УДК 004. 056.55:004.312.2 **doi: 10.26906/SUNZ.2024.4.139**

В. М. Рудницький[1,2], Н. В. Лада[1,2], В. В. Ларін[1], Д. А. Підласий[2]

[1] Державний НДІ випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна
[2] Черкаський державний технологічний університет, Черкаси, Україна

ДИСКРЕТНО-КАЗУАЛЬНЕ МОДЕЛЮВАННЯ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ОПЕРАЦІЙ КЕРОВАНИХ ІНФОРМАЦІЄЮ

Анотація. У статті запропоновано метод багатоваріантного синтезу дискретно-казуальних моделей елементарних функцій операцій керованих інформацією. Реалізація даного методу розширить можливості проектування мало ресурсних пристроїв реалізації СЕТ-операцій для побудови криптографічних систем з подвійним управлінням процесом шифрування. Для даних систем захисту інформації управління процесом шифрування буде визначатися як ключем,так і інформацією яка зашифровується. Дискретно-казуальні моделі елементарних функцій операцій керованих інформацією порівняно з дискретно-алгебраїчними моделями суттєво зменшую складність реалізації багатоопераднихСЕТ-операцій, так як їх представлення, дозволяє при об'єднанні використовувати методи мінімізації. Збільшення кількості варіантів представлення дискретно-казуальних моделей елементарних функції дозволить забезпечити впровадження декількох стратегій їх об'єднання для спрощення моделей побудованих СЕТ-операцій. Багатоваріантність дискретно-казуальних моделей елементарних функцій операцій керованих інформацією дозволяє інтегрувати їх в СЕТ-операціях сумісно з дискретно-казуальними моделями елементарних функцій перестановок керованих інформацією. Сфера використання отриманих результатів: мобільні і стаціонарні системи малоресурсного криптографічного захисту конфіденційної інформації.

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

Вступ

Постановка проблеми. Одним із позитивних наслідків стрімкого розвитку комп'ютерних мереж і телекомунікаційних систем стало створення глобального інформаційного простору. Негативною стороною стало виникнення кіберзлочинності, протидія якій вимагає захисту конфіденційної інформації. Одним з провідних напрямів захисту інформації був і залишається криптографічний захист [1]. За останні десятиріччя системи криптографічного захисту набули значного розвитку [2, 3]. На сьогоднішній день особливо актуальною є малоресурсна криптографія, адже саме вона забезпечує захист інформації в обмежених часових та енергетичних умовах [4, 5]. Одним із шляхів розвитку молоресурсної криптографії є побудова шифрів на основі СЕТ-операцій (Cryptographic Encoding Theory – операцій) [6]. СЕТ-операції представляють собою дискретні моделі таблиць підстановок які реалізуються в СЕТ-шифрах. Зменшення складності дискретних моделей СЕТ-операцій для прямого і оберненого перетвлорення інформації приводить до зменшення ресурсів необхідних на реалізацію криптосистеми.

Аналіз останніх досліджень і публікацій. В монографії [6] представлені результати дослідження архітектури СЕТ-операцій, та принципів побудови технологій потокового шифрування на їх основі. Проте особливості побудови самих моделей СЕТ-операцій не розглядалися. Побудова дискретних моделей СЕТ-операцій пов'язана з складністю опису лінійних і нелінійних перетворень за допомогою єдиного математичного апарату достатньо складна і не завжди ефективна [7]. Серед нелінійних СЕТ-операцій особливе місце займають операції керовані інформацією [7]. Адже саме застосування СЕТ-операцій забезпечує подвійне управління процесом шифрування. Результат шифрування буде залежати як від криптографічного ключа, так і від інформації, яка зашифровується.

Відповідно до [7] СЕТ-операції керовані інформацією поділяються на СЕТ-операції перестановок керованих інформацією і СЕТ-операції на основі елементарних функцій керованих інформацією.

Стаття [8] присвячена синтезу дискретно-алгебраїчних моделей елементарних функцій операцій керованих інформацією. В статті [9] запропоновано використовувати дискретно-казуальне представлення моделей елементарних функцій і СЕТ-операцій. Результати дискретно-казуального моделювання СЕТ-операції перестановок керованих інформацією наведені в [10]. В роботах [7-10] відмічається що побудова всіх СЕТ-операцій і елементарних функцій керованих інформацією починається з визначення ключового елементу моделі (вхідної змінної яке забезпечує управління процесом перетворення).

