Особенностью этой функции является бинарный характер ее значений.

С точки зрения характеристической функции нечеткие множества есть естественное обобщение обычных множеств, когда мы отказываемся от бинарного характера этой функции и предполагаем, что она может принимать любые значения на отрезке [0,1]. В теории нечетких множеств характеристическая функция называется функцией. принадлежности, а ее значение $\mu_A(x)$ – степенью принадлежности элемента *x* нечеткому множеству *A*.

Более строго, нечетким множеством *A* называется совокупность пар

$$A = \{\langle x, \mu_A(x)\rangle \mid x \in U\},$$

где μ_A – функция принадлежности, т. е. $\mu_A : U \to [0,1]$.

Итого, в нашу оптимизационную задачу необходимо включить нечеткую функцию принадлежности элементов тренировочного набора $\mu_A(x)$. В результате «шумы» будут иметь меньшую степень принадлежности, чем корректные значения, и суть задачи в необходимости построения гиперплоскости *H*, разделяющей два нечетких множества.

В работе рассматривались вопросы применения методов интеллектуального анализа данных (Data Mining) для одной из задач обеспечения компьютерной безопасности – задачи выявления вторжений в компьютерные системы. Поскольку традиционные сигнатурные методы не обеспечивают должного уровня защиты, использование Data Mining методов в СОВ является активно развивающимся направлением. Основное внимание в работе уделено методам анализа данных на основе потенциальных функций, которые перспективны для данного направления.

Информация, которая может быть основой построения описанных методов, может быть подана в разных формах, например, в виде трудно объяснимых проблем в компьютерных системах, диапазонов пороговых значений, параметров входного/выходного трафика, непредусмотренных адресов пакетов, атрибутов, временных параметров, запросов и т. д.

Однако следует помнить, что реализация описанной методики построения СОВ вряд ли заменит промышленную полнофункциональную систему, с многолетним опытом работы на рынке безопасности. В цикле статей [1, 2] и данной статье предлагается лишь дополнить функциональность системы SiteProtector дополнительным эвристическим модулем обнаружения атак на случай появления атаки, по каким либо причинам не внесенной в базу данных сигнатур атак.

Література: ***1.*** *Голяка А. Таксономия, тенденции развития систем обнаружения вторжений. «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні»* ***2.*** *Голяка А. Архитектура, взаимодействие компонентов, преимущества siteprotector. «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні»* ***3.*** *Eleazar Eskin Christina Leslie and William Stafford Noble. The spectrum kernel: A string kernel for SVM protein classification. In Proceedings of the Pacific Symposium on Biocomputing (PSB-2002), Kaua'I, Hawaii, 2002.* ***4.*** *N. Cristianini and J. Share-Taylor. An Introduction to Support Vector Machines. Cambridge University Press, Cambridge, UK, 2000.* ***5.*** *D. E. Denning. An intrusion detection model. IEEE Transactions o Software Engineering, SE-13:222-232, 1987.* ***6.*** *W. Fan and S. Stolfo. Ensemble-based adaptive intrusion detection. In Proceeding of 2002 SIAM International Conference on Data Mining, Arlington, VA, 2002.* ***7.*** *K. Muller, S. Mika, G. Ratsch, K. Tsuda, B. Scholkopf, "An Introduction to Kernel-Based Learning Algorithms," IEEE Neural Networks, 12(2):181-201, May 2001.* ***8.*** *М. А. Айзерман, Э. М. Браверман, Л. И. Розоноэр. Метод потенциальных функций в теории обучения машин. Наука, Москва, 1970, 384 с.*

УДК 638.322

РЕАЛІЗАЦІЯ ПОВНИХ ПІДСТАНОВОК ЗА ДОПОМОГОЮ БАГАТОМОДУЛЬНОГО КАСКАДУ НАЙПРОСТІШИХ КОНСТРУКТИВНИХ МОДУЛІВ

Володимир Тарасенко, Олександр Тесленко, Олена Яновська
НТУУ «КПІ»

Анотація: **Досліджується можливість реалізації масових повних підстановок за допомогою найпростішого одновимірного каскаду конструктивних модулів.**

Summary: **A possibility of large-scal complete permutations realization with the simplest one-dimensional cascade of constructive modules is considered.**
Ключові слова: **Одновимірний каскад конструктивних модулів, повні підстановки, масові підстановки.**

Вступ

Розвиток технології ПЛІС [1, 2] зробив можливою реалізацію в мікросхемах фактично довільного проекту спеціалізованих комп'ютерних засобів за короткий проміжок часу. Це спонукає до розробки методів та інженерних методик створення апаратних засобів спеціалізованих обчислень, практичне використання яких раніше було не завжди економічно доцільним. Сюди можна віднести засоби для реалізації результатів досліджень в таких розділах математики як скінчені групи та скінчені поля, які мають важливе практичне значення, наприклад, у завадостійкому кодуванні при передачі інформації каналами зв'язку, ущільненні даних, в криптографічних перетвореннях та ін. Прикладом таких спеціалізованих обчислень є підстановки. Підстановкою називають взаємно однозначне відображення множини перших натуральних k чисел на себе [3]. Множина чисел підстановки в цьому випадку має вигляд {0,1,…k – 1}. Повною підстановкою будемо називати підстановку, для якої k=2n, де n - деяке натуральне число, що визначає розрядність підстановки.

