УДК 004.056.55:004.312.2
DOI https://doi.org/10.32782/2663-5941/2025.4.2/35

Рудницький В.М.
Черкаський державний технологічний університет

Бабенко В.Г.
Черкаський державний технологічний університет

Рудницький С.В.
Черкаський державний технологічний університет

Короткий Т.К.
Черкаський державний технологічний університет

Ковтюх В.А.
Черкаський державний технологічний університет

ОСОБЛИВОСТІ ГРУП НЕСИМЕТРИЧНИХ CET-ОПЕРАЦІЙ СИНТЕЗОВАНИХ З ТОЧНІСТЮ ДО ПЕРЕСТАНОВКИ ПЕРШОГО ОПЕРАНДА

Одним із перспективних шляхів розвитку малоресурсної криптографії є CET-шифрування. Стаття присвячена дослідженню, що вирішує завдання, яке полягає у дослідженні можливості застосування методу генерації груп несиметричних 2-операндних CET-операцій з точністю до перестановки першого операнда для побудови малоресурсних несиметричних систем потокового шифрування підвищеної криптостійкості. Об'єкт дослідження: процеси взаємоперетворення моделей 2-операндних CET-операцій в процесі їх модифікації з точністю до перестановки. Використання різних методів генерації синтезу груп операцій з точністю до перестановки приводить до генерації різних псевдовипадкових CET-операцій. При чому дані послідовності можуть відрізняються не тільки послідовностями операцій, але і різними їх наборами. Для вирішення завдання на прикладі несиметричної 2-операндної CET-операції розглянуті процеси її модифікації з точністю до перестановки першого операнда одноопераднною CET-операцією та встановлено, що така модифікація реалізується шляхом модифікації одноопераднних CET-операцій, з яких вона побудована. На основі моделей модифікації CET-операцій реалізуються генератори псевдовипадкових послідовностей прямих і обернених модифікованих 2-операндних CET-операцій. За результатами аналізу встановлено, що модифікація одноопераднних CET-операцій в процесі шифрування забезпечує збільшення кількості таблиць підстановки, що реалізує потоковий шифр. Для практичної реалізації доцільно будувати потокові шифри з використанням груп модифікованих несиметричних 2-операндних CET-операцій з точністю до перестановки першого операнда. Збільшення кількості таблиць підстановки при послідовній модифікації CET-операцій призводить до ускладнення криптоаналізу та до підвищення криптографічної стійкості криптографічного алгоритму. Сфера використання отриманих результатів: мобільні і стаціонарні системи малоресурсного криптографічного захисту конфіденційної інформації.

Ключові слова: *малоресурсна криптографія, CET-шифрування, 2-операндні CET-операції, несиметричні криптографічні перетворення, потокове шифрування.*

Постановка проблеми. Проблема захисту інформації в комп'ютерних системах від некомпетентності користувачів, некоректності програмного забезпечення та несанкціонованого доступу до інформації стала актуальною при створенні перших засобів електронно-обчислювальної техніки. Побудова перших комп'ютерних мереж привела до виникнення і широкого розповсюдження кіберзлочинності [1, 2]. Ефективно протидіяти несанкціонованому доступу до конфіденційної інформації в комп'ютерних мережах можна на основі широкого впровадження криптографічних

алгоритмів [3]. Проте застосування криптографічного захисту має і негативні наслідки, пов'язані з відволіканням обчислювальних ресурсів, збільшенням часу обробки інформації та збільшенням вартості роботи системи [4, 5]. Зменшити негативні наслідки від впровадження криптографічних систем можливо на основі застосування малоресурсної (легкої) криптографії. Одним із перспективних шляхів розвитку малоресурсної криптографії є СЕТ-шифрування [6].

Аналіз останніх досліджень і публікацій. Традиційно при побудові потокових шифрів використовується криптографічне додавання інформації з псевдовипадковою послідовністю. На практиці в якості криптографічного додавання використовується додавання за модулем [7]. Додавання за модулем в теорії СЕТ-шифрування розглядається як 2-операндна СЕТ-операція [6]. Крім того методи синтезу СЕТ-операцій з точністю до перестановки дозволяють синтезувати групи модифікованих операцій [8, 9]. Реалізація симетричних систем потокового шифрування простіша за реалізацію несиметричних систем потокового шифрування. Виходячи з цього, початковий вектор дослідження був спрямований на синтез симетричних 2-операндних СЕТ-операцій для забезпечення простоти реалізації криптоалгоритмів [6, 20]. Для підвищення криптостійкості потокових шифрів було запропоновано замість однієї одноопераднної СЕТ-операції використовувати групи операцій з точністю до перестановки [19]. У роботах [10-12) показано, що синтезувати групи симетричних 2-операндних СЕТ-операцій і генерувати їх послідовності можна з точністю до перестановки результату перетворення. Генерувати послідовності несиметричних СЕТ-операцій доцільно з точністю до перестановки другого операнда [13, 14]. На сьогоднішній день метод синтезу груп несиметричних СЕТ-операцій з точністю до перестановки першого операнда не досліджувався через складність реалізації оберненого криптографічного перетворення.

