УДК 004.056.55:004.312.2 **doi: 10.26906/SUNZ.2023.4.096**

В. М. Рудницький[1,3], В. В. Ларін[1], О. Г. Мельник[2], Д. А. Підласий [3]

[1] Державний НДІ випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна
[2] Черкаський інститут пожежної безпеки імені Героїв Чорнобиля, Черкаси, Україна
[3] Черкаський державний технологічний університет, Черкаси, Україна

ДИСКРЕТНО-КАЗУАЛЬНЕ ПРЕДСТАВЛЕННЯ МОДЕЛЕЙ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ І СЕТ-ОПЕРАЦІЙ

Анотація. У статті запропоновано один з перспективних напрямків розвитку малоресурсної криптографії, а саме СЕТ-шифрування. Основною перевагою СЕТ- шифрування вважається можливість створення технології побудови шифрів з заданими характеристиками. Проведений огляд літературних джерел по тематиці статті. Обґрунтовано необхідність створення в СЕТ-операціях елементарних функцій, які забезпечують лінійне і нелінійне перетворення вхідних Сі-квантів в вихідні, що приводить до складності моделей операцій. Застосування дискретно-алгебраїчного опису моделей забезпечує можливість однакового представлення, як лінійних так і нелінійних СЕТ-операцій. Запропонований дискретно-казуальний опис забезпечує спрощення моделей СЕТ-операцій без втрати інформативності, а також забезпечує можливість моделювання багатоопераднних СЕТ-операцій, які поєднують в собі як лінійні так і нелінійні одноопераднді СЕТ-операції. Дискретно алгебраїчний опис моделей виявився громіздким і не придатним для моделювання і дослідження багатоопераднних СЕТ-операцій.

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

Вступ

Постановка проблеми. На теперішній час в теорії СЕТ-шифрування класифіковано лише 3Сі-квантові СЕТ-операції. Слід додатково відмітити, що класифіковані групи операцій, описуються за допомогою різного математичного представлення. Лише застосування дискретно-алгебраїчного представлення забезпечує уніфікований опис СЕТ-операцій, але приводить до збільшення складності моделей, складності реалізації, і ускладнює їх сприйняття.

Класифікуються СЕТ-операції по кількості операндів та по кількості Сі-квантів інформації, яка кодується. В даному дослідженні обмежимося 2 і 3Сі-квантовими СЕТ-операціями, операціями, які кодують 2 або 3 Сі-кванти інформації.

Традиційно в криптографії використовується достатньо обмежений набір операцій криптографічного перетворення. Це операції додавання за модулями, підстановки, перестановки та зсуви. Також перестановки, зсуви та операції які керуються інформацією. Основною вимогою до можливості застосування будь якої операції в крипто алгоритмі є наявність операції оберненого перетворення. Застосування СЕТ-операцій дозволяє значно збільшити кількість криптографічних перетворень на основі яких будуються крипто алгоритми. Крім того, в процесі побудови та дослідження СЕТ-операцій виявляються нові принципи і підходи для побудови криптоалгоритмів.

Для сприйняття перелічених гіпотез та розуміння сутності СЕТ-операцій розглянемо приклад з якого почалося їх дослідження.

Всім відомо що традиційне потокове шифрування полягає в послідовному побітовому додаванню по модулю два інформації і псевдовипадкової (гамуючої) послідовності. В результаті виконання додаванню по модулю два, біт інформації, в залежності від значення біта псевдовипадкової послідовності залишиться незмінним, або буде інвертований. Іншими словами, над бітом інформації можуть бути виконані дві операції: операція повтору, якщо біт псевдовипадкової послідовності рівний «0», або операція інверсії, якщо біт псевдовипадкової послідовності рівний «1».

Аналіз останніх досліджень і публікацій.

Основою СЕТ-шифрування є СЕТ-операції, які будуються з елементарних функцій криптографічного перетворення [1]. Тому класифікація СЕТ-операцій взаємопов'язана з класифікацією елементарних функцій [2]. Дослідження елементарних функцій і побудованих на їх основі 3Сі-кванових СЕТ-операцій проводилось на основі класифікованих груп [2]. При цьому для кожної класифікованої групи визначався математичний апарат, який дозволяє описувати СЕТ-операції [3] – [4], а також моделювати групи класифікованих операцій [5] – [7]. На сьогоднішній день задача опису і моделювання СЕТ-операцій, побудованих на основі елементарних функцій з різних класифікованих груп не розглядалася.