Максимальна продуктивність апаратної реалізації спеціалізованних обчислень забезпечується з використанням комбінаційних схем. Взагалі складність комбінаційних схем зростає експоненційно зі зростанням кількості розрядів k, що може обмежити ефективну реалізацію довільних масових підстановок. Задача розробки ефективної структури для реалізації підстановок зводиться, з одного боку, до дослідження властивостей підстановок, що можуть призвести до спрощення їх апаратної реалізації, а з іншого боку – до пошуку простої технологічної структури, що дозволяє реалізувати такі підстановки. За таку структуру можна прийняти одновимірний каскад конструктивних модулів (ОККМ), структурна схема якого подана на рис. 1, де кожний конструктивний модуль (КМ), як і каскад у цілому, є комбінаційною схемою. Структура КМ подана на Рис. 2. Будемо вважати, що на первинні (не бокові) входи кожного конструктивного модуля подаються розряди двійкових кодів із монотонним зростанням номерів, а на первинних (не бокових) виходах кожного конструктивного модуля формуються значення розрядів результатів із тими самими номерами. Особливостями ОККМ є теоретична необмеженість розрядності вхідних і вихідних даних (шляхом нарощування кількості конструктивних модулів), тобто на ОККМ реалізуються масові перетворювачі інформації з лінійною залежністю складності реалізації від кількості розрядів.

Якщо кількість бокових входів і виходів із кожного боку дорівнює одиниці, то такі каскади називають простими [4]. Якщо при цьому на кожний модуль ОККМ подається один розряд вхідних даних, на виходах модуля формується один розряд результату, то такі каскади називають найпростішими. На Рис. 3 подана структура найпростішого КМ.

Теоретична можливість реалізації повних підстановок на структурах такого типу досліджувалася в [5]. Метою даної статті є розробка методики реалізації повних підстановок за допомогою найпростішого багатомодульного каскаду конструктивних модулів.