Постановка завдання. Метою роботи є дослідження можливості застосування методу генерації груп СЕТ-операцій з точністю до перестановки першого операнда для побудови малоресурсних несиметричних систем потокового шифрування підвищеної криптостійкості.

Виклад основного матеріалу. ***Результати моделювання груп несиметричних 2-операндних СЕТ-операцій з точністю до перестановки першого операнда.*** При вдосконаленні і побудові систем потокового шифрування можна використовувати методи генерації псевдовипадкових послідовностей СЕТ-операцій з точністю до перестановки першого операнда, другого операнда, або результату криптографічного перетворення [6, 15]. При побудові несиметричних систем потокового шифрування на сьогоднішній день використовується генерація псевдовипадкових послідовностей СЕТ-операцій з точністю до перестановки другого операнда [15, 16]. Це пов'язано з простотою генерації груп прямих і обернених несиметричних СЕТ-операцій. Використання різних методів генерації синтезу груп операцій з точністю до перестановки приводить до генерації різних псевдовипадкових СЕТ-операцій. При чому дані послідовності можуть відрізняються не тільки послідовностями операцій, але і різними їх наборами.

Дослідимо особливості застосування методу синтезу СЕТ-операцій з точністю до перестановки першого операнда, а також визначимо переваги та недоліки їх застосування в несиметричних системах потокового шифрування.

Моделювання процесів прямого і оберненого криптографічного перетворення в групі несиметричних 2-операндних СЕТ-операцій з точністю до перестановки першого операнда проведемо на прикладі 2Сі-квантової СЕТ-операції [6]. Дане обмеження пов'язане з мінімальною кількістю СЕТ-операцій, на основі яких будуються несиметричні 2-операндні СЕТ-операції, а також простотою застосування математичного апарату для моделювання взаємних перетворень моделей операцій [17].

Коректність отриманих за результатами моделювання взаємозв'язків між прямими і оберненими модифікованими СЕТ-операціями з точністю до перестановки першого операнда перевіримо на основі обчислювального експерименту.

Задамо модель несиметричної 2-операндної 2Сі-квантової СЕТ-операції [6] кортежем із чотирьох одноопераднних 2Сі-квантових СЕТ-операцій. Якщо

$$C_1(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}=z;\ C_2(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}=z;$$

$$C_3(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}=z;\ C_4(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}=z,$$

де $C_i(x)$ – i-та одноопераднна СЕТ-операція; x_1 і x_2 – перший і другий Сі-кванти першого операнда (вхідна інформація); z – результат криптографічного перетворення (2 Сі-кванти), тоді:

$$C(x, y)=C\left(C_1(x), C_2(x), C_3(x), C_4(x)\right)=z \quad (1)$$

$$C(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, якщо\ y_1=0; y_2=0;\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, якщо\ y_1=0; y_2=1;\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ y_1=1; y_2=0;\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ y_1=1; y_2=1.\end{cases}=z, \quad (2)$$

де $C(x,y)$ – це 2-операндна СЕТ-операція; y_1 і y_2 – перший і другий Сі-кванти другого операнда (інформація керування); z – результат криптографічного перетворення (2 Сі-кванти).

На основі моделі (2) отримаємо удосконалену дискретну модель СЕТ-операції:

$$C(x,y)=\begin{bmatrix}x_1\cdot\bar{y}_1\oplus x_2\cdot\left(y_1\vee\bar{y}_2\right)\oplus y_2\\ x_1\cdot(y_1\vee y_2)\oplus x_2\cdot\bar{y}_1\oplus\bar{y}_2\end{bmatrix}=z. \quad (3)$$

При побудові несиметричних систем потокового СЕТ-шифрування необхідно для кожної прямої СЕТ-операції знайти її обернену.

Для несиметричної 2-операндної СЕТ-операції, що задана моделлю (1), модель оберненої операції можна представити [6]:

$$C^{/}(z,y)=C\left(C_1^{/}(z),C_2^{/}(z),C_3^{/}(z),C_4^{/}(z)\right)=x. \quad (4)$$

Побудуємо дискретну модель оберненої удосконаленої СЕТ-операції. Для цього використаємо моделі обернених одноопераднних 2Сі-квантових СЕТ-операцій наведених в [18].

