КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.23.616
УДК 004.056.55:004.312.2

Рудницький Володимир Миколайович
доктор технічних наук, професор, головний науковий співробітник
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна
ORCID 0000-0003-3473-7433
rvn_2008@ukr.net

Лада Наталія Володимирівна
кандидат технічних наук, провідний науковий співробітник
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна
ORCID 0000-0002-7682-2970
ladanatali256@gmail.com

Підласий Дмитро Андрійович
Викладач кафедри іноземних мов та міжнародної комунікації
Черкаський державних технологічний університет, Черкаси, Україна
ORCID 0000-0002-9916-5256
stahlmann119@gmail.com

Мельник Ольга Григорівна
кандидат технічних наук, старший науковий співробітник, доцент кафедри управління у сфері цивільного захисту
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України, Черкаси, Україна
ORCID 0000-0002-9671-108X
melnyk.olja.2014@gmail.com

СИНТЕЗ ДИСКРЕТНО-АЛГЕБРАЇЧНИХ МОДЕЛЕЙ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ОПЕРАЦІЙ КЕРОВАНИХ ІНФОРМАЦІЄЮ

Анотація. Розвиток сучасних засобів обміну інформацією приводить до зростання вимог в сфері кібербезпеки. Як наслідок значна кількість діючих мало ресурсних криптоалгоритмів може стати в найближчому майбутньому неефективна. Одним з перспективних шляхів розвитку мало ресурсної криптографії вважається СЕТ-шифрування. В статті проводиться аналіз опублікованих результатів моделювання СЕТ-операцій, яка є основою СЕТ-шифрування. В свою чергу основою побудови СЕТ-операцій є елементарні функції. За результатами аналізу встановлено, що елементарні функції операцій керованих інформацією не досліджувалися. Метою даної статті є дослідження елементарних функцій операцій керованих інформацією та розроблення методу синтезу групи елементарних функцій операцій керованих інформацією для автоматизації побудови СЕТ-операцій з заданими характеристиками. В статті показано, що відомі дискретні моделі елементарних функцій операцій керованих інформацією не відображають їх фізичний зміст і особливості використання при побудові СЕТ-операцій. Пропонується для моделювання даних елементарних функцій використовувати дискретно-алгебраїчне представлення. Результати аналізу синтезованих моделей елементарних функцій операцій керованих інформацією дозволили розробити метод їх синтезу. Даний метод адаптований для використання в автоматизованій системі моделювання СЕТ-операцій. Наведено приклади моделей СЕТ-операцій побудованих на основі елементарних функцій операцій керованих інформацією. Розроблений метод синтезу групи елементарних функцій операцій керованих інформацією забезпечує розширення можливостей генерації елементарних функцій для автоматизованої системи побудови та дослідження СЕТ-операцій. Наведені в статті наукові результати створюють можливість експериментального моделювання СЕТ-операцій, алгоритми реалізації яких будуть визначатися як самими операціями, так і інформацією яка

перетворюється. Дані операції забезпечать можливість модифікації криптографічного алгоритму під управлінням інформації, яка буде шифруватися.

Ключові слова: шифрування; потокове шифрування; СЕТ-шифрування; малоресурсна криптографія; операції керовані інформацією; елементарні функції; дискретно-алгебраїчні моделі.

ВСТУП

На сьогоднішній день малоресурсна криптографія набуває все більшого розповсюдження [1] – [3]. Сучасні засоби обміну інформацією, на зразок мобільних телефонів, ноутбуків, систем «розумного будинку», IoT, SMART-гаджетів тощо стають все більш компактними і відповідно обмеженими в ресурсах, в той же час обсяги інформації що потребує криптографічного захисту під час обробки, передачі та зберігання зростають ще більшими темпами [4], [5]. Таким чином значна кількість зараз діючих криптоалгоритмів в найближчому майбутньому в існуючих обмеженнях виявиться недіючими або неефективними [6] – [8].

Аналіз останніх досліджень і публікацій. Одним з нових напрямків розвитку малоресурсної криптографії є СЕТ-шифрування. Проте в даний час СЕТ-шифруванню приділяється недостатня увага [9] – [11]. Ця теорія виникла на зламі комп'ютерної інженерії та кібербезпеки і дозволяє досліджувати шляхи покращення криптосистем на рівні елементарних функцій, їх дискретно-алгебраїчних моделей. СЕТ-шифрування забезпечує перетворення інформації на основі псевдовипадкових наборів СЕТ-операцій які реалізують дискретні моделі таблиць підстановок [12], [13].