Однозначність визначення ключового елементу приводить до однозначності побудови СЕТ-операцій для прямого і оберненого криптографічного перетворення.

Проте в елементаних функціях операцій керованих інформацією ключовим елементом може бути будь яка вхідна змінна, що повинно привести до збільшення кількості моделей і криптографічного перетворення і розширенні можливостей при моделювання СЕТ-операцій.

Метою роботи є розробка методу багатоваріантного синтезу дискретно-казуальних моделей елементарних функцій операцій керованих інформацією який розширить можливості проектування мало ресурсних пристроїв реалізації СЕТ-операцій для побудови криптографічних систем з подвійним управлінням процесом шифрування.

Основний матеріал

Група елементарних функцій операцій керованих інформацією включає в себе 8 елементарних функцій [11]. Дискретні моделі даних елементарних функцій наведені в табл. 1. Індекс елементарної функції відповідають значенню десяткової цифри результату перетворення її двійкового коду згідно упорядкованої таблиці істинності.

Таблиця 1 – **Елементарні функції операцій, керованих інформацією**

Елементарна функція	Елементарна функція
$f_{23}(x) = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3$	$f_{232}(x) = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$
$f_{43}(x) = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$	$f_{212}(x) = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$
$f_{77}(x) = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$	$f_{178}(x) = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$
$f_{113}(x) = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3$	$f_{142}(x) = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$

Серед наведених в табл.1 елементарних функцій 4 елементарні функції будуть прямими і 4 елементарні функції інверсними. Пряма і відповідна їй інверсна елементарні функції знаходяться в одному рядку табл.1. Для елементарних функцій операцій керованих інформацією невідомо які з них будуть прямими, а які інверсними. Тому умовно визначимо в якості прямих елементарних функцій елементарні функції з меншими індексами, які представлені в першому стовпці табл. 1.

На основі моделей елементарних функцій представлених в табл. 1 можна зробити висновок, що пряма елементарна функція відрізняється від інверсної інверсією відповідних Сі-кванті. Якщо, відома пряма елементарна функція, то побудувати інверсну можна інвертуванням і ній Сі квантів x_1, x_2 і x_3. Наприклад: інвертувавши вхідні Сі-кванти в функції $f_{43}(x) = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$, отримаємо $f_{212}(x) = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$. І навпаки, при інвертуванні вхідних Сі-квантів в інверсній елементарній функції буде отримана пряма елементарна функція. Побудову інверсної елементарної функції операції керованої інформацією можна представити:

$$f_i(x) \oplus 1 = f_i(\bar{x}) = f_j(x), \qquad (1)$$

де $\oplus$ – додавання за модулем 2; $j = \bar{i}$ – десяткове представлення інверсного двійкового коду десяткового числа i.

Елементарна функція операції керованої інформацією реалізує вибір результату логічного множення, або логічного додавання двох Сі-квантів вхідної інформації в залежності вад значення третього Сі-канта інформації.

Під Сі-квантом інформації підрозумівається мінімальний обсяг інформації з яким оперує СЕТ-операція (біт, байт, слово,…) [6].

Використаємо дискретно-казуальне представлення моделей елементарних функцій операцій керованих інформацією [9].

Наприклад,

$$f_{23}(x) = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3 =$$
$$= \begin{Bmatrix} x_2 \cdot x_3, \ якщо\ x_1 = 0 \\ x_2 \vee x_3, \ якщо\ x_1 = 1 \end{Bmatrix} = (x_2 \cdot x_3)(x_1)(x_2 \vee x_3).$$

Результати побудови елементарних функцій операцій керованих інформацією наведені в табл. 2.

