НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

«До захисту допущено»
В.о. завідувача кафедри
_____ Михайло САВЧУК
«__» _____ 2021 р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності: 113 Прикладна математика

на тему: **«Криптографічні властивості S-блоків, побудованих на одновимірних клітинних автоматах»**

Виконав: студент 4 курсу, групи ФІ-74
Бублик Єгор Іванович

Керівник: к. т. н., доц. кафедри ММЗІ Яковлєв С.В. _____

Консультант: _ _____

Рецензент: звання, степінь, посада Прізвище І.П. _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2021

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

Рівень вищої освіти — перший (бакалаврський)
Спеціальність (освітня програма) — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Михайло САВЧУК
«__» _____ 2021 р.

ЗАВДАННЯ
на дипломну роботу

Студент: Бублик Єгор Іванович

1. Тема роботи: «*Криптографічні властивості S-блоків, побудованих на одновимірних клітинних автоматах*»,
керівник: к. т. н., доц. кафедри ММЗІ Яковлєв С.В.,
затверджені наказом по університету №__ від «__» _____ 2021р.

2. Термін подання студентом роботи: «4» червня 2021р.

3. Вихідні дані до роботи: *(впишіть вихідні дані до роботи)*

4. Зміст роботи: *(впишіть теми та задачі, які ви розкриваєте у роботі; можна робити це попунктно)*

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): *(якщо у вас є окремий ілюстративний матеріал окрім власне роботи (креслення, макети тощо), зазначайте; інакше вказуйте «Презентація доповіді»)*

6. Дата видачі завдання: 10 вересня 2020 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2020 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Вересень-жовтень 2020 р.	Виконано
3	Пошук бієктивних правил серед множини ЕКА радіусу 2	Лютий-березень 2021 р.	Виконано
4	Формулюваня та тестування методів побудови S-блоків на основі одновимірних клітинних автоматів	Квітень 2021 р.	Виконано
5	Порівняльний аналіз результатів тестування	Травень 2021 р.	Виконано

Студент _____ Бублик Є.І.

Керівник _____ Яковлєв С.В.

РЕФЕРАТ

Кваліфікаційна робота містить: 45 стор., 9 рисунків, 12 таблиць, 14 джерел.

Метою даної роботи пошук правил з множини одновимірних клітинних автоматів з правилами радіусу 1 і 2 та порівняльний аналіз схем їх поєднання для отримання криптографічно оптимальних S-блоків, придатних для застосування в легкій криптографії.

Були досліджені множини одновимірних клітинних автоматів з правилами радіусу 1 і 2, виконаний порівняльний аналіз методів побудови S-блоків і сформульована стратегія їх застосування для побудови криптографічно стійких S-блоків; у якості ілюстрації отримані два S-блоки з криптографічними властивостями порівняно високої якості.

S-БЛОК, КЛІТИННИЙ АВТОМАТ, ДИФЕРЕНЦІАЛЬНИЙ КРИПТОАНАЛІЗ, ЛІНІЙНИЙ КРИПТОАНАЛІЗ, НЕРУХОМА ТОЧКА, ЦИКЛОВА СТРУКТУРА

ABSTRACT

Qualification work contains: 45 pages, 9 figures, 12 tables, 14 sources.

The aim of the work is to search for rules of one-dimensional cellular automata of radii 1 and 2 and ways of their composition in order to obtain cryptographicaly optimal S-boxes suitable for implementation in lightweight cryptography.

The sets of elementary cellular automata with rules of radii 1 and 2 were explored, comparative analysis of S-boxes construction methods was performed and presented a strategy for constructing cryptographicaly resilient S-boxes; obtained two S-boxes of relatively high cryptographic properties for the sake of illustration.

S-BOX, CELLULAR AUTOMATA, DIFFERENTIAL CRYPTOANALYSIS, LINEAR CRYPTOANALYSIS, FIXED POINT, CYCLIC STRUCTURE

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

КА — клітинний автомат

ЕКА — елементарний клітинний автомат

АНФ — алгебраїчна нормальна форма

НП — нерухома точка

MDP — максимальна ймовірність диференціалів (maximal differential probability)

MLP — максимальний лінійний потенціал (maximal linear potential)

ВСТУП

Актуальність. Наразі криптографія, як метод захисту інформації застосовується практично в усіх сферах людської діяльності, де виникає необхідність в захищеному обміні данними. Велика кількість симетричних криптосистем побудовані на так званій підстановочно-перестановочній мережі (Substitution-Permutation Network, SP-мережа). Один із основних компонентів таких мереж — S-блок — забезпечує нелінійність перетворень і протистояння кореляційному аналізу. Утім, у більшості сучасних криптосистем S-блоки реалізовані через таблиці, в яких відшукується потрібне значення вихідного блоку біт. Такий спосіб обчислення стає неефективним при перенесенні симетричної криптосистеми на SP-мережі на вбудовані системи з дуже обмеженими обчислювальними ресурсами та пам'яттю. Тому в останні роки зусиллями багатьох дослідників ведеться робота по оптимізації обчислень у S-блоках. Одним із перспективних варіантів для реалізації цієї мети є використання кліттиних обчислень (cellular computation) - тобто побудова S-блоків на основі клітинних автоматів. Такий підхід дозволяє у повній мірі використовувати переваги паралельних обчислень, є економним за пам'яттю та реалізація займає порівняно малу площу на інтегральній схемі.

Досі дослідження клітинних автоматів для використання їх при побудові S-блоків велися серед множини елементарних клітинних автоматів з околом радіусу 1 й оборотних клітинних автоматів. Але не були розглянуті деякі схеми побудови S-блоків із клітинних автоматів, а також поза увагою дслідників залишилися множина елементарних клітинних автоматів з околом радіусу 2.

Метою нашого дослідження є покращення методів синтезу криптографічно надійних S-блоків.

Завданням є формулювання та порівняльний аналіз методів побудови S-блоків на основі одновимірних клитинних автоматів. Для

цього необхідно здійснити:

1) Огляд існуючої літератури на тему застосування клітинних автоматів для цілей криптографії, зокрема, для побудови S-блоків, аналіз існуючих методів побудови S-блоків на основі клітинних автоматів.

2) Формулювання методів побудови S-блоків 8×8 на основі елементарних клітинних автоматів з околами 1 і 2.

3) Їх порівняльний аналіз.

Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предметом дослідження є криптографічні застосування одновимірних клітинних автоматів.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи криптографічного аналізу булевих функцій, методи комп'ютерного моделювання, методи дискретної математики, методи теорії автоматів, методи математичного моделювання.

Наукова новизна отриманих результатів полягає у тому, що вперше були запроновані методи побудови S-блоків на основі елементарних клітинних автоматів з околами радіусу 2 та показано, що S-блоки, одержані таким чином, мають прийнятні криптографічні характеристики.

Практичне значення результатів полягає в виробленні методу одержання криптографічно якісних S-блоків, що мають низьке енергоспоживання та знижену площу інтегральної схеми.

Апробація результатів та публікації. Результати дослідження, описані в даній роботі, частково були освітлені в доповіді на XIX Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих учених «Теоретичні та прикладні проблеми фізики, математики й інформатики» (місто Київ, 11-13 травня 2021 року).

1 КЛІТИННІ АВТОМАТИ ТА ЇХ ЗАСТОСУВАННЯ В КРИПТОГРАФІЇ

Поняття клітинного автомату (cellular automaton) було вперше введене у 40-х роках Станіславом Уламом і Джоном фон Нейманом. До 70-х років лише невилика кількість дослідників працювали в їх напрямку. Після появи знаменитої «Game of Life» Джона Конвея значний поштовх отримали дослідження двовимірних клітинних автоматів. Після публікації книги «A New Kind of Science» Стівена Вольфрама та деяких статей на цю тему були отримані фундаментальні результати в дослідженнях елементарних клітинних автоматів. З того часу вони використовуються в численних галузях прикладної математики: обчислювальні моделі, моделювання дискретних динамічних систем, моделювання процесів фундаментальної фізики тощо.

1.1 Базові визначення

У цих початкових підрозділах ми додержуємось визначень, що були введені в [6].

В загальному випадку ми розглядаємо автомати, побудовані на нескінченній прямокутній сітці. Формально її можна визначити як простір $\mathbb{Z}^d$, де кожній клітині відповідає кортеж $(x_0, x_1, ..., x_{d-1})$.

Означення 1.1. Автомат, визначений на такому просторі, називається *d-вимірним клітинним автоматом.*

Означення 1.2. Множина станів клітинного автомату задається як *скінченна множина* S.

Означення 1.3. Відповідно, у кожний момент часу стан усього автомату, або його *конфігурація* визначається відображенням простору клітин на простір станів $c : \mathbb{Z}^d \to S$.

Тоді *простір усіх конфігурацій* $S^{\mathbb{Z}^d}$ позначимо як $C(d, S)$ або просто C, якщо з контексту відомо, про які d та S йде мова.

