Подальші дослідження можуть бути направлені на продовження оптимізації швидкості алгоритмів, які є основою створення та модернізації криптобібліотек, що використовуються в програмних системах реального часу з великою кількістю криптоопераций.

Література: ***1.*** *Б. Страуструп. Язык программирования Си++. — 3-е изд. — спб., М.: «Невский діалект», издательство «Бином», 1999. — 991 с.* ***2.*** *Б. Э. Смит, М. Т. Джонсон. Архитектура и программирование микропроцессора INTEL 80386. — М.: «Конкорд», 1992. — 334 с.* ***3.*** *Сингер М. Мини-ЭВМ PDP-11: Программирование на языке ассемблера и организация машины. — М.: «Мир», 1984. — 272 с.* ***4.*** *Дональд Кнут. Искусство программирования, том 1. Основные алгоритмы = The Art of Computer Programming, vol. 1. Fundamental Algorithms. — 3-е изд. — М.: «Вильямс», 2006. — С. 720.* ***5.*** *A. Menezes, P. van Oorschot, S. Vanstone. Handbook of Applied Cryptography. — CRC-Press, 1996. — 816 p. — (Discrete Mathematics and Its Applications).* ***6.*** *Венбо Мао. Современная криптография: теория и практика = Modern Cryptography: Theory and Practice. — М.: «Вильямс», 2005. — 768 с.* ***7.*** *Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М.: «Диалектика», 2004. — 432 с.* ***8.*** *Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с.*

УДК 681.325.59:519.6

АВТОКОРИГУЮЧІ ВЛАСТИВОСТІ ЕЛЕМЕНТАРНИХ АВТОМАТІВ

Ярослав Клятченко, Оксана Тарасенко-Клятченко
НТУУ «КПІ»

Анотація: **Розроблена методика і запропонована система показників для дослідження та оцінки ефекту від врахування автокоригуючих властивостей функцій переходів елементарних автоматів.**
Summary: **Developed methods and proposed a system of indexes for research and evaluation the self-correction effect for transition function of elementary automaton.**
Ключові слова: **Автокорекція, спотворення сигналу.**

І Постановка задачі

Латентні автокоригуючі властивості довільних перемикальних функцій, що полягають у формуванні правильних їх значень за наявності спотворень (техногенних або умисних) їх аргументів, досить повно досліджені в роботах [1, 2]. Врахування цих властивостей забезпечує більш високу ймовірність отримання правильного результату деякого логічного перетворення, що описується заданими перемикальними функціями, ніж це могло бути обумовлено тільки ймовірностями появи неспотворених значень аргументів. Відомо також [3], що дуже багато структур цифрових пристроїв можна подати як композицію логічного перетворювача та технічної пам'яті на основі елементарних автоматів (ЕА) – тригерів різних типів. При цьому ЕА є автоматами другого роду (автоматами Мура) з двома стійкими станами [4], для яких функція виходів однозначно визначається станом автомата. Тому в умовах потенційної загрози вхідних спотворень стосовно ЕА можуть виникати наступні ситуації:

- спотворення вхідних сигналів нема і ЕА перемикається правильно (тобто, відповідно до його функції переходів (ФП));
- спотворення вхідних сигналів є і ЕА перемикається неправильно (переходить не в той стан, який задається його ФП);
- спотворення вхідних сигналів є, але ЕА до нього нечутливий (наприклад, ЕА типу *RS* не перемикається і зберігає свій попередній стан, коли на його входах два нулі);
- спотворення вхідних сигналів є, але ЕА переходить в той же стан, який задається неспотвореними вхідними сигналами (наприклад, ЕА типу *R* переходить в нуль під дією вхідних сигналів як *R=1, S=0*, так і *R=1, S=1*).