СЕТ-операції будуються на основі елементарних функцій. Тому не дослідивши елементарні функції неможливо синтезувати СЕТ-операції і розробляти методи їх генерації. Основні результати дослідження 2Сі-квантових елементарних функцій для побудови СЕТ-операцій наведені в [14], [15]. Роботи [16], [17] присвячені визначенню і класифікації 3Сі-квантових елементарних функцій. Подальші дослідження елементарних функцій проводились по класифікованих групах. Результати дослідження елементарних функцій для побудови матричних СЕТ-операцій наведені в роботах [18], [19]. В роботах [20], [21] наведено результати дослідження елементарних функцій для побудови нелінійних розширених матричних СЕТ-операцій. Синтезу елементарних функцій перестановок керованих інформацією присвячені роботи [22], [23]. Проте на сьогоднішній день елементарні функції операцій керованих інформацією не досліджувалися.

Мета статті. Дослідити елементарні функції операцій керованих інформацією та розробити метод синтезу групи елементарних функцій операцій керованих інформацією для автоматизації побудови СЕТ-операцій з заданими характеристиками.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Серед трьох розрядних елементарних функцій які можуть використовуватися в криптографічних перетвореннях на сьогоднішній день не досліджувались елементарні функції операцій керованих інформацією. Проте дані елементарні функції мають важливе значення в теорії шифрування, так як дозволяють будувати 3Сі-квантові одноопернадні СЕТ-операції які керуються інформацією.

Відповідно до класифікації трьох розрядних елементарних функцій для криптографічних перетворень [17] група елементарних функцій операцій керованих

інформацією включає в себе 8 елементарних функцій. Дані елементарні функції наведені в табл. 1.

Таблиця 1

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

В табл. 1 індекси елементарних функцій відповідають значенню десяткової цифри результату перетворення, за умови впорядкування повної множини вхідних даних по зростанню їх значень.

Як видно з табл. 1 елементарні функції операцій керованих інформацією поділено на дві групи: прямі елементарні функції і обернені елементарні функції. Поділ було виконано на основі результатів реалізації перетворення. Кожній прямій елементарній функції відповідає обернена елементарна функція. Розподіл на прямі і обернені елементарні функції було виконано в порядку зростання індексів елементарних функцій. В кожній парі функцій прямою вважалася та індекс якої менший.

Наприклад. Для пари елементарних функцій f_{23} і f_{232} функція f_{23} вважається прямою, а f_{232} — оберненою, так як 23<232. Для пари елементарних функцій f_{212} і f_{43} функція f_{212} вважається оберненою, а f_{43} — прямою, так як 212>43.

Проте коректність розподілу на прямі і обернені елементарні функції не досліджувалась. Встановити коректність розподілу можливо лише при детальному дослідження особливостей елементарних функцій та їх поєднання в СЕТ-операції. Дослідимо прямі елементарні функції.

Розглянемо елементарну функцію $f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3$.

Для встановлення особливостей даної елементарної функції побудуємо її таблицю істинності та синтезуємо спрощені дискретні моделі. Дані дискретні моделі не обов'язково повинні представляти собою мінімальні диз'юнктивно-нормальні форми представлення. Дані моделі в першу чергу повинні відображати фізичну сутність даної елементарної функції.

Таблиця істинності f_{23} представлена в табл. 2.

Для побудови спрощених дискретних моделей елементарної функції використаємо карти Корно [24], та побудуємо різні варіанти об'єднання контурів.

На основі трьох варіантів контурів отримаємо дискретні моделі та перейдемо до дискретно-алгебраїчного представлення [25] елементарної функції:

$$f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3 = \begin{cases} x_2 \cdot x_3 & якщо \quad x_1 = 0 \\ x_2 \vee x_3 & якщо \quad x_1 = 1 \end{cases}, \tag{1}$$

$$f_{23} = x_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} x_1 \cdot x_3 & якщо \quad x_2 = 0 \\ x_1 \vee x_3 & якщо \quad x_2 = 1 \end{cases}, \tag{2}$$

ISSN 2663 - 4023

$$f_{23} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_1 \cdot x_2 & якщо \quad x_3 = 0 \\ x_1 \vee x_2 & якщо \quad x_3 = 1 \end{cases}, \qquad (3)$$

Таблиця 2

Таблиця істинності елементарної функції f_{23}

Вхідні дані			**Результат перетворення**
x_1	x_2	x_3	f_{23}
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

На основі отриманих дискретно-алгебраїчних представлень елементарної функції f_{23} можна зробити припущення, що дана елементарна функція для вибору операції логічного додавання ($\vee$), або логічного множення ($\cdot$) буде використовувати будь який вхідний Сі-квант (x_1, x_2, або x_3).

По аналогії були отримані дискретно-алгебраїчні моделі елементарних функцій операцій керованих інформацією, та побудовані їх функціональні схеми.