Основна частина

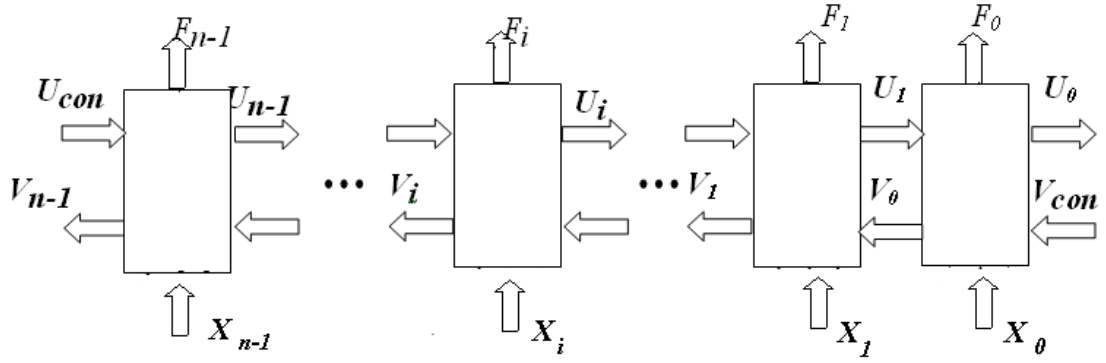

Рисунок 1– Структура ОККМ

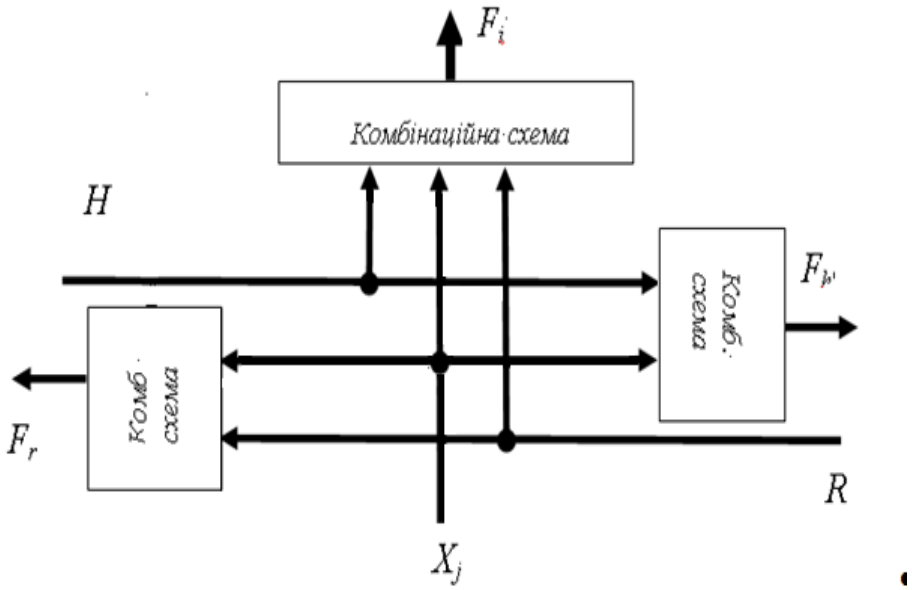

Рисунок 2 – Структура модуля каскаду ОККМ

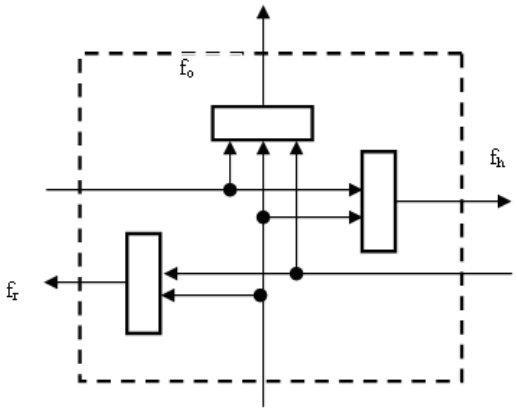

Рисунок 3 – Структура найпростішого модуля

Практичний інтерес має реалізація масових повних підстановок, тобто підстановок, значення розрядності аргументу яких пробігає деякий ряд натуральних чисел. Структура ОККМ дозволяє збільшувати розрядність вхідних даних шляхом нарощування кількості модулів, але необхідно забезпечувати реалізацію повних підстановок на кожному кроці такого нарощування. При цьому можливі наступні два варіанти. **За першим** з них новий модуль до каскаду може підключатись тільки з якоїсь однієї сторони – або зі сторони молодших розрядів, або зі сторони старших розрядів. Для подальшого це не має суттєвого значення, тому будемо вважати, що нові модулі до каскаду підключаються зі сторони старших розрядів. **За другим варіантом** нові КМ можуть підключатись як зі сторони старших, так і зі сторони молодших розрядів. У випадку найпростіших ОККМ будемо вважати, що значення розрядності пробігає ряд натуральних чисел (n=1, 2, 3,….). Доречною є наступна методика побудови та вивчення властивостей n-розрядного ОККМ: (n –1)-розрядний ОККМ розглядається як окремий (n – 1) розрядний конструктивний модуль (до певної міри ігноруючи внутрішню структуру), до якого підключається найпростіший однорозрядний КМ. Це дозволяє використати результати досліджень з реалізації повних підстановок на двомодульному каскаді, які наведені в [5] та суть яких полягає в наступному.

Простий двомодульний каскад зображений на рис. 4. Позначимо $\mathbf{X_{1,t}}$ кортеж (впорядковану послідовність) аргументів $\langle x_1, x_2, ..x_t \rangle$, що надходять на первинні входи правого модуля ОККМ (молодші розряди аргументу), аналогічно $\mathbf{X_{t+1,n}} \to \langle x_{t+1}, x_{t+2}, ...x_n \rangle$ – кортеж аргументів, що надходять на первинні входи лівого модуля (старші розряди аргументу), $\mathbf{F_{1,t}}$ – кортеж функцій $\langle f_1, f_2, .. f_t \rangle$, що реалізуються на первинних виходах правого модуля ОККМ, аналогічно $\mathbf{F_{t+1,n}} \to \langle f_{t+1}, f_{t+2}, ... f_n \rangle$ – кортеж функцій, що реалізуються на первинних виходах лівого модуля ОККМ, $\mathbf{S}_{1,t}$ – множина кодів значень аргументів із кортежа $\mathbf{X_{1,t}}$, $\mathbf{S_{t+1,n}}$ – множина кодів значень аргументів із $\mathbf{X}_{t+1,n}$