Всі відомі методи оцінки достовірності (вірогідності) функціонування цифрових пристроїв в умовах потенційної загрози вхідних спотворень [5] орієнтовані тільки на ситуації 1) і 2). Це було спричинене тим, що безумовно приймалася гіпотеза про дуже малу ймовірність техногенного спотворення вхідних сигналів, а можливість їх умисного спотворення взагалі не допускалась. Однак відомо [6], що нормативні

документи, які, наприклад, регламентують внутрішній комп'ютерний обмін інформацією, допускають ймовірність техногенного спотворення окремого вхідного сигналу на рівні 10^{-7}, а для сучасних апаратних засобів та систем критичного застосування, виконаних на основі ПЛІС, та ж ймовірність оцінюється величинами порядку $10^{-5}…10^{-6}$. Ймовірність же умисного спотворення сигналів, наприклад, в інформаційних технологіях, що потребують захисту, вища на декілька порядків. Крім того, число схемотехнічних компонент типу ЕА в апаратних засобах на основі тих же ПЛІС сягає 10^6 і навіть більше [7]. Нестрого кажучи, в сучасних цифрових апаратних засобах мала ймовірність окремого вхідного спотворення багатократно "посилюється" великою внутрішньою складністю ПЛІС і інших подібних компонент-напівфабрикатів. Очевидно, що надалі оцінки достовірності функціонування цифрових апаратних засобів без врахування ситуацій 3) та 4) не будуть повними.

Тому виникає задача створення системи показників, які б характеризували якісний і кількісний аспект впливу факторів, породжених ситуаціями 3) і 4), на достовірність функціонування ЕА, а також розробки методики врахування автокоригуючих властивостей ЕА в оцінках достовірності функціонування цифрових пристроїв.

II Метод розв'язку задачі

Основний методичний прийом розв'язку поставленої задачі базується на тому, що оскільки ФП ЕА часто задають як перемикальні функції, то до них можна застосовувати весь апарат дослідження, вже напрацьований для власне перемикальних функцій. Тобто можна встановити наявність автокоригуючих здатностей у ЕА шляхом дослідження їх ФП, поданих як перемикальні функції.

Будемо називати детермінованим спотворенням аргумента (вхідного сигналу) $x_i \in \{0,1\}, i = \overline{1,n}$, довільну заміну його істинного значення іншим значенням, що належить до тієї ж множини допустимих значень, що і неспотворене значення, але не дорівнює йому.

Нехай функціонування ЕА описується ФП

$$Q^{(S+1)} = f\left(x_1, x_2, ..., x_{n-1}, x_n, Q^{(S)}\right),$$

де $x_i, Q^{(S+1)}, Q^{(S)} \in \{0,1\}; i = \overline{1,n}$, x_i – незалежні вхідні змінні (сигнали), $Q^{(S)}$ та $Q^{(S+1)}$- стани ЕА в s-й та в s+1-й моменти дискретного часу. Число можливих детермінованих спотворень змінних x_i позначимо як b. (Найчастіше в роботі цифрових пристроїв з двозначними сигналами зустрічаються детерміновані спотворення трьох типів: "Константа 1", "Константа 0" та "Інверсія". В такому випадку b=3). Будемо позначати далі як $x_i^l (l = \overline{0,b})$ змінну x_i із спотворенням типу l. При цьому x_i^0 означає відсутність спотворення x_i, x_i^1 - спотворення типу "Константа 1", x_i^2 - спотворення типу "Константа 0", x_i^3 - спотворення типу "Інверсія" і т. д.. Автокоригуюча здатність відносно однократних вхідних спотворень вказаних вище типів в тій чи іншій мірі властива практично всім перемикальним функціям. Деяким винятком тут є функції суми по модулю 2 та її заперечення, які не мають автокоригуючих властивостей стосовно спотворень типу "Інверсія". Найсильніше автокоригуючу здатність виявляють функції, що містять тільки один нуль або тільки одну одиницю в своїх таблицях істинності (диз'юнкція, кон'юнкція, штрих Шеффера, стрілка Пірса [3], тощо).