Стан автомату змінюється в дискретні проміжки часу синхронно для всіх клітин. Стан кожної клітини визначається за деяким правилом у залежності від станів клітин її окілу. Окіл може визначатися різними способами, найчастіше - це клітини, що задовольняють деякій умові провідстань від основної клітини.

Означення 1.4. Формально *правило* є функцією $f : S^n \to S$, де n - потужність окілу точки, до якої застосовується правило.

З цих визначень можна вивести глобальне правило зміни конфігурації автомату.

Означення 1.5. *Глобальною функцією* зміни конфігурації автомату називається функція $G : C \to C$, $G(c) = e$ таке, що $e(x) = f(c(x^{(0)}), c(x^{(1)}),..., c(x^{(n-1)}))$ для усіх клітин x з простору $\mathbb{Z}^d$ та відповідних їм n сусідніх клітин $(x^{(0)}, x^{(1)},..., x^{(n-1)})$.

Ще одним важливим визначенням перенесення поняття нерухомої точки на КА і його узагальнення.

Означення 1.6. *Нерухомою конфігурацією* називається така конфігурація c, що $G(c) = c$.

Означення 1.7. *Періодичною в часі конфігурацією* конфігурацією називається така конфігурація c, для якої існує $k : G^k(c) = c$.

Ці визначення дають поняття про клітинний автомат як про математичний об'єкт, чиї основні властивості складають дискретність і однорідність у часі та просторі, локальність процесу оновлення станів.

Означення 1.8. *Клітинним автоматом* називається трійка (S, N, f), де S - множина станів, $N \in (S^{\mathbb{Z}^d})^n$ - вектор окілу, а $f : S^n \to S$ - локальне правило.

У теорії КА найчастіше розглядають два види околів: окіл фон Неймана й окіл Мура.

Означення 1.9. *Околом фон Неймана* точки $x = (x_0, x_1,..., x_{d-1}$ називається множина точок $N_x = \{y \mid \|x - y\| \leqslant 1\}$, де $\|y\| = \|y_0\| + \|y_1\| + ... + \|y_{d-1}\|$ - відома як Manhattan norm.

За норми фон Неймана кожна точка має $2d + 1$ сусідів. У двовимірному випадку, наприклад, це сама точка та точки безпосередньо згори, знизу, зправа та зліва (1.1).

Означення 1.10. *Околом Мура* точки називається називається множина точок $N_x = \{y \mid \|x - y\| \leqslant 1\}$, де $\|y\| = max\{y_0, y_1,..., y_{d-1}\}$ - відома як max norm.

За такої норми кожна точка має 3^d сусідів. Беручи знову двовимірний випадок, маємо квадрат з самою точкою в центрі (1.1).

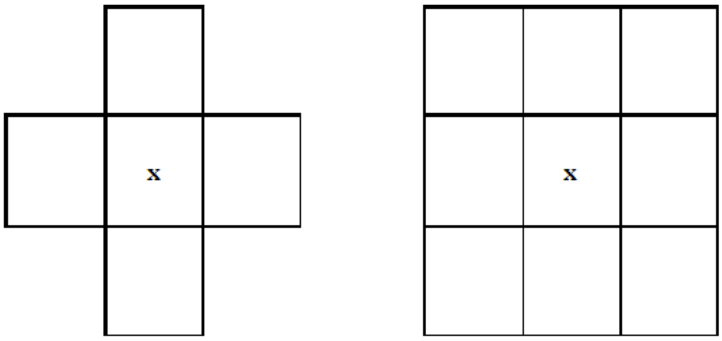


Рисунок 1.1 – околи фон Неймана та Мура

Означення 1.11. Узагальнюючи попередні означення, визначимо *окіл радіусу* r як множину точок $N_x = \{y \mid \|x - y\| \leqslant r\}$, де норма є Manhattan norm для околу фон Неймана та max norm для околу Мура.

Означення 1.12. Маючи визначення радіусу околу, говорять про *КА радіусу* r, як про КА, правило якого використовує окіл радіусу r.

Оскільки ми надалі розглядаємо переважно одновимірні КА, для нас неважливо, окіл якого типу вони мають, адже в одновимірному випадку одидва визначення еквівалентні.

1.2 Елементарні КА та їх класифікація

Означення 1.13. *Елементарним КА* називається одновимірний КА радіусу 1.

В окіл такого КА входить три точки, тому кількість можливих конфігурацій одного околу дорівнює вісьми, що дає 256 можливих елементарних автоматів.

Вольфрам, який вніс значний вклад у дослідження та класифікацію елементарних автоматів, запропонував оригінальну систему кодування правил елементарних автоматів [13]. Нехай у нас є бітова послдовність

$$f(111)f(110)f(101)f(100)f(011)f(010)f(001)f(000)$$

тоді її біти утворюють деяке число, десятковий запис якого ми і використаємо для позначення конкретного правила. Зрозуміло що такий спосіб кодування правил дає унікальні коди кожному правилу. Таким чином автомат з правилом, що дає бітову послідовність

$$f(111) = 0, f(110) = 1, f(101) = 1, f(100) = 0$$

$$f(011) = 1, f(010) = 1, f(001) = 1, f(000) = 0$$

називається Правило 110.

Одна з переваг цього кодування полягає в легкості його перенесення на більші радіуси, чим ми потім скористємося. Існує простий та інтуїтивно зрозумілий спосіб візуалізації елементарних КА.

Означення 1.14. *Просторово-часовою діаграмою* елементарного КА при початковій конфігурації c називається матриця над простором $\{0, 1\}$, $i-$тий рядок якої містить стан КА в $i-$тий в момент часу.

Просторово-часові діаграми найчастіше зображуються в вигляді сітки, де чорні клітинки відповідають стану 1, а білі - стану 0. На 1.2 можна побачити діаграму відомого КА Правило 110.

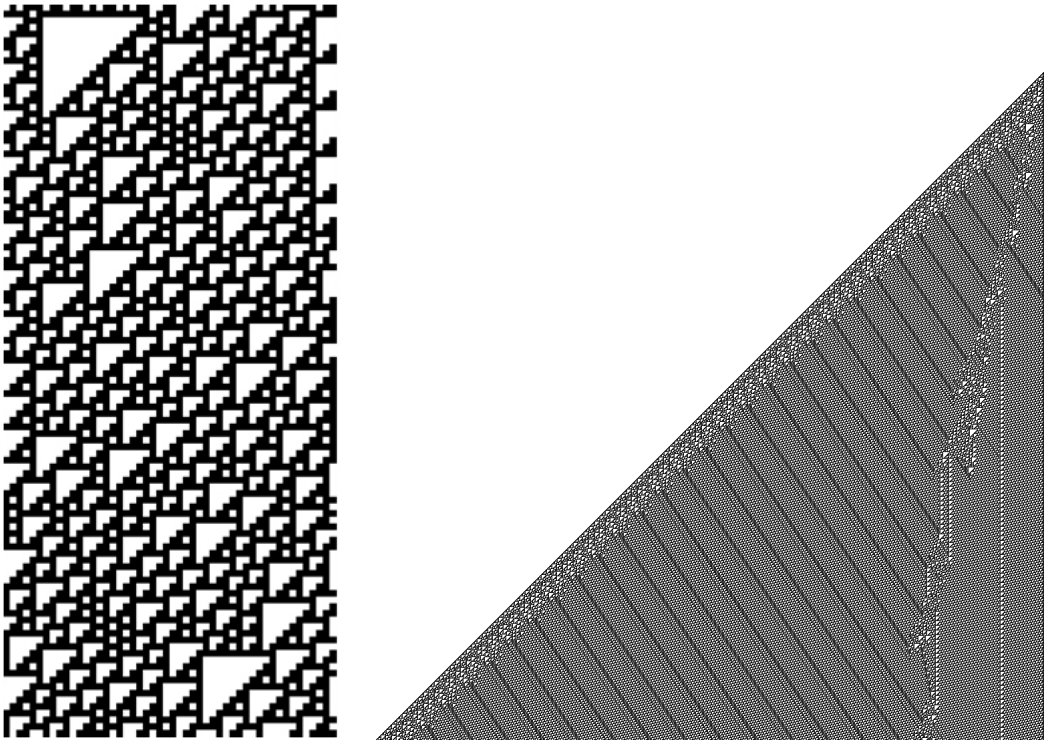


Рисунок 1.2 – Правило 110 за різного масштабування

Вольфрам випробовував кожне правило з великою кількістю випадкових початкових конфігурацій. На основі цих досліджень ним була запропонована классифікація правил на чотири родини:

1. Правила, що майже для всіх початкових конфігурацій приходять до нерухомої конфігурації.

