УДК 004. 056.55:004.312.2 **doi: 10.26906/SUNZ.2020.4.043**

С. В. Лада

Управління ДСНС України у Черкаській області, Черкаси, Україна

ДОСЛІДЖЕННЯ МНОЖИН НЕСИМЕТРИЧНИХ ДВООПЕРАНДНИХ ДВОРОЗРЯДНИХ ОПЕРАЦІЙ З ПОДВІЙНИМ ЦИКЛОМ КРИПТОПЕРЕТВОРЕННЯ

Анотація. Робота присвячена дослідженню множин несиметричних двоопераднних дворозрядних криптоопераций з подвійним циклом криптоперетворення для їх застосування в потокових і блокових шифрах. Серед множини несиметричних двохоперандних двохрозрядних операцій синтезованих за результатами обчислювального експерименту визначено множини операцій, які включають в себе операції прямого і оберненого перетворення. Виходячи з взаємозв'язків між кортежами одноопераднних операцій прямого і оберненого криптоперетворення, дані множини і включені в них операції було названо операціями подвійного циклу перетворення. Запропоновано послідовність перетворень результатів експерименту, представленого парами кортежів одноопераднних операцій кодування і декодування, яка забезпечує побудову математичних моделей операцій, придатних для практичної реалізації.

Ключові слова: криптографічне кодування, криптоперетворення, несиметричні операції криптоперетворення, синтез операцій.

Вступ

Постановка проблеми. Сучасні потреби якісної роботи таких організацій як ДСНС України вимагають забезпечення захисту великих обсягів конфіденційність інформації з максимальною швидкістю та максимальною надійністю. Одним з високоефективних напрямів захисту інформації є криптографічний захист. Як відомо, сучасні криптосистеми використовують потокове та блокове шифрування. Однією з головних переваг потокового шифрування над блоковим є висока швидкість виконання операцій криптоперетворення, що досягається за рахунок застосування симетричних операцій [1]. Проте застосування асиметричних алгоритмів блокового шифрування має в більшості випадків переваги по надійності та криптостійкості, а значить несиметричні операції криптоперетворення також заслуговують необхідності дослідження. Виходячи з цього, актуальними стають завдання «інтеграції» принципів асиметричного блокового шифрування в потокове на основі несиметричних операцій криптоперетворення.

Аналіз останніх досліджень і публікацій.

За останні роки з'явилась значна кількість публікацій присвячених криптографічному кодуванню, одному з напрямів розвитку комп'ютерної криптографії [2-5]. В рамках даного напряму, особливої уваги заслуговують дослідження присвячені розширенню спектра операцій придатних до криптоперетворення, що базуються не на класичному додаванню по модулю, а на різноманітних модифікаціях [6-8], а також на побудові операцій з заданими властивостями [9-11]. Проте, слід зазначити, що майже всі дослідження нових модифікованих операцій, таких як наприклад операції з точністю до перестановки зосереджені на симетричних операціях [12-14]. Дослідженню множин несиметричних операцій увага майже не приділялась.

В роботі [15] для експериментального синтезу двохоперандних операцій криптографічного перетворення інформації була використана множина одноопераднних операцій (табл. 1). В роботі [16] на основі обчислювального експерименту з синтезу двохоперандних дворозрядних криптоопераций на основі одноопераднних були знайдені пари операцій прямого та коректного оберненого криптоперетворення інформації на основі повного перебору. З цих пар було виділено 20 множин несиметричних двоопераднних двохрозрядних операцій. Проведений в роботі [16] поділ на множини базувався на виокремленні двохоперандних операцій, таблиці істинності яких співпадають з точністю до перестановки.

Метою роботи є дослідження множин несиметричних двоопераднних дворозрядних криптоопераций з подвійним циклом криптоперетворення для застосування в потокових і блокових шифрах.