Таким чином, правильне функціонування ЕА визначається його ФП, визначеною за відсутності спотворень, тобто

$$Q^{(S+1)} = f\left(x_1^0, x_2^0, ..., x_{n-1}^0, Q^{(S)}\right), \quad (1)$$

однак внаслідок можливих однократних спотворень вхідних змінних вона може бути реалізована і згідно з одним із наступних варіантів:

$$\begin{array}{cc}
\left.\begin{array}{c}\text{1-й}\\ \text{2-й}\\ \cdots\cdots\cdots\\ \\ b\text{+1-й}\\ b\text{+2-й}\\ \cdots\cdots\\ (b+1)^n\text{-1-й}\end{array}\right\} & \left.\begin{array}{l}
Q^{(S+1)} = f(x_1^0, x_2^0, ..., x_{n-1}^0, x_n^1, Q^{(S)}),\\
Q^{(S+1)} = f(x_1^0, x_2^0, ..., x_{n-1}^0, x_n^2, Q^{(S)}),\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
Q^{(S+1)} = f(x_1^0, x_2^0, ..., x_{n-1}^0, x_n^b, Q^{(S)}),\\
Q^{(S+1)} = f(x_1^0, x_2^0, ..., x_{n-1}^1, x_n^0, Q^{(S)}),\\
Q^{(S+1)} = f(x_1^0, x_2^0, ..., x_{n-1}^1, x_n^1, Q^{(S)}),\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
Q^{(S+1)} = f(x_1^b, x_2^b, ..., x_{n-1}^b, x_n^b, Q^{(S)}).
\end{array}\right\}
\end{array} \quad (2)$$

Всього може бути $(b+1)^n$ різних варіантів (1) та (2) реалізації ФП. Тут і далі будемо також вважати, що оскільки значення $Q^{(S)}$ формуються самим ЕА, то вони не зазнають дії "зовнішніх" спотворень. Поставимо у відповідність кожній змінній x_i набір ймовірностей $p_{i0}, p_{i1},..., p_{ib}$, де кожна компонента $p_{il}(i=\overline{1,n}; l=\overline{0,b})$ є ймовірністю появи неспотвореного (l=0) та b спотворених значень x_i. Очевидно, що можливі значення x_i^l у виразах (1) і (2) відповідають повній групі подій та, крім того, $\sum_{l=0}^{b} p_{il} = 1$. Отже, ймовірність реалізації ФП за умов, врахованих у формулі (1), можна визначити як

$$R_0 = \prod_{i=1}^{n} p_{i0},$$

а ймовірності реалізації ФП за виразами (2) складають:

$$\left.\begin{aligned} R_1 &= p_{10}p_{20}\cdots p_{n-10}p_{n1},\\ R_2 &= p_{10}p_{20}\cdots p_{n-10}p_{n2},\\ &\cdots\cdots\cdots\cdots\cdots\\ R_b &= p_{10}p_{20}\cdots p_{n-10}p_{nb},\\ R_{b+1} &= p_{10}p_{20}\cdots p_{n-11}p_{n0},\\ R_{b+2} &= p_{10}p_{20}\cdots p_{n-11}p_{n1},\\ &\cdots\cdots\cdots\cdots\cdots\\ R_{(b+1)^n-1} &= p_{1b}p_{2b}\cdots p_{n-1b}p_{nb}. \end{aligned}\right\} \quad (3)$$

Внаслідок ефекту автокорекції значення ФП (2) можуть частково або навіть повністю збігатися зі значеннями функції (1). Позначимо кількість таких збігів як $s_r, r=\overline{1,(b+1)^n-1}$. Очевидно, що $0 \le S_r \le 2^n$, крім того $S_r = 0$ означає повну розбіжність (тобто відсутність автокорекції) значень деякої r-ї функції із переліку (2) і функції (1), а $S_r = 2^n$ означає повний збіг (повну автокорекцію) значень тих же функцій. При врахуванні тільки одноразових спотворень система ймовірностей (3) вироджується в систему вигляду:

$$\left.\begin{aligned} R_1 &= p_{10}p_{20}\cdots p_{n-10}p_{n1},\\ R_2 &= p_{10}p_{20}\cdots p_{n-10}p_{n2},\\ &\cdots\cdots\cdots\cdots\cdots\\ R_b &= p_{10}p_{20}\cdots p_{n-10}p_{nb},\\ R_{b+1} &= p_{10}p_{20}\cdots p_{n-11}p_{n0},\\ R_{b+2} &= p_{10}p_{20}\cdots p_{n-12}p_{n0},\\ &\cdots\cdots\cdots\cdots\cdots\\ R_{bn} &= p_{1b}p_{20}\cdots p_{n-10}p_{n0}. \end{aligned}\right\} \quad (4)$$