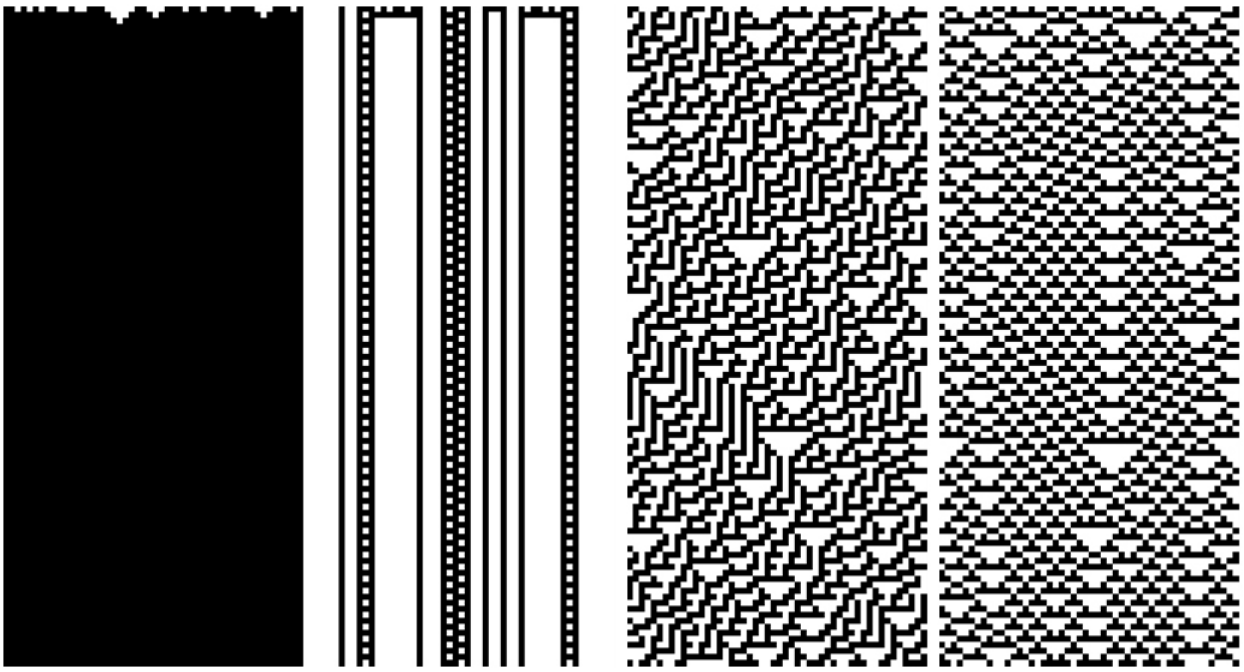
2. Правила, що майже для всіх початкових конфігурацій приходять до періодичної в часі конфігурації.

3. Правила, що майже для всіх початкових конфігурацій приходять до випадкової поведінки.

4. Правила, що утворють локальні структури зі складною взаємодією на діаграмах.

На 1.3 можна побачити представників усіх чотирьох класів за Вольфрамом.

Формулювання двох останніх правил є незадовільним для формальної теорії. Натомість існує формалізована версія класифікації



(а) *Правило 254* **(б)** *Правило 108* **(в)** *Правило 30* **(г)** *Правило 54*

Рисунок 1.3 – Представники чотирьох класів елементарних автоматів за Вольфрамом

Вольфрама[3]. Для визнчення цієї класифіцації нам необхідно навести додаткові визначення.

Означення 1.15. *Скінченною конфігурацією c* КА називається відображення скінченного підпростору $\mathbb{Z}^d$ на множину станів S:

$$Z_1 \times Z_2 \times ... \times Z_d \to S$$

де $\forall i = \overline{1,d} : Z_i \in \mathbb{Z}, \|Z\| < \aleph_0$.

Означення 1.16. Відповідно, *простором скінченних конфігурацій* C_F називається сукупність усіх скінченних конфігурацій КА.

Отже, нехай ми маємо КА з нерухомою конфігурацією c_0. Серед перераховних нижче властивостей, які визначають відповідні класи, КА належить до того класу, чия власивість виконуються і знаходиться найнижче в списку.

(1) $\forall c \in C_F \exists n \geqslant 1 : G^n(c) = q$. Інакше кажучи, кожна скінченна

конфігурація досягає стану q.

(2) $\forall c \in C_F \exists n, m, n \neq m : G^n(c) = G^m(c)$.

(3) Нехай є дві скіченні конфігурації $c, e \in C_F$. Тоді існує алгоритм, який визначає, чи існує таке n, що $G^n(c) = e$.

(4) обмеження не накладаються

Хоча наведена класифікація дозволяє однозначно віднести КА до одного з класів, задача визначення, до якого класу належить дана КА, як довели її автори, є невирішуваною.

Як було зазначено у вступі, одним із напрямків застосування КА є моделювання фундаментальних фізичних процесів. Оскільки такі процеси завжди є оборотними (тобто за повним описом системи можна визначити не тільки її майбутній стан, але й минулий), то й автомати, які ці процеси моделюють, мають бути оборотними. Значні теоретичні результати щодо боротності КА були отримані ще на початку 70-х років.

Означення 1.17. КА називається *оборотним КА*, якщо для глобальної функції $G(c)$ існує обернена до неї функція $G(c)$.

У статті [1] автори показали, що задача визначення оборотності для одновимірного КА є вирішуваною.

Теорема 1.1. *Існує алгоритм, який вирішує належність одновимірного КА до класу оборотних.*

Утім пошук самого оборотного автомату є нелегкою задачею: часто обернені автомати мають настільки великий окіл, що стають обчислювально неефективними.

1.3 Булеві функції та їх характеристики

У симетричній криптографії всі операції над даними розглядаються як операції над бітовими векторами, що формалізується за допомогою булевих функцій.

Означення 1.18. *Одновимірною булевою функцією* називається відображення $f : \{0,1\}^n \to \{0,1\}$

Означення 1.19. (n,m)*-вимірною булевою функцією* F називається відображення $f : \{0,1\}^n \to \{0,1\}^m$.

Такі функції ми будмо розглядати як вектор одновимірних булевих функцій.

Означення 1.20. *Алгебраїчною нормальною формою (АНФ)* булевої функції f від n змінних називається її представлення в вигляді поліному Жегалкіна:

$$P(x_1,...,x_n) = a_0 \oplus \bigoplus_{k=1}^{n} \bigoplus_{1 \leqslant i_1 \leqslant ... \leqslant i_k \leqslant n} a_{i_1,...,i_k} x_{i_1} ... x_{i_k}$$

Означення 1.21. *Алгебраїчним степенем* $deg(f)$ булевої функції f називається максимальний степінь доданків з ненульовим коефіцієнтом у АНФ.

АНФ й алгебраїчний степінь використовуються для визначення якісних ознак булевої функції. Зі збільшенням алгебраїчного степеня функції збільшується її нелінійність. Однак вимога максимізації вступає в кофлікт з вимогою збалансованості функції.

Означення 1.22. Булева функція $(n,m) - F$ називається *збалансованою*, якщо $\forall y \in V_m : \#\{x \in V_n : F(x) = y\} = 2^{n-m}$

Максимальний степінь збалансованої функції від n аргументів дорівнює $n-1$.

Означення 1.23. *Перетворенням Уолша-Адамара* булевої функції $(n,m) - F$ називається

$$W_F(a) = \sum_{x \in V_n} (-1)^{F(x) \oplus a \cdot x}$$

Означення 1.24. *Нелінійністю* булевої функції $(n,m) - F$

називається

$$NL_F = 2^{n-1} - max_{a \in V_n} |W_F(a)|$$

Існують також величини, які характеризують стійкість перетворень до диференціального та лінійного криптоаналізу — це максимум імовірності диференціалів (MDP) і максимальний лінійний потенціал (MLP).

Означення 1.25. *Диференціалом функції* f називається пара довільних векторів $(a, b) \in (V_n)^2$.

Означення 1.26. *Імовірність диференціалу* (a, b) функції f визначається як

$$DP^f_{\oplus}(a, b) = \frac{1}{2^n} \sum_{x \in V_n} [f(a \oplus x) = f(x) \oplus b],$$

де $[A]$ позначає індикатор події A. Відповідно, таблиця розподілу диференціалів будується за усіма парами (a, b).

Означення 1.27. *Максимумом імовірностей диференціалів* є величина $MDP^f = \max_{a \neq 0, b} DP^f_{\oplus}(a, b)$.

Означення 1.28. Лінійним потенціалом лінійної апроксимації (α, β) булевої функції $f : V_n \to V_n$, де (α, β) — довільна пара векторів з V_n, є величина

$$LP^f(\alpha, \beta) = \left| \frac{1}{2^n} \sum_{x \in V_n} (-1)^{\alpha \cdot x \oplus \beta \cdot f(x)} \right|^2.$$

Означення 1.29. *Максимальним лінійним потенціалом* називається величина $MLP(f) = \max_{\alpha, \beta \neq 0} LP^f(\alpha, \beta)$.

Також важливим показником стійкості до деяких видів алгебраїчних атак є значення кількості нерухомих точок і циклів довжини 2.