Таблиця 2 – **Елементарні функції операцій керованих інформацією**

Елементарна функція	Елементарна функція
$f_{23}(x) = (x_2 \cdot x_3)(x_1)(x_2 \vee x_3)$	$f_{232}(x) = (\bar{x}_2 \vee \bar{x}_3)(x_1)(\bar{x}_2 \cdot \bar{x}_3)$
$f_{43}(x) = (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3)$	$f_{212}(x) = (\bar{x}_2 \vee x_3)(x_1)(\bar{x}_2 \cdot x_3)$
$f_{77}(x) = (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3)$	$f_{178}(x) = (x_2 \vee \bar{x}_3)(x_1)(x_2 \cdot \bar{x}_3)$
$f_{113}(x) = (x_2 \vee x_3)(x_1)(x_2 \cdot x_3)$	$f_{142}(x) = (\bar{x}_2 \cdot \bar{x}_3)(x_1)(\bar{x}_2 \vee \bar{x}_3)$

Аналіз табл. 2. показав, що елементарні функції $f_{113}(x)$ і $f_{142}(x)$ доречно поміняти місцями, що забезпечить наявність всіх варіантів інверсії Сі-квантів x_2 і x_3. В результаті перестановки між стовпцями функції $f_{113}(x)$ і $f_{142}(x)$, в першому стовпці при нульовому значення змінної x_1 буде виконуватися логічне множення Сі-квантів, а при одиничному значенні логічне додавання Сі квантів. В другому стовпці навпаки, при нульовому значення змінної x_1 буде виконуватися логічне додавання Сі-квантів, а при одиничному значенні логічне множення Сі-квантів.

Дискретно-казуальні моделі мають властивість: інверсія результату реалізації функції управління приведе до перестановки місцями функцій перетворення [10]:

$$f(x) = (f_1(x))(f_2(x))(f_3(x)) = (f_3(x))(\overline{f_2(x)})(f_1(x), \qquad (2)$$

де $f_1(x)$, $f_2(x)$, $f_3(x)$ – будь які дискретні функції.

З врахуванням перестановки функції $f_{113}(x)$ і $f_{142}(x)$, і властивості (2) отримаємо елементарні функції операцій керованих інформацією, представлені в табл. 3. Упорядкована послідовність формування інверсій вхідних Сі-квантів наведена в табл. 4.

Таблиця 3 – **Елементарні функції операцій керованих інформацією**

Елементарна функція	Елементарна функція
$f_{23}(x) = (x_2 \cdot x_3)(x_1)(x_2 \vee x_3)$	$f_{232}(x) = (\bar{x}_2 \cdot \bar{x}_3)(\bar{x}_1)(\bar{x}_2 \vee \bar{x}_3)$
$f_{43}(x) = (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3)$	$f_{212}(x) = (\bar{x}_2 \cdot x_3)(\bar{x}_1)(\bar{x}_2 \vee x_3)$
$f_{77}(x) = (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3)$	$f_{178}(x) = (x_2 \cdot \bar{x}_3)(\bar{x}_1)(x_2 \vee \bar{x}_3)$
$f_{142}(x) = (\bar{x}_2 \cdot \bar{x}_3)(x_1)(\bar{x}_2 \vee \bar{x}_3)$	$f_{113}(x) = (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3)$

Після формування набору інверсій будується модель елементарної функції операції керованої інформацією. Виходячи з цього табл. 4 можна назвати таблицею синтезу елементарних функції.

Отримані в табл. 4 перші 4 елементарні функції будуть прямими, а наступні інверсними. Взаємозв'язок між прямими і інверсними елементарними функціями визначається відповідно до виразу (1),

або як: $№_{пр} + №_{ін} = 7$, де $№_{пр}$ – порядковий номер прямої елементарної функції ($№_{пр} \in \{0,.., 3\}$); $№_{ін}$ – порядковий номер інверсної елементарної функції ($№_{ін} \in \{4,.., 7\}$).

Таблиця 4 – **Таблиця синтезу елементарних функцій**

№ п/п	Код цифри			Сі-кванти			Синтезована елементарна функція
				x_1	x_2	x_3	
0	0	0	0	x_1	x_2	x_3	$f_{23}(x) = (x_2 \cdot x_3)(x_1)(x_2 \vee x_3)$
1	0	0	1	x_1	x_2	$\bar{x}_3$	$f_{43}(x) = (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3)$
2	0	1	0	x_1	$\bar{x}_2$	x_3	$f_{77}(x) = (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3)$
3	0	1	1	x_1	$\bar{x}_2$	$\bar{x}_3$	$f_{142}(x) = (\bar{x}_2 \cdot \bar{x}_3)(x_1)(\bar{x}_2 \vee \bar{x}_3)$
4	1	0	0	$\bar{x}_1$	x_2	x_3	$f_{113}(x) = (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3)$
5	1	0	1	$\bar{x}_1$	x_2	$\bar{x}_3$	$f_{178}(x) = (x_2 \cdot \bar{x}_3)(\bar{x}_1)(x_2 \vee \bar{x}_3)$
6	1	1	0	$\bar{x}_1$	$\bar{x}_2$	x_3	$f_{212}(x) = (\bar{x}_2 \cdot x_3)(\bar{x}_1)(\bar{x}_2 \vee x_3)$
7	1	1	1	$\bar{x}_1$	$\bar{x}_2$	$\bar{x}_3$	$f_{232}(x) = (\bar{x}_2 \cdot \bar{x}_3)(\bar{x}_1)(\bar{x}_2 \vee \bar{x}_3)$