Метою роботи є розробка спеціалізованої комп'ютерної системи, яка дозволить моделювати замкнені тонкостінні циліндричні оболонки та здійснювати розрахунок механічних характеристик задач пружно-деформованого стану оболонкових конструкцій із підвищеною точністю.

Основний матеріал

Відповідно до класифікації [2] група елементарних функцій перестановок має самі прості моделі:

$$f_{15} = x_1;\ f_{51} = x_2;\ f_{85} = x_3;$$
$$f_{240} = \bar{x}_1;\ f_{204} = \bar{x}_2;\ f_{170} = \bar{x}_3. \quad (1)$$

Нижні індекси в позначенні елементарних функцій відображають десяткову позначення двійкового коду, який відповідає результату перетворення, відповідно до таблиці істинності функції. Нижні інде-

 © Рудницький В. М., Ларін В. В., Мельник О. Г., Підласий Д. А., 2023

кси в позначенні аргументу, відповідають порядковому номеру Сі-кванта вхідної інформації.

На основі елементарних функцій (1) будуються СЕТ-операції перестановок Сі-квантів [5]:

$$C_{51,170,15}(x)=\begin{bmatrix} x_2 \\ \bar{x}_3 \\ x_1 \end{bmatrix};$$
$$C'_{51,170,15}(x)=C_{85,15,204}(x)=\begin{bmatrix} x_3 \\ x_1 \\ \bar{x}_2 \end{bmatrix}. \quad (2)$$

Наведений приклад СЕТ-операцій (2), для прямого і оберненого перетворення інформації показує простору представлення моделей даної групи.

Розглянемо елементарні функції побудовані на основі додавання за модулем два [5]:

$$f_{60}=x_1\oplus x_2;\ f_{90}=x_1\oplus x_3;\ f_{102}=x_2\oplus x_3;$$
$$f_{105}=x_1\oplus x_2\oplus x_3;\ f_{195}=x_1\oplus x_2\oplus 1. \quad (3)$$

На основі даних елементарних функцій (3) будуються матричні СЕТ-операції. Наприклад:

$$C_{102,105,90}(x)=\begin{bmatrix} x_2\oplus x_3 \\ x_1\oplus x_2\oplus x_3 \\ x_1\oplus x_3 \end{bmatrix};$$
$$C'_{102,105,90}(x)=C_{90,102,105}(x)=$$
$$=\begin{bmatrix} x_1\oplus x_2 \\ x_2\oplus x_3 \\ x_1\oplus x_2\oplus x_3 \end{bmatrix} \quad (4)$$

При використанні інверсних елементарних функцій, також використовується матричне представлення (лінійне), з додатковим гамуванням. Наприклад:

$$C_{102,105,165}(x)=\begin{bmatrix} x_2\oplus x_3 \\ x_1\oplus x_2\oplus x_3 \\ x_1\oplus x_3 \end{bmatrix}\oplus\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix};$$
$$C'_{102,105,165}(x)=C_{90,153,150}(x)=$$
$$=\begin{bmatrix} x_1\oplus x_2 \\ x_2\oplus x_3 \\ x_1\oplus x_2\oplus x_3 \end{bmatrix}\oplus\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}.$$

При синтезі СЕТ-операцій одночасно можуть використовуватися елементарні функції перестановок та елементарні функції побудовані на основі додавання за модулем два. Наприклад:

$$C_{102,60,51}(x)=\begin{bmatrix} x_2\oplus x_3 \\ x_1\oplus x_2 \\ x_2 \end{bmatrix};$$
$$C'_{102,105,165}(x)=C_{102,85,90}(x)=\begin{bmatrix} x_2\oplus x_3 \\ x_3 \\ x_1\oplus x_3 \end{bmatrix}. \quad (5)$$

Побудова та використання моделей даних СЕТ-операцій не викликає складності, тому що вони представляються матричними (лінійними) моделями, або матричними моделями з додатковим гамуванням. Група елементарних функцій перестановок керованих інформацією забезпечує вибір Сі-кванта результату з двох вхідних Сі-квантів. Вибір залежить від значення Сі-кванта управління [7]. Результуючий Сі-квант, може бути як прямим так і інвертованим. Наприклад:

$$f_{46}=x_1\cdot\bar{x}_2\vee x_2\cdot\bar{x}_3;\ f_{53}=x_1\cdot\bar{x}_2\vee x_2\cdot x_3;$$
$$f_{58}=\bar{x}_1\cdot x_2\vee x_1\cdot\bar{x}_3;\ f_{71}=\bar{x}_2\cdot x_3\vee x_1\cdot x_2. \quad (6)$$