1.4 Огляд криптографічних застосувань клітинних автоматів

Основним напрямком, у якому ведуться досліждення КА у розрізі їх криптографічного застосування з середини 80-х років і досьогодні, є конструювання генераторів псевдовипадкових послідовностей. Згідно з класифікацією Вольфрама, до третього класу належать автомати, що на більшості початкових станів породжують випадкову непердбачувану поведінку. Автомати з такою властивістю активно досліджувались самим Вольфрамом, Кнутом та багатьма іншими.

Зокрема, у статті [14] Вольфрам запропонував потоковий шифр, побудований на автоматі Правило 30. Згенерована ним послідовність бітів використовувалась як шифруюча гамма. У цій же статті були представлені оцінки довжин найбільших циклів: виявилося, що абсолютна більшість станів автомату лежить на циклах максимальної довжини, а сама довжина залежить лише від розміру регістра, що займає автомат, приблизно як $2^{0.61N}$, де N - розмір регістра.

Однак, як було показано пізнішими дослідниками [7], твердження Вольфрама про NP-повноту задачі відновлення початкового стану, було несправедливим. Натомість були розроблені гібридні схеми, що могли використовувати одразу кілька правил, досягаючи таким чином більшої стійкості.

Наразі найпопулярнішим способом конструювання генераторів на КА є відбір правил за допомогою генетичного алгоритму оптимізації, де в якості цільової функції беруть міру ентропії породженої послідовності, як, наприклад, у [2]. Після відбору правил послідовності проходять додаткові випробування різними статистичними тестами. У роботі [9] показано, що випадково перемішуючи правила 90, 105, 150 і 165 можна отримати задовільний за якістю генератор послідовностей.

Мотивацією для використання елементарних КА для побудови S-блоків є відповідність багатьох правил критеріям, що висуваються до булевих функцій, які застосовуються як S-блоки класичних симетричних криптосистем таких, як DES, AES, і їх похідних. Також визначною є висока ефективність обчислень на автоматах у порівнянні з класичним табличним методом, де, як у схемі DES, потрібне значення вихідної четвірки бітів відшукується за таблицею. За рахунок паралельності обчислень на клітинних автоматах, процес шифрування можна оптимізовувати з застосуванням сучасних паралельних архітектур. Далі наведені деякі результати досліджень у цьому напрямку.

У роботі [12] була запропонована наступна схема. Задається вектор з елементарного КА, до якого входять:

— розмір автомату

— номер правила

— початкова конфігурація

— бітова маска, що визначає клітини автомату, яким відповідатимуть вхідні біти S-блоку, і які складатимуть вихід S-блоку, при цьому біти, що не присутні у вході/виході, ми називатимемо *фоновими клітинами*.

Відповідно до цієї схеми ними були протестовані всі 256 правил на 5, 6, 7, 8, 10, 30, 50, 100 кроках роботи КА, та серед них за критеріями нелінійності й автокореляції були обрані правила 30, 57, 86, 99, 135, 149. Для цих автоматів значення нелінійності й автокореляції коливалися в межах $[101, 108]$ і [56,80] відповідно.

Далі обрані правила випробовувались на відповідність критерію бієктивності. Для 8-бітного S-блоку, побудованого по вище описаній схемі, ці правила були випробувані на автоматах розміру від 8 до 500 клітин. Виявилося, що в випадку 8-бітового автомату лише близько 20% можливих виходів можна було спостерігати. З цих міркувань і були застосовані автомати зі збільшеною кількістю клітин. У результаті

випробування було встановлено, що правила 57 і 99 починають давати лише 8% можливих виходів, і з цієї причини вони були відкинуті й не використовувалися в подальших дослідженнях. Натомість інші правила досягали максимального показника у 62% при розмірі КА в 100 бітів і спадали до 56% при збільшенні розміру КА. Саме розмір у 100 бітів використовувався в подальших експериментах.

Варто зазначити, що розташування бітів входу/виходу серед клітин автомату має малий вплив на бієктивність: авторами статті вона оцінювалась у 2%.

Після цього правила 30, 86, 135, 149 були знову випробувані на нелінійнсть і автокореляцію, але з автоматом розміру 100, фонові біти якого задавалися випадково, а біти входу/виходу займали перші 8 бітів автомату. Найкращий результат дало правило 146, маючи одночасно найнижчий показник автокореляції та найвищий показник нелінійності.

Порівнявши свої результати з класичними методами проєктування S-блоків, автори дійшли висновку, що їх метод щонайменше дає таку саму якість, приносячи переваги КА над look-up tables.

Ті самі автори у своїй наступній статті [11] розробили S-блок на основі елементарного КА, призначений замінити собою актуальний 6×4 S-блок схеми DES, та порівняли їх між собою.

Оскільки блоки $n \times k$ й $n \times n$ дещо відрізняються за своєю структурою, то автори модифікували схему, запропоновану ними раніше. Тепер n початкових клітин автомату отримували вхідні біти S-блоку, а на вихід подавалися біти з перших k клітин.

Експерименти проводилися над правилами 30, 86, 135, 149, відсіяними в попередній роботі, за тими самими принципами, але на цей раз для більшої точності кількість випробувань з випадковими фоновими бітами була збільшена до 10000. Такі самі тести проводилися на класичних табличних S-блоках, що використовуються в схемі DES.

У результаті експериментів дослідники дійшли висновку, що, хоча показники нелінійності й автокореляції для S-блоків на обраних автоматах

є задовільними, вони в більшості випадків програють класичним S-блокам. Утім, за показниками строго лавинного критерію, S-блоки на автоматах у середньому знаходяться на рівні найкращих S-блоків схеми DES.

Подібну спробу застосування КА для заміни існуючих блоків здійснили дослідники в роботі [8]. Ними була запропонована альтернатива до S-блоків шифру AES, яка базується на двовимірних оборотних КА, описаних ними в [5]. Їх ключовою особливістю є залежність наступного стану клітини одночасно від поточного стану її околу та її власного стану на попередньому кроці.

Робота S-блоку представлена у вигляді матричного рівняння

$$N = f(M, C)$$

де N, M - вихдна та вхідна матриця відповідно, а

$$C = \begin{pmatrix} 63 & 36 & 63 & 36 \\ C6 & 6C & C6 & 6C \\ 8D & D8 & 8D & D8 \\ 1B & B1 & 1B & B1 \end{pmatrix}$$

У якості правил були використані правила 30, 45 і 229. Після досліджень за критеріями збалансованості вихідних векторів, кореляційного імунітету, нелінійності та швидкості обчислень були отримані такі результати:

— Усі S-блоки на автоматах завжди дають збалансовані вектори, навідміну від S-блоків шифру AES.

— S-блоки на автоматах мають показники кореляційного імунітету або порівняні з блоками AES, або набагато кращі.

— За нелінійністю отримати значної переваги не вдалося

— Швидкість обчислення вихідного вектору майже в 30 разів

перевершує швидкість табличних S-блоків.

Не зважаючи на позитивні результати, представлені в цій роботі, весь аналіз проводився лише на вісьми тестових векторах, і не включав у себе аналіз стійкості до диференційного та лінійного криптоаналізу.

Інші дослідники [4] розгляниули можливість застосуванняя простих одновимірних правил до конструювання S-блоків 4×4. Ідея такого S-блоку полягає в тому, щоб, застосовуючи одне правило, провадити ітерації над блоком вхідних бітів, циклічно зсуваючи їх на кожній ітерації, і отримати вихідний блок бітів за чотири ітерації автомату.

Побудувавши шифратор на ASIC-схемі з техпроцесом 180нм, вони досягли значної оптимізації площі схеми та її енергоспоживання. Наприклад, у порівнянні з найбільш оптимізованою імплементацією S-блоку шифру GIFT, їм удалося досягти 35% виграшу в площі схеми та 44% зменшення енергоспоживання.

Також представлена ними схема мала високу стійкість до side-channel attack, що є важливим показником якості з точки зору апаратної імплементації КА.

Вони шукали глобальні функції виду

$$G(X, Y, Z, W) = (f(X, Y, Z, W), f(Y, Z, W, X), f(Z, W, X, Y), f(W, X, Y, Z))$$

які були б бієктивними та криптографічно оптимальними. Бієктивність глобальних функцій визначалась наявними алгоритмами для вирішення ін'єктивності [1] та сюр'єктивності [10] глобальних функцій.

Висновки до розділу 1

З розглянутих нами джерел можна зробити висновок, що криптографічні властивості усіх елементарних КА були широко досліджені й отримані результати показують потенціал подальших досліджень у цьому напрямку.

Лише декілька елементарних КА показують результати достатні, аби можна було розглядати їх в якості альтернативи до наявних табличних S-блоків, але в той же час недостатні, аби такі рішення однозначно перевершували їх. Ми побачили, що на основі КА може бути розроблений та застосований на практиці S-блок, що забезпечує високу стійкість до загальноприйнятих методів криптоаналізу і водночас показує високу обчислювальну ефективність разом зі зменшеним споживанням енергії.

Для розв'язання нашої задачі ми застосуємо більш глибокий аналіз правил, ніж у наведених дослідженнях, і розширимо множину можливих правил збільшенням радіусу околу.