Отримані в процесі дослідження і класифіковані дискретні і дискретно-алгебраїчні моделі елементарних функцій (1) – (3) зведені в табл. 3. Слід відмітити, що для класифікації дискретно-алгебраїчних моделей елементарних функцій операцій керованих інформацією було необхідно дослідити і порівняти крім самих моделей функціональні схеми їх реалізації.

Отримані результати синтез дискретно-алгебраїчних моделей елементарних функцій операцій керованих інформацією (табл. 3), а також побудовані їх функціональні схеми дозволили зробити наступні висновки:

1. Елементарна функція операції керованою інформацією може бути реалізована на основі однієї з трьох дискретних, або дискретно-алгебраїчних моделей.
2. Дискретно-алгебраїчні моделі елементарної функції керованої інформацією залежать від номера (індексу) Сі-кванта, значення якого управляє вибором операції перетворення інформації.
3. Зміна Сі-кванта, значення якого управляє вибором операції перетворення інформації елементарною функцією приводить до перестановки Сі-квантів як в моделях елементарних функцій, так і в їх функціональних схемах реалізації.
4. Дві прямі елементарні функції, побудовані на основі одного і того ж Сі-кванта управління вибором операції перетворення інформації відрізняються інверсним значенням одного і того ж Сі-кванта вхідної інформації (включаючи Сі-квант управління вибором операції).
5. Так як елементарні функції операцій керованих інформацією перетворюють три вхідних Сі кванта інформації, і вони відрізняються інверсією одного з них,

ISSN 2663 - 4023

то група прямих елементарних функцій операцій керованих інформацією включає в себе чотири елементарних функції.

6. Пряма і обернена елементарні функції відрізняються інверсними значеннями всіх вхідних Сі-квантів інформації.

Таблиця 3

Класифікація дискретних і дискретно-алгебраїчних моделей елементарних функцій операцій керованих інформацією