Оскільки

$$C_1^{/}(z)=\begin{bmatrix}z_1\oplus z_2\oplus 1\\ z_2\oplus 1\end{bmatrix}=x;\ C_2^{/}(z)=\begin{bmatrix}z_1\oplus 1\\ z_1\oplus z_2\oplus 1\end{bmatrix}=x;$$

$$C_3^{/}(z)=\begin{bmatrix}z_2\oplus 1\\ z_1\end{bmatrix}=x;\ C_4^{/}(z)=\begin{bmatrix}z_2\\ z_1\oplus 1\end{bmatrix}=x,$$

тоді:

$$C^{/}(z,y)=\begin{cases}\begin{bmatrix}z_1\oplus z_2\oplus 1\\ z_2\oplus 1\end{bmatrix}, якщо\ y_1=0; y_2=0;\\ \begin{bmatrix}z_1\oplus 1\\ z_1\oplus z_2\oplus 1\end{bmatrix}, якщо\ y_1=0; y_2=1;\\ \begin{bmatrix}z_2\oplus 1\\ z_1\end{bmatrix}, якщо\ y_1=1; y_2=0;\\ \begin{bmatrix}z_2\\ z_1\oplus 1\end{bmatrix}, якщо\ y_1=1; y_2=1.\end{cases}=x. \quad (5)$$

На основі моделі (5) отримаємо:

$$C^{/}(z,y)=\begin{bmatrix}z_1\cdot\bar{y}_1\oplus z_2\cdot\left(y_1\vee\bar{y}_2\right)\oplus\left(\bar{y}_1\vee\bar{y}_2\right)\\ z_1\cdot(y_1\vee y_2)\oplus z_2\cdot\bar{y}_1\oplus\left(\bar{y}_1\vee y_2\right)\end{bmatrix}=x. \quad (6)$$

Модифікація СЕТ-операції з точністю до перестановки першого операнда реалізується шляхом криптографічного перетворення одноопераднною СЕТ-операцією вхідних даних, які надходять в перший операнд.

Модифікуємо моделі прямої СЕТ-операції (3) з точністю до перестановки першого операнда одноопераднною операцією $C_4(x)$.

$$C_4(x,y)=C\left(C_4(x),y\right)=z_4, \quad (7)$$

де $C_4(x,y)$ – несиметрична 2-операндна СЕТ-операція модифікована з точністю до перестановки першого операнда одноопераднною операцією $C_4(x)$; z_4 – результат криптографічного перетворення даною модифікованою СЕТ-операцією.

Модифіковані одноопераднною СЕТ-операцією вхідні дані в процесі реалізації 2-операндної СЕТ-операції будуть перетворюватися однією із її одноопераднних операцій.

Відповідно до моделі (7), кортежну модель СЕТ-операції (1) можна представити:

$$C_4(x,y)=C\left(C_1(C_4(x)),C_2(C_4(x)),C_3(C_4(x)),C_4(C_4(x))\right)=z_4. \quad (8)$$

Модель модифікованої 2-операндної СЕТ-операції з точністю до перестановки першого операнда (7) на основі попереднього додаткового перетворення одноопераднною СЕТ-операцією $C_4(x)$ можна представити:

$$C_4(x,y)=\begin{cases}C_1\left(C_4(x)\right), якщо\ y_1=0; y_2=0\\ C_2\left(C_4(x)\right), якщо\ y_1=0; y_2=1\\ C_3\left(C_4(x)\right), якщо\ y_1=1; y_2=0\\ C_4\left(C_4(x)\right), якщо\ y_1=1; y_2=1\end{cases}=z_4. \quad (9)$$

Модифікуємо одноопераднні операції $C_1(x)$ – $C_4(x)$ шляхом попереднього додаткового перетворення СЕТ-операцією $C_4(x)$ вхідних Сі-квантів інформації. Для цього в СЕТ-операції $C_1(x)$ – $C_4(x)$ замість першого і другого Сі-квантів першого операнда x_1 і x_2, підставимо першу і другу елементарні функції СЕТ-операції $C_4(x)$: $f_1(x)=x_2\oplus 1$, $f_2(x)=x_1$ відповідно:

$$C_1(C_4(x))=\begin{bmatrix}(x_2\oplus 1)\oplus(x_1)\\ (x_1)\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=C_5(x)=z_4. \quad (10)$$

$$C_2\left(C_4(x)\right)=\begin{bmatrix}(x_2\oplus 1)\oplus 1\\(x_2\oplus 1)\oplus(x_1)\end{bmatrix}=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}=C_6(x)=z_4. \quad (11)$$

$$C_3\left(C_4(x)\right)=\begin{bmatrix}(x_1)\\(x_2\oplus 1)\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}=C_7(x)=z_4. \quad (12)$$

$$C_4\left(C_4(x)\right)=\begin{bmatrix}(x_1)\oplus 1\\(x_2\oplus 1)\end{bmatrix}=\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}=C_8(x)=z_4. \quad (13)$$