На основі даних елементарних функцій будуються СЕТ-операції перестановок керованих інформацією. Дані СЕТ-операції описуються дискретними, або дискретно-алгебраїчними моделями [4]. Наприклад:

$$C_{39,58,116}(x)=\begin{bmatrix} x_2\cdot\bar{x}_3\vee x_1\cdot x_3 \\ \bar{x}_1\cdot x_2\vee x_1\cdot\bar{x}_3 \\ \bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2 \end{bmatrix};$$
$$C'_{39,58,116}(x)=C_{46,27,92}(x)=\begin{bmatrix} x_1\cdot\bar{x}_2\vee x_2\cdot\bar{x}_3 \\ x_1\cdot\bar{x}_3\vee x_2\cdot x_3 \\ \bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2 \end{bmatrix};$$
$$C_{39,58,116}(x)=\begin{bmatrix} \begin{cases} x_2 & якшо\ \ x_3=0 \\ x_1 & якшо\ \ x_3=1 \end{cases} \\ \begin{cases} x_2 & якшо\ \ x_1=0 \\ \bar{x}_3 & якшо\ \ x_1=1 \end{cases} \\ \begin{cases} x_3 & якшо\ \ x_2=0 \\ \bar{x}_1 & якшо\ \ x_2=1 \end{cases} \end{bmatrix};$$
$$C'_{39,58,116}(x)=C_{46,27,92}(x)=\begin{bmatrix} \begin{cases} x_1 & якшо\ \ x_2=0 \\ \bar{x}_3 & якшо\ \ x_2=1 \end{cases} \\ \begin{cases} x_1 & якшо\ \ x_3=0 \\ x_2 & якшо\ \ x_3=1 \end{cases} \\ \begin{cases} x_3 & якшо\ \ x_1=0 \\ \bar{x}_2 & якшо\ \ x_1=1 \end{cases} \end{bmatrix}. \quad (7)$$

При синтезі СЕТ-операцій елементарних функцій перестановок керованих інформацією можуть поєднуватися з елементарними функції перестановок, або елементарними функціями побудованими на основі додавання за модулем два.

Наприклад:

$$C_{39,85,27}(x)=\begin{bmatrix} x_2\cdot\bar{x}_3\vee x_1\cdot x_3 \\ x_3 \\ x_1\cdot\bar{x}_3\vee x_2\cdot x_3 \end{bmatrix};$$
$$C'_{39,85,27}(x)=C_{71,29,51}(x)=$$
$$=\begin{bmatrix} \bar{x}_2\cdot x_3\vee x_1\cdot x_2 \\ x_1\cdot\bar{x}_2\vee x_2\cdot x_3 \\ x_2 \end{bmatrix}; \quad (8)$$
$$C_{53,58,102}(x)=\begin{bmatrix} \bar{x}_1\cdot x_2\vee x_1\cdot x_3 \\ \bar{x}_1\cdot x_2\vee x_1\cdot\bar{x}_3 \\ x_2\oplus x_3 \end{bmatrix};$$
$$C'_{53,58,102}(x)=C_{60,27,78}(x)=$$
$$=\begin{bmatrix} x_1\oplus x_2 \\ x_1\cdot\bar{x}_3\vee x_2\cdot x_3 \\ x_1\cdot\bar{x}_3\vee\bar{x}_2\cdot x_3 \end{bmatrix}. \quad (9)$$

Розглянуті СЕТ-операції (7) – (9), включають в себе нелінійні елементарні функції перестановок керованих інформацією. Тому їх синтез і аналіз вимагають сумісного дослідження лінійних і нелінійних криптографічних перетворень [6]. На сьогоднішній день відсутні публікації про результати досліджень СЕТ-операцій, отримані на основі поєднання елементарних функцій перестановок керованих інформацією з елементарними функції перестановок (приклад (8)), або з елементарними функціями побудованими на основі додавання за модулем два (приклад (9)).

Розглянемо групу елементарних функцій операцій керованих інформацією [2]. По аналогії з елементарними функціями перестановок керованих інформацією їх доцільно представляти дискретними, або дискретно-алгебраїчними моделями.

