обернених криптографічних перетворень. Встановлено відповідність між прямими та оберненими СЕТ-операціями, що підтверджує коректність побудованих моделей.

Проведене дослідження показало, що СЕТ-операції розширеного матричного криптографічного перетворення доцільно описувати у вигляді дискретно-казуальних моделей, у яких вибір елементарної функції перетворення здійснюється залежно від значень керівних змінних. Це дозволяє розглядати їх як СЕТ-операції, керовані інформацією.

Отримані результати свідчать про можливість інтерпретації операцій розширеного матричного криптографічного перетворення як операцій нелінійного перетворення в межах дискретно-казуального підходу. Побудовані моделі дозволяють розглядати їх як реалізацію набору вироджених матричних перетворень, які вибирають залежно від вхідних змінних, що підтверджує несиметричний характер прямих та обернених СЕТ-операцій.

Отже, застосування дискретно-казуального моделювання розширює можливості дослідження елементарних функцій і СЕТ-операцій, забезпечує єдиний формальний апарат їх опису та створює передумови для подальшої уніфікації методів аналізу й синтезу малоресурсних криптографічних перетворень.

Подальші дослідження доцільно спрямувати на формалізацію критеріїв нелінійності СЕТ-операцій розширеного матричного криптографічного перетворення в межах дискретно-казуального апарату, а також на оцінювання їх криптографічних властивостей із позицій стійкості до відомих криптоаналітичних атак.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Rudnytskyi V., Lada N., Kuchuk G. & Pidlasyi D. Architecture of CET-operations and Stream Encryption Technologies : Monograph. Cherkasy, 2024. 374 p. ISBN 978-966-2554-81. URL: https://dndivsovt.com/index.php/monograph/issue/view/22/22 (last accessed: 07.01.2026).

2. Рудницький В. М., Лада Н. В., Рудницька Ю. В., Короткий Т. К. Моделювання симетричних двохоперандних операцій криптографічного кодування на основі об’єднання одноопераднних операцій // Сучасна спеціальна техніка. 2021. № 4. С. 32–38.

3. Лада Н. В., Рудницька Ю. В. Класифікація груп несиметричних двохоперандних операцій криптоперетворення інформації на основі перестановочних схем їх синтезу // Проблеми інформатизації : матеріали VI Міжнар. наук.-техн. конф. : тези доп. (Черкаси – Баку – Бельсько-Бяла – Харків, 14–16 листоп. 2018 р.). Харків : НТУ «ХПІ», 2018. С. 11.

4. Лада Н. В., Бреус Р. В., Рудницька Ю. В., Висоцький С. В. Аналіз групи двохоперандних симетричних операцій криптоперетворення // Проблеми інформатизації : матеріали VII Міжнар. наук.-техн. конф. : тези доп. (Черкаси – Харків – Баку – Бельсько-Бяла, 13–15 листоп. 2019 р.). Харків : НТУ «ХПІ», 2019. Т. 1. С. 85.
5. Рудницька Ю. В., Рудницький С. В. Моделювання симетричних операцій криптографічного кодування // Проблеми інформатизації : X Міжнар. наук.-техн. конф. : тези доп. (Черкаси – Баку – Бельсько-Бяла – Харків, 24–25 листоп. 2022 р.). Харків : НТУ «ХПІ», 2022. Т. 2. С. 10.
6. Koblitz N. Algebraic Aspects of Cryptography. Springer-Verlag, Berlin, 1998. 215 p. https://doi.org/10.1007/978-3-662-03642-6
7. Cryptology and Computational Number Theory // Proc. of Symp. in Appl. Math. 1990. 171 p. ISBN 978-0821801550.
8. Хорошко В. А., Чекатков А. А. Методи й засоби захисту інформації. Київ, 2003. 504 с.
9. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних : підручник. Київ : ТОВ «НВП» ІНТЕРСЕРВІС», 2009. 716 с.
10. Дмитришин О. В. Методи і засоби блокового шифрування підвищеної стійкості на основі арифметичних операцій за модулем : дис. ... канд. техн. наук : 05.13.05. Вінниця, 2012. 180 с.
11. Бабенко В. Г. Метод підвищення швидкодії систем захисту інформації на основі використання спеціалізованих логічних функцій : дис. ... канд. техн. наук : 05.13.21. Черкаси, 2009. 166 с.
12. Чечельницький В. Я. Методологія підвищення ефективності телекомунікаційних систем на основі інтеграції канального кодування та шифрування даних : дис. ... д-ра техн. наук : 05.12.02. Одеса, 2013. 407 с.
13. Горбенко Ю. І., Ганзя Р. С. Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/27194/1/8-40-48.pdf (дата звернення: 20.12.2025).
14. Горбенко Ю. І., Ганзя Р. С. Аналіз стійкості популярних криптосистем проти квантового криптоаналізу на основі алгоритму Гровера // Захист інформації : наук.-практ. журн. Київ, 2014. Т. 16, № 2. С. 106–112. https://doi.org/10.18372/2410-7840.16.6915
15. Bernstein D., Buchmann J., Dahmen E. Post-Quantum Cryptography. Berlin : Springer, 2009. 246 p. ISBN 978-3-540-88701-0. https://doi.org/10.1007/978-3-540-88702-7
16. Goldreich O. Foundations of Cryptography. Vol. 1 (Basic tools). Vol. 2 (Basic applications). Cambridge University Press, Cambridge, United Kingdom, 2001 (Vol. 1). 372 p. ISBN 978-0-511-54689-1 ; 2004 (Vol. 2). 798 p. ISBN 978-0-521-83084-3. https://doi.org/10.1017/CBO9780511721656
17. Vergili I., Yücel M. D. Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen S-Boxes. Turk J Elec Engin. 2001. Vol. 9, № 2. P. 137–145.
18. Соколов А. В. Новые методы синтеза нелинейных преобразований современных шифров. Lap Lambert Academic Publishing, Germany, 2015. 100 с.
19. Menezes A. J., Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. Pub. CRC Press, 1996. 816 p.
20. Hatzivasilis G., Fysarakis K., Papaefstathiou I., Manifavas Ch. A Review of Lightweight Block Ciphers // J. Cryptographic Engineering. 2018. Vol. 8 (2). P. 141–184. https://doi.org/10.1007/s13389-017-0160-y