Моделі прямих елементарних функцій	Моделі обернених елементарних функцій
$f_{23}=x_1\cdot x_2\vee x_1\cdot x_3\vee \bar{x}_1\cdot x_2\cdot x_3=\begin{cases}x_2\cdot x_3 & якщо\ x_1=0\\ x_2\vee x_3 & якщо\ x_1=1\end{cases}$	$f_{232}=\bar{x}_1\cdot\bar{x}_2\vee\bar{x}_1\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot\bar{x}_3=\begin{cases}\bar{x}_2\vee\bar{x}_3 & якщо\ x_1=0\\ \bar{x}_2\cdot\bar{x}_3 & якщо\ x_1=1\end{cases}$
$f_{23}=x_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot x_3=\begin{cases}x_1\cdot x_3 & якщо\ x_2=0\\ x_1\vee x_3 & якщо\ x_2=1\end{cases}$	$f_{232}=\bar{x}_1\cdot\bar{x}_2\vee\bar{x}_2\cdot\bar{x}_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3=\begin{cases}\bar{x}_1\vee\bar{x}_3 & якщо\ x_2=0\\ \bar{x}_1\cdot\bar{x}_3 & якщо\ x_2=1\end{cases}$
$f_{23}=x_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3=\begin{cases}x_1\cdot x_2 & якщо\ x_3=0\\ x_1\vee x_2 & якщо\ x_3=1\end{cases}$	$f_{232}=\bar{x}_1\cdot\bar{x}_3\vee\bar{x}_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3=\begin{cases}\bar{x}_1\vee\bar{x}_2 & якщо\ x_3=0\\ \bar{x}_1\cdot\bar{x}_2 & якщо\ x_3=1\end{cases}$
$f_{43}=x_1\cdot x_2\vee x_1\cdot\bar{x}_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3=\begin{cases}x_2\cdot\bar{x}_3 & якщо\ x_1=0\\ x_2\vee\bar{x}_3 & якщо\ x_1=1\end{cases}$	$f_{212}=\bar{x}_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot x_3=\begin{cases}\bar{x}_2\vee x_3 & якщо\ x_1=0\\ \bar{x}_2\cdot x_3 & якщо\ x_1=1\end{cases}$
$f_{43}=x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3=\begin{cases}x_1\cdot\bar{x}_3 & якщо\ x_2=0\\ x_1\vee\bar{x}_3 & якщо\ x_2=1\end{cases}$	$f_{212}=\bar{x}_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot x_3=\begin{cases}\bar{x}_1\vee x_3 & якщо\ x_2=0\\ \bar{x}_1\cdot x_3 & якщо\ x_2=1\end{cases}$
$f_{43}=x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee x_1\cdot x_2\cdot x_3=\begin{cases}x_1\vee x_2 & якщо\ x_3=0\\ x_1\cdot x_2 & якщо\ x_3=1\end{cases}$	$f_{212}=\bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot\bar{x}_2\cdot\bar{x}_3=\begin{cases}\bar{x}_2\cdot x_3 & якщо\ x_3=0\\ \bar{x}_2\vee x_3 & якщо\ x_3=1\end{cases}$
$f_{77}=x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3=\begin{cases}\bar{x}_2\cdot x_3 & якщо\ x_1=0\\ \bar{x}_2\vee x_3 & якщо\ x_1=1\end{cases}$	$f_{178}=\bar{x}_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_3\vee x_1\cdot x_2\cdot\bar{x}_3=\begin{cases}x_2\vee\bar{x}_3 & якщо\ x_1=0\\ x_2\cdot\bar{x}_3 & якщо\ x_1=1\end{cases}$
$f_{77}=x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot x_3=\begin{cases}x_1\vee x_3 & якщо\ x_2=0\\ x_1\cdot x_3 & якщо\ x_2=1\end{cases}$	$f_{178}=\bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot\bar{x}_3=\begin{cases}\bar{x}_1\cdot\bar{x}_3 & якщо\ x_2=0\\ \bar{x}_1\vee\bar{x}_3 & якщо\ x_2=1\end{cases}$
$f_{77}=x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3=\begin{cases}x_1\cdot\bar{x}_2 & якщо\ x_3=0\\ x_1\vee\bar{x}_2 & якщо\ x_3=1\end{cases}$	$f_{178}=\bar{x}_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot x_2\cdot x_3=\begin{cases}\bar{x}_1\vee x_2 & якщо\ x_3=0\\ \bar{x}_1\cdot x_2 & якщо\ x_3=1\end{cases}$
$f_{113}=\bar{x}_1\cdot x_2\vee x_1\cdot x_3\vee x_1\cdot x_2\cdot x_3=\begin{cases}x_2\vee x_3 & якщо\ x_2=0\\ x_2\cdot x_3 & якщо\ x_2=1\end{cases}$	$f_{142}=x_1\cdot\bar{x}_2\vee x_1\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot\bar{x}_3=\begin{cases}\bar{x}_2\cdot\bar{x}_3 & якщо\ x_1=0\\ \bar{x}_2\vee\bar{x}_3 & якщо\ x_1=1\end{cases}$
$f_{113}=\bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3=\begin{cases}\bar{x}_1\cdot x_3 & якщо\ x_2=0\\ \bar{x}_1\vee x_3 & якщо\ x_2=1\end{cases}$	$f_{142}=x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot\bar{x}_3\vee x_1\cdot x_2\cdot\bar{x}_3=\begin{cases}x_1\vee\bar{x}_3 & якщо\ x_2=0\\ x_1\cdot\bar{x}_3 & якщо\ x_2=1\end{cases}$
$f_{113}=\bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3=\begin{cases}\bar{x}_1\cdot x_2 & якщо\ x_3=0\\ \bar{x}_1\vee x_2 & якщо\ x_3=1\end{cases}$	$f_{142}=x_1\cdot\bar{x}_3\vee\bar{x}_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3=\begin{cases}x_1\cdot\bar{x}_2 & якщо\ x_3=0\\ x_1\vee\bar{x}_2 & якщо\ x_3=1\end{cases}$

На основі отриманих висновків можна побудувати метод синтезу дискретно-алгебраїчних моделей елементарних функції керованих інформацією.

1. Побудувати дискретно-алгебраїчну модель елементарної функції операцій керованих інформацією, яка не включає операції інверсій.
2. Побудувати на її основі три модифікації даної елементарної функції на основі перестановок вхідних Сі квантів. Так як операції логічного додавання і логічного множення комутативні ($x_i\cdot x_j=x_j\cdot x_i;\ x_i\cdot x_j=x_j\cdot x_i;\ i\neq j\in\{1,2,3\}$), то буде побудовано три модифікації елементарної функції.

3. Для побудови наступної елементарної функції і її модифікацій, необхідно вибрати один із вхідних Сі-квантів інформації, і модифікувати його в всіх трьох дискретно-алгебраїчних моделях елементарної функція які не включають операції інверсій.
4. Послідовний вибір всіх вхідних Сі-квантів інформації забезпечить побудову групи дискретно-алгебраїчних моделей прямих елементарних функції операцій керованих інформацією, та всіх їх модифікацій.
5. На основі послідовного вибору всіх модифікацій дискретно-алгебраїчних моделей прямих елементарних функції операцій керованих інформацією, і інверсії всіх вхідних Сі-квантів моделей, побудувати групу модифікацій дискретно-алгебраїчних моделей обернених елементарних функції операцій керованих інформацією.

Перехід від дискретно-алгебраїчних до дискретних моделей елементарних функцій не представляє складності. Виходячи з цього синтезувати повну групу дискретних моделей операцій керованих інформацією та їх модифікацій можна на основі синтезованої повної групи дискретно-алгебраїчних моделей операцій керованих інформацією.