Наприклад:

$$f_{77} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_2 \cdot x_3 & якщо \quad x_1 = 0; \\ \bar{x}_2 \vee x_3 & якщо \quad x_1 = 1; \end{cases}$$

$$f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_2 \vee x_3 & якщо \quad x_1 = 0; \\ \bar{x}_2 \cdot x_3 & якщо \quad x_1 = 1. \end{cases}$$

При побудові СЕТ-операцій дані елементарні функції можуть поєднуватися з елементарними функціями перестановок керованих інформацією. Наприклад:

$$C_{23,43,113}(x) = \begin{bmatrix} x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3 \\ x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \end{bmatrix};$$

$$C'_{23,43,113}(x) = C_{43,23,77}(x) = \begin{bmatrix} x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \\ x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \end{bmatrix}; \quad (10)$$

$$C_{23,58,113}(x) = \begin{bmatrix} x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3 \\ \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \end{bmatrix};$$

$$C'_{23,43,113}(x) = C_{46,23,77}(x) = \begin{bmatrix} x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \\ x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \end{bmatrix}. \quad (11)$$

Представимо СЕТ-операції (10) і (11) дискретно-алгебраїчними.

$$C_{23,43,113}(x) = \begin{bmatrix} \begin{cases} x_2 \cdot x_3 & якщо \quad x_1 = 0 \\ x_2 \vee x_3 & якщо \quad x_1 = 1 \end{cases} \\ \begin{cases} x_1 \cdot \bar{x}_3 & якщо \quad x_2 = 0 \\ x_1 \vee \bar{x}_3 & якщо \quad x_2 = 1 \end{cases} \\ \begin{cases} \bar{x}_1 \cdot x_2 & якщо \quad x_3 = 0 \\ \bar{x}_1 \vee x_2 & якщо \quad x_3 = 1 \end{cases} \end{bmatrix};$$

$$C'_{23,43,113}(x) = C_{43,23,77}(x) = \begin{bmatrix} \begin{cases} x_2 \cdot \bar{x}_3 & якщо \quad x_1 = 0 \\ x_2 \vee \bar{x}_3 & якщо \quad x_1 = 1 \end{cases} \\ \begin{cases} x_1 \cdot x_3 & якщо \quad x_2 = 0 \\ x_1 \vee x_3 & якщо \quad x_2 = 1 \end{cases} \\ \begin{cases} x_1 \cdot \bar{x}_2 & якщо \quad x_3 = 0 \\ x_1 \vee \bar{x}_2 & якщо \quad x_3 = 1 \end{cases} \end{bmatrix}; \quad (12)$$

$$C_{23,58,113}(x) = \begin{bmatrix} \begin{cases} x_1 \cdot x_3 & якщо \quad x_2 = 0 \\ x_1 \vee x_3 & якщо \, x_2 = 1 \end{cases} \\ \begin{cases} x_2 & якщо \quad x_1 = 0 \\ \bar{x}_3 & якщо \quad x_1 = 1 \end{cases} \\ \begin{cases} \bar{x}_1 \cdot x_2 & якщо \quad x_3 = 0 \\ \bar{x}_1 \vee x_2 & якщо \quad x_3 = 1 \end{cases} \end{bmatrix};$$

$$C'_{23,58,113}(x) = C_{46,23,77}(x) = \begin{bmatrix} \begin{cases} x_1 & якщо \quad x_2 = 0 \\ \bar{x}_3 & якщо \quad x_2 = 1 \end{cases} \\ \begin{cases} x_1 \cdot x_3 & якщо \quad x_2 = 0 \\ x_1 \vee x_3 & якщо \quad x_2 = 1 \end{cases} \\ \begin{cases} x_1 \cdot \bar{x}_2 & якщо \quad x_3 = 0 \\ x_1 \vee \bar{x}_2 & якщо \quad x_3 = 1 \end{cases} \end{bmatrix}. \quad (13)$$

При синтезі СЕТ-операцій елементарні функцій операції керованих інформацією можуть поєднуватися з елементарними функціями розширеного матричного криптографічного перетворення. До групи елементарних функцій розширеного матричного криптографічного перетворення належать елементарні функції отримані шляхом додавання по модулю два до елементарної функції перестановки нелінійного доданку. Наприклад:

$$f_{30} = x_1 \oplus (x_2 \cdot x_2);$$

$$f_{57} = x_2 \oplus (x_1 \cdot \bar{x}_3);$$

$$f_{106} = x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2).$$

$$C_{30,57,106}(x) = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix};$$

$$C'_{30,57,106}(x) = C_{45,54,106}(x) = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}; \quad (14)$$

$$C_{30,77,120}(x) = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_2) \\ x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix};$$

$$C^{/}_{30,77,120}(x) = C_{43,108,54}(x) = \begin{bmatrix} x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \end{bmatrix}. \quad (15)$$