2 ПОСТАНОВКА ЗАДАЧІ ТА РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В цьому розділі детально описуються: постановка задачі нашого дослідження; методи побудови S-блоків з ЕКА радіусу 1 і 2, що були нами застосовані; дослідження характеристик S-блоків у залежності від різних методів їх побудови; відбір найкращих отриманих S-блоків для кожного з методів і їх порівняльний аналіз.

2.1 Постановка задачі

Нами визначені наступні складові задачі нашого дослідження:

1) На основі всіх ЕКА радіусу 1 і 2 побудувати відповідні їм S-блоки.

2) Серед побудованих таким чином S-блоків відібрати бієктивні.

3) Для S-блоків, побудованих з різною кількістю ітерацій правила, наявністю бітових зсувів між ітераціями та комбінуванням декількох правил, розрахувати наступні параметри:

а) кількість нерухомих точок;

б) кількість циклів довжини 2;

в) максимальну ймовірність диференціалів;

г) максимальний лінійний потенціал;

4) Дослідити поведінку цих параметрів у залежності від кількості ітерацій правила, наявності бітових зсувів і різних методів комбінування правил.

5) Відібрати найкращі S-блоки за наведеними параметрами.

6) Порівняти їх із відомими аналогами.

2.2 Отримані результати

У цьому розділі описуються методи побудови S-блоків з ЕКА радіусу 1 і 2, а також результати виконання задачі, окресленої в попередньому розділі.

2.2.1 Конструювання S-блоків з ЕКА

Частиною задачі нашого дослідження є конструювання S-блоків 8×8 з класу одновимірних правил радіусу 2, їх перевірка за основними криптографічними характеристиками та відбір правил з найкращими показниками для використання в якості S-блоків.

S-блоки породжуються з правил таким чином.

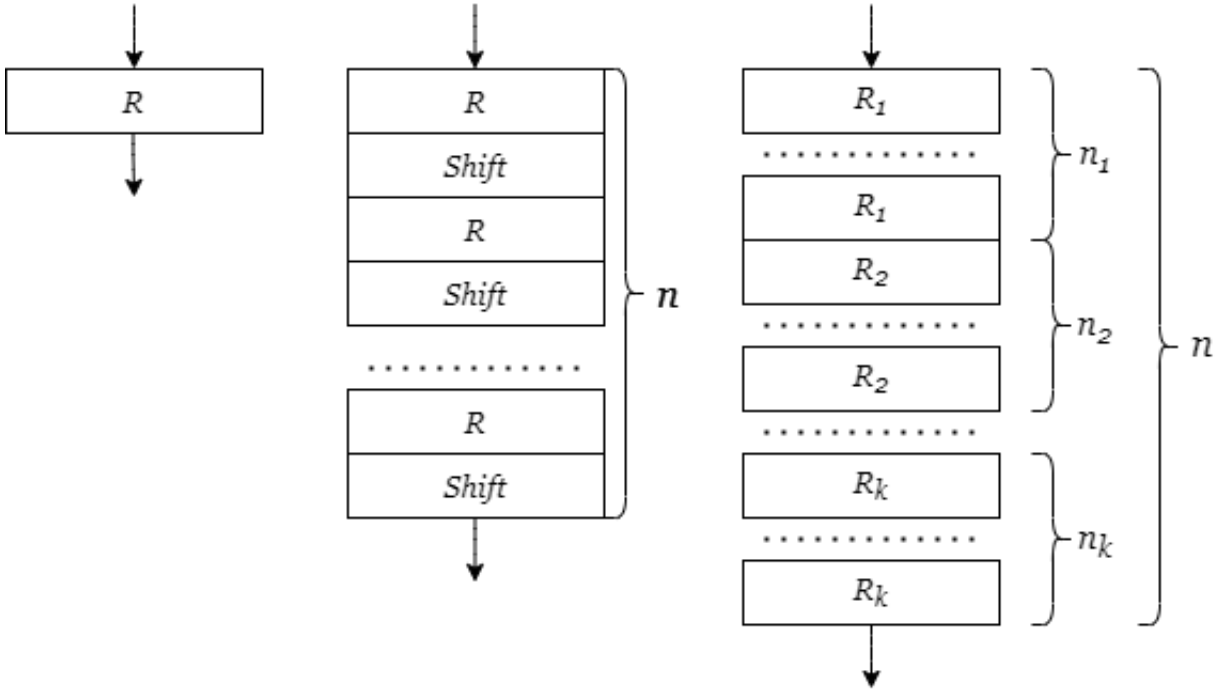


Рисунок 2.1 – Методи побудови S-блоків з базових бієктивних правил

Вхідний бітовий вектор задає початкову конфігурацію елементарного клітинного автомату розміру 8 бітів. Крайні біти автомату

пов'язані, утворюючи таким чином циклічну структуру. Така структура необхідна для того, щоб біти, близькі до краю (біти 0 і 7 у випадку радіусу околу, рівному одиниці, та біти 0, 1, 6, 7, коли радіус околу дорівнює 2), мали визначений окіл.

Вихід S-блоку отримуємо, застосувавши відповідне правило.

Для покращення характеристик S-блоку правило можна застосовувати кілька разів. Також ми пропонуємо застосовувати циклічні бітові зсуви між ітераціями правила та комбінувати кілька бієктивних правил з гарними характеристиками для отримання покращених S-блоків. Ілюстрацію даних методів наведено на рис. 2.1.

Вплив таких модифікацій на характеристики S-блоку буде детально описано в наступних підрозділах, що стосуються безпосередньо дослідження.

2.2.2 ЕКА радіусу 1

Серед 256 ЕКА радіусу 1 було відібрано 8 правил, що утворюють бієктивні S-блоки. Були розраховані характеристики S-блоків, побудованих за найпростішою моделлю. Усі бієктивні правила разом із розрахованими для них характеристиками наведені в таблиці 2.1.

Хоча попередні дослідники отримували результати, які допускали потенційне використання побудованих на їх основі S-блоків на практиці, наші розрахунки показали, що за показниками стійкості до диференціального та лінійного криптоаналізу такі S-блоки мають найгіршу можливу оцінку. З цієї причини подальші дослідження на цій множині правил нами проводитися не будуть.

Незбіжність наших результатів із результатами попередніх дослідників пояснюється тим, що, виходячи з області застосування побудованих нами S-блоків, ми розглядаємо виключно бієктивні правила. Таким чином з поля нашого зору випадають багато тих ЕКА радусу 1, що вважалися гарними кандидатами для побудови на них S-блоку.

Номер правила	Нерухомі точки	2-цикли	$2^8 \cdot$ MDP	$2^8 \cdot$ MLP
f	2	2	256	256
33	0	128	256	256
55	2	2	256	256
69	4	8	256	256
96	4	8	256	256
aa	2	2	256	256
cc	256	128	256	256
f0	2	2	256	256

Таблиця 2.1 – Характеристики бієктивних S-блоків, побудованих на ЕКА радіусу 1

2.2.3 ЕКА радіусу 2

Серед множини ЕКА радіусу 2 було знайдено 131 бієктивне правило. Для кожного правила були обчислені характеристики S-блоків з однією та двома ітераціями цього правила. У таблицях з 2.2 по 2.9 наведені розподіли цих характеристик у форматі значення характеристики — кількість S-блоків, що відповідають цьому значенню. Стовпці зі значеннями характеристик, яким не відповідає жоден S-блок, задля лаконічності, були пропущені, а значення MDP і MLP, як і в таблиці 2.1, пронормовані до проміжку від 0 до 256.

Кількість НП	0	2	4	6	8	10	14	16	80	144
Кількість S-блоків	18	60	16	4	8	10	8	2	4	1

Таблиця 2.2 – Розподіл кількості нерухомих точок для S-блоків з однією ітерацією правила.

За розподілом, наведеним у таблиці 2.2, спостерігаємо, що всі значення кількості НП не перевищують 144 і зосереджені біля значення 2.

Кількість 2-циклів	2	6	8	10	14	20	26	32	60	128
Кількість S-блоків	70	10	29	2	1	4	2	4	1	8

Таблиця 2.3 – Розподіл кількості 2-циклів для S-блоків з однією ітерацією правила.

З розподілу значень кількості 2-циклів у таблиці 2.3 бачимо, що, хоча кількома S-блоками досягнуте максимальне значення, більшість зосереджена на трьох найменших значеннях.

Ці розподіли свідчать про загальну тенденцію S-блоків, побудованих таким чином, до мінімізації числа циклів.

$2^8 \cdot MDP$	46	48	54	56	64	68	72	80	84
Кількість S-блоків	3	4	4	15	11	4	7	5	5
$2^8 \cdot MDP$	100	108	112	132	140	146	148	152	256
Кількість S-блоків	2	7	14	6	2	1	6	3	32

Таблиця 2.4 – Розподіл MDP для S-блоків з однією ітерацією правила.

Значення MDP в таблиці 2.4 розподілені досить нервіномірно, причому чверть усіх S-блоків мають найгірше можливе значення цієї характеристики, а найкраще значення дорівнює 46, що є незадовільним показником.