Можливість зміни в елементарній функції Сі-кванта управління вибором операції перетворення інформації забезпечує можливість застосування будь якої елементарної функції для формування будь якого вихідного Сі-кванта в СЕТ-операціях базової групи. Дане твердження базується на тому, що в операціях базової групи вихідні Сі-кванти інформації формуються елементарними функціями, які залежать від однойменних вхідних Сі-квантів управління [19].

Розроблений метод синтезу дозволяє автоматизувати процес побудови СЕТ-операцій. Наприклад

Пряма СЕТ-операція:

$$C(x)=\begin{bmatrix} f_{77}(x) \\ f_{23}(x) \\ f_{113}(x) \end{bmatrix}=\begin{bmatrix} \begin{cases} \bar{x}_2 \cdot x_3 \quad если \quad x_1=0 \\ \bar{x}_2 \vee x_3 \quad если \quad x_1=1 \end{cases} \\ \begin{cases} x_1 \cdot x_3 \quad если \quad x_2=0 \\ x_1 \vee x_3 \quad если \quad x_2=1 \end{cases} \\ \begin{cases} \bar{x}_1 \cdot x_2 \quad якщо \quad x_3=0 \\ \bar{x}_1 \vee x_2 \quad якщо \quad x_3=1 \end{cases} \end{bmatrix}=\begin{bmatrix} x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \end{bmatrix}, \qquad (4)$$

Обернена СЕТ-операція:

$$C'(x)=\begin{bmatrix} f_{43}(x) \\ f_{113}(x) \\ f_{23}(x) \end{bmatrix}=\begin{bmatrix} \begin{cases} x_2 \cdot \bar{x}_3 \quad если \quad x_1=0 \\ x_2 \vee \bar{x}_3 \quad если \quad x_1=1 \end{cases} \\ \begin{cases} \bar{x}_1 \cdot x_3 \quad якщо \quad x_2=0 \\ \bar{x}_1 \vee x_3 \quad якщо \quad x_2=1 \end{cases} \\ \begin{cases} x_1 \cdot x_2 \quad если \quad x_3=0 \\ x_1 \vee x_2 \quad если \quad x_3=1 \end{cases} \end{bmatrix}=\begin{bmatrix} x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \\ x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3 \end{bmatrix}, \qquad (5)$$

Побудовані на основі розробленого методу СЕТ-операції забезпечують формування вихідних Сі-квантів на основі логічного множення, або логічного додавання вхідних залежності від значення вхідних Сі-квантів інформації. Слід відмітити, що для кожного вихідного Сі-кванта, алгоритми їх формування будуть відрізнятися (4), (5).

Тому якість криптографічного перетворення інформації буде залежати як від вибраних моделей СЕТ-операцій, так і від самої інформації. Як показує практика без автоматизації процесу дослідження, визначити оптимальні набори СЕТ-операцій для інформаційних потоків з різними статистичними характеристиками неможливо.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

1. За результатами дослідження елементарних функцій операцій керованих інформацією було встановлено наступне:
   - кожна елементарна функція операцій керованих інформацією має три модифікації і може бути представлена трьома дискретно алгебраїчними моделями, які відрізняються перестановками вхідних Сі-квантів інформації, в залежності від визначеного Сі-кванта управління вибором операції перетворення інформації;
   - моделі прямих елементарних функцій можу мати не більше одного інвертованого вхідного Сі-кванта, в тому числі і Сі-квант управління вибором операції;
   - моделі обернених елементарних функцій операцій керованих інформацією, відрізняються прямих елементарних функцій інверсією всіх вхідних Сі-квантів інформації.
2. Наявність трьох модифікацій кожної елементарної функції забезпечує можливість застосування будь якої елементарної функції для формування будь якого вихідного Сі-кванта в СЕТ-операціях базової групи.
3. Розроблений метод синтезу групи елементарних функцій операцій керованих інформацією забезпечує побудову всіх елементарних функцій операцій керованих інформацією, а такої їх модифікацій. Даний метод забезпечує розширення можливостей генерації елементарних функцій для автоматизованої системи побудови та дослідження СЕТ-операцій.
4. Отримані наукові результати забезпечують підґрунтя для розробки методів синтезу СЕТ операцій, в яких алгоритм перетворення інформації буде визначатися як ключовою послідовністю так і інформацією яка перетворюється. Можливість додаткової модифікації алгоритму під управлінням інформації яка буде шифруватися створить додаткові складності для криптоаналізу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Zakaria, A., et al. (2023). Systematic literature review: Trend analysis on the design of lightweight block cipher. *Journal of King Saud University - Computer and Information Sciences, 35(5), 101550*. https://doi.org/10.1016/j.jksuci.2023.04.003
2. Thakor, V., Razzaque, A., & Khandaker M. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access, 9*, 28177–28193. https://doi.org/10.1109/ACCESS.2021.3052867
3. Kumar C., Prajapati S., & Verma R. (2022). A Survey of Various Lightweight Cryptography Block ciphers for IoT devices. *IEEE International Conference on Current Development in Engineering and Technology (CCET),* 1–6. https://doi.org/10.1109/CCET56606.2022.10080556
4. Amraoui, N., & Zouari, B. (2022). Securing the operation of Smart Home Systems: a literature review. *J. Reliable Intell. Environ. 8(3),* 67–74. https://doi.org/10.1007/s40860-021-00160-3
5. Aboshosha B., Dessouky, M., & El-Sayed A. (2019). Energy Efficient Encryption Algorithm for Low Resources Devices. *Proceedings of the first international conference Environmental Efficiency For Human Well Being*

