УДК 004.056.55:004.312.2
DOI: 10.15587/2312-8372.2020.202099

СИНТЕЗ МНОЖИН НЕСИМЕТРИЧНИХ ДВООПЕРАНДНИХ ДВОРОЗРЯДНИХ КРИПТООПЕРАЦІЙ З ТОЧНІСТЮ ДО ПЕРЕСТАНОВКИ

Лада Н. В., Дзюба В. А., Бреус Р. В., Лада С. В.

Об'єктом дослідження є процеси побудови операцій для криптографічного захисту інформації, тому що вимоги до інформаційної безпеки постійно зростають. Підвищення стійкості криптографічних перетворень напряму залежать від складності та варіативності криптоалгориму. Підвищити варіативність можливо за рахунок збільшення спектру операцій криптоперетворення. Значно збільшити кількість операцій криптоперетворення можливо за рахунок синтезу несиметричних операцій. Дана робота присвячена створенню методологічного забезпечення синтезу та аналізу множин двоопераднних дворозрядних криптоопераций з точністю до перестановки. Проведені дослідження базуються на результатах обчислювального експерименту, що полягає в синтезі двохопераднних дворозрядних криптоопераций на основі одноопераднних, з подальшим пошуком пар операцій прямого та коректного оберненого криптоперетворення на основі повного перебору. В процесі обчислювального експерименту отримані пари двохоперандних операцій, представлені кортежами з чотирьох одноопераднних операцій. Формалізація отриманих результатів забезпечила математичне представлення операцій, придатне для практичної реалізацій. Для спрощення складності практичної реалізації, синтезовані операції поділені на 24 множини по 24 операції. Поділ операцій відбувався за рахунок застосування шаблонів таблиць істинності множин операцій з точністю до перестановки операндів. Встановлено, що на основі використання шаблону будь-якої операцій може бути побудована вся множина операцій з точністю до перестановки. Крім того, аналіз синтезованих множин показав, що множини симетричних і несиметричних операції не перетинаються. Отримано 20 множин несиметричних двоопераднних двохрозрядних операцій, а також 4 множини симетричних операцій. Подальше дослідження кожної синтезованої множини несиметричних операцій криптоперетворення забезпечить можливість встановлення взаємозв'язків між операндами операції та між операціями в цілому. Застосування синтезованих несиметричних операцій дасть змогу підвищити надійність криптоалгоритмів потокового шифрування інформації за рахунок значного збільшення варіативності крипографічних перетворень. В свою чергу застосування синтезованих множин операцій спростить практичну реалізацію в комп'ютерній криптографії.

Ключові слова: *комп'ютерна криптографія, несиметричні операції криптоперетворення, множини операцій, варіативність криптоалгоритмів.*

1. Вступ

В сучасній науковій літературі за останні роки з'явилися роботи, присвячені дослідженням модифікованих симетричних операцій в криптоалгоритмах потокового шифрування, відмінних від класичного додавання по модулю [1–3]. До таких досліджень відносяться, наприклад, операції додавання по модулю з точністю до перестановки [4]. Однак операції криптоперетворення інформації не обмежуються симетричними. Більшість з них є асиметричними, тобто операція при кодуванні буде відмінною від операції декодування. Цих операції на порядок більше [5, 6].

Слід зазначити, що по аналогії з симетричними операціями, що використовуються в потоковому шифруванні дослідження асиметричних операцій буде більш ефективним в розрізі групування на математичні групи. Виокремлення математичних груп асиметричних операцій потокового шифрування дасть змогу дослідити властивості таких операцій та встановити взаємозв'язки між ними. Також це спростить програмну та апаратну реалізацію криптоалгоритмів з їх застосуванням та покращить якість шифрування за рахунок використання різних

операцій з різних математичних груп [7, 8]. Але не дивлячись на перспективи їх застосування, дослідженню даних операцій в потоковому шифруванню зовсім не приділялося уваги. Таким чином, *об'єктом дослідження* є процеси побудови операцій для криптографічного захисту інформації, тому що вимоги до інформаційної безпеки постійно зростають. *Метою дослідження* є створення методологічного забезпечення синтезу та аналізу множин двоопераднних дворозрядних криптоопераций з точністю до перестановки.

2. Методика проведення досліджень

Проведення дослідження базується на застосуванні підходів, описаних в роботах [9, 10]. Відправною крапкою проведення дослідження є результати обчислювального експерименту по пошуку двоопераднних дворозрядних операцій криптопепретворення.