$2^8 \cdot MLP$	64	100	144	196	256
Кількість S-блоків	29	22	33	18	29

Таблиця 2.5 – Розподіл MLP для S-блоків з однією ітерацією правила.

S-блоки розподілені майже рівномірно між п'ятьма значеннями MLP (таблиця 2.5). І, хоча найкращого значення за даної вибірки досягає значна кількість S-блоків, це найкраще значення є незадовільним у рамках нашого дослідження.

З цих причин ми переходимо до S-блоків із двома ітеріціями правила, припускаючи, що такий підхід надасть більш якісні за параметрами MDP та MLP S-блоки.

Кількість НП	4	12	16	20	28	40	52	64	120	256
Кількість S-блоків	70	10	29	2	1	4	2	4	1	8

Таблиця 2.6 – Розподіл кількості нерухомих точок для S-блоків з двома ітераціями правила.

З розподілу, наведеному в таблиці 2.6, спостерігаємо розширення діапазону значень у порівнянні з попередньою схемою, однак більшість S-блоків досі зосереджені біля мінімальних значень характеристики.

Кількість 2-циклів	2	8	10	12	14	16	18	20	30	34	60	68	98	128
Кількість S-блоків	17	47	1	9	2	3	7	1	1	4	1	8	2	28

Таблиця 2.7 – Розподіл кількості 2-циклів для S-блоків з двома ітераціями правила.

Діапазон і тенденція до скупчення біля мінімальних значень кількості 2-циклів збереглися в порівнянні з попередньою схемою, як можна спостерігати за розподілу в таблиці 2.7.

За таблицею 2.8 спектр значень, що приймають характеристики, розширився. Мінімальне значення спало, що свідчить про відносне покращення якості S-блоків. Однак більшість з них зосереджені на проміжку неприпустимих для нас значень.

$2^8 \cdot MDP$	16	20	24	26	30	32	36	40	46
Кількість S-блоків	2	5	2	3	1	3	5	2	3
$2^8 \cdot MDP$	48	54	60	64	80	84	98-150	151-255	256
Кількість S-блоків	2	2	9	4	8	2	20	19	39

Таблиця 2.8 – Розподіл MDP для S-блоків з двома ітераціями правила.

$2^8 \cdot MLP$	30	36	42	49	60	64	100	105	110	121	132	144	169	196	225	256
Кількість S-блоків	3	4	2	7	1	20	3	2	4	8	3	27	2	4	6	35

Таблиця 2.9 – Розподіл MLP для S-блоків з двома ітераціями правила.

Відповідно до даних у таблиці 2.9, спектр значень розширився більш ніж у три рази, розподіл став більш нерівномірним, але мінімальне значення даної характеристики спало. Це, вкупі зі згаданими вище причинами дає нам мотивацію до подальшого збільшення числа ітерацій правила в S-блоці.

S-блок	Кількість HT	Кількість 2-циклів	$2^8 \cdot$ MDP	$2^8 \cdot$ MLP
8f40bf34	2	2	46	64
c54bc5cc	2	2	46	64
c587c5cc	2	2	48	64
f102df0e	2	2	48	64
AES	0	1	4	4

Таблиця 2.10 – Загальна талбиця найкращих S-блоків з однією ітерацією правила

Серед S-блоків, побудованих на EKA радіусу 2 з однією та двома ітераціями, ми відібрали 4 та 3 відповідно найкращих, оптимальних за показниками S-блоки. Їх характеристики в порівнянні з S-блоком схеми

AES наведені в таблицях 2.10 і 2.11.

За наведеними даними можна спостерігати, що, по-перше, навідміну від EKA радіусу 1, EKA радусу 2 породжують S-блоки з кращими характеристиками; а по-друге, зі збільшенням числа ітерацій правила мінімальні значення MDP і MLP серед усіх S-блоків зменшується. Останнє дає нам привід вважати, що з подальшим збільшенням кількості ітерацій правила ми зможемо приблизити значення характеристик до бажаного рівня.

Також можна спостерігати, що найкращі правила в випадку однієї ітерації зі збільшенням кількості ітерацій поступаються іншим правилам, котрі навпаки, свої досить посередні характеристики покращили більш ніж у два рази. Така поведінка дає нам привід вважати, що поведінку будь-якого правила складно передбачити.

Усього нами були обчислені характеристики S-блоків з кількістю ітерацій правила, що сягає вісьми. На основі цих данних і наведених на рисунку 2.2 узагальнюючих графіків ми можемо зробити деякі важливі спостереження.

За графіком мінімумів можна бачити, як при переході від однієї до трьох ітерацій поступово спадають мінімальні значення MDP та MLP. Це явище, строго кажучи, не свідчить про загальне покращення показників S-блоків, але дає причину вважати, що збільшення кількості ітерацій поліпшить характеристики деякої підмножини S-блоків, тому в цілому такий метод їх оптимізації по MDP та MLP є доцільним.

S-блок	Кількість HT	Кількість 2-циклів	$2^8 \cdot$ MDP	$2^8 \cdot$ MLP
d2ff2d	4	2	26	49
4b00b4ff	4	2	26	49
59599559	4	2	26	49
AES	0	1	4	4

Таблиця 2.11 – Загальна талбиця найкращих S-блоків з двома ітераціями правила

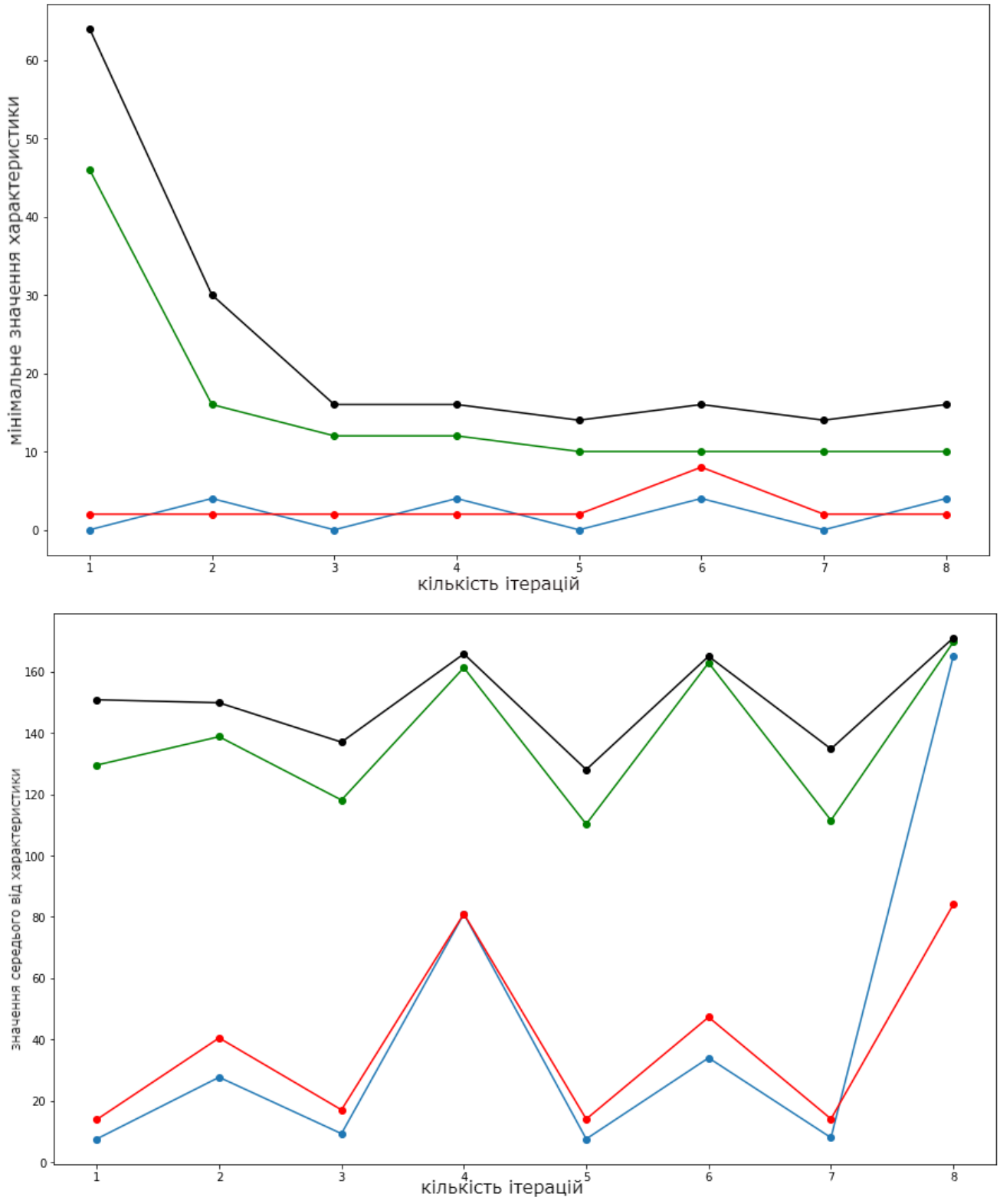


Рисунок 2.2 – Мінімуми ті середні значення характеристик за різної кількості ітерацій правила. Чорному кольору відповідає MDP, зеленому — MLP, червоному — 2-цикли, синьому — нерухомі точки.