Підставивши результати модифікації одноопе-рандних СЕТ-операцій (10) – (11) в модель модифікованої 2-операндної СЕТ-операції (9) отримаємо:

$$C_4(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, якщо\ y_1=0; y_2=0;\\ \begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}, якщо\ y_1=0; y_2=1;\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, якщо\ y_1=1; y_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, якщо\ y_1=1; y_2=1.\end{cases}=z_4. \quad (14)$$

На основі моделі (14) отримаємо удосконалену модифіковану дискретну модель СЕТ-операції:

$$C_4(x,y)=\begin{bmatrix}x_1\cdot\left(y_1\vee\bar{y}_2\right)\oplus x_2\cdot\bar{y}_1)\oplus(y_1\oplus y_2\oplus 1)\\ x_1\cdot\bar{y}_1\oplus x_2\cdot(y_1\vee y_2)\oplus\left(\bar{y}_1\vee y_2\right)\end{bmatrix}=z_4. \quad (15)$$

Побудуємо обернену 2-операндну СЕТ-операцію до модифікованої несиметричної 2-операндної СЕТ-операції заданої моделлю (8).

Представимо модель як удосконалену модифіковану дискретну модель СЕТ-операції (15) її кортежною моделлю. Підставивши в (14) позначення прямих одноопе-рандних СЕТ-операцій, отримаємо:

$$C_4(x,y)=\begin{cases}C_5(x), якщо\ y_1=0; y_2=0;\\ C_6(x), якщо\ y_1=0; y_2=1;\\ C_7(x), якщо\ y_1=1; y_2=0;\\ C_8(x), якщо\ y_1=1; y_2=1.\end{cases}=z_4. \quad (16)$$

Відповідно до (16) кортежну модель прямої модифікованої 2-операндної СЕТ-операції можна представити:

$$C_4(x,y)=C\left(C_5(x),C_6(x),C_7(x),C_8(x)\right)=z_4. \quad (17)$$

Відповідно до (17) кортежну модель оберненої модифікованої 2-операндної СЕТ-операції можна представити:

$$C_4^{/}(z_4,y)=C\left(C_5^{/}(z_4),C_6^{/}(z_4),C_7^{/}(z_4),C_8^{/}(z_4)\right)=x. \quad (18)$$

Побудуємо дискретну модель оберненої удосконаленої модифікованої СЕТ-операції. Відповідно до [18] моделі обернених одноопе-рандних СЕТ-операцій до одноопе-рандних СЕТ-операцій $C_5(x)-C_8(x)$ можна представити.

$$C_5^{/}(z_4)=\begin{bmatrix}z_{4.2}\oplus 1\\z_{4.1}\oplus z_{4.2}\end{bmatrix}=x; \quad (19)$$

$$C_6^{/}(z_4)=\begin{bmatrix}z_{4.1}\oplus z_{4.2}\oplus 1\\z_{4.1}\end{bmatrix}=x; \quad (20)$$

$$C_7^{/}(z_4)=\begin{bmatrix}z_{4.1}\\z_{4.2}\end{bmatrix}=x; \quad (21)$$

$$C_8^{/}(z_4)=\begin{bmatrix}z_{4.1}\oplus 1\\z_{4.2}\oplus 1\end{bmatrix}=x, \quad (22)$$

де $z_{4.1}$, $z_{4.2}$ – перший і другий Сі-кванти результату криптографічного перетворення інформації модифікованою 2-операндною СЕТ-операцією (15).

Підставивши моделі (21) – (22) в кортежну модель оберненої СЕТ-операції (18) отримаємо:

$$C_4^{/}(z_4,y)=\begin{cases}\begin{bmatrix}z_{4.2}\oplus 1\\z_{4.1}\oplus z_{4.2}\end{bmatrix}, якщо\ y_1=0; y_2=0;\\ \begin{bmatrix}z_{4.1}\oplus z_{4.2}\oplus 1\\z_{4.1}\end{bmatrix}, якщо\ y_1=0; y_2=1;\\ \begin{bmatrix}z_{4.1}\\z_{4.2}\end{bmatrix}, якщо\ y_1=1; y_2=0;\\ \begin{bmatrix}z_{4.1}\oplus 1\\z_{4.2}\oplus 1\end{bmatrix}, якщо\ y_1=1; y_2=1.\end{cases}=x. \quad (23)$$