Основний матеріал

Виходячи з того, що одним із шляхів вирішення проблеми підвищення якості криптосистем є збільшення варіативності операцій придатних для криптоперетворення, можемо висунути гіпотезу, що якість потокового шифрування може бути підвищена за рахунок застосування в ньому несиметричних операцій криптоперетворення. Проведемо аналіз отриманих множин. При проведенні дослідження виявилося, що множини несиметричних двоопераднних операцій можна поділити на 2 групи. До першої групи відносяться 6 множин, які умовно можна назвати множинами несиметричних двоопераднних операцій подвійного циклу криптоперетворення, тобто дана множина містить всі операції як для кодування так і для декодування (табл. 2). До другої групи належать 14 множин потрійного циклу крипто перетворення.

Аналіз даних множин (табл. 1) показав, що за алгоритмом проведення оберненого крипто перетворення можна утворити три математичні групи несиметричних двохоперандних двохрозрядних операцій. Отже були встановлені нові раніше невідомі взаємозв'язки між одноопераднними та двохоперандними операціями, що забезпечило синтез нових математичних груп несиметричних двохоперандних операцій криптоперетворення.

Таблиця 1 – **Одноопернадні двохрозрядні операції криптографічного перетворення інформації**

$F_1 = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_7 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{13} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{19} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
$F_2 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$	$F_8 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{14} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{20} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
$F_3 = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}$	$F_9 = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$	$F_{15} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$	$F_{21} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$
$F_4 = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{10} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{16} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{22} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
$F_5 = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$	$F_{11} = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$	$F_{17} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$	$F_{23} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$
$F_6 = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$	$F_{12} = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{18} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{24} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$

Таблиця 2 – **Множини несиметричних двоопернадних двохрозрядних операцій «подвійного циклу криптоперетворення»**