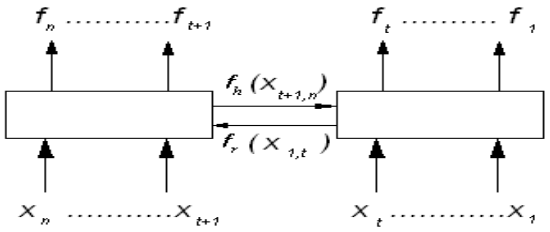

Рисунок 4 – Двомодульний каскад

Значення логічної функції $f_r\left(\mathbf{X_{1,t}}\right)$ на боковому виході правого модуля поділяє множину $\mathbf{S}_{1,t}$ на дві підмножини $\mathbf{S}_a$ і $\mathbf{S}_b$ так, що для будь-яких значень аргументів $a_1, a_2 \in \mathbf{S}_a \left(a_1 \neq a_2\right)$ значення функції $f_r\left(a_1\right) \neq f_r\left(a_2\right)$, відповідно $\mathbf{F_{t+1,n}}\left(a_1, \mathbf{X_{t+1,n}}\right) = \mathbf{F_{t+1,n}}\left(a_2, \mathbf{X_{t+1,n}}\right)$, для будь-яких $b_1, b_2 \in \mathbf{S}_b \left(b_1 \neq b_2\right)$ $f_r\left(b_1\right) \neq f_r\left(b_2\right)$, відповідно $\mathbf{F_{t+1,n}}\left(b_1, \mathbf{X_{t+1,n}}\right) = \mathbf{F_{t+1,n}}\left(b_2, \mathbf{X_{t+1,n}}\right)$, а $\mathbf{F_{t+1,n}}\left(a_1, \mathbf{X_{t+1,n}}\right) \neq \mathbf{F_{t+1,n}}\left(b_1, \mathbf{X_{t+1,n}}\right)$, $\left(f_r\left(a_1\right) \neq f_r\left(b_1\right)\right)$. Згідно з наведеним, два кортежі логічних функцій будемо вважати однаковими, якщо: 1) вони містять однакову кількість функцій; 2) функції кортежу залежать від одних і тих самих змінних; 3) функції з однаковими позиціями в кортежі рівні між собою. Аналогічно позначимо $\mathbf{S}_c$ і $\mathbf{S}_d$ підмножини кодів аргументів із $\mathbf{X_{t+1,n}}$, на які розбивається множина $\mathbf{S}_{t+1,n}$ за значенням логічної функції $f_h\left(\mathbf{X_{t+1}}, n\right)$. Шляхом декартового множення можна утворити наступні множини кодів аргументів із $\mathbf{X}$: $\mathbf{S_{ca}} = \mathbf{S_c} \times \mathbf{S_a}$, $\mathbf{S}_{d\mathbf{a}} = \mathbf{S}_d \times \mathbf{S_a}$, $\mathbf{S_{cb}} = \mathbf{S_c} \times \mathbf{S}_b$ та $\mathbf{S}_{db} = \mathbf{S}_d \times \mathbf{S}_b$. Утворені множини попарно не мають спільних елементів, а їх об'єднання дорівнює $\mathbf{S}_{1,n}$ – множині всіх кодів аргументів із $\mathbf{X}$.

Парою підстановки будемо називати впорядковану пару кодів – коду аргументу із $\mathbf{S}_{1,t}$ (або $\mathbf{S}_{t+1,n}$) та коду значень функцій (далі – коду функцій) із кортежу $\mathbf{F}_{1,t}$ (або $\mathbf{F}_{t+1,n}$). Нехай $\mathbf{P}^{\wedge}_{ca}$ - множина пар підстановки з кодами функцій із $\mathbf{F}_{1,t}\left(\mathbf{X}_{1,t}, c\right)$, коли аргументи із $\mathbf{X}_{1,t}$ приймають всі можливі коди із множини $\mathbf{S}_a$, а $\mathbf{T}^{\wedge}_{ca}$ – множина пар підстановки з кодами функцій із $\mathbf{F}_{t+1,n}\left(a, \mathbf{X}_{t+1,n}\right)$, коли аргументи із $\mathbf{X}_{t+1,n}$ приймають всі можливі коди із множини $\mathbf{S}_c$. Аналогічно визначимо множини пар підстановки $\mathbf{P}^{\wedge}_{da}$, $\mathbf{T}^{\wedge}_{da}$, $\mathbf{P}^{\wedge}_{cb}$, $\mathbf{T}^{\wedge}_{cb}$ та $\mathbf{P}^{\wedge}_{db}$, $\mathbf{T}^{\wedge}_{db}$. Указані множини пар підстановки однозначно визначають повну підстановку та кортеж функцій $\mathbf{F}\left(\mathbf{X}\right)$, які реалізує двомодульний каскад. Надалі множини $\mathbf{P}^{\wedge}$ та $\mathbf{T}^{\wedge}$ з однаковим комплектом літерних індексів будемо називати спорідненими.

Як показано в [5], якщо кортеж функцій $\mathbf{F}\left(\mathbf{X}\right)$ відтворює повну підстановку, то коди функцій пар підстановок, які містяться в одній і тій же множині пар підстановки, різні. Це дає можливість на базі множин пар підстановки $\mathbf{P}^{\wedge}_{ca}$, $\mathbf{T}^{\wedge}_{ca}$, $\mathbf{P}^{\wedge}_{da}$, $\mathbf{T}^{\wedge}_{da}$, $\mathbf{P}^{\wedge}_{cb}$, $\mathbf{T}^{\wedge}_{cb}$ та $\mathbf{P}^{\wedge}_{db}$, $\mathbf{T}^{\wedge}_{db}$ сформувати множини $\mathbf{P}_{ca}$, $\mathbf{T}_{ca}$, $\mathbf{P}_{da}$, $\mathbf{T}_{da}$, $\mathbf{P}_{cb}$, $\mathbf{T}_{cb}$ та $\mathbf{P}_{db}$, $\mathbf{T}_{db}$, в яких елементами будуть лише коди функцій.