Унікальність елементарних функцій операцій керованих інформацією полягає в тому що будь який вхідний Сі-квант: x_1, x_2, або x_3, може бути управляючим.

Продемонструємо це на прикладі $f_{23}(x)$. Функціональні схеми реалізації елементарної функції $f_{23}(x)$, в залежності від вибраних Сі-квантів управління наведені на рис. 1 –3.

Як видно з рис. 1 –3 Функціональні схеми реалізації елементарної функції $f_{23}(x)$ відрізняються лише нумерацією вхідних Сі-квантів.

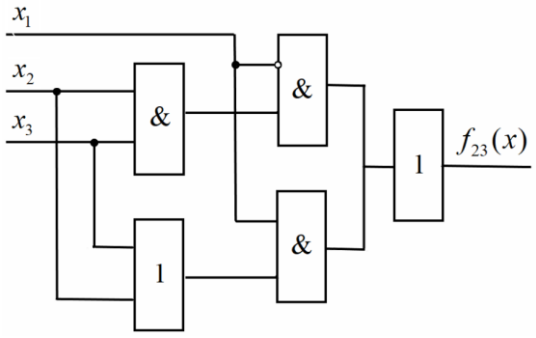

Рис. 1. Функція $f_{23}(x)$ при управлінні на основі x_1

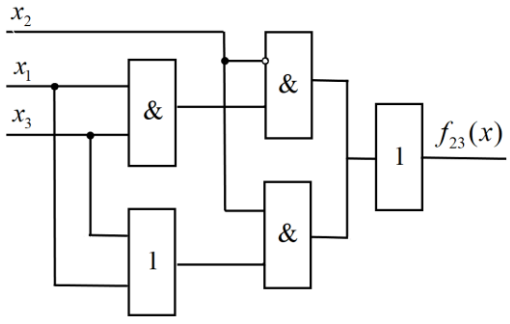

Рис. 2. Функція $f_{23}(x)$ при управлінні на основі x_2

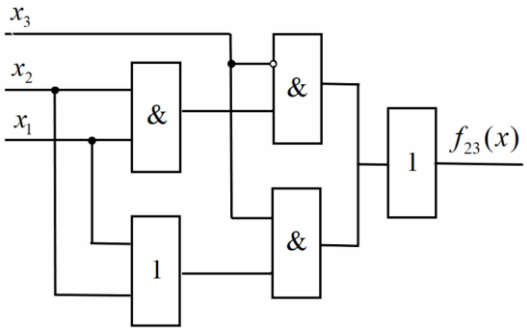

Рис. 3. Функція $f_{23}(x)$ при управлінні на основі x_3

Для елементарної функції $f_{23}(x)$ отримаємо:

$$f_{23} = (x_2 \cdot x_3)(x_1)(x_2 \vee x_3); \quad (3)$$

$$f_{23} = (x_1 \cdot x_3)(x_2)(x_1 \vee x_3); \quad (4)$$

$$f_{23} = (x_1 \cdot x_2)(x_3)(x_1 \vee x_2). \quad (5)$$

На основі моделей (3) – (5) можна зробити висновок, що три модифікації елементарної функції операцій керованих інформацією можна на основі трьох перестановок:

$$\tilde{x}_1 \leftrightarrow \tilde{x}_1; \ \tilde{x}_1 \leftrightarrow \tilde{x}_2; \ \tilde{x}_1 \leftrightarrow \tilde{x}_3. \quad (6)$$

Позначка над i-ю змінною $\tilde{x}_i$ в моделі (6) – змінні переставляються разом з наявними інверсіями.