Однак, слід зауважити, що,згідно тих самих мінімумів MDP та MLP, збільшення кількості ітерацій правила більше трьох заради їх оптимізації не приносить таких помітних результатів, як на відрізку від 1 до 3.

Приведені вище спостереження дають нам право вважати недоцільним ітерувати одне правило більше п'яти разів, оскільки це не тільки не покращить їх характеристики, але й створить надлишкове обчислювальне навантаження, якого ми, виходячи з мети нашого дослідження, маємо уникати.

Мінімуми нерухомих точок періодично коливаються, приймаючи значення 0 при непарній кількості ітерацій і значення 4 при парній. Така поведінка пояснюється постійною наявністю щонайменше двох 2-циклів: при парній кількості ітерацій вони стають нерухомими точками.

Поведінка мінімумів 2-циклів на всьому проміжку, окрім піку на шести ітераціях, є статичною. Причиною такого стрибка є та обставина, що серед усіх натуралних чисел від 1 до 8 шістка єдина у базисі свого розкладу на прості дільники має два числа, а не одне. Тому ці S-блоки зберігають 2-цикли й від S-блоків із двома ітераціями, і від S-блоків із тьома.

Навідміну від мінімумів, поведінка усереднених показників має очевидну періодичну структуру. MDP та MLP, виказуючи на початку тенденцію до зниження, згодом приходять до періодичного коливання. Середні значення зростають при парній кількості ітерацій.

2-цикли також виявляють періодичну поведінку. Середні значення при непарній кількості залишаються на одному рівні, при парній — мають виражені піки на значеннях, що є степенями двійки — 4 та 8. Для встановлення того, чи роповсюджується така поведінка на більшу кількість ітерацій, потрібні додаткові обчислення.

Нерухомі точки в цілому мають ту саму поведінку, що й 2-цикли, але при кількості ітерацій, що дорівнює степеням двійки, середнє значення, вочевидь, зростає за прогрессією.

Зі зроблених спостережень за середніми значеннями ми можемо

зробити висновок, що серед S-блоків з парною кількістю ітерацій менше потенційно придатних для практичного використання, тому коло пошуків можна скоротити до S-блоків з непарною кількістю ітерацій правила.

Взагалом, виходячи зі спостережень за характеристиками S-блоків у залежності від кількості ітерацій правила, оптимальним ми вважаємо використання трьох ітерацій правила, оскільки четверта ітерація значно погіршує усереднені характеристики, а п'ята не надає покращення, заради якого варто збільшувати кількість ітерацій майже в два рази.

Далі ми дослідили вплив бітових зсувів на характеристики S-блоків. Для цього ми будемо робити циклічний бітовий зсув на певну кількість бітів після кожної ітерації та спостерігати за зміною характеристик за різних зсувів.

Випробувавши цей метод спочатку на всіх S-блоках із трьома ітераціями правила для зсуву на 1 і 4 біти, було з'ясовано, що зсуви впливають лише на кількість нерухомих точок і 2-циклів, причому, у досить непередбачуваній мірі. Заради отримання більш детальних результатів, були обчислені характеристики обмеженої множини S-блоків для всіх можливих зсувів. Результати цих обчислень наведені в таблиці 2.12.

З даної таблиці ми можемо спостерігати кілька закономірностей. По-перше, існує деяка множина циклічних послідовностей значень НП та 2-циклів, на кожну з яких припадає декілька S-блоків. Наприклад, для S-блоків d2ff2d, 4b00b4ff і 59599559 значення належать одній послідовності. Те, що це не є простим збігом, підтверджує той факт, що пара 3a783a33 та 70fbd408f також поділяє між собою одну послідовність. Без сумніву, при більш детальному розгляді всіх S-блоків ми зможемо розбити їх множину на класси за послідовностями, яким вони відповідають.

По-друге, ми переконалися, що майже в усіх випадках за допомогою бітових зсувів характеристики S-блоку можна покращити. Наприклад, для S-блоку 3ab43a33 спостерігаємо, що зі значення (14, 10) при

	0		1		2		3		4		5		6		7	
	НП	2-ц.	НП	2-ц.	НП	2-ц.	НП	2-ц.	НП	2-ц.	НП	2-ц.	НП	2-ц.	НП	2-ц.
d2ff2d	0	8	2	2	36	44	2	2	0	8	2	2	12	44	2	2
12ed02fd	2	2	0	8	2	2	12	8	2	2	0	8	2	2	12	8
2cf100ff	10	8	0	30	22	12	0	6	2	8	8	30	6	12	8	6
39723933	10	6	12	8	2	10	0	32	2	6	12	8	2	10	0	32
3a783a33	14	8	0	2	2	4	0	2	6	8	0	2	2	4	0	2
3ab43a33	14	10	4	4	6	14	0	4	6	10	4	4	22	14	0	4
40fb30cf	10	6	0	32	2	10	12	8	2	6	0	32	2	10	12	8
4b00b4ff	0	8	2	2	36	44	2	2	0	8	2	2	12	44	2	2
50af10ef	2	2	0	8	2	2	12	8	2	2	0	8	2	2	12	8
59599559	0	8	2	2	12	44	2	2	0	8	2	2	36	44	2	2
70fb408f	14	8	0	2	2	4	0	2	6	8	0	2	2	4	0	2

Таблиця 2.12 – Значення НП і 2-циклів для різних зсувів. У першому рядку вказано, на скільки біт діє циклічний зсув вліво після кожної ітерації правила.

відсутності зсуву ця характеристика покращується до (0, 4) при зсуві на три або сім бітів. Утім, як передбачити, чи подіє такий метод гарантовано, ще належить з'ясувати. Наразі впевнено стверджувати, на скільки біт треба здійснювати зсув для оптимізації характеристик, можна, лише знаючи, якому циклу належить данний S-блок.

Також належить дослідити вплив довільних бітових перестановок на ті самі характеристики, а саме, чи можливо повністю позбавитися від циклів за їх допомогою, а якщо неможливо, то встановити нижню границю для оптимізації числа НП та 2-циклів таким шляхом.

Далі була досліджена можливість оптимізації характеристик S-блоків шляхом комбінування декількох правил. При цьому будуть розглянуті різні схеми: з двома різними правилами, з трьома різними правилами та обидва перераховані варіанти зі зсувами. Записувати різні види комбінацій будемо в такій нотації: $k_1 : R_1 \to k_2 : R_2 \to ... \to k_n : R_n$, де k_i — це кількість ітерацій правила $R_i, i = \overline{1, n}$.

Перебравши всі комбінації для схеми виду $3 : R_1 \rightarrow 3 : R_2$, ми отримали S-блоки, характеристики яких складно передбачити, виходячи тільки з даних про характеристики тих S-блоків, композицією яких вони є. Проілюструємо це кількома прикладами.

При комбінуванні правил d2ff2d та 12ed02fd, які окремо мають характеристики (0, 8, 20, 30) і (2, 2, 24, 30) відповідно, ми отримали S-блок з характеристиками (2, 1, 24, 25). Тобто жодна характеристика не перевищує відповідну максимальну з обох правил, а два параметри при цьому навіть покращились.

При комбінуванні правил d2ff2d та 39723933, де друге має характеристики (2, 6, 16, 20), отримано S-блок із характеристиками (2, 1, 24, 27). Бачимо, що значення MDP погіршилось у порівнянні з обома складовими. Із цього прикладу стає очевидною несправедливість припущення про те, що комбінування двох S-блоків із різними правилами гарантовано дає не гірший S-блок за розглянутими нами параметрами.

При комбінуванні правил 2cf100ff і 50af10ef, що мають значення характеристик (10, 8, 14, 36) і (2, 2, 24, 16) відповідно, був отриманий S-блок із параметрами (4, 2, 8, 14). На цьому прикладі ми спостерігаємо значне покращення за значеннями MDP та MLP. З усіх випробуваних комбінацій саме ця виявилася найкращою. Застосувавши циклічний бітовий зсув на 3 біти під час роботи S-блоку за першим правилом, ми покращили його характеристики до значень (2, 1, 8, 14).

Також варто зауважити, що порядок застосування двох правил має вплив на властивасті всього S-блоку. Наприклад, згаданий вище приклад комбінування правил d2ff2d та 12ed02fd при зворотньому їх застосуванні породить S-блок із характеристиками (2, 1, 20, 20).

Утім, порядок застосування правил, згідно наших спостережень, впливає лише на значення MDP та MLP, залишаючи значення кількості НП та 2-циклів постійними. Це значить, що зміна порядку застосування правил є недієвою при намірі оптимізації двох останніх характеристик, і єдиним способом досі залишається випробування циклічних бітових

зсувів.