На основі моделі (23) отримаємо:

$$C_4^{/}(z_4,y)=\begin{bmatrix}z_{4.1}\cdot(y_1\vee y_2)\oplus z_{4.2}\cdot\bar{y}_1\oplus\left(\bar{y}_1\vee y_2\right)\\ z_{4.1}\cdot\bar{y}_1\oplus z_{4.2}\cdot\left(y_1\vee\bar{y}_2\right)\oplus(y_1\cdot y_2)\end{bmatrix}=x. \quad (24)$$

Побудована модель оберненої 2-розрядної СЕТ-операції (24) дозволяє розшифровувати інформацію зашифровану прямою СЕТ-операцією (15). Проте $C_4(x,y)=z_4$ лише одна із операцій, яка належить групі операцій з точністю до перестановки першого операнда. Групу 2-операндних СЕТ-операцій з точністю до перестановки першого операнда можна представити як

$$C_i(x,y)=C\left(C_i(x),y\right)=z_i, \quad (25)$$

де i – індекс (номер) одноопе-рандної СЕТ-операції, на основі якої була реалізована модифікація 2-операндної СЕТ-операції.

Побудова моделі (24) представляє собою побудову лише однієї оберненої СЕТ-операції з групи

операцій (25). Тому на практиці використовувати даний підхід для реалізації оберненого перетворення складно і нераціонально.

Будь-яку операцію з групи операцій (25) можна представити як функцію від 2-операндної і 1-операндної СЕТ-операції:

$$C_i(x, y) = f\left(C(x, y), C_i(x)\right). \quad (26)$$

Обернену операцію для будь-якої 2-операндної СЕТ-операції з групи СЕТ-операцій (26) можна представити як

$$C_i^{/}(x, y) = f\left(C^{/}(x, y), C_i^{/}(x)\right). \quad (27)$$

На основі функції (27) можна представити три варіанти синтезу оберненої СЕТ-операції:

- з точністю до перестановки результату перетворення

$$C_i^{/}(x, y) = C_i^{/}\left(C^{/}(x, y)\right); \quad (28)$$

- з точністю до перестановки першого операнда

$$C_i^{/}(x, y) = C^{/}\left(C_i^{/}(x), y\right); \quad (29)$$

- з точністю до перестановки другого операнда

$$C_i^{/}(x, y) = C^{/}\left(x, C_i^{/}(y)\right). \quad (30)$$

Розглянемо можливість побудови оберненого СЕТ-операції (24) на основі моделі (28). Для цього підставимо в модель оберненої одноопераднодної СЕТ-операції $C_4^{/}(z)$ обернену 2-операндну операцію (6):

$$C_4^{/}(z_4, y) = C_4^{/}\left(C^{/}(z_4, y)\right) = \\ = C\left(C_4^{/}\left(C_1^{/}(z_4)\right), C_4^{/}\left(C_2^{/}(z_4)\right), C_4^{/}\left(C_3^{/}(z_4)\right), C_4^{/}\left(C_4^{/}(z_4)\right)\right). \quad (31)$$

На основі кортежної моделі оберненої СЕТ-операції (31) отримаємо:

$$C_4^{/}(z_4, y) = \begin{cases} C_4^{/}\left(C_1^{/}(z_4)\right), \textit{якщо } y_1 = 0; y_2 = 0; \\ C_4^{/}\left(C_2^{/}(z_4)\right), \textit{якщо } y_1 = 0; y_2 = 1 \\ C_4^{/}\left(C_3^{/}(z_4)\right), \textit{якщо } y_1 = 1; y_2 = 0 \\ C_4^{/}\left(C_4^{/}(z_4)\right), \textit{якщо } y_1 = 1; y_2 = 1 \end{cases} = x. \quad (32)$$

Визначимо одноопераднодні обернені СЕТ-операції, з яких побудовано кортеж оберненої 2-операндної СЕТ-операції (31):

$$C_4^{/}\left(C_1^{/}(z_4)\right) = \begin{bmatrix} (z_{4.2} \oplus 1) \\ (z_{4.1} \oplus z_{4.2} \oplus 1) \oplus 1 \end{bmatrix} = \begin{bmatrix} z_{4.2} \oplus 1 \\ z_{4.1} \oplus z_{4.2} \end{bmatrix} = x; \quad (33)$$

$$C_4^{/}\left(C_2^{/}(z_4)\right) = \begin{bmatrix} (z_{4.1} \oplus z_{4.2} \oplus 1) \\ (z_{4.1} \oplus 1) \oplus 1 \end{bmatrix} = \begin{bmatrix} z_{4.1} \oplus z_{4.2} \oplus 1 \\ z_{4.1} \end{bmatrix} = x; \quad (34)$$