(EBQL), 3(3), 26–37. https://doi.org/10.21625/archive.v3i3.520
6. Sabani, M., et al. (2023). Evaluation and Comparison of Lattice-Based Cryptosystems for a Secure Quantum Computing Era. *Electronics, 12(12),* 2643. https://doi.org/10.3390/electronics12122643
7. Suomalainen J., et al. (2018). Evaluating the Efficiency of Physical and Cryptographic Security Solutions for Quantum Immune IoT. *Cryptography, 2(1):5*. https://doi.org/10.3390/cryptography2010005
8. Yalamuri, G., Honnavalli, P., & Eswaran, S. (2022). A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats. *Procedia Comput. Sci. 215,* 834–845. https://doi.org/10.1016/j.procs.2022.12.086
9. Easttom, W. (2021). Modern Cryptography. Applied Mathematics for Encryption and Information Security. *Springer Cham.* https://doi.org/10.1007/978-3-030-63115-4
10. Zheng, Z. (2022). Modern Cryptography Volume 1. A Classical Introduction to Informational and Mathematical Principle. *Springer: Singapore.* https://doi.org/10.1007/978-981-19-0920-7
11. Zheng, Z., Tian, K., & Liu, F. (2023). Modern Cryptography Volume 2. A Classical Introduction to Informational and Mathematical Principle. *Springer: Singapore*. https://doi.org/10.1007/978-981-19-7644-5
12. Dalai, D., Gupta, K., & Maitra, S. (2004). Results on algebraic immunity for cryptographically significant boolean functions. *Progress in Cryptology - INDOCRYPT 2004, Lecture Notes in Computer Science, 334,* 92–106. https://doi.org/10.1007/978-3-540-30556-9_9
13. Mouha, N., et al. (2011). The Differential Analysis of S-Functions. *SAC 2010: Selected Areas in Cryptography, Lecture Notes in Computer Science, 6544,* 36–56. https://doi.org/10.1007/978-3-642-19574-7_3
14. Рудницький, В., Бабенко, В., & Жиляєв, Д. (2011). Алгебраїчна структура множини логічних операцій кодування. *Наука і техніка Повітряних Сил Збройних Сил України, 2 (6),* 112–114.
15. Рудницький, В., Миронець, І., & Бабенко, В. (2011). Систематизація повної множини логічних функцій для криптографічного перетворення інформації. *Системи обробки інформації, 8(98),* 184–188.
16. Бабенко, В., Рудницький, С., & Мельник, Р. (2012). Визначення множини трирозрядних елементарних операцій криптографічного перетворення. *Вісник Інженерної академії України, 3(4),* 77–79.
17. Бабенко, В., Мельник, О., & Мельник, Р. (2013). Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації. *Безпека інформації, 19(1),* 56–59.
18. Рудницький, В., Бабенко, В., & Рудницький, С. (2012). Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. *Зб. наук. пр. Х.: ХУПС ім. І. Кожедуба, 4(33),* 198–200.
19. Голуб, С., Бабенко, В., & Рудницький, С. (2012). Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два. *Системи обробки інформації, 3(1),* 119–122.
20. Бабенко, В., Мельник, О., & Стабецька, Т. (2014). Синтез нелінійних операцій криптографічного перетворення. *Безпека інформації, 20(2),* 143–147.
21. Рудницький, В., Бабенко, В., & Стабецька Т. (2014). Узагальнений метод синтезу обернених нелінійних операцій розширеного матричного криптографічного перетворення. *Системи обробки інформації, 6(122),* 118–121.
22. Рудницький, В., Миронюк, Т., Мельник, О., & Щербина, В. (2014). Синтез елементарних функцій перестановок, керованих інформацією. *Безпека інформації, 20(3),* 242–247.
23. Миронюк, Т. (2016). Визначення елементарних операцій базової групи перестановок, керованих інформацією. *Вісник Черкаського державного технологічного університету, 2,* 100–105.
24. Veitch, E. (1952). Chart Method for Simplifying Truth Functions. *ACM '52: Proceedings of the 1952 ACM national meeting (Pittsburgh),* 127–133. https://doi.org/10.1145/609784.609801
25. Бабенко, В., Мельник, Р., & Рудницький, С. (2012). Дослідження способів запису трьохрозрядних криптографічних операцій. *Системи управління, навігації та зв'язку, 1(21),* 170–173.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023