Для того щоб кортеж функцій, який реалізується простим двомодульним каскадом, відтворював повну підстановку, необхідно, щоб сукупність множини значень функцій $\mathbf{P}$ (або $\mathbf{T}$) розбивались на дві пари так, щоб множини, які належать до однієї пари не мали спільних елементів і були доповненням одна до одної в множині $\mathbf{S}_{1,t}$ (або $\mathbf{S}_{t+1,n}$), тобто згідно з [5] забезпечувалась балансність та ортогональність логічних функцій із кортежів $\mathbf{F}_{1,t}$ та $\mathbf{F}_{t+1,n}$.

Можливі три варіанти розбиття чотирьох множин кодів функцій на дві пари, що необхідно для забезпечення балансності. Перший варіант (позначимо його а) – ($\mathbf{P}_{ca}$, $\mathbf{P}_{cb}$), ($\mathbf{P}_{da}$, $\mathbf{P}_{db}$). Другий варіант (позначимо його б) – ($\mathbf{P}_{ca}$, $\mathbf{P}_{da}$), ($\mathbf{P}_{cb}$, $\mathbf{P}_{db}$). Третій варіант (позначимо його в) – ($\mathbf{P}_{ca}$, $\mathbf{P}_{db}$), ($\mathbf{P}_{da}$, $\mathbf{P}_{cb}$). У кожному із цих варіантів виділимо два випадки наявності спільних елементів, що важливо для забезпечення ортогональності. У першому з них серед чотирьох множин $\mathbf{P_{ca}, P_{cb}, P_{da}, P_{db}}$ кодів функцій існують три множини, які попарно мають спільні елементи (тобто, обов'язково існує множина, яка має спільні елементи з двома іншими). Такі типи конструктивних модулів будемо позначать цифрою 3. В другому випадку серед множин $\mathbf{P_{ca}, P_{cb}, P_{da}, P_{db}}$ попарно спільні елементи можуть мати тільки дві множини (тобто будь-яка з множин може мати спільні елементи лише з однією з інших). Такі типи конструктивних модулів будемо позначать цифрою 2.

Таким чином, можна виділити наступні типи конструктивних модулів простого двомодульного каскаду: 3а, 3б, 3в, 2а, 2б, 2в. Характеристики даних модулів наведені в [6]. Загальні властивості типів модулів двомодульного ОККМ наведені в табл. 1.

Таблиця 1

	Ознака входження множин в пару за значенням коду на боковому вході та боковому виході конструктивного модуля			
Тип модуля	За однаковим кодом на вході	За однаковим кодом на виході	За різними кодами на вході й виході	Бокова функція
Тип 3а	Множини пари не мають спільних елементів	Множини пари можуть мати спільні елементи	Множини пари можуть мати спільні елементи	Довільна
Тип 3б	Множини пари можуть мати спільні елементи	Множини пари не мають спільних елементів	Множини пари можуть мати спільні елементи	Рівномірна
Тип 3в	Множини пари можуть мати спільні елементи	Множини пари можуть мати спільні елементи	Множини пари не мають спільних елементів	Довільна
Тип 2а	Множини пари не мають спільних елементів	Множини пари співпадають	Множини пари не мають спільних елементів	Довільна
Тип 2б	Множини пари не мають спільних елементів	Множини пари не мають спільних елементів	Множини пари співпадають	Рівномірна
Тип 2в	Множини пари співпадають	Множини пари не мають спільних елементів	Множини пари не мають спільних елементів	Рівномірна

Як показано в [5], повні підстановки можна реалізувати за допомогою пари модулів наступних типів: (3а-2а), (3б-2в), (3в-2б), (2а-2а), (2а-2б), (2б-2в), (2в-2в).

На основі наведених результатів розглянемо ітераційний процес формування *n*-розрядного ОККМ (Рис. 5), створеного з найпростіших модулів **за першим варіантом**. Нехай n=1, тоді відповідно до першого варіанту перший модуль ОККМ не має бокових виводів в сторону молодших розрядів. Функція на боковому виході першого КМ в сторону старших розрядів залежить від однієї змінної, тому можливі лише чотири варіанти формування множин $\boldsymbol{S}_0$ та $\boldsymbol{S}_1$: перший – $\boldsymbol{S}_{0=}\{0\}$, $\boldsymbol{S}_{1=}\{1\}$, $f_{r1}= x$; другий – $\boldsymbol{S}_{0=}\{1\}$, $\boldsymbol{S}_{1=}\{0\}$, $f_{r1}=$ not x; третій $\boldsymbol{S}_0 = \{0,1\}$, $\boldsymbol{S}_1 = \varnothing$, $f_{r1}= 0$; четвертий. $\boldsymbol{S}_0 = \varnothing$, $\boldsymbol{S}_1 = \{0,1\}$, $f_{r1}= 1$. При конкретному значенні змінної на боковому вході першого КМ (0 або 1) на первинному виході модуля реалізується функція змінної x, яка в свою чергу може бути тотожньою, інверсією, константою – 0 або 1. Перелік всіх можливих варіантів

поданий в таблиці 2, де $f_{o1}(0,x)$- функція на первинному виході при значенні 0 змінної на боковому вході, $f_{o1}(1,x)$ - функція на первинному виході при значенні 1 змінної на боковому вході.