Симетричні операції криптоперетворення мають наступні властивості [11]:

$$A\hat{o}B=C;\ B\hat{o}A=C;\ A\hat{o}C=B;\ C\hat{o}A=B;\ B\hat{o}C=A;\ C\hat{o}B=A, \qquad (1)$$

де A і B – вхідна інформація; C – результат виконання операції; ô – позначення операції.

На відміну від симетричних операцій, які виконують пряме та обернене перетворення, несиметричні операції існують лише в поєднанні прямої та оберненої операції. При цьому обернена операція може змінюватися при перестановці операндів. Виходячи з цього пари операцій для несиметричного криптоперетворення повинні мати наступні властивості:

$$A\hat{o}B=C;\ B\hat{o}A=C;\ A\tilde{o}C=B;\ C\acute{o}A=B;\ B\tilde{o}C=A;\ C\acute{o}B=A, \qquad (2)$$

де A і B – вхідна інформація; C – результат виконання операції; ô – позначення прямої операції; õ, ó – позначення обернених операцій.

Слід відмітити, що за умови ô=õ=ó несиметрична операція буде співпадати з симетричною.

Для експериментального синтезу двохоперандних операцій використаємо множину одноопераднних операцій криптоперетворення, наведену в табл. 1 [12].

Таблиця 1

Одноопераднні двохрозрядні операції криптографічного перетворення інформації

$_1=\begin{bmatrix} 1 \\ 2 \end{bmatrix}$	$_7=\begin{bmatrix} 1 \\ 2\oplus \end{bmatrix}$	$_{13}=\begin{bmatrix} 1\oplus \\ 2 \end{bmatrix}$	$_{19}=\begin{bmatrix} 1\oplus \\ 2\oplus \end{bmatrix}$
$_2=\begin{bmatrix} 1\oplus & 2 \\ 2 & \end{bmatrix}$	$_8=\begin{bmatrix} 1\oplus & 2 \\ 2\oplus & \end{bmatrix}$	$_{14}=\begin{bmatrix} 1\oplus & 2\oplus \\ 2 & \end{bmatrix}$	$_{20}=\begin{bmatrix} 1\oplus & 2\oplus \\ 2\oplus & \end{bmatrix}$
$_3=\begin{bmatrix} 1 & \\ 1\oplus & 2 \end{bmatrix}$	$_9=\begin{bmatrix} 1 & \\ 1\oplus & 2\oplus \end{bmatrix}$	$_{15}=\begin{bmatrix} 1\oplus & \\ 1\oplus & 2 \end{bmatrix}$	$_{21}=\begin{bmatrix} 1\oplus & \\ 1\oplus & 2\oplus \end{bmatrix}$
$_4=\begin{bmatrix} 2 \\ 1 \end{bmatrix}$	$_{10}=\begin{bmatrix} 2 \\ 1\oplus \end{bmatrix}$	$_{16}=\begin{bmatrix} 2\oplus \\ 1 \end{bmatrix}$	$_{22}=\begin{bmatrix} 2\oplus \\ 1\oplus \end{bmatrix}$
$_5=\begin{bmatrix} 2 & \\ 1\oplus & 2 \end{bmatrix}$	$_{11}=\begin{bmatrix} 2 & \\ 1\oplus & 2\oplus \end{bmatrix}$	$_{17}=\begin{bmatrix} 2\oplus & \\ 1\oplus & 2 \end{bmatrix}$	$_{23}=\begin{bmatrix} 2\oplus & \\ 1\oplus & 2\oplus \end{bmatrix}$
$_6=\begin{bmatrix} 1\oplus & 2 \\ 1 & \end{bmatrix}$	$_{12}=\begin{bmatrix} 1\oplus & 2 \\ 1\oplus & \end{bmatrix}$	$_{18}=\begin{bmatrix} 1\oplus & 2\oplus \\ 1 & \end{bmatrix}$	$_{24}=\begin{bmatrix} 1\oplus & 2\oplus \\ 1\oplus & \end{bmatrix}$

В процесі експерименту використаємо табличне представлення одноопераднних і двохоперандних операцій. Виходячи з цього двохоперандну операцію криптоперетворення можна представити матрицею , де – результати виконання одноопераднної операції [13].