Синтез елементарних функцій операцій керованих інформацією відповідно до табл..4 і послідовна реалізація над кожною з них моделей перестановок (6) забезпечує багатоваріантну побудову повної множини елементарних функцій операцій керованих інформацією. Даний результат можна трактувати як метод багатоваріантного синтезу дискретно-казуальних моделей елементарних функцій операцій керованих інформацією. За результатами реалізації даного методу буде побудовано 24 дискретно-казуальні моделі елементарних функцій операцій керованих інформацією, які наведені в табл.5.

Таблиця 5 – **Багатоваріантні модної елементарних функцій операцій керованих інформацією**

Елементарна функція	Елементарна функція
$f_{23}(x) = (x_2 \cdot x_3)(x_1)(x_2 \vee x_3)$	$f_{232}(x) = (\bar{x}_2 \cdot \bar{x}_3)(\bar{x}_1)(\bar{x}_2 \vee \bar{x}_3)$
$f_{23}(x) = (x_1 \cdot x_3)(x_2)(x_1 \vee x_3)$	$f_{232}(x) = (\bar{x}_1 \cdot \bar{x}_3)(\bar{x}_2)(\bar{x}_1 \vee \bar{x}_3)$
$f_{23}(x) = (x_1 \cdot x_2)(x_3)(x_1 \vee x_2)$	$f_{232}(x) = (\bar{x}_1 \cdot \bar{x}_2)(\bar{x}_3)(\bar{x}_1 \vee \bar{x}_2)$
$f_{43}(x) = (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3)$	$f_{212}(x) = (\bar{x}_2 \cdot x_3)(\bar{x}_1)(\bar{x}_2 \vee x_3)$
$f_{43}(x) = (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3)$	$f_{212}(x) = (\bar{x}_1 \cdot x_3)(\bar{x}_2)(\bar{x}_1 \vee x_3)$
$f_{43}(x) = (x_1 \cdot x_2)(\bar{x}_3)(x_1 \vee x_2)$	$f_{212}(x) = (\bar{x}_1 \cdot \bar{x}_2)(x_3)(\bar{x}_1 \vee \bar{x}_2)$
$f_{77}(x) = (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3)$	$f_{178}(x) = (x_2 \cdot \bar{x}_3)(\bar{x}_1)(x_2 \vee \bar{x}_3)$
$f_{77}(x) = (x_1 \cdot x_3)(\bar{x}_2)(x_1 \vee x_3)$	$f_{178}(x) = (\bar{x}_1 \cdot \bar{x}_3)(x_2)(\bar{x}_1 \vee \bar{x}_3)$
$f_{77}(x) = (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2)$	$f_{178}(x) = (\bar{x}_1 \cdot x_2)(\bar{x}_3)(\bar{x}_1 \vee x_2)$
$f_{142}(x) = (\bar{x}_2 \cdot \bar{x}_3)(x_1)(\bar{x}_2 \vee \bar{x}_3)$	$f_{113}(x) = (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3)$
$f_{142}(x) = (x_1 \cdot \bar{x}_3)(\bar{x}_2)(x_1 \vee \bar{x}_3)$	$f_{113}(x) = (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3)$
$f_{142}(x) = (x_1 \cdot \bar{x}_2)(\bar{x}_3)(x_1 \vee \bar{x}_2)$	$f_{113}(x) = (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2)$

Коректність запропонованого методу підтверджується співпаданням кількості побудованих дискретно казуальних моделей з кількістю дискретно-алгебраїчних моделей наведених в [8]. Запропонований метод має меншу алгоритмічну складність порівняна з методом синтезу дискретно-алгебраїчних моделей елементарних функцій операцій керованих інформацією. Він не вимагає додаткового перетворення дискретно-алгебраїчних моделей в дискретно-казуальні моделі.

Висновки

Розроблено метод багатоваріантного синтезу дискретно-казуальних моделей елементарних функцій операцій керованих інформацією. Даний результат розширить можливості проектування мало ресурсних пристроїв реалізації СЕТ-операцій для побудови криптографічних систем з подвійним управлінням процесом шифрування.

Дискретно-казуальні моделі елементарних функцій операцій керованих інформацією порівняно з дискретно-алгебраїчними моделями суттєво зменшують складність реалізації багатоопераднихСЕТ-операцій. Збільшення кількості варіантів представлення дискретно-казуальних моделей елементарних функції дозволить спростити процес побудови СЕТ-операцій. Крім багатоваріантність дискретно-казуальних моделей елементарних функцій операцій керованих інформацією дозволяють інтегрувати їх в СЕТ-операціях сумісно з дискретно-казуальними моделями елементарних функцій перестановок керованих інформацією.