Volodymyr Rudnytskyi
Doctor of Engineering Science, professor, Chief Researcher
State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine
ORCID 0000-0003-3473-7433
rvn_2008@ukr.net

Nataliia Lada
Candidate of Technical Sciences (PhD), Leading Researcher
State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine
ORCID 0000-0002-7682-2970
ladanatali256@gmail.com

Dmytro Pidlasyi
Assistant of Foreign Languages and International Communications Department
Cherkasy State Technological University, Cherkasy, Ukraine
ORCID 0000-0002-9916-5256
stahlmann119@gmail.com

Olga Melnyk
Candidate of Technical Sciences (PhD), Senior Researcher, Associate Professor of the Department of Management in the Sphere of Civil Protection
Cherkasy Institute of Fire Safety named after Heroes of Chornobyl of National University of Civil Defense of Ukraine, Cherkasy, Ukraine
ORCID 0000-0002-9671-108X
melnyk.olja.2014@gmail.com

SYNTHESIS OF DISCRETE AND ALGEBRAIC MODELS OF ELEMENTARY FUNCTIONS OF DATA-CONTROLLED OPERATIONS

Abstract. Improvement of modern data exchange applications increases the complexity of cybersecurity. This leads to most applicable low-cost cryptographic algorithms becoming ineffective in the near future. On the other hand, CET encryption offers a great opportunity for development of the low-cost cryptography. The following article analyzes previously published results of CET-operations modeling, which serves as the foundation of CET encryption. The CET operations mentioned above use elementary functions as their basis. The results of our analysis allow to conclude that elementary functions of data-controlled operations have not been researched in the past. The primary goal of this article is to research these elementary functions of data-controlled operations and develop a method suitable for synthesis of a group of elementary functions of data-controlled operations. This can assist in automating the process of creating CET operations with defined attributes. This article proves that known discrete models of elementary functions of data-controlled operations do not represent their content and usage specifications during creation of CET operations. We suggest using discrete and algebraic presentation for modeling elementary functions data. The results of our analysis of the synthesized models of elementary functions of data-controlled operations allow us to develop a proper method of their synthesis. This method is adapted for usage in the automated systems of CET-operations modeling. We also provide examples of models of CET operations created based on elementary functions of data-controlled operations. The aforementioned method for synthesis of a group of elementary functions of data-controlled operations allows expanding possibilities for generating these elementary functions within the automated system used for research and creation of CET operations. Presented scientific results can be used for experimental modeling of CET operations, while the implementation algorithms of such operations will be defined by the operations themselves, as well as transformed data. Utilization of these operations allows modification of cryptographic algorithms controlled by encrypted data.

Keywords: encryption; stream encryption; CET-encryption; low-cost cryptography; data-controlled operations; elementary functions; discrete and algebraic models.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Zakaria, A., et al. (2023). Systematic literature review: Trend analysis on the design of lightweight block cipher. *Journal of King Saud University - Computer and Information Sciences, 35(5), 101550*. https://doi.org/10.1016/j.jksuci.2023.04.003

2 Thakor, V., Razzaque, A., & Khandaker M. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access, 9,* 28177–28193. https://doi.org/10.1109/ACCESS.2021.3052867

3 Kumar C., Prajapati S., & Verma R. (2022). A Survey of Various Lightweight Cryptography Block ciphers for IoT devices. *IEEE International Conference on Current Development in Engineering and Technology (CCET),* 1–6. https://doi.org/10.1109/CCET56606.2022.10080556

4 Amraoui, N., & Zouari, B. (2022). Securing the operation of Smart Home Systems: a literature review. *J. Reliable Intell. Environ. 8(3),* 67–74. https://doi.org/10.1007/s40860-021-00160-3

5 Aboshosha B., Dessouky, M., & El-Sayed A. (2019). Energy Efficient Encryption Algorithm for Low Resources Devices. *Proceedings of the first international conference Environmental Efficiency For Human Well Being (EBQL), 3(3),* 26–37. https://doi.org/10.21625/archive.v3i3.520

6 Sabani, M., et al. (2023). Evaluation and Comparison of Lattice-Based Cryptosystems for a Secure Quantum Computing Era. *Electronics, 12(12),* 2643. https://doi.org/10.3390/electronics12122643