Тоді ймовірність правильної реалізації ФП ЕА складає

$$P = R_0 + \sum_{q=1}^{bn} s_q R_q.$$

За рівних ймовірностей R_q (в практичних розрахунках часто приймають саме таку гіпотезу [8]) остаточно маємо

$$P = R_0 + R_q(\sum_{q=1}^{bn} s_q).$$

Тут другий доданок виражає приріст ймовірності правильної реалізації ФП за рахунок автокоригуючих властивостей ЕА, а сума в дужках відповідає числу M однократних детермінованих спотворень ФП, до яких вона нечутлива. В роботах [1, 2] характеристику M стосовно перемикальних функцій названо абсолютною автокоригуючою здатністю. Характеристика M разом із відносною автокоригуючою здатністю $L=M/N$, де N – загальне число всіх можливих спотворень детермінованого типу, є найповнішими характеристиками автокоригуючих властивостей ФП ЕА.

III Приклади

Визначення характеристик M, L та P для практичних типів ЕА зручно і наочно проводити на основі табличного подання ФП цих ЕА. Розглянемо спочатку ЕА з одним входом, де нетривіальними є лише автомати типів T та $Д$. ФП ЕА T-типу можна записати як $Q^{(s+1)} = \underline{x}Q^{(s)} \vee x\underline{Q}^{(s)}$, а її табличний вигляд показаний на рис.1,а. Враховуючи вищевказані число і характер однократних детермінованих спотворень, неважко впевнитися, що число варіантів функціонування ЕА T-типу буде дорівнювати всього чотирьом. Зауважимо, що в це число входить і "зразковий" варіант на рис. 1,а, інші ж подані рис. 1,б,в,г, де жирним шрифтом вказані значення ФП, які збігаються із зразковими. Аналіз таблиць на рис. 1 показує, що для ЕА T-типу M=4, N=12, L=1/3, а правильна робота ЕА можлива не тільки за відсутності вхідних спотворень, але і частково за наявності константних спотворень і зовсім неможлива при інверсних спотвореннях вхідних сигналів. З використанням раніш введених позначень можна записати, що ймовірність правильної роботи ЕА T-типу при наявності детермінованих спотворень вхідних сигналів становить $P= p_0+0{,}5p_1+0{,}5p_2$.

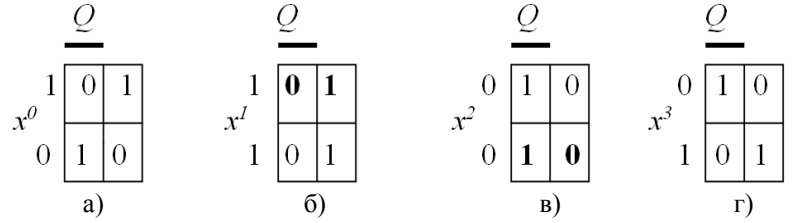

Рисунок 1 – Таблична форма для ЕА Т-типу

Для ЕА $Д$-типу його ФП $Q^{(s+1)} = x$ відрізняється від попередньої, однак, як неважко переконатися, вирази для характеристик M, N, L та P ЕА $Д$-типу будуть такими ж, як і для ЕА T-типу.

Розглянемо тепер ЕА з двома входами, з множини яких виберемо лише практично найважливіші ЕА типів *SR, S, R, E* та *JK*. Принагідно зауважимо, що ЕА *SR*-типу має невизначені переходи, а всі інші їх не мають. Для першого ЕА ФП має вигляд $Q^{(s+1)} = \overline{x_1}\, x_2 \vee x_2\, Q^{(s)}$ (тут x_1=*S*, x_2 =*R*), а її табличний "зразковий" варіант поданий у лівому верхньому куті рис. 2.