Для того, щоб операція відповідала виразу (2), необхідне виконання наступних умов:

1. У кожному стовпці матриці перетворення не повинно бути повтору команди (значення операнда).

2. У кожному рядку матриці перетворення не повинно бути повтору значення операнда (команди).

3. Матриця повинна бути симетрична відносно головної діагоналі для побудови симетричних операцій (=), і несиметричною – для побудови несиметричних операцій (≠).

В процесі експерименту будемо синтезувати двоопераднні операції шляхом поєднання чотирьох одноопераднних операцій шляхом повного перебору. Для знаходження пар несиметричних операцій був проведений програмний пошук оберненого криптоперетворення для всіх можливих синтезованих двохоперандних двухразрядних операцій. Сутність пошуку полягає в наступному: над множиною вхідних даних виконувалась операція криптоперетворення, яка бралася за пряму. Якщо для прямої операції існує обернена, то результат виконання оберненої операції повинен співпасти з множиною вхідних даних. В якості прямої операції обирались всі синтезовані операції криптоперетваренння. Для кожної прямої операції шукалась обернена перебором всієї множини вхідних операцій. Найдені пари операцій і будуть несиметричними і симетричними операціями криптоперетворення.

В процесі експерименту було отримано 576 операцій, з яких 96 – симетричні операції, а 480 – несиметричні. Симетричні операції досліджувалися в ряді робіт [14–16]. Несиметричні операції отримані та оприлюднюються вперше, та потребують подальшого дослідження.

Для значного зменшення обсягів робіт при дослідженні симетричних операцій їх поділили на 4 групи операцій. Подальше дослідження кожної групи окремо забезпечили можливість встановлення взаємозв’язків між операндами операції та між операціями в цілому.

Розглянемо можливість поділу несиметричних операцій на множини операцій по аналогії з симетричними операціями. Отримані результати забезпечать можливість подальших досліджень, направлених на автоматичний синтез даних операцій та їх практичне застосування в комп’ютерній криптографії.

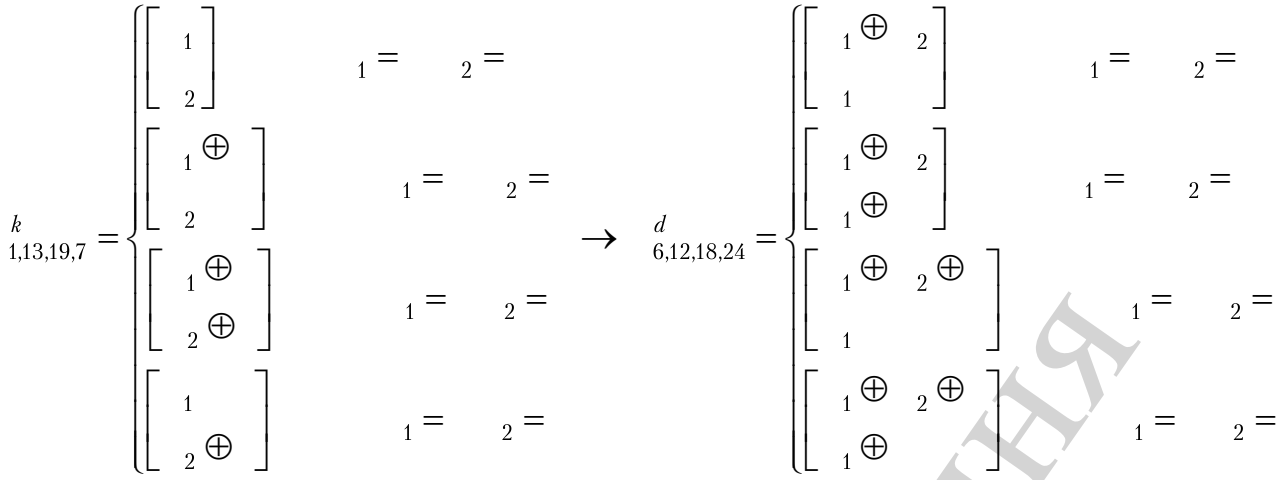
В процесі обчислювального експерименту отримані пари двохоперандних операцій, представлені кортежами одноопераднних операцій.

Наприклад: «1, 13, 19, 7» → «6, 12, 18, 24»

Формалізуємо дані кортежі в операції прямого та оберненого несиметричного криптоперетворення.