21. Rogaway Ph., Bellare M., Black J. OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption // ACM Transactions on Information and System Security. 2003. Vol. 6 (3). P. 365–403. https://doi.org/10.1145/937527.937529

22. Рудницький В. М., Бабенко В. Г., Жиляєв Д. А. Алгебраїчна структура множини логічних операцій кодування // Наука і техніка Повітряних Сил Збройних Сил України : наук.-техн. журн. Харків : ХУПС, 2011. № 2 (6). С. 112–114.

23. Лада Н. В., Козловська С. Г., Рудницький С. В. Побудова математичної групи симетричних операцій на основі додавання за модулем два // Сучасна спеціальна техніка : наук.-практ. журн. Київ, 2019. № 4 (59). С. 33–41. URL: http://suchasnaspetstehnika.com/journal/ukr/2019_4/6.pdf (дата звернення: 20.12.2025).

24. Рудницький В. М., Ларін В. В., Лада Н. В. Дискретно-казуальне моделювання СЕТ-операцій перестановок керованих інформацією : Колективна монографія. Черкаси : ДНДІ ВС ОВТ, 2025. С. 91–134. ISBN 978-617-8725-03-7.

Стаття надійшла до редакції 30.01.2026.
Прийнято до друку 02.03.2026.
Дата публікації 30.06.2026.

REFERENCES

1. Rudnytskyi, V., Lada, N., Kuchuk, G. & Pidlasyi, D. (2024). Architecture of CET-operations and Stream Encryption Technologies: Monograph. ISBN 978-966-2554-81. Retrived from https://dndivsovt.com/index.php/monograph/issue/view/22/22

2. Rudnytskyi, V. M., Lada, N. V., Rudnytska, Yu. V., & Korotkyi, T. K. (2021). Modeliuvannia symetrychnykh dvokhoperandnykh operatsii kryptohrafichnoho koduvannia na osnovi obiednannia odnooperandnykh operatsii [Modeling of Symmetric Two-Operand Operations of Cryptographic Coding Based on the Union of One-Operand Operations]. *Suchasna spetsialna tekhnika [Modern Special Technology], 4,* 32–38 [in Ukrainian].

3. Lada, N. V., & Rudnytska, Yu. V. (2018). Klasyfikatsiia hrup nesymetrychnykh dvokhoperandnykh operatsii kryptoperetvorennia informatsii na osnovi perestanovochnykh skhem yikh syntezu [Classification of Groups of Asymmetric Two-Operand Operations of Cryptographic Information Conversion Based on Permutation Schemes of Their Synthesis]. In *Problemy informatyzatsii: materialy VI Mizhnar. nauk.-tekhn. konf. [Problems of Informatization: Materials of the VI International Scientific and Technical Conference].* Cherkasy – Baku – Belsko-Biala – Kharkiv, November 14–16, 2018. (pp. 11). Kharkiv: NTU «KhPI» [in Ukrainian].