Дискретно-алгебраїчні моделі СЕТ-операцій (14) і (15) можна представити.

$$C_{30,57,106}(x) = \begin{bmatrix} \begin{cases} x_2 \cdot x_3 & якщо \ \ x_1 = 0 \\ \overline{x_2 \cdot x_3} & якщо \ \ x_1 = 1 \end{cases} \\ \begin{cases} x_1 \cdot \bar{x}_3 & якщо \ \ x_2 = 0 \\ \overline{x_1 \cdot \bar{x}_3} & якщо \ \ x_2 = 1 \end{cases} \\ \begin{cases} \bar{x}_1 \cdot \bar{x}_2 & якщо \ \ x_3 = 0 \\ \overline{\bar{x}_1 \cdot \bar{x}_2} & якщо \ \ x_3 = 1 \end{cases} \end{bmatrix};$$

$$C^{/}_{30,57,106}(x) = C_{45,54,1067}(x) = \begin{bmatrix} \begin{cases} x_2 \cdot \bar{x}_3 & если \ \ x_1 = 0 \\ \overline{x_2 \cdot \bar{x}_3} & если \ \ x_1 = 1 \end{cases} \\ \begin{cases} x_1 \cdot x_3 & если \ \ x_2 = 0 \\ \overline{x_1 \cdot x_3} & если \ \ x_2 = 1 \end{cases} \\ \begin{cases} \bar{x}_1 \cdot \bar{x}_2 & якщо \ \ x_3 = 0 \\ \overline{\bar{x}_1 \cdot \bar{x}_2} & якщо \ \ x_3 = 1 \end{cases} \end{bmatrix}; \quad (16)$$

$$C_{30,77,120}(x) = \begin{bmatrix} \begin{cases} x_2 \cdot x_3 & якщо \ \ x_1 = 0 \\ \overline{x_2 \cdot x_3} & якщо \ \ x_1 = 1 \end{cases} \\ \begin{cases} \bar{x}_2 \cdot x_3 & якщо \ \ x_1 = 0 \\ \bar{x}_2 \vee x_3 & якщо \ \ x_1 = 1 \end{cases} \\ \begin{cases} \bar{x}_2 \cdot \bar{x}_3 & якщо \ \ x_1 = 0 \\ \overline{\bar{x}_2 \cdot \bar{x}_3} & якщо \ \ x_1 = 1 \end{cases} \end{bmatrix};$$

$$C^{/}_{30,77,120}(x) = C_{43,108,54}(x) = \begin{bmatrix} \begin{cases} x_1 \cdot \bar{x}_3 & якщо \ \ x_2 = 0 \\ x_1 \vee \bar{x}_3 & якщо \ \ x_2 = 1 \end{cases} \\ \begin{cases} \bar{x}_1 \cdot \bar{x}_3 & якщо \ \ x_2 = 0 \\ \overline{\bar{x}_1 \cdot \bar{x}_3} & якщо \ \ x_2 = 1 \end{cases} \\ \begin{cases} x_1 \cdot x_3 & якщо \ \ x_2 = 0 \\ \overline{x_1 \cdot x_3} & якщо \ \ x_2 = 1 \end{cases} \end{bmatrix}. \quad (17)$$

Моделі нелінійних СЕТ-операцій (10) - (17) не забезпечують простоту взаємозв'язків між операціями прямого і оберненого криптографічного перетворення, що суттєво ускладнює їх застосування в криптографічних системах.

Слід відмітити, що математичний опис даних моделей суттєво відрізняється від математичного опису моделей (2), (4) і (5).

Дискретно-алгебраїчне представлення моделей СЕТ-операцій дозволяє описати як лінійні так і нелінійні криптографічні перетворення. Наприклад, елементарні функції перестановок (1) можна представити:

$$f_{15} = x_1 = \begin{cases} x_1 & якщо \ \ x_2 = 0; \\ x_1 & якщо \ \ x_2 = 1; \end{cases} = \begin{cases} x_1 & якщо \ \ x_3 = 0; \\ x_1 & якщо \ \ x_3 = 1; \end{cases}$$

$$f_{51} = x_2 = \begin{cases} x_2 & якщо \ \ x_1 = 0; \\ x_2 & якщо \ \ x_1 = 1; \end{cases} = \begin{cases} x_2 & якщо \ \ x_3 = 0; \\ x_2 & якщо \ \ x_3 = 1; \end{cases}$$