Таблиця 2

$f_{o1}(0,x)$	$f_{o1}(1,x)$	$f_{r1}(x)$	Тип модуля
0 , 1	0 , 1	0 , 1	-
0 (1)	0 (1)	x, $\bar{x}$	-
0 (1)	1 (0)	x, $\bar{x}$	2в
0 , 1	x, $\bar{x}$	0 , 1	-
0 , 1	x, $\bar{x}$	x, $\bar{x}$	-
x, $\bar{x}$	0 , 1	0 , 1	-
x, $\bar{x}$	0 , 1	x, $\bar{x}$	-
x, $\bar{x}$	x, $\bar{x}$	0 , 1	2а1
$x(\bar{x})$	$x(\bar{x})$	x, $\bar{x}$	2а2
$x(\bar{x})$	$\bar{x}(x)$	x, $\bar{x}$	2б

Із всіх можливих комбінацій функцій на боковому та первинному виході згідно з [5] необхідно виключити комбінації, в яких обидві функції є константами. Таким чином можливі лише наступні типи найпростіших КМ – 2а1, 2а2, 2б та 2в. Відмітимо, що у випадку модуля типу 2а2 відсутня залежність функції на первинному виході від значення на боковому вході, а у випадку типу 2а1 – функція на боковому виході модуля є константою. Крім того, модулі типу 2в не реалізують підстановку при n=1. Такий тип модулів може бути використаний в наступних ітераціях.

Визначимо перемикальні функції, які реалізують модулі відповідних типів.

Тип 2а1.

1. $f_{o1}(f_{h2},x_1) = x_1$, $f_{r1}(x_1)= 0$
2. $f_{o1}(f_{h2},x_1) = \text{not } x_1$, $f_{r1}(x_1)= 0$
3. $f_{o1}(f_{h2},x_1) = x_1 \oplus f_{h2}$, $f_{r1}(x_1)= 0$
4. $f_{o1}(f_{h2},x_1) = \text{not } x_1 \oplus f_{h2}$, $f_{r1}(x_1)= 0$
5. $f_{o1}(f_{h2},x_1) = x_1$, $f_{r1}(x_1)= 1$
6. $f_{o1}(f_{h2},x_1) = \text{not } x_1$, $f_{r1}(x_1)= 1$
7. $f_{o1}(f_{h2},x_1) = x_1 \oplus f_{h2}$, $f_{r1}(x_1)= 1$
8. $f_{o1}(f_{h2},x_1) = \text{not } x_1 \oplus f_{h2}$, $f_{r1}(x_1)= 1$

Тип 2а2

1. $f_{o1}(f_{h2},x_1) = x_1$, $f_{r1}(x_1)=x_1$
2. $f_{o1}(f_{h2},x_1) = \text{not } x_1$, $f_{r1}(x_1)=x_1$
3. $f_{o1}(f_{h2},x_1) = x_1$, $f_{r1}(x_1) = \text{not } x_1$
4. $f_{o1}(f_{h2},x_1) = \text{not } x_1$, $f_{r1}(x_1) = \text{not } x_1$

Тип 2б.

1. $f_{o1}(f_{h2},x_1) = x_1 \oplus f_{h2}$, $f_{r1}(x_1)=x_1$
2. $f_{o1}(f_{h2},x_1) = \text{not } x_1 \oplus f_{h2}$, $f_{r1}(x_1)=x_1$
3. $f_{o1}(f_{h2},x_1) = x_1 \oplus f_{h2}$, $f_{r1}(x_1)= \text{not } x_1$
4. $f_{o1}(f_{h2},x_1) = \text{not } x_1 \oplus f_{h2}$, $f_{r1}(x_1)= \text{not } x_1$

Тип 2в.

5. $f_{o1}(f_{h2},x_1) = f_{h2}$, $f_{r1}(x_1)=x_1$
6. $f_{o1}(f_{h2},x_1) = \text{not } f_{h2}$, $f_{r1}(x_1)=x_1$
7. $f_{o1}(f_{h2},x_1) = f_{h2}$, $f_{r1}(x_1)= \text{not } x_1$
8. $f_{o1}(f_{h2},x_1) = \text{not } f_{h2}$, $f_{r1}(x_1)= \text{not } x_1$

Відмітимо, що кількість модулів кожного з типів повністю узгоджується з теоретичними розрахунками, наведеними в [6].