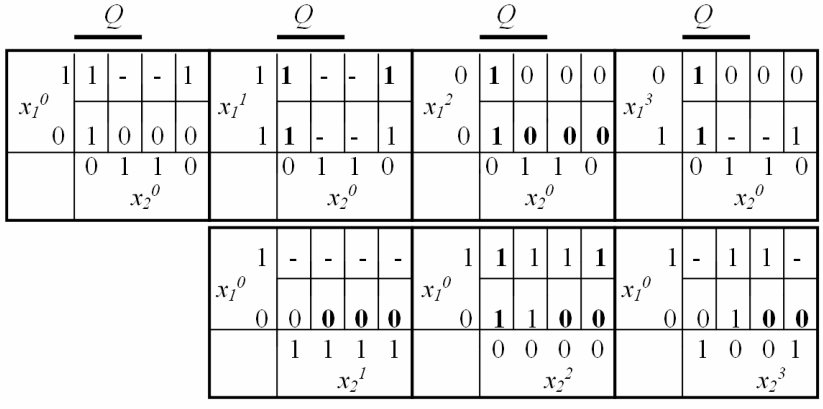

Рисунок 2 – Таблична форма для ЕА з двома входами типів *SR*

Тут дефіси відповідають невизначеним переходам ЕА на заборонених наборах значень аргументів. Аналіз рис. 2 показує, що для ЕА *SR*-типу M=20, N=48, L=5/12, а ймовірність його правильної роботи складає $P=p_0^2+(3/8)p_0\ p_1+(5/8)p_0\ p_2+(2/8)p_0\ p_3+(3/8)p_0\ p_1+(5/8)p_0\ p_2+(2/8)p_0\ p_3= p_0^2+0{,}75p_0\,p_1+1{,}25p_0\,p_2+0{,}5p_0\,p_3$.

Для ЕА типу *S* ФП має вигляд $Q^{(s+1)}= x_1 \vee \overline{x_2}\, Q^{(s)}$. Таблиці ж "зразкової" ФП і її варіантів, що побудовані за аналогією з таблицями для ЕА *SR*-типу за наявності вхідних однократних спотворень, подані на рис. 3.

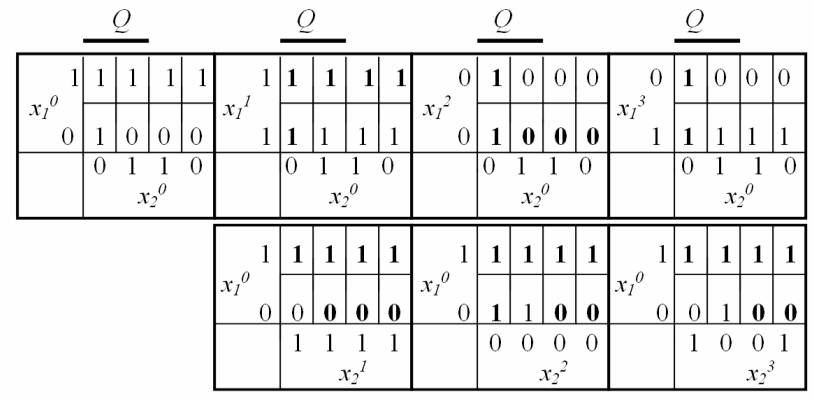

Рисунок 3 – Таблична форма для ЕА типу S

Для цього ЕА M=32, N=48, L=2/3,

$P=p_0^2+(5/8)p_0\ p_1+(5/8)p_0\ p_2+(2/8)p_0\ p_3+(7/8)p_0\ p_1+(7/8)p_0\ p_2+(6/8)p_0\ p_3= p_0^2+1{,}5p_0\,p_1+1{,}5p_0\,p_2+p_0\,p_3$.