Множина 1		Множина 2	
$O_{1,20,13,8} \leftrightarrow O_{2,7,14,19}$	$O_{18,21,12,3} \leftrightarrow O_{15,6,9,24}$	$O_{1,7,21,15} \leftrightarrow O_{3,9,13,19}$	$O_{20,2,17,11} \leftrightarrow O_{23,5,8,14}$
$O_{8,1,20,13} \leftrightarrow O_{7,14,19,2}$	$O_{21,12,3,18} \leftrightarrow O_{24,15,6,9}$	$O_{7,1,15,21} \leftrightarrow O_{9,3,19,13}$	$O_{17,11,2,20} \leftrightarrow O_{14,8,23,5}$
$O_{13,8,1,20} \leftrightarrow O_{14,19,2,7}$	$O_{4,23,10,17} \leftrightarrow O_{5,16,11,22}$	$O_{15,21,1,7} \leftrightarrow O_{13,19,9,3}$	$O_{4,16,24,12} \leftrightarrow O_{6,18,10,22}$
$O_{20,13,8,1} \leftrightarrow O_{19,2,7,14}$	$O_{10,17,4,23} \leftrightarrow O_{11,22,5,16}$	$O_{21,15,7,1} \leftrightarrow O_{19,13,3,9}$	$O_{12,24,4,16} \leftrightarrow O_{10,22,18,6}$
$O_{3,18,21,12} \leftrightarrow O_{6,9,24,15}$	$O_{17,4,23,10} \leftrightarrow O_{16,11,22,5}$	$O_{11,17,20,2} \leftrightarrow O_{8,14,5,23}$	$O_{16,4,12,24} \leftrightarrow O_{18,6,22,10}$
$O_{12,3,18,21} \leftrightarrow O_{9,24,15,6}$	$O_{23,10,17,4} \leftrightarrow O_{22,5,16,11}$	$O_{2,20,11,17} \leftrightarrow O_{5,23,14,8}$	$O_{24,12,16,4} \leftrightarrow O_{22,10,6,18}$
Множина 3		Множина 4	
$O_{1,16,10,19} \leftrightarrow O_{4,7,13,22}$	$O_{18,8,2,24} \leftrightarrow O_{14,6,12,20}$	$O_{1,7,19,13} \leftrightarrow O_{3,9,15,21}$	$O_{18,6,24,12} \leftrightarrow O_{16,4,10,22}$
$O_{10,1,19,16} \leftrightarrow O_{7,22,4,13}$	$O_{24,2,8,18} \leftrightarrow O_{20,12,6,14}$	$O_{7,1,13,19} \leftrightarrow O_{9,3,21,15}$	$O_{24,12,18,6} \leftrightarrow O_{22,10,4,16}$
$O_{16,19,1,10} \leftrightarrow O_{13,4,22,7}$	$O_{3,23,11,15} \leftrightarrow O_{5,9,21,17}$	$O_{13,19,7,1} \leftrightarrow O_{15,21,3,9}$	$O_{5,23,17,11} \leftrightarrow O_{2,20,8,14}$
$O_{19,10,16,1} \leftrightarrow O_{22,13,7,4}$	$O_{11,3,15,23} \leftrightarrow O_{9,17,5,21}$	$O_{19,13,1,7} \leftrightarrow O_{21,15,9,3}$	$O_{11,17,23,5} \leftrightarrow O_{8,14,2,20}$
$O_{2,18,24,8} \leftrightarrow O_{6,20,14,12}$	$O_{15,11,23,3} \leftrightarrow O_{17,21,9,5}$	$O_{6,18,12,24} \leftrightarrow O_{4,16,22,10}$	$O_{17,11,5,23} \leftrightarrow O_{14,8,20,2}$
$O_{8,24,18,2} \leftrightarrow O_{12,14,20,6}$	$O_{23,15,3,11} \leftrightarrow O_{21,5,17,9}$	$O_{12,24,6,18} \leftrightarrow O_{10,22,16,4}$	$O_{23,5,11,17} \leftrightarrow O_{20,2,14,8}$
Множина 5		Множина 6	
$O_{1,13,7,19} \leftrightarrow O_{4,10,16,22}$	$O_{14,2,8,20} \leftrightarrow O_{18,12,6,24}$	$O_{1,19,13,7} \leftrightarrow O_{2,8,14,20}$	$O_{18,24,12,6} \leftrightarrow O_{15,3,9,21}$
$O_{7,19,1,13} \leftrightarrow O_{10,4,22,16}$	$O_{20,8,2,14} \leftrightarrow O_{24,6,12,18}$	$O_{7,13,19,1} \leftrightarrow O_{8,2,20,14}$	$O_{24,18,6,12} \leftrightarrow O_{21,9,3,15}$
$O_{13,1,19,7} \leftrightarrow O_{16,22,4,10}$	$O_{3,21,9,15} \leftrightarrow O_{5,11,23,17}$	$O_{13,7,1,19} \leftrightarrow O_{14,20,2,8}$	$O_{5,17,11,23} \leftrightarrow O_{4,22,10,16}$
$O_{19,7,13,1} \leftrightarrow O_{22,16,10,4}$	$O_{9,15,3,21} \leftrightarrow O_{11,5,17,23}$	$O_{19,1,7,13} \leftrightarrow O_{20,14,8,2}$	$O_{11,23,5,17} \leftrightarrow O_{10,16,4,22}$
$O_{8,20,14,2} \leftrightarrow O_{12,18,24,6}$	$O_{15,9,21,3} \leftrightarrow O_{17,23,11,5}$	$O_{6,12,24,18} \leftrightarrow O_{3,15,21,9}$	$O_{17,5,23,11} \leftrightarrow O_{16,10,22,4}$
$O_{2,14,20,8} \leftrightarrow O_{6,24,18,12}$	$O_{21,3,15,9} \leftrightarrow O_{23,17,5,11}$	$O_{12,6,18,24} \leftrightarrow O_{9,21,15,3}$	$O_{23,11,17,5} \leftrightarrow O_{22,4,16,10}$

Дослідимо для прикладу деякі операції четвертої множини несиметричних двоопернадних дворозрядних операцій подвійного циклу криптоперетворення».

Нехай буду вибрана операція $O_{1,7,19,13}$, тоді оберненою операцією буде операція $O_{3,9,15,21}$. Для взаємозв'язків прямої і оберненої операції введемо позначення:

$O^k_{1,7,19,13}$ – операція кодування,

$O^d_{3,9,15,21}$ – операція декодування.

Розглянемо більш детально операцію $O^k_{1,7,19,13}$.