Так як $\overset{k}{\rightarrow}$ $\overset{d}{}$, то $\overset{d}{}_{1,13,19,7} \rightarrow \overset{d}{}_{1,13,19,7} = \overset{k}{}_{6,12,18,24}$, або $\overset{d}{}_{1,13,19,7} \rightarrow \overset{d}{}_{6,12,18,24}$, де $\rightarrow$ відображення взаємозв’язку між прямою та оберненою операціями (операціями кодування та декодування). Індексами в двохоперандних операціях позначено кортежі одноопераднних операцій в нумерації табл. 1.

Підставивши одноопераднні операції в позначення двохоперандної, отримаємо:



де $_i$, $_i$ – значення *i*-тих розрядів першого та другого операндів, відповідно.

Для поділу експериментально отриманих операцій на множини запропоновано використати шаблони таблиць істинності операцій з точністю до перестановки. Побудовано 24 шаблони множин операцій з точністю до перестановки операндів, деякі з них наведено в табл. 2.

Таблиця 2

Шаблони таблиць істинності множин операцій з точністю до перестановки операндів

Значення операндів	Шаблон 1				Шаблон 2				…	Шаблон 24			
	0	1	2	3	0	1	2	3	…	0	1	2	3
0	a	b	d	c	a	d	c	b	…	a	d	c	b
1	b	c	a	d	b	a	d	c		b	c	a	d
2	c	d	b	a	c	b	a	d		c	b	d	a
3	d	a	c	b	d	c	b	a		d	a	b	c

Примітка: $a,b,c,d \in \{0,1,2,3\}$, $a \neq b \neq c \neq d$

Шаблони операцій необхідні для побудови множин операцій шляхом перебору таблиць істинності експериментально синтезованих операцій.

3. Результати досліджень та обговорення

За результатами перебору синтезованих операцій на основі запропонованих шаблонів було отримано 24 множини операцій по 24 операції в кожній множині. Приклади побудованих множин операцій наведено в табл. 3.

Аналіз синтезованих множин показав, що 20 множин складаються виключно з несиметричних двоопераднних операцій. Отримані результати дозволяють стверджувати, що множини симетричних і несиметричних операції не перетинаються. Крім того, використання шаблону відповідно кожній множині дає змогу утворити всю множину несиметричних операцій з будь-якої операції даної множини.

Унікальність кожної з 576 таблиць істинності свідчить про те, що всі синтезовані операції є різними, а наявність отриманої в результаті практичного експерименту відповідних операцій декодування дає змогу їх практично реалізовувати. Застосування синтезованих множин операцій забезпечить підвищення варіативності крипографічних перетворень потокового шифрування.

Таблиця 3
Множини двохоперандних двохрозрядних операцій

№	Множина 1	Множина 2	…	Множина 24
1	k 1,8,20,13 → d 3,11,15,23	k 1,20,13,8 → d 2,7,14,19	…	k 1,19,16,10 → d 2,11,17,20
2	k 13,20,8,1 → d 15,23,3,11	k 4,23,10,17 → d 5,16,11,22	…	k 5,17,9,21 → d 4,24,12,16
3	k 2,19,7,14 → d 5,21,17,9	k 5,16,11,22 → d 4,23,10,17	…	k 2,8,18,24 → d 1,21,15,7
4	k 24,9,15,6 → d 22,7,4,13	k 8,1,20,13 → d 7,14,19,2	…	k 10,16,1,19 → d 11,20,2,17
5	k 6,15,9,24 → d 4,13,22,7	k 10,17,4,23 → d 11,21,5,16	…	k 9,21,17,5 → d 12,4,16,24
…	…	…	…	
20	k 5,22,16,11 → d 2,24,8,18	k 14,19,2,7 → d 13,8,1,20	…	k 14,20,6,12 → d 13,9,3,19
21	k 16,5,11,22 → d 18,2,24,8	k 15,6,9,24 → d 18,21,12,3	…	k 15,3,11,23 → d 18,22,10,6
22	k 10,23,17,4 → d 12,20,6,14	k 21,12,3,18 → d 24,15,6,9	…	k 22,4,13,7 → d 23,8,14,5
23	k 3,12,18,21 → d 1,10,19,16	k 19,2,7,14 → d 20,13,8,1	…	k 20,14,12,6 → d 19,3,9,13
24	k 21,18,12,3 → d 19,16,1,10	k 24,15,6,9 → d 21,12,3,18	…	k 23,11,15,3 → d 22,6,18,10

4. Висновки

За результатами обчислювального експерименту побудовано 576 двохрозрядних двохоперандних операцій криптографічного кодування, з яких 96 – симетричні операції, а 480 – несиметричні.