$$C_4^{/}\left(C_3^{/}(z_4)\right) = \begin{bmatrix} (z_{4.1}) \\ (z_{4.2} \oplus 1) \oplus 1 \end{bmatrix} = \begin{bmatrix} z_{4.1} \\ z_{4.2} \end{bmatrix} = x; \quad (35)$$

$$C_4^{/}\left(C_4^{/}(z_4)\right) = \begin{bmatrix} (z_{4.1} \oplus 1) \\ (z_{4.2}) \oplus 1 \end{bmatrix} = \begin{bmatrix} z_{4.1} \oplus 1 \\ z_{4.2} \oplus 1 \end{bmatrix} = x. \quad (36)$$

Підставивши в модель оберненої 2-операндної СЕТ-операції (32) моделі обернених одноопераднодних СЕТ-операцій (33) – (36), отримаємо:

$$C_4^{/}(z_4, y) = \begin{cases} \begin{bmatrix} z_{4.2} \oplus 1 \\ z_{4.1} \oplus z_{4.2} \end{bmatrix}, \textit{якщо } y_1 = 0; y_2 = 0; \\ \begin{bmatrix} z_{4.1} \oplus z_{4.2} \oplus 1 \\ z_{4.1} \end{bmatrix}, \textit{якщо } y_1 = 0; y_2 = 1; \\ \begin{bmatrix} z_{4.1} \\ z_{4.2} \end{bmatrix}, \textit{якщо } y_1 = 1; y_2 = 0; \\ \begin{bmatrix} z_{4.1} \oplus 1 \\ z_{4.2} \oplus 1 \end{bmatrix}, \textit{якщо } y_1 = 1; y_2 = 1. \end{cases} = x. \quad (37)$$

Оскільки побудована модель оберненої 2-операндної СЕТ-операції (37) співпала з моделлю оберненої 2-операндної СЕТ-операції (23), то удосконалена модель оберненої 2-операндної СЕТ-операції буде описуватися моделлю (24).

Результат моделювання дозволяє встановити взаємозв'язки між модифікованими прямими і оберненими несиметричними 2-операндними СЕТ-операціями.

Нехай модифікація прямої несиметричної 2-операндної СЕТ-операції була реалізована з точністю до перестановки першого операнда одноопераднодною СЕТ-операцією на основі моделі (25). Отримати обернену до неї 2-операндну СЕТ-операцію можна шляхом модифікації оберненої 2-операндної СЕТ-операції з точністю до перестановки результату перетворення оберненою одноопераднодною СЕТ-операцією на основі моделі:

$$C_i^{/}(z_i, y) = C_i^{/}\left(C^{/}(z_i, y)\right) = x. \quad (38)$$

Дана модель забезпечить обернене перетворення інформації.

Коректність наведених результатів моделювання підтверджена результатами обчислювального експерименту.

Обговорення результатів моделювання груп несиметричних СЕТ-операцій з точністю до перестановки першого операнда. У процесі модифікації несиметричної 2-операндної СЕТ-операції з точністю до перестановки першого операнда змінюється математична модель СЕТ-операції. Про це свідчать побудовані моделі СЕТ-операції до її модифікації (3) і після модифікації (15). Необхідно відмітити, що в результаті модифікації СЕТ-операції буде змінюватися як сама модель операції, так і результат її реалізації.

Модифікації СЕТ-операцій з точністю до перестановки другого операнда [16, 18] забезпечує зміну результату криптографічного перетворення за рахунок зміни послідовності одноопенандних СЕТ-операцій в кортежі 2-операндної операції. Модифікація СЕТ-операцій з точністю до перестановки першого операнда приводить до модифікації не послідовності одноопперандних операцій в кортежі, а модифікації самих одноопперандних СЕТ-операцій. Про це свідчать кортежні моделі операції до її модифікації (1) і після модифікації (17).

Збільшення кількості одноопперандних СЕТ-операцій при використанні групи модифікованих несиметричних СЕТ-операцій з точністю до перестановки першого операнду забезпечує збільшення кількості таблиць підстановки, які реалізуються в процесі шифрування. Збільшення кількості таблиць підстановки, які реалізуються, забезпечує збільшення криптостійкості алгоритму шифрування.

Якщо при шифруванні було використано модифікацію СЕТ-операції з точністю до перестановки першого операнда відповідно до моделі (25), то при розшифруванні необхідно використовували модифікацію оберненої СЕТ-операції з точністю до перестановки результату перетворення відповідно до моделі (38).