4. Lada, N. V., Breus, R. V., Rudnytska, Yu. V., & Vysotskyi, S. V. (2019). Analiz hrupy dvokhoperandnykh symetrychnykh operatsii kryptoperetvorennia [Analysis of the Group of Two-Operand Symmetric Cryptographic Conversion Operations]. In *Problemy informatyzatsii: materialy VII Mizhnar. nauk.-tekhn. konf. [Problems of Informatization: Materials of the VII International Scientific and Technical Conference].* Cherkasy – Kharkiv – Baku – Belsko-Biala, November 13–15, 2019. (Vol. 1, pp. 85). Kharkiv: NTU «KhPI» [in Ukrainian].

5. Rudnytska, Yu. V., & Rudnytskyi, S. V. (2022). Modeliuvannia symetrychnykh operatsii kryptohrafichnoho koduvannia [Modeling of Symmetric Cryptographic Coding Operations]. In *Problemy informatyzatsii: materialy VII Mizhnar. nauk.-tekhn. konf. [Problems of Informatization: Materials of the X International Scientific and Technical Conference]*. Cherkasy – Baku – Belsko-Biala – Kharkiv, November 24–25, 2022. (Vol. 2, pp. 10). Kharkiv: NTU «KhPI» [in Ukrainian].

6. Koblitz, N. (1998). *Algebraic Aspects of Cryptography.* Springer-Verlag, Berlin. https://doi.org/10.1007/978-3-662-03642-6

7. Cryptology and Computational Number Theory. (1990). *Proc. of Symp. in Appl. Math.* ISBN 978-0821801550.

8. Khoroshko, V. A., & Chekatkov, A. A. (2003). *Metody y zasoby zakhystu informatsii [Methods and Means of Information Protection]*. Kyiv [in Ukrainian].

9. Yudin, O. K., Korchenko, O. H., & Konakhovych, H. F. (2009). *Zakhyst informatsii v merezhakh peredachi danykh: pidruchnyk [Information Protection in Data Transmission Networks: textbook]*. Kyiv [in Ukrainian].

10. Dmytryshyn, O. V. (2012). *Metody i zasoby blokovoho shyfruvannia pidvyshchenoi stiikosti na osnovi aryfmetychnykh operatsii za modulem: dys. ... kand. tekhn. nauk: 05.13.05 [Methods and Means of Block Encryption of Increased Stability Based on Arithmetic Operations by Modulus: dissertation ... Candidate of Technical Sciences: 05.13.05]*. Vinnytsia [in Ukrainian].

11. Babenko, V. H. (2009). *Metod pidvyshchennia shvydkodii system zakhystu informatsii na osnovi vykorystannia spetsializovanykh lohichnykh funktsii: dys. ... kand. tekhn. nauk: 05.13.21 [Method of Increasing the Speed of Information Protection Systems Based on the Use of Specialized Logical Functions: dissertation ... Candidate of Technical Sciences: 05.13.21]*. Cherkasy [in Ukrainian].

12. Chechelnytskyi, V. Ya. (2013). *Metodolohiia pidvyshchennia efektyvnosti telekomunikatsiinykh system na osnovi intehratsii kanalnoho koduvannia ta shyfruvannia danykh : dys. ... d-ra tekhn. nauk: 05.12.02 [Methodology for Increasing the Efficiency of Telecommunication Systems Based on the Integration of Channel Coding and Data Encryption: dissertation ... Dr. Tech. Sciences: 05.12.02]*. Odesa [in Ukrainian].

13. Horbenko, Yu. I., & Hanzia, R. S. (n. d.). *Analiz shliakhiv rozvytku kryptohrafii pislia poiavy kvantovykh kompiuteriv [Analysis of the Development of Cryptography After the Advent of Quantum Computers]*. Retrived from http://ena.lp.edu.ua:8080/bitstream/ntb/27194/1/8-40-48.pdf [in Ukrainian].

14. Horbenko, Yu. I., & Hanzia, R. S. (2014). Analiz stiikosti populiarnykh kryptosystem proty kvantovoho kryptoanalizu na osnovi alhorytmu Hrovera [Analysis of the stability of popular cryptosystems against quantum cryptanalysis based on Grover's algorithm]. *Zakhyst informatsii: nauk.-prakt. zhurn. [Information Protection: Scientific and Practical Journal], 16,* 2, 106–112. https://doi.org/10.18372/2410-7840.16.6915 Kyiv [in Ukrainian].