Синтезовані операції поділено на 24 множини по 24 операції, з яких 20 множин несиметричних операцій та 4 множини симетричних операцій. Поділ операцій проводився на основі використання 24 шаблонів таблиць істинності.

Так як вся множна операцій описується одним шаблоном, то з будь-якої однієї операції будь-якої множини можна побудувати всю множину операцій на основі заданої.

Встановлено, що таблиці істинності синтезованих операцій не повторяються, тому вони всі різні. Застосування синтезованих операцій забезпечить підвищення варіативності алгоритмів криптоперетворення, а застосування множин операцій спростить їх практичну реалізацію.

References

1. Rudnytskyi, V. M., Opirskyi, I. R., Melnyk, O. H., Pustovit, M. O. (2018). Syntez hrupy operatsii strohoho stiikoho kryptohrafichnoho koduvannia dlia pobudovy potokovykh shyfriv. *Bezpeka informatsii, 24 (3),* 195–200.
2. Pustovit, M. O., Melnyk, O. H., Sysoienko, S. H. (2017). Syntez operatsii obernenoho hrupovoho matrychnoho kryptohrafichnoho peretvorennia informatsii. *Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu. Seriia: Tekhnichni nauky, 4,* 118–124.
3. Bernstein, D., Buchmann, J., Dahmen, E. (2009). *Post-quantum cryptography*. Berlin: Springer, 246. doi: http://doi.org/10.1007/978-3-540-88702-7
4. Lada, N. V., Kozlovska, S. H. (2018). Applying cryptographic addition operations by module twowith accuracy of permutation in stream ciphers. *Control, Navigation and Communication Systems. Academic Journal, 1 (47),* 127–130. doi: http://doi.org/10.26906/sunz.2018.1.127
5. Adki, V., Hatkar, S. (2016). A Survey on Cryptography Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering, 6 (6),* 469–475.
6. Rudnytskyi, V., Opirskyy, I., Melnyk, O., Pustovit, M. (2019). The implementation of strict

stable cryptographic coding operations. *Advanced Information Systems, 3 (3),* 109–112. doi: http://doi.org/10.20998/2522-9052.2019.3.15

7. Ferguson, N., Schneier, B. (2003). *Practical Cryptography: Designing and Implementing Secure Cryptographic Systems*. Wiley, 432.

8. Kozlovska, S. H. (2018). Syntez hrup dvokhoperandnykh operatsii kryptoperetvorennia na osnovi perestanovochnykh skhem. *Suchasna spetsialna tekhnika, 4 (55),* 44–50.

9. Rudnitsky, V., Berdibayev, R., Breus, R., Lada, N., Pustovit, M. (2019). Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation. *Advanced Information Systems, 3 (4),* 109–114. doi: http://doi.org/10.20998/2522-9052.2019.4.16

10. Rudnytskyi, V. M., Lada, N. V., Babenko, V. H. (2018). *Kryptohrafichne koduvannia: syntez operatsii potokovoho shyfruvannia z tochnistiu do perestanovky*. Kharkiv: TOV «DISA PLIuS», 184.

11. Lada, N., Kozlovska, S., Rudnitskaya, Y. (2019). Researching and Synthesizing a Group of Symmetric Modified Modulo-4 Addition Operations. *Central Ukrainian Scientific Bulletin. Technical Sciences, 2 (33),* 181–189. doi: http://doi.org/10.32515/2664-262x.2019.2(33).181-189

12. Hoffstein, J., Pipher. J., Silverman. J. H. (2008). *An Introduction to Mathematical Cryptography*. Springer, 523. doi: http://doi.org/10.1007/978-1-4939-1711-2

13. Mao, W. (2003). *Modern Cryptography: Theory and Practice.* Prentice Hall PTR, 648.

14. Melnyk, R. P. (2012). Zastosuvannia operatsii rozshyrenoho matrychnoho kryptohrafichnoho peretvorennia dlia zakhystu informatsii. *Systemy obrobky informatsii, 9 (107),* 145–147.

15. Rudnytskyi, V. M. (Ed.) (2018). *Kryptohrafichne koduvannia: obrobka ta zakhyst informatsii*. Kharkiv: TOV «DISA PLIuS», 139.