$$f_{85} = x_3 = \begin{cases} x_3 & якщо \ \ x_1 = 0; \\ x_3 & якщо \ \ x_1 = 1; \end{cases} = \begin{cases} x_3 & якщо \ \ x_2 = 0; \\ x_3 & якщо \ \ x_2 = 1; \end{cases}$$

$$f_{240} = \bar{x}_1 = \begin{cases} \bar{x}_1 & якщо \ \ x_2 = 0; \\ \bar{x}_1 & якщо \ \ x_2 = 1; \end{cases} = \begin{cases} \bar{x}_1 & якщо \ \ x_3 = 0; \\ \bar{x}_1 & якщо \ \ x_3 = 1. \end{cases}$$

Елементарні функції побудовані на основі додавання за модулем два (3) можна описати наступним чином:

$$f_{60} = x_1 \oplus x_2 = \begin{cases} x_2 & якщо \ \ x_1 = 0; \\ \bar{x}_2 & якщо \ \ x_1 = 1; \end{cases} = \begin{cases} x_1 & якщо \ \ x_2 = 0; \\ \bar{x}_1 & якщо \ \ x_2 = 1; \end{cases}$$

$$f_{90} = x_1 \oplus x_3 = \begin{cases} x_3 & якщо \ \ x_1 = 0; \\ \bar{x}_3 & якщо \ \ x_1 = 1; \end{cases} = \begin{cases} x_1 & якщо \ \ x_3 = 0; \\ \bar{x}_1 & якщо \ \ x_3 = 1; \end{cases}$$

$$f_{102} = x_2 \oplus x_3 = \begin{cases} x_3 & якщо \ \ x_2 = 0 \\ \bar{x}_3 & якщо \ \ x_2 = 1 \end{cases} = \begin{cases} x_2 & якщо \ \ x_3 = 0 \\ \bar{x}_2 & якщо \ \ x_3 = 1 \end{cases}$$

$$f_{105} = x_1 \oplus x_2 \oplus x_3 = \begin{cases} x_2 \oplus x_3 & якщо \ \ x_1 = 0; \\ \overline{x_2 \oplus x_3} & якщо \ \ x_1 = 1; \end{cases} = \begin{cases} x_1 \oplus x_3 & якщо \ \ x_2 = 0; \\ \overline{x_1 \oplus x_3} & якщо \ \ x_2 = 1; \end{cases} = \begin{cases} x_1 \oplus x_2 & якщо \ \ x_3 = 0; \\ \overline{x_1 \oplus x_2} & якщо \ \ x_3 = 1; \end{cases}$$

$$f_{195} = x_1 \oplus x_2 \oplus 1 = \begin{cases} \bar{x}_2 & якщо \;\; x_1 = 0; \\ x_2 & якщо \;\; x_1 = 1; \end{cases} =$$

$$= \begin{cases} \bar{x}_1 & якщо \;\; x_2 = 0; \\ x_1 & якщо \;\; x_2 = 1. \end{cases}$$

Наведені моделі елементарних функцій свідчать про те що будь яку СЕТ-операцію дискретно-алгебраїчною моделлю. Проте дискретно-алгебраїчні моделі СЕТ-операцій достатньо громіздкі (складні) і ускладнюють пошук взаємозв'язків між прямими і оберненими операціями, а також взаємозв'язків в групах СЕТ-операцій.

Вирішити протиріччя між розширенням можливості однотипного опису СЕТ-операцій і зменшенням складності самих моделей полягає в представлення СЕТ-операцій як адаптованого дискретного аналога опису системи ситуаційного управління.

В ситуаційному управління стан системи описується за допомогою трьох подій

$$(A; B; C),$$

де A – подія яка передувала події B, B – подія яка реалізується в даний час, C – подія яка буде реалізована лише після успішного завершення події B [8]. Опишемо стан дискретної системи управління наступним чином: в залежності від результату завершення події B буде реалізована подія A, або подія С. Нехай події A, B і C представляють собою реалізацію дискретних функцій $f_1(x)$, $f_2(x)$ і $f_3(x)$. Для спрощення сприйняття дискретної функції як набору її трьох складових, доцільно кожну складову взяти в дужки. В результаті отримаємо модель:

$$f(x) = (f_1(x))(f_2(x))(f_3(x)) \qquad (18)$$

Модель (18) трактується наступним чином: в залежності від результату виконання функції $f_2(x)$ буде реалізована функція $f_1(x)$, або $f_3(x)$. Для однозначного трактування моделі (18) будемо вважати, що за умови $f_2(x) = 0$ буде виконуватися функція $f_1(x)$, інакше буде виконуватися функція $f_3(x)$.