СПИСОК ЛІТЕРАТУРИ

1. 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
2. Ryan, M. (2021). Evolution of Applied Cryptography. In: Ransomware Revolution: The Rise of a Prodigious Cyber Threat. Advances in Information Security, vol 85. Springer, Cham. https://doi.org/10.1007/978-3-030-66583-8_3
3. 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
4. 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
5. Khudoykulov, Z. (2024). A Comparison of Lightweight Cryptographic Algorithms. In: Aliev, R.A., et al. 12th World Conference “Intelligent System for Industrial Automation” (WCIS-2022). WCIS 2022. Lecture Notes in Networks and Systems, vol 912. Springer, Cham. https://doi.org/10.1007/978-3-031-53488-1_36
6. Архітектура СЕТ-операцій і технології потокового шифрування. Architecture of CET-operations and stream encryption technologies: монографія / В. М. Рудницький, Н. В. Лада, Г. А. Кучук, Д. А. Підласий. – Черкаси: вид. Пономаренко Р.В., 2024. – 374 с. https://dndivsovt.com/index.php/monograph/issue/view/22/22
7. Бабенко Віра. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації / Віра Бабенко, Ольга Мельник, Руслан Мельник // Безпека інформації: наук. журнал. – Київ : НАУ, 2013. – Том 19. – № 1. – С. 56–59. https://jrnl.nau.edu.ua/index.php/Infosecurity/issue/view/220.
8. Рудницький В.М., Лада Н.В., Підласий Д.А., Мельник О. Г. Синтез дискретно-алгебраїчних моделей елементарних функцій операцій керованих інформацією. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». Київ: Київський університет імені Бориса Грінченка. Том 3 № 23 (2024): Кібербезпека: освіта, наука с. 6-16. DOI: https://doi.org/10.28925/2663-4023.2024.23.616
9. Рудницький В.М., Ларін В.В., Мельник О. Г, Підласий Д. А. Дискретно-казуальне представлення моделей елементарних функцій і СЕТ-операцій. Системи управління, навігації та зв’язку, 2023. №4 ст.96-101. DOI: doi:https://doi.org/10.26906/SUNZ.2023.4.096.
10. V. Rudnytskyi, N. Lada, V. Larin, D. Holovniak, H. Haponenko, D. Pidlasyi and T. Stabetska Discrete and casual modeling of cet-operations of data-controlled permutations. Journal of Xidian University Volume 18 – Issue 6 – June 2024 Page No: 747-767. Doi.10.37896/jxu18.6/067
11. Рудницький В. М., Бабенко В. Г., Жиляєв Д. А. Алгебраїчна структура множини логічних операцій кодування. Наука і техніка Повітряних Сил Збройних Сил України. 2011. Вип. 2 (6). С. 112–114.

Received (Надійшла) 10.09.2024
Accepted for publication (Прийнята до друку) 13.11.2024

Discrete-casual modeling of elementary functions of operations controlled by information

V. Rudnitsky, N. Lada, V. Larin, D. Pidlasy

Abstract. The article proposes a method of multivariate synthesis of discrete-casual models of elementary functions of operations controlled by information. The implementation of this method will expand the possibilities of designing low-resource devices for the implementation of SET operations for the construction of cryptographic systems with double control of the encryption process. For these information protection systems, management of the encryption process will be determined by both the key and the information to be encrypted. Discrete-casual models of elementary functions of operations controlled by information, compared to discrete-algebraic models, significantly reduce the complexity of implementing multi-operand SET operations, since their representation allows the use of Boolean function minimization methods when combined. Increasing the number of options for presenting discrete-casual models of elementary functions will allow for the implementation of several strategies for combining them to simplify the models of constructed SET operations. The multivariate nature of discrete-casual models of elementary functions of operations controlled by information allows to integrate them in SET-operations compatible with discrete-casual models of elementary functions of operations controlled permutations. Scope of use of the obtained results: mobile and stationary systems of low-resource cryptographic protection of confidential information.

Keywords: low-resource cryptography, SET encryption, information-driven operations, elementary functions, discrete-casual models, stream encryption.