Для ЕА типів R і E ФП мають вигляд відповідно $Q^{(s+1)}= x_1\,\underline{x_2} \vee \underline{x_2}\,Q^{(s)}$ та $Q^{(s+1)}=x_1\,Q^{(s)} \vee \underline{x_2}\,\underline{Q^{(s)}}$, їх табличні форми відрізняються від попередньої та одна від одної, однак їх аналіз приводить до таких же результатів, що вже відомі для ЕА S-типу.

Для дуже поширеного так званого "універсального" ЕА JK-типу ФП має вигляд $Q^{(s+1)}=x_1\,\overline{Q^{(s)}} \vee x_2\,\overline{Q}^{(s)}$, а в табличній інтерпретації їй відповідає лівий верхній кут рис. 4.

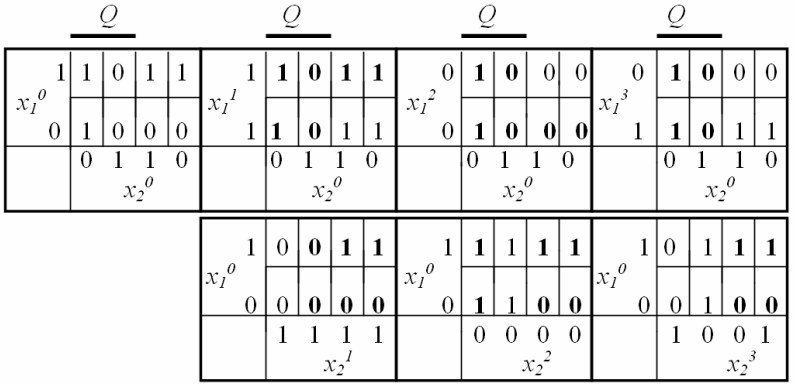

Рисунок 4 - Таблична форма для ЕА типів *JK*

Стосовно ж оцінок M, N, L, P неважко переконатися, що вони будуть такими ж, як і в попередніх випадках, де йшлося про ЕА з повними системами переходів.

Для ЕА типу *SRT* з багатьма невизначеними переходами і трьома входами (далі $x_1=S$, $x_2=R$, $x_3=T$) ФП має вигляд $Q^{(s+1)}= x_1\,x_2\,\overline{x_3} \vee \overline{x_2}\,\overline{x_3}\,Q^{(s)} \vee x_1\,\overline{x_2}\,\overline{x_1}\,\overline{Q^{(s)}}$, а її таблична форма приведена в лівому верхньому куті рис. 5. У цьому випадку M=32, N=144, L=2/9,

$P=p_0^3+(2/16)p_0^2\ p_1+(6/16)p_0^2\ p_2+(3/16)p_0^2\ p_1+(7/16)p_0^2\ p_2+(2/16)p_0^2\ p_3\ +(3/16)p_0^2\ p_1\ +(7/16)p_0^2\ p_2+(2/16)p_0^2\,p_3=p_0^3+0{,}5p_0^2\,p_1+1{,}25p_0^2\,p_2+0{,}25p_0^2\,p_3$.

Основні характеристики ЕА, що отримані в розглянутих прикладах, для зручності їх огляду і аналізу зібрані в підсумкову таблицю.