Модель (18) будемо називати дискретно-казуальною моделлю.

Слід відмітити що в дискретно-казуальній моделі (18) функції $f_1(x)$, $f_2(x)$ і $f_3(x)$ можуть бути представлені дискретно-казуальними моделями.

Дискретно-казуальний опис дає можливість спростити дискретно-алгебраїчні моделі елементарних функцій і СЕТ-операцій.

Дискретно казуальний метод дозволяю описувати розглянуті раніше моделі СЕТ-операцій.

СЕТ-операції з використанням елементарних функцій перестановок керованих інформацією. Наприклад моделі (7) – (8).

$$C_{39,58,116}(x) = \begin{bmatrix} (x_2)(x_3)(x_1) \\ (x_2)(x_1)(\bar{x}_3) \\ (x_3)(x_2)(\bar{x}_1) \end{bmatrix};$$

$$C'_{39,58,116}(x) = C_{46,27,92}(x) = \begin{bmatrix} (x_1)(x_2)(\bar{x}_3) \\ (x_1)(x_3)(x_2) \\ (x_3)(x_1)(\bar{x}_2) \end{bmatrix};$$

$$C_{39,85,27}(x) = \begin{bmatrix} (x_2)(x_3)(x_1) \\ (x_3)(x_1)(x_3) \\ (x_1)(x_3)(x_2) \end{bmatrix};$$

$$C'_{39,85,27}(x) = C_{71,29,51}(x) = \begin{bmatrix} (x_3)(x_2)(\bar{x}_1) \\ (x_1)(x_2)(x_3) \\ (x_2)(x_1)(x_2) \end{bmatrix}.$$

СЕТ-операції з використанням елементарних функцій операцій керованих інформацією. Наприклад моделі (12) і (13):

$$C_{23,43,113}(x) = \begin{bmatrix} (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \end{bmatrix};$$

$$C'_{23,43,113}(x) = C_{43,23,77}(x) =$$

$$= \begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2) \end{bmatrix};$$

$$C_{23,58,113}(x) = \begin{bmatrix} (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (x_1)(x_2)(\bar{x}_1) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \end{bmatrix};$$

$$C'_{23,58,113}(x) = C_{46,23,77}(x) =$$

$$= \begin{bmatrix} (x_2)(x_1)(\bar{x}_3) \\ (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2) \end{bmatrix}.$$

СЕТ-операції з використанням елементарних функцій розширеного матричного криптографічного перетворення. Наприклад моделі (16) і (17).

$$C_{30,57,106}(x) = \begin{bmatrix} (x_2 \cdot x_3)(x_1)(\overline{x_2 \cdot x_3}) \\ (x_1 \cdot \bar{x}_3)(x_2)(\overline{x_1 \cdot \bar{x}_3}) \\ (\bar{x}_1 \cdot \bar{x}_2)(x_3)(\overline{\bar{x}_1 \cdot \bar{x}_2}) \end{bmatrix};$$

$$C'_{30,57,1063}(x) = C_{45,54,106}(x) =$$

$$= \begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \cdot \bar{x}_3) \\ (x_1 \cdot x_3)(x_2)(\overline{x_1 \cdot x_3}) \\ (\bar{x}_1 \cdot \bar{x}_2)(x_2)(\overline{\bar{x}_1 \cdot \bar{x}_2}) \end{bmatrix}.$$

$$C_{30,77,120}(x) = \begin{bmatrix} (x_2 \cdot x_3)(x_1)(\overline{x_2 \cdot x_3}) \\ (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (\bar{x}_2 \cdot \bar{x}_3)(x_1)(\overline{\bar{x}_2 \cdot \bar{x}_3}) \end{bmatrix};$$

$$C'_{30,77,120}(x) = C_{43,108,54}(x) = \begin{bmatrix} (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) \\ (\bar{x}_1 \cdot \bar{x}_3)(x_2)(\overline{\bar{x}_1 \cdot \bar{x}_3}) \\ (x_1 \cdot x_3)(x_2)(\overline{x_1 \cdot x_3}) \end{bmatrix}.$$

Наведені дискретно-казуальні моделі СЕТ-операцію підтверджують гіпотезу про можливість на їх основі уніфікувати опис лінійних і нелінійних операцій криптографічного перетворення інформації.

Дані моделі спрощують подальший процес дослідження груп СЕТ-операцій.