Розглянемо другий варівнт побудови ОККМ. Нехай n=2, перша ітерація. Розглянемо логічні функції найпростішого КМ (Рис. 3) при його підключенні в ОККМ на рис. 5 – $f_{o2}(f_{h3},x_2, f_{r1})$, $f_{h2}(f_{h3},x_2)$, $fr_2(x_2,f_{r1})$. Якщо зафіксувати конкретне значення f_{h3}, то фактично одержимо старший модуль двомодульного каскаду (Рис. 4.). Таким чином, найпростіший КМ має два типи в сторону молодших розрядів, які позначимо L0 та

L1. Оскільки функції $fo_2(0,x_2, fr_1)$, та $fo_2(1,x_2, fr_1)$, (відповідно $f_{h2}(0,x_2)$, та $f_{h2}(1,x_2)$) не залежні одна від одної, то як L0, так і L1 можуть бути будь-якими із наведених вище 12 типів. Для реалізації повної підстановки, згідно з [6], необхідно і достатньо, щоб будь-який із типів L0 та L1 був сумісний із типом першого модуля. При цьому функція $f_{r2}(x_2,f_{r1})$ може бути довільною. Відзначимо, що двомодульний каскад реалізує дві повні підстановки (при f_{h3}=0, та f_{h3}=1). Характер функції $f_{r2}(x_2,f_{r1})$ має значення при визначенні типу «об'єднаного КМ» із першого та другого модулів. Очевидно, що тип може бути лише 2а, 3а та 2б.

Друга та наступні ітерації виконуються аналогічно. Взагалі ймовірним типом «об'єднаного КМ» є тип 3а, що обмежує підключення наступних КМ лише типами 2а, тому важливим є визначення умов, при виконанні яких «об'єднаний КМ» буде мати типи 2а та 2б. Напрямок вирішення цієї задачі полягає в наступному. Кожна з двох підстановок «об'єднаного КМ» є в свою чергу деякою перестановкою елементів із множини $\mathbf{S}_{1,t}$. Дві перестановки в свою чергу утворюють підстановку, яка характеризується своїми циклами. Тому, якщо функція fr_i на $(i-1)$-ій ітерації приймає однакові значення в межах будь-якого циклу, то «об'єднаний КМ» буде належати до типу 2а. Якщо кількість елементів будь-якого циклу парна, а функція f_{ri} на $(i-1)$-ій ітерації приймає різні значення на половині елементів будь-якого циклу, то «об'єднаний КМ» буде належати до типу 2б.

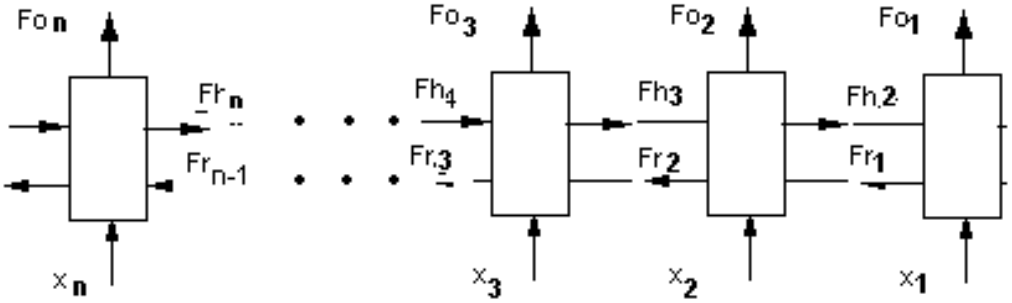

Рисунок 5 – Найпростіший багатомодульний ОККМ

Другий варіант побудови ОККМ. Тут, на відміну від попереднього, функція $f_{r2}(x_2,f_{r1})$ не може бути довільною. При фіксуванні значень f_{ri} отримаємо типи в сторону старших розрядів – Н0 та Н1. КМ згідно з рис. 3 в цьому випадку характеризується четвіркою типів – Н0, Н1, L0, L1, наприклад 2а1, 2а2, 2б, 2а1. В цьому плані ОККМ в цілому може трактуватись як один модуль зі своїми правосторонніми та лівосторонніми типами. Новий модуль до каскаду може підключатися як зі сторони молодших розрядів так і зі сторони старших розрядів. При підключенні модуля до другого модуля або до каскаду кожний лівосторонній тип модуля має бути сумісним з кожним правостороннім типом попереднього модуля чи каскаду. Згідно з [6] це є необхідною і достатньою умовою для вітворення новим ОККМ повних підстановок при будь-яких значеннях на правому боковому вході першого модуля та лівому боковому вході останнього модуля.

Шляхом повного перебору всіх можливих функцій (як на первинних виходах, так і на бокових) було доведено існування 75 різних комбінацій правосторонніх та лівосторонніх типів найпростіших ОККМ, що можуть бути використані для реалізації повної підстановки. При побудові найпростіших ОККМ із розглянутих модулів необхідно дотримуватись сумісності типів. Сумісність типів згідно з попередніми твердженнями забезпечує реалізацію повних підстановок за допомогою каскаду найпростіших ОККМ.