На основі моделей модифікації СЕТ-операцій реалізуються генератори псевдовипадкових послідовностей прямих і обернених модифікованих 2-операндних СЕТ-операцій.

Коректність наведених теоретичних результатів підтверджена результатами обчислювального експерименту.

Подальші дослідження будуть направлені на дослідження особливостей побудови високопродуктивних малоресурсних криптографічних систем на основі груп несиметричних СЕТ-операцій синтезованих з точністю до перестановки першого операнда.

Висновки:

1. Групи несиметричних 2-операндних СЕТ-операцій можуть бути синтезовані з точністю до перестановки першого операнда. Модифікацію несиметричної 2-операндної СЕТ-операції доцільно реалізувати криптографічним перетворенням першого операнду одноопперандною СЕТ-операцією.

2. Для групи несиметричних 2-операндних СЕТ-операцій з точністю до перестановки першого операнда група обернених СЕТ-операцій будується з точністю до перестановки результатів перетворення. Модифікацію оберненої несиметричної 2-операндної СЕТ-операції необхідно реалізувати криптографічним перетворенням попереднього результату розшифрування оберненою одноопперандною СЕТ-операцією.

3. Модифікація несиметричної 2-операндної СЕТ-операції з точністю до перестановки першого операнда реалізується шляхом модифікації одноопперандних СЕТ-операцій, з яких вона побудована.

4. Модифікація одноопперандних СЕТ-операцій в процесі шифрування забезпечує збільшення кількості таблиць підстановок, які реалізує потоковий шифр, що ускладнює криптоаналіз і приводить до підвищення криптостійкості.

Список літератури:

1. Kumar C., Prajapati S., Verma R. A Survey of Various Lightweight Cryptography Block ciphers for IoT devices. *CCET 2022: IEEE International Conference on Current Development in Engineering and Technology*. (Bhopal, 23–24 December 2022). Bhopal India, 2022. P. 1–6. DOI: 10.1109/CCET56606.2022.10080556.

2. Khaled Salah Mohamed. New Frontiers in Cryptography. *Quantum, Blockchain, Lightweight, Chaotic and DNA.* Springer Cham, 2020. 104 p. DOI: 10.1007/978-3-030-58996-7.

3. Khudoykulov Z. A Comparison of Lightweight Cryptographic Algorithms. *Lecture Notes in Networks and Systems*. 2024. Vol. 912. P. 295–304. DOI: 10.1007/978-3-031-53488-1_36.

4. Lohachab A., Lohachab A., Jangra A. A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. *Internet of Things*. 2020. Vol. 9. P. 100174. DOI: 10.1016/j.iot.2020.100174.

5. Haythem P., Zorkta Y., Allawi D., Al-Nakkar M. Improved lightweight encryption algorithm (ILEA). *INCET 2020: International Conference for Emerging Technology.* (Belgaum, 05–07 June 2020). Belgaum, India, 2020. P. 1–4. DOI: 10.1109/INCET49848.2020.9154170.

6. Рудницький В. М., Лада Н. В., Кучук Г. А., Підласий Д. А. Архітектура СЕТ-операцій і технології потокового шифрування. Architecture of CET-operations and stream encryption technologies: монографія. Черкаси: видавець Пономаренко Р.В. 2024. 374 с. ISBN 978-966-2554-81-6

7. Massey J. L. An introduction to contemporary cryptology. *Proceedings of the IEEE*, 1988. Vol. 76, № 5. P. 533–549. DOI: 10.1109/5.4440.

8. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. *Системи обробки інформації.* 2014. Вип. 2 (118). С. 116–118. URL: http://nbuv.gov.ua/UJRN/soi_2014_2_26.

9. Бабенко В. Г., Лада Н. В. Аналіз результатів виконання модифікованих операцій додавання за модулем два з точністю до перестановки. *The scientific potential of the present:* proceedings of the Internat. sci. conf., (St. Andrews, Scotland, UK, December, 1, 2016). Vinnytsia: PE Rogalska I. O., 2016. С. 108–111.

10. Лада Н. В., Козловська С. Г., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій додавання за модулем чотири. *Центральноукраїнський науковий вісник.* 2019. Вип. 2 (33). С. 181–189. DOI: 10.32515/2664-262X.2019.2(33).181-189.

11. Лада Н. В., Рудницький С. В., Зажома В. М., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій правостороннього додавання за модулем чотири. *Системи управління, навігації та зв'язку.* 2020. № 1(59). С. 93–96. DOI: 10.26906/SUNZ.2020.1.093.