Необхідно відмітити, що дискретно-казуальне представлення дискретних функцій створює можливість будувати багатоопернадні СЕТ-операції, моделі яких поєднують в собі кортежі нелінійних, або лінійних і нелінійних СЕТ-операцій.

Дане застосування дискретно-казуального моделювання є особливо перспективним.

На сьогоднішній день відомі моделі багатоопернадних операцій які реалізують кортежі лінійних одноопернадних СЕТ-операцій. Моделі даних СЕТ операцій будуються на основі додавання за модулем.

Висновки

В процесі дослідження класифікованих груп 3Сі-кванових елементарних функцій було встановлено що групи елементарних функцій і як наслідок групи СЕТ-операцій моделюються різним математичним апаратом.

Поєднання в СЕТ-операціях елементарних функцій, які забезпечують лінійне і нелінійне перетворення вхідних Сі-квантів в вихідні приводить до складності моделей операцій. Застосування дискретно-алгебраїчного опису моделей забезпечує можливість однакового представлення як лінійні так і нелінійні СЕТ-операцій. Дискретно алгебраїчного опису моделей виявився громіздким і не придатним для моделювання і дослідження багатоопернадних СЕТ-операцій. Запропонований дискретно-казуальний опис забезпечує спрощення моделей СЕТ-операцій без втрати інформативності, а також забезпечує можливість моделювання багатоопернадних СЕТ-операцій, які поєднують в собі як лінійні так і нелінійні одноопернадні СЕТ-операції. Подальші дослідження будуть направлені на розробку методів синтезу багатоопернадних СЕТ-операцій і груп операцій з використанням дискретно-казуального представлення моделювання.

СПИСОК ЛІТЕРАТУРИ

1. Рудницький В. М., Лада Н.В., Мельник О. Г. Класифікація СЕТ-операцій. Проблеми інформатизації Тези доповідей одинадцятої міжнародної науково-технічної конференції (16-17 листопада 2023 року) Том 2: секції 3, 6 Баку – Харків – Бельсько-Бяла. 2023 с.35.
2. 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.
3. Синтез елементарних функцій перестановок, керованих інформацією / В. М. Рудницький, Т. В. Миронюк, О. Г. Мельник, В. П. Щербина // Безпека інформації. – Т. 20, № 3. – Київ : НАУ, 2014. – С. 242–247.
4. Бабенко В. Г. Дослідження способів запису трьохрозрядних криптографічних операцій / В. Г. Бабенко, Р. П. Мельник, С. В. Рудницький // Системи управління, навігації та зв'язку : зб. наук. праць. – Вип. 1 (21), т. 2. – К. : Центр. наук.-досл. ін-т навігації і управл., 2012. – С. 170–173.
5. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. Зб. наук. пр. Харків. ун-ту Повітряних Сил. Харків: ХУПС ім. І. Кожедуба, 2012. Вип. 4 (33). С. 198–200.
6. Бабенко В. Г., Мельник О. Г., Стабецька Т. А. Синтез нелінійних операцій криптографічного перетворення. Безпека інформації. 2014. Т. 20. №2. С. 143–147.
7. Миронюк Т. В. Визначення елементарних операцій базової групи перестановок, керованих інформацією / Т. В. Миронюк // Вісник Черкаського державного технологічного університету. – 2016. – № 2. - С. 100–105.
8. Поспелов Д. А. Ситуационное управление : Теория и практика / Поспелов Д. А. – М. : Наука, 1986.

Received (Надійшла) 01.10.2023
Accepted for publication (Прийнята до друку) 29.11.2023

Discrete-casual presentation of models of elementary functions and set operations

V. Rudnitsky, V. Larin, O. Melnyk, D. Pidlasy

Abstract. The article proposes one of the promising directions for the development of low-resource cryptography, namely SET-encryption. The main advantage of SET encryption is the possibility of creating a technology for building ciphers with specified characteristics. A review of literary sources on the topic of the article was conducted. The need to create elementary functions in SET operations that provide linear and non-linear transformation of input C-quants into outputs is substantiated, which leads to the complexity of operation models. The use of a discrete-algebraic description of models provides the possibility of the same presentation of both linear and non-linear SET operations. The proposed discrete-casual description provides simplification of models of SET operations without loss of informativeness, and also provides the possibility of modeling multi-operand SET operations, which combine both linear and nonlinear single-operand SET operations. The discrete algebraic description of the models turned out to be cumbersome and not suitable for modeling and researching multi-operand SET operations.

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