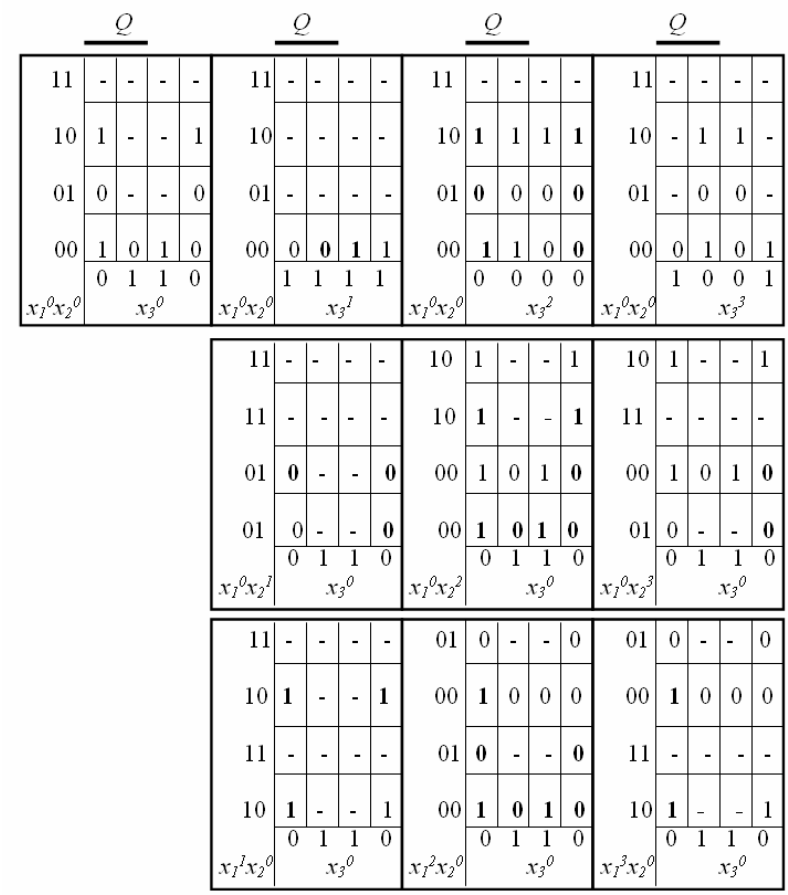

Рисунок 5 – Таблична форма для ЕА типу *SRT*
з багатьма невизначеними переходами і трьома входами

Таблиця - Основні характеристики ЕА

Тип ЕА	*M*	*N*	*L*	*P*
T, D	4	12	1/3	$p_0+0,5p_1+0,5p_2$
SR	20	48	5/12	$p_0^2+0,75p_0p_1+1,25p_0p_2+0,5p_0p_3$
S, R, E, JK	32	48	2/3	$p_0^2+1,5p_0p_1+1,5p_0p_2+p_0p_3$
SRT	32	144	2/9	$p_0^2+0,5p_0p_1+1,25p_0p_2+0,25p_0p_3$

IV Висновки

Викладена методика і запропонована система показників для оцінки ефекту від врахування автокоригуючих властивостей ФП ЕА, який викликає приріст ймовірності правильного функціонування ЕА. Ця методика дозволяє оптимізувати цифрові структури, що використовують ЕА, за показниками достовірності функціонування на основі відомих ймовірностей появи неспотворених вхідних сигналів і їх детермінованих спотворень.

За викладеною методикою можна, в принципі, оцінювати ефект від врахування автокоригуючих властивостей будь-яких ЕА, ФП яких подані у вигляді перемикальних функцій, а також отримувати подібні оцінки з врахуванням багаторазових детермінованих вхідних спотворень. Однак при цьому число і розмірність використовуваних таблиць, а також труднощі маніпулювання ними, порівняно з розглянутими прикладами, швидко зростають, що обумовлює доцільність розробки комп'ютерно-орієнтованих методик оцінки вказаного ефекту.

Аналіз підсумкової таблиці з врахуванням практичних припущень ($p_0 >> p_1,p_2,p_3$; $p_1 \approx p_2 \approx p_3$) показує, що відносна автокоригуюча здатність більш висока у ЕА з повністю визначеною системою переходів (типів *S,R,E,JK*). Найнижчий показник *L* для ЕА типу *SRT* обумовлений невизначеністю половини всіх можливих переходів цього ЕА.