12. Rudnytskyi V., Babenko V., Lada N., Tarasenko Ya., Rudnytska Yu. Constructing Symmetric Operations of Cryptographic Information Encoding. *CEUR Workshop Proceedings*. 2021. Vol. 3187. P. 182–194. DOI: 10.5281/zenodo.10953357.

13. Breus R. Synthesising the two-bit two-operand operations of strict stable cryptographic coding by the second operand's conversion. *Control, Navigation and Communication Systems.* 2019. Vol. 5 (57). P. 29–32. DOI: 10.26906/SUNZ.2019.5.029.

14. Лада Н. В., Бреус Р. В., Лада С. В. Генерація моделей прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. *Science and Education a New Dimension Natural and Technical Science.* 2020. VIII (29), № 238. P. 27–29. DOI: 10.31174/SEND-NT2020-238VIII29-05.

15. Лада Н. В., Головняк Д. В., Сапожніков С. К. Механізми практичної реалізації несиметричних двохоперандних СЕТ-операцій. *Проблеми інформатизації:* тези доповідей одинадцятої міжнародної науково-технічної конференції (Черкаси, 16–17 листопада 2023 року). Черкаси: ЧДТУ, 2023. Т. 2. С. 34.

16. Бабенко В., Мельник О. Мельник Р. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації. *Безпека інформації.* 2013. Т. 19. № 1. С. 56–59. DOI: 10.18372/2225-5036.19.4705.

17. Бабенко В. Г., Мельник Р. П., Рудницький С. В. Дослідження способів запису трьохрозрядних криптографічних операцій. *Системи управління, навігації та зв'язку.* 2012. Т. 2, № 1 (21). С. 170–173.

18. Rudnytskyi V., Lada N., Babenko V., Kuchuk H., Pidlasyi D., Kamak D., Ivashchenko Ye. Modeling of groups of dual-cycle non-commutative two-operand CET-operations. *Journal of Xidian University.* 2024. Vol. 18, № 10. P. 916–958. DOI: 10.37896/jxu18.10/069.

19. Rudnytsky V.M., Lada N.V., Fedotova-Piven I.M., Pustovit M.O., Nesterenko O.B. Construction of two-digit two operand operations of strict stable cryptographic coding. *Control, navigation and communication systems.* 2018. Vol. 6. № 52. P. 113–115. DOI: 10.26906/SUNZ.2018.6.113

20. Tazetdinov V., Sysoienko S., Tazetdinov O., Al-Azzeh J., Mesleh A. Neural network system for selection of table tennis equipment with elements of crypto protection. *Lecture Notes on Data Engineering and Communications Technologies.* 2024. Vol. 221. P. 126–140. DOI: 10.1007/978-3-031-71801-4_10.

Rudnytskyi V.M., Babenko V.H., Rudnytskyi S.V., Korotkyi T.K., Kovtiukh V.A. PARTICULAR FEATURES OF GROUPS OF ASYMMETRIC SET OPERATIONS SYNTHESIZED WITH AN ACCURACY OF FIRST OPERAND PERMUTATION

The article is devoted to a study that solves the problem of investigating the possibility of using the method of generating groups of asymmetric 2-operand CET operations with an accuracy of permutation of the first operand to build low-resource asymmetric stream encryption systems with increased cryptographic strength. The object of research: processes of mutual transformation of models of 2-operand CET operations in the process of their modification with an accuracy of permutation. To solve the problem, using the example of an asymmetric 2-operand CET operation, the processes of its modification with an accuracy of up to the permutation of the first operand by a single-operand CET operation are considered. It is advisable to modify the asymmetric 2-operand CET operation by cryptographic transforming the first operand with a randomly selected single-operand CET operation. The results of modeling the processes of reverse information transformation have shown that when modifying a direct asymmetric 2-operand CET operation with an accuracy of permutation of the first operand, the modification of the reverse CET operation should be realized by the reverse single-operand CET operation with an accuracy of permutation of the transformation result. It is established that the modification of an asymmetric 2-operand CET operation with an accuracy of permutation of the first operand is realized by modifying the single-operand CET operations from which it is constructed. According to the results of the analysis, it was found that the modification of single-operand CET operations

in the encryption process increases the number of substitution tables that implement the stream cipher. The increasing number of substitution tables during the successive modification of the CET operations leads to the complication of cryptanalysis and to the increase of cryptographic strength of the cryptographic algorithm. Scope of application: mobile and stationary systems of low-resource cryptographic protection of confidential information.

Key words: *low-resource cryptography, CET encryption, 2-operand CET operations, asymmetric cryptographic transformations, stream encryption.*

Дата надходження статті: 15.07.2025
Дата прийняття статті: 21.07.2025
Опубліковано: 27.10.2025