Якщо значення першого операнда позначити через x, а другого операнда через k, який одночасно є командою вибору перетворення першого операнда, тоді відповідно до табл. 1 отримаємо:

$$O^k_{1,7,19,13}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix},якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix},\ якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix},якщо\ k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_1\oplus k_2\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_1\oplus k_2\end{bmatrix},якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_1\oplus k_2\end{bmatrix},\ якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_1\oplus k_2\end{bmatrix},якщо\ k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_1\oplus k_2\end{bmatrix};$$

$$\text{декодування}-O^d_{3,9,15,21}=\begin{cases}\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_2\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_2\end{bmatrix},якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_2\end{bmatrix},\ якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_2\end{bmatrix},якщо\ k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_2\end{bmatrix}.$$

За результатами взаємоперетворення отримано: якщо $O^k_{1,7,19,13}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus x_2\oplus k_2\end{bmatrix}$ – кодування, тоді $O^d_{3,9,15,21}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_2\end{bmatrix}$ – декодування. Якщо операція – $O_{3,9,15,21}$, тоді оберненою буде $O_{1,7,19,13}$:

$$O^k_{3,9,15,21}=\begin{cases}\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_2\end{bmatrix},\ якщо k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_2\end{bmatrix},якщо k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_2\end{bmatrix},\ якщо k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_2\end{bmatrix},якщо k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_2\end{bmatrix};$$

$$O^d_{1,7,19,13}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix},якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix},\ якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix},якщо\ k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_1\oplus k_2\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_1\oplus k_2\end{bmatrix},якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_1\oplus k_2\end{bmatrix},\ якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_1\oplus k_2\end{bmatrix},якщо\ k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_1\oplus k_2\end{bmatrix}.$$

Якщо $O^k_{3,9,15,21}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_2\end{bmatrix}$ – операція кодування, тоді $O^d_{1,7,19,13}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus x_2\oplus k_2\end{bmatrix}$ буде операцією декодування.

Розглянуті послідовності взаємоперетворень дозволяють перейти від результатів обчислювального експерименту по пошуку пар несиметричних операцій криптоперетворення подвійного циклу до математичних моделей даних операцій, що забезпечує можливість практичного застосування їх в комп'ютерній криптографії як на апаратному так і програмному рівні.

Висновки

Серед множини несиметричних двохоперандних двохрозрядних операцій синтезованих за результатами обчислювального експерименту визначено множини операцій, які включають в себе операції прямого і оберненого перетворення.

Виходячи з взаємозв'язків між кортежами однооперандних операцій прямого і оберненого криптоперетворення, дані множини і включені в них опе-

рації було названо операціями подвійного циклу перетворення.

Запропоновано послідовність перетворень результатів експерименту, представленого парами кортежів одноопераднних операцій кодування і декодування, яка забезпечує побудову математичних моделей операцій, придатних для практичної реалізації.