Моделювання роботи каскаду

Для підтвердження результатів теоретичного дослідження найпростішого ОККМ була розроблена програма [7], яка дозволяє моделювати роботу найпростішого нерегулярного ОККМ та проводити класифікацію модулів за визначеними типами. Програма виконує наступні функції:

- перевірка можливості реалізації повної підстановки при заданих умовах;
- визначення типу об'єднаного конструктивного модуля, що утворюється з декількох найпростіших;
- визначення шляхом повного перебору всіх можливих типів конструктивних модулів, що утворюються з пари найпростіших модулів.

В результаті моделювання роботи найпростішого ОККМ були отримані такі результати.

1. Всі найпростіші КМ можна розділити на 5 груп за ознакою наявності та кількості їх типів: модулі, що не мають жодного типу (такі модулі не можуть бути використані для реалізації повних підстановок), модулі, що мають 1, 2 або 3 типи (такі модулі можуть бути використані для реалізації повних підстановок за певних умов) і модулі, що мають всі 4 типи (такі модулі можуть бути використані для реалізації повних підстановок).
2. Кількість комбінацій чотирьох типів дорівнює 75. При цьому, якщо один з типів модуля є 2в, то всі інші його типи також 2в.
3. Модулі, сусідні типи яких є сумісними, реалізують повну підстановку.
4. Якщо пара модулів реалізує повну підстановку, то її об'єднаний тип завжди належить до класифікації, що наведена вище.
5. Шляхом повного перебору доведено, що об'єднаний тип двох модулів не залежить від типів модулів, а тільки від комбінації бокових та основних функцій. При цьому, якщо каскад модулів реалізує повну підстановку, то його відповідний об'єднаний тип 2а, 2б або 3а. Якщо каскад не реалізує повну підстановку, то його об'єднаний тип або не входить в наведену вище класифікацію, або 2в (останній випадок дає можливість нарощувати каскад). Модулі типу 3б та 3в не можуть бути отримані шляхом об'єднання двох найпростіших модулів модулів.

Висновки

В статті розглянуто методику реалізації повних підстановок за допомогою найпростішого каскаду конструктивних модулів при довільній розрядності підстановок. Кожний такий модуль має прості логічні функції, каскад легко нарощується, тому реалізація як окремого модуля, так і каскада в цілому за допомогою сучасних технологій не викликає ускладнень. Тому метод є перспективним для реалізації масових підстановок довільної розрядності. Необхідно відмітити, що найпростіший ОККМ може реалізувати до двох різних підстановок на найпростіших ОККМ першого варіанту і до чотирьох різних підстановок для другого варіанту найпростіших ОККМ; для цього необхідно лише змінити значення на бокових входах.

*Література:**1.** Опанасенко В. Н., Сахарин В. Г. ПЛИС типа FPGA фирмы Xilinx: возможности, проектирование и применение. Электронные системы и компоненты. – 2003, № 4, с.7-11. **2.** Кузелин М. О., Кнышев Д. А., Зотов В. Ю. Современные семейства ПЛИС фирмы Xilinx. – М: «Горячая линия-Телеком», 2004, 440 с. **3.** Кострикин А. И. Введение в алгебру. М. Наука, 1994, 232 с **4.** Тарасенко В. П., Тесленко О. К., Яновська О. Ю. Проблеми апаратної реалізації підстановок. Наукові записки УНДІЗ, №2, 2007, с 52-58 **5.** Михайлюк А. Ю., Тарасенко В. П., Тесленко А. К. "Анализ эффективности применения нетрадиционных элементарных функций шифрования". Матеріали Третьої міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікацій-них системах» К.2000. с. 161-168 **6.** Тарасенко В. П., Тесленко О. К, Яновська О. Ю. Реалізація повних підстановок на простому двомодульному каскаді конструктивних модулів, Інформаційні технології та комп'ютерна інженерія, № 1(11), 2008, с.88-97. **7.** Яновська О. Ю. Тесленко О. К., Тарасенко В. П., Комп'ютерна програма дослідження реалізації повних підстановок на найпростіших нерегулярних структурах (SuperModuli), Свідоцтво про реєстрацію авторського права на твір № 25782 від 24.09.2008.*

УДК 681.3

АЛГОРИТМИ КОДУВАННЯ-ДЕКОДУВАННЯ УЗАГАЛЬНЕНИХ ЗАВАДОСТІЙКИХ КОДІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ В УМОВАХ ПРИРОДНИХ ВПЛИВІВ

Вячеслав Василенко
Національний авіаційний університет

Анотація: **Для використання в задачах забезпечення цілісності інформаційних об'єктів в умовах природних впливів пропонуються узагальнені завадостійкі коди з удосконаленими алгоритмами кодування – декодування.**