7 Suomalainen J., et al. (2018). Evaluating the Efficiency of Physical and Cryptographic Security Solutions for Quantum Immune IoT. *Cryptography, 2(1):5*. https://doi.org/10.3390/cryptography2010005

8 Yalamuri, G., Honnavalli, P., & Eswaran, S. (2022). A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats. *Procedia Comput. Sci. 215,* 834–845. https://doi.org/10.1016/j.procs.2022.12.086

9 Easttom, W. (2021). Modern Cryptography. Applied Mathematics for Encryption and Information Security. *Springer Cham.* https://doi.org/10.1007/978-3-030-63115-4

10 Zheng, Z. (2022). Modern Cryptography Volume 1. A Classical Introduction to Informational and Mathematical Principle. *Springer: Singapore.* https://doi.org/10.1007/978-981-19-0920-7

11 Zheng, Z., Tian, K., & Liu, F. (2023). Modern Cryptography Volume 2. A Classical Introduction to Informational and Mathematical Principle. *Springer: Singapore*. https://doi.org/10.1007/978-981-19-7644-5

12 Dalai, D., Gupta, K., & Maitra, S. (2004). Results on algebraic immunity for cryptographically significant boolean functions. *Progress in Cryptology - INDOCRYPT 2004, Lecture Notes in Computer Science, 334,* 92–106. https://doi.org/10.1007/978-3-540-30556-9_9

13 Mouha, N., et al. (2011). The Differential Analysis of S-Functions. *SAC 2010: Selected Areas in Cryptography, Lecture Notes in Computer Science, 6544,* 36–56. https://doi.org/10.1007/978-3-642-19574-7_3

14 Rudnitskyi, V., Babenko, V., & Zhylyaev, D. (2011). Construction of reverse functions for the systems of protection to information. *Scientific and Technical Journal: Science and Technology of the Air Force of Ukraine, 2(6),* 112–114.

15 Rudnytskyi, V., Myronets, I., & Babenko, V. (2011). Systematization of the full set of logical functions of cryptographic data conversion. *Information Processing Systems: Ukrainian Scientific Journal of Ivan Kozhedub Kharkiv National Air Force University, 8(98),* 184–188.

16 Babenko, V., Rudnytskyi, S., & Melnyk, R. (2012). Determination of the set of three-element elementary operations of cryptographic transformation. *Ukrainian Scientific Journal Bulletin of Engineering Academy of Ukraine, 3(4),* 77–79.

17 Babenko, V., Melnyk, O., & Melnyk, R. (2013). Classification of three-digit elementary functions for cryptographic transformation of the information. *Ukrainian Scientific Journal of Information Security. Kyiv: National Aviation University, 19(1),* 56–59.

18 Rudnytskyi, V., Babenko, V., & Rudnytskyi, S., (2012). The synthesis method of matrix models of cryptographic operations data encoding and decoding. *Scientific Works of Kharkiv National Air Force University, 4(33),* 198–200.

19 Golub, S., Babenko, V., & Rudnytskyi, S. (2012). The method of synthesis of the operations of cryptographic transformations on the basis of addition modulo two. *Information Processing Systems: Ukrainian Scientific Journal of Ivan Kozhedub Kharkiv National Air Force University, 3(1),* 119–122.

20 Babenko, V., Melnyk, O., & Stabetskaya, T. (2014). The synthesis of nonlinear operations for cryptographic transformation. *Ukrainian Scientific Journal of Information Security. Kyiv: National Aviation University, 20(2),* 143–147.

21 Rudnytskyi, V., Babenko, V., & Stabetskaya, T. (2014). Generalized method of synthesis of feedback nonlinear operations of expanded matrix cryptographic transformations. *Information Processing Systems: Ukrainian Scientific Journal of Ivan Kozhedub Kharkiv National Air Force University, 6(122),* 118–121.

22 Rudnytskyi, V., Myronyuk, T., Melnyk, O., & Scherbyna, V. (2014). Synthesis of elementary transposition functions controlled by information. *Ukrainian Scientific Journal of Information Security. Kyiv: National Aviation University. 20(3),* 242–247.

23 Myronyuk, T. (2016). Definition of elementary operations of core group permutations, controlled by information. *Ukrainian Scientific Journal Bulletin of Cherkasy State Technological University. Cherkasy: ChSTU. 2,* 100–105.

24 Veitch, E. (1952). Chart Method for Simplifying Truth Functions. *ACM '52: Proceedings of the 1952 ACM national meeting (Pittsburgh),* 127–133. https://doi.org/10.1145/609784.609801.

25 Babenko, V., Melnyk, R., & Rudnytskyi, S. (2012). Research methods recording of three-bit cryptographic operations. *Control, Navigation and Communication Systems. Academic Journal, 1(21),* 170–173.