СПИСОК ЛІТЕРАТУРИ

1. V. Rudnitsky, R. Berdybaev, R. Breus, N. Lada, M.Pustovit. Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation. Сучасні інформаційні системи. Щоквартальний науково-технічнийй журнал – Х.: НТУ «ХПІ» 2019, Т 3, №4 С. 109-114. doi: http:// doi.org/10.20998/2522-9052.2019.4.16
2. Криптографічне кодування: обробка та захист інформації: колективна монографія / під ред.. В.М. Рудницького. – Харків: ТОВ «ДІСА ПЛЮС», 2018. – 139 с.
3. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія / В.М.Рудницький, Н.В. Лада, В.Г. Бабенко. - Харків: ТОВ «ДІСА ПЛЮС», 2018. – 184 с.
4. Breus R. Синтез двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування шляхом перетворення другого операнда / R. Breus // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2019. – Т. 5 (57). – С. 29-32. – doi:https://doi.org/10.26906/SUNZ.2019.5.029.
5. Рудницький В.М., Лада Н.В., Федотова-Півень І.М., Пустовіт М.О., Нестеренко О.Б. Побудова двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, 2018. Т. 6(52). С. 113–115. doi:http://doi.org/10.26906/SUNZ.2018.6.113
6. Fedotova-Piven I.M. The inversion method of four-bit boolean sac cryptotransforms / I.M. Fedotova-Piven, V.M. Rudnitskiy, O.B. Piven, T.V. Mironyuk // Radio Electronics, Computer Science, Control.- NU «Zaporizhzhia Polytechnic». - 2019. № 4(51). – P. 199-210. doi: http:// doi.org/10.15588/1607-3274-2019-4-19 p-ISSN 2313-688X
7. Faure E.V., Shcherba A.I. and Rudnytskyi V.M. The Method and Criterion for Quality Assessment of Random Number Sequences. Cybernetics and Systems Analysis Volume 52, Issue 2 (March 2016), pp 277-284. doi:http://doi.org/10.1007/s10559-016-9824-3.
8. Лада Н.В., Козловська С. Г., Рудницький С. В. Побудова математичної групи симетричних операцій на основі додавання за модулем два. Сучасна спеціальна техніка: науково-практичний журнал. Київ, 2019. No 4 (59). С. 33-41. - Режим доступу:http://suchasnaspetstehnika.com/journal/ukr/2019_4/6.pdf
9. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. Збірник наукових праць Харківського університету Повітряних Сил. Харків: ХУПС ім. І.Кожедуба, 2012 Вип. 4 (33). С. 198-200.
10. Lada N., Dzyuba V., Breus R., Lada S. Synthesis of sets of non-symmetric two-operand two-bit crypto operations within the permutation accuracy Technology audit and production reserves, 2020, № 2/2 (52), С. 28-31. - DOI: 10.15587/2312-8372.2020.202099
11. Рудницький В. М., Миронюк Т. В., Мельник О. Г., Щербина В. П. Синтез елементарних функцій перестановок, керованих інформацією. Безпека інформації. К.: НАУ, 2014. Т. 20, № 3. С. 242–247. - Режим доступу: http://nbuv.gov.ua/UJRN/bezin_2014_20_3_7
12. Лада Н. В., Козловська С. Г. Застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах (2018). Системи управління, навігації та зв'язку: зб. наук. праць. Полтава: ПНТУ, Т. 1 (47), 127-130. doi:http://doi.org/ 10.26906/SUNZ.2018.1.127
13. Лада Н. В., Козловська С. Г., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій додавання за модулем чотири (2019). Центральноукраїнський науковий вісник. Технічні науки. Збірник наукових праць. Кропивницький: КНТУ. Вип. 2 (33), 181–189. doi:http://doi.org/10.32515/2664-262X.2019.2(33).181-189
14. Rudnitsky V., Berdybaev R., Breus R., Lada N., Pustovit M. Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation (2019). Сучасні інформаційні системи. Щоквартальний науково-технічнийй журнал. Х.: НТУ «ХПІ», Т 3, №4 С. 109-114. doi: http:// doi.org/10.20998/2522-9052.2019.4.16
15. 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. Х.: ХУПС ім. І. Кожедуба. 2011. No 2 (6). С. 112-114 - Режим доступу: http://nbuv.gov.ua/UJRN/Nitps_2011_2_30.
16. Lada N., Dzyuba V., Breus R., Lada S. Synthesis of sets of non-symmetric two-operand two-bit crypto operations within the permutation accuracy. Technology audit and production reserves, 2020, № 2/2 (52), С. 28-31. doi: http://doi.org/10.15587/2312-8372.2020.202099.

Received (Надійшла) 16.08.2020
Accepted for publication (Прийнята до друку) 07.10.2020

Investigation of sets of asymmetric two-operate two-discharge operations with a double cycle of crypto transformation

S. Lada

The work is devoted to the study of sets of asymmetric two - operand two - bit cryptocurrencies with a double cycle of cryptocurrency for their application in stream and block ciphers. Among the set of asymmetric two-operand two-bit operations synthesized by the results of a computational experiment, many operations are defined, which include direct and inverse transformation operations. Based on the relationships between tuples of single-operand direct and reverse cryptocurrency operations, these sets and the operations included in them have been called double-loop conversion operations. The sequence of transformations of results of the experiment presented by pairs of tuples of single-operand operations of coding and decoding which provides construction of the mathematical models of operations suitable for practical realization is offered.

Keywords: cryptographic coding, cryptocurrency conversion, asymmetric cryptocurrency operations, synthesis of operations.