15. Bernstein, D., Buchmann, J., & Dahmen, E. (2009). *Post-Quantum Cryptography.* Berlin. ISBN 978-3-540-88701-0. https://doi.org/10.1007/978-3-540-88702-7

16. Goldreich, O. (2004). *Foundations of Cryptography. Vol. 1 (Basic tools). Vol. 2 (Basic applications).* Cambridge, United Kingdom. ISBN 978-0-511-54689-1; ISBN 978-0-521-83084-3. https://doi.org/10.1017/CBO9780511721656

17. Vergili, I., Yücel, M. D. (2001). Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen S-Boxes. *Turk J. Elec Engin, 9,* 2, 137–145.
18. Sokolov, A. V. (2015). *Novye metody sinteza nelinejnyh preobrazovanij sovremennyh shifrov [New Methods of Synthesis of Nonlinear Transformations of Modern Ciphers]*. Lap Lambert Academic Publishing, Germany [in Russian].
19. Menezes, A. J., Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography.*
20. Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, Ch. (2018). A Review of Lightweight Block Ciphers. *J. Cryptographic Engineering, 8* (2), 141–184. https://doi.org/10.1007/s13389-017-0160-y
21. Rogaway, Ph., Bellare, M., Black, J. (2003). OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption. *ACM Transactions on Information and System Security, 6* (3), 365–403. https://doi.org/10.1145/937527.937529
22. Rudnytskyi, V. M., Babenko, V. H., & Zhyliaiev, D. A. (2011). Alhebraichna struktura mnozhyny lohichnykh operatsii koduvannia [Algebraic Structure of the Set of Logical Coding Operations]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy : nauk.-tekhn. zhurn. [Science and Technology of the Air Force of the Armed Forces of Ukraine: scientific and technical journal], 2* (6), 112–114. Kharkiv [in Ukrainian].
23. Lada, N. V., Kozlovska, S. H., & Rudnytskyi, S. V. (2019). Pobudova matematychnoi hrupy symetrychnykh operatsii na osnovi dodavannia za modulem dva [Construction of a Mathematical Group of Symmetric Operations BASED on Addition Modulo Two]. *Suchasna spetsialna tekhnika : nauk.-prakt. zhurn. [Modern Special Technique: scientific and practical journal], 4* (59), 33–41. Retrived from http://suchasnaspetstehnika.com/journal/ukr/2019_4/6.pdf Kyiv [in Ukrainian].
24. Rudnytskyi, V. M., Larin, V. V., & Lada, N. V. (2025). Dyskretno-kazualne modeliuvannia SET-operatsii perestanovok kerovanykh informatsiieiu: Kolektyvna monohrafiia [Discrete-Casual Modeling of SET-Operations of Information-Driven Permutations: Collective monograph]. ISBN 978-617-8725-03-7. Cherkasy [in Ukrainian].

V. M. Rudnytskyi, V. V. Larin, S. A. Trystan, P. M. Piontkivskyi

CONSTRUCTION AND RESEARCH OF ADVANCED MATRIX CRYPTOCONVERSION OPERATIONS BASED ON DISCRETE-CASUAL LOGIC

This article examines the possibility of constructing models of CET-operations for an extended matrix cryptographic transformation. The correspondence between direct and inverse operations is verified based on the relationships between them.

A study of extended matrix cryptographic transformation operations was conducted using discrete-causal logic. Sets of two-operand three-bit CET-operations of cryptographic transformation were constructed by combining one-operand two-bit CET-operations.

It has been found that discrete-causal modeling belongs to a modeling framework that allows for the description of all elementary functions and CET-operations used to construct stream encryption cryptographic systems.

Models have been developed that confirm the hypothesis that CET-operations of the extended matrix cryptographic transformation can be regarded as nonlinear transformation operations. It has been established that the obtained discrete-causal model of an extended matrix cryptographic transformation implements four degenerate matrices, which are selected depending on the values of the input variables.

It has been proven that the CET-operations of the extended matrix cryptographic transformation are information-driven. It is emphasized that the application of discrete-causal modeling allows for a uniform description of all elementary functions upon which CET-operations are based. Furthermore, it has been established that discrete-causal modeling allows for expanding the scope of research into elementary functions and CET-operations.

The results of this study can be applied to mobile and stationary systems for resource-constrained cryptographic protection of confidential information, encryption systems, cryptographic protocols, and so on.

Keywords: *discrete-causal model; stream encryption; CET-encryption; CET-operations; two-operand three-bit operations; one-operand operations.*