Література: ***1.*** *Тарасенко-Клятченко О. В. Сравнительный анализ корректирующих свойств переключательных функций // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні.- К.: 2002, вип.5, с. 189…194.* ***2.*** *Тарасенко В. П. Метод оценки автокорректирующих свойств поразрядных логических операций/ В.П. Тарасенко, О.В. Тарасенко-Клятченко// Радиоэлектроника и информатика. -2001. - № 1(14). -С.83-86.* ***3.*** *Самофалова К. Г., Цифровые ЕВМ. Теория и проектирование / Самофалова К. Г., Корнійчук В. И., Тарасенко В. П. // К.: «Вища школа», 1989, - 424 с.* ***4.*** *Компьютерная схемотехника (краткий курс)/ Процюк Р. О., Корнійчук В. И., Кузьменко П. В., Тарасенко В. П. - К.: вид-во «Корнійчук», 2006, - 432 с.* ***5.*** *Щербаков Н. С. Достоверность работы цифровых устройств /Н. С. Щербаков; –М.: «Машиностроение», 1989. -224 с.* ***6.*** *Кулик А. Я. Адаптивні алгоритми передавання інформації / Вінниця: «Універсум», 2003, -213с.* ***7.*** *Отказобезопасные информационно-управляющие системы на программируемой логике/Е. С. Бахмач, А. Д. Герасименко, В. А. Головир, А. А. Сиора, В. В. Скляр, В. И. Токарев, В. С. Харченко; -Харьков-Кировоград.: -Изд-во НАУ „ХАИ" и НПП „Радий", 2008. -380 с* ***8.*** *Бондаренко М. Ф., Кривуля Г. Ф., Рябцев В. Г., Фрадков С. О., Хаханов В. И. Проектирование и диагностика компьютерных сетей и систем / -К.: НМЦВО, 2000, -306 с.*

УДК 621.391:519.2

ЗАСТОСУВАННЯ ТЕОРІЇ УЗАГАЛЬНЕНИХ МАРКІВСЬКИХ ШИФРІВ ДО ОЦІНЮВАННЯ СТІЙКОСТІ СУЧАСНИХ БЛОКОВИХ АЛГОРИТМІВ ШИФРУВАННЯ ДО МЕТОДІВ РІЗНИЦЕВОГО КРИПТОАНАЛІЗУ

Людмила Ковальчук, Сергей Пальченко*, Леонид Скрипник
*ІСЗЗІ НТУУ «КПІ», *ФТІ НТУУ «КПІ»*

Анотація: **Представлено теоретичне підґрунтя для оцінювання стійкості узагальнених марківських шифрів відносно різницевого криптоаналізу. Даний застосовано інструментарій для оцінювання стійкості БШ «Мухомор».**
Summary: **In this article presented theory for evaluation of Generalized Markov Cipher resistance. And use this method for evaluation of "Muhomor" block cipher.**
*Ключові слова***: Безпека інформації, криптологія, блочні алгоритми шифрування, диференціальний криптоаналіз, узагальнені марківські шифри, «Калина».**

I Вступ

У зв'язку з інтенсивним розвитком математичних методів у сфері криптоаналізу та захисту інформації багато криптографічних систем та протоколів, що застосовуються, вже не задовольняють сучасним вимогам. Наслідком цього є низка програм та конкурсів, зокрема міжнародних, таких як AES [1], NESSIE [2] та інші. Аналогічні процеси почали відбуватися і в Україні. Про це свідчить конкурс на новий Національний стандарт симетричного блочного шифрування, що розпочався кілька років тому. У конкурсі брали участь 5 алгоритмів. На даний момент переможця не визначено, але, на думку авторів даної роботи, найбільш перспективними є алгоритми «Калина» [3] та «Мухомор» [4], розроблені Харківським національним університетом радіоелектроніки.

У даній роботі основна увага приділяється формалізації опису та дослідженню основних властивостей стійкості до різницевого криптоаналізу шифру «Мухомор». Детальний аналіз стійкості до різницевого та декількох інших видів криптоаналізу шифру «Калина» було представлено у роботах [5, 6]. Специфіка даного алгоритму полягає в тому, що він, як і діючий стандарт блокового шифрування ГОСТ 28147-89 [7], не є марківським шифром (МШ). Тому до нього не може бути застосована класична теорія оцінювання стійкості, яку побудовано і розвинуто в роботах [8 – 12].

До недавнього часу взагалі не існувало робіт, в яких були отримані науково обґрунтовані оцінки стійкості немарківських блокових шифрів (БШ) до різницевого та лінійного криптоаналізу. Найперша з таких робіт [13] з'явилась у 2004 році. Її результати були допрацьовані, систематизовані та узагальнені у