Також були випробувані комбінації виду $2 : R_1 \to 3 : R_2$. Узагалом, така схема дає S-блоки, порівняні за значеннями характеристик із попередньою схемою, при цьому значно переважаючи за якістю значень НП та 2-циклів, що пояснюється загальною кількістю ітерацій, яка в цій схемі дорівнює 5.

Найкращим S-блоком, отриманим за такою схемою, є композиція двох ітерацій правила 2cf100ff і трьох ітерацій правила 4b00b4ff. Його характеристики дорівнюють (0, 0, 8, 16), що лише незначно поступається за MLP найкращому S-блоку, побудованому за попередньою схемою. Однак за рахунок відсутності зсувів і однієї ітерації правила даний S-блок виграє за швидкодією.

Ще двома схемами, для яких випробування проводилися лише частково, були схеми, що комбінують три правила: $3 : R_1 \to 3 : R_2 \to 3 : R_3$ і $2 : R_1 \to 3 : R_2 \to 2 : R_3$. Але, не дивлячись на загальну якість породжуваних таким чином S-блоків, нам не вдалося знайти такий, що перевершив би показники двох згаданих вище.

З огляду на велику кількість схем і комбінацій для кожної з них, за потреби знайти S-блоки з кращими властивостями доведеться виконати досить великий об'єм обчислень, що виходить за рамки даної роботи. Тому на цьому ми завершуємо пошук S-блоків і натомість наведемо деякі інші характеристики обох тих, що були відібрані вище.

В S-блоці $3 : 2CF100FF \to 3 : 50AF10EF$ всі змінні суттєві. Значення коефіцієнту поширення в середньому дорівнює 1016 для всіх змінних, алгебраїчний степінь усіх компонентних функцій дорівнює 7, а нелінійність кожної — 104.

Алгебраїчний степінь є максимальним для класу збалансованих функцій, коефіцієнт поширення в середньому наближається до необхідного для відповіднсті строгому лавинному критерію в середньому, значення нелінійності наближається до нелінійності бент-функцій. Такі властивості свідчать про добру криптографічну якість S-блоку.

В S-блоці $2 : 2CF100FF \rightarrow 3 : 4B00B4FF$ всі змінні суттєві. Значення коефіцієнту поширення в середньому дорівнює 1024 для всіх змінних, тобто даний S-блок відповідає строгому лавинному критерію в середньому. Алгебраїчний степінь для всіх компонентних функцій дорівнює 6, нелінійність — 108.

За сукупністю обчислених характеристик цей S-блок має високі криптографічні якості, та потенціально може бути використаний для побудови SP-мереж в умовах обмежень на споживання енергії та площу інтегральної схеми.

Таблиці підстановки описаних вище S-блоків наведені в таблицях 2.13 та 2.14.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	FF	46	8C	C6	19	45	8D	E8	32	80	8A	D9	1B	27	D1	3E
1	64	88	1	9	15	94	B3	F	36	BC	4E	A1	A3	B0	7C	B7
2	C8	10	11	97	2	B4	12	E9	2A	A5	29	E0	67	EF	1E	5D
3	6C	90	79	99	9C	AD	43	A6	47	4F	61	82	F8	98	6F	81
4	91	51	20	C9	22	25	2F	2C	4	2D	69	FB	24	6B	D3	26
5	54	49	4B	DA	52	AA	C1	65	CE	7	DF	AF	3C	95	BA	CD
6	D8	3B	21	34	F2	1C	33	50	39	7F	5B	F5	86	BE	4D	C5
7	8E	F0	9E	6A	C2	56	5	DD	F1	EA	31	2E	DE	37	3	3F
8	23	63	A2	74	40	EC	93	1F	44	84	4A	87	5E	D0	58	DB
9	8	CB	5A	F4	D2	70	F7	AE	48	CC	D6	53	A7	41	4C	C0
A	A8	E4	92	16	96	FD	B5	13	A4	6D	55	B2	83	D7	CA	E6
B	9D	1A	E	28	BF	FA	5F	E2	78	35	2B	EE	75	17	9B	9F
C	B1	3A	76	8F	42	C3	68	ED	E5	7A	38	57	66	A9	A0	60
D	72	B	FE	89	B6	59	EB	73	D	14	7D	71	9A	77	8B	CF
E	1D	C7	E1	F6	3D	AB	D4	30	85	C4	AC	B9	A	B8	BB	E7
F	E3	7B	D5	18	62	DC	5C	F3	BD	C	6E	F9	6	FC	7E	0

Таблиця 2.13 – S-блок за схемою $2 : 2CF100FF \rightarrow 3 : 0x4B00B4FF$.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	A5	4B	9A	96	30	35	EA	2D	B3	60	19	6A	1D	D5	1F
1	5A	66	67	C3	C0	FE	32	D6	D4	97	3A	45	AB	ED	3E	E2
2	B4	76	CC	F2	CE	61	87	B2	81	B	FD	21	64	D	AD	52
3	A9	3C	2F	44	74	7D	8A	A7	57	95	DB	CD	7C	FC	C5	31
4	69	C	EC	47	99	BF	E5	7B	9D	58	C2	43	F	5F	65	3F
5	3	EF	16	D7	FB	AA	42	38	C8	9	1A	8D	5B	E0	A4	20
6	53	23	78	A8	5E	24	88	B9	E8	68	FA	B1	15	36	4F	41
7	AE	6D	2B	7A	B7	83	9B	DD	F8	92	F9	A	8B	80	62	93
8	D2	4D	18	75	D9	8C	8E	8F	33	E1	7F	6B	CB	A2	F6	71
9	3B	79	B0	59	85	90	86	29	1E	22	BE	D3	CA	E6	7E	98
A	6	A3	DF	BD	2C	A1	AF	9F	F7	EB	55	1C	84	C6	70	10
B	91	54	12	DC	34	D8	1B	A0	B6	3D	C1	EE	49	5	40	C9
C	A6	BA	46	C7	F0	B5	51	B8	BC	AC	48	94	11	E9	73	4C
D	D1	DE	D0	CF	F5	E	63	8	2A	6E	6C	50	9E	77	82	E4
E	5D	E3	DA	5C	56	4A	F4	26	6F	E7	7	4	37	28	BB	72
F	F1	2E	25	13	F3	2	14	39	17	89	1	9C	C4	4E	27	FF

Таблиця 2.14 – S-блок за схемою $3 : 0x2CF100FF \to 3 : 0x50AF10EF$.

Висновки до розділу 2

У результаті нашого дослідження S-блоків, побудованих на ЕКА радіусу 1 і 2, та схем побудови S-блоків на їх основі ми дійшли декількох висновків:

1) S-блоки, побудовані на ЕКА радіусу 1, не мають достатнього рівня стійкості до диференціального та лінійного криптоаналізу, тому доцільним є використиння більш складних схем породження S-блоків.

2) S-блоки, побудовані на ЕКА радіусу 2, покращують свої характеристики зі збільшенням кількості ітерацій правила. Це значить, що вдосконалення схеми породження S-блоків з автоматів потенційно надасть S-блоки р досить високими показниками стійкості.

3) З підвищенням кількості ітерацій уже після третьої ітерації це покращення є незначним. Тому оптимальними для використання є дво- та триітеративні компоненти.

4) Застосування бітових зсувів між ітераціями правила здатне оптимізувати кількість НП і 2-циклів S-блоку.

5) Комбінування двох правил, що застосовуються послідовно, здатне породити ще більш оптимізовані S-блоки. Зокрема, були отримані два S-блоки з характеристиками 2, 1, 8, 14 і 0, 0, 8, 16 нерухмих точок, 2-циклів, MDP та MLP відповідно. Обидва вони мають високі алгебраїчні степені компонентних функцій, високу нелінійність, а остання також відповідає строгому лавинному критерію в середньому.

Тобто в результаті даного дослідження був отриманий метод, за допомогою якого можна породжувати прийнятні за криптографічними властивостями S-блоки, що мають потенціал використання в шифрах, призначених для цілей легкої криптографії — за рахунок порівняно низького споживання енергії та зменшеної площі схеми для обчислювальних компонентів, побудованих на клітинних автоматах.

ВИСНОВКИ

У результаті огляду літератури, що стосується криптографічних застосувань клітинних автоматів, було з'ясовано, що множина ЕКА радіусу 1 була широко досліджена з точки зору криптографічних властивостей автоматів, що до неї належать, і отримані результати вказують на перспективність подальших досліджень інших множин одновимірних правил. Також було з'ясовано, що генерація S-блоків на основі одновимірних правил може породити криптографічно стійкі S-блоки, що мають знижене енергоспоживання та площу інтегральної схеми порівняно з наявними аналогами.

Однак, поза увагою дослідників залишилася проблема генерації криптографічно стійких S-блоків 8×8, на якій і було зосереджене наше дослідження.

Нами були сформульовані та випробувані такі техніки отримання S-блоків із ЕКА радіусу 1 і 2: ітерувати одне правило кілька разів, застососувати бітові зсуви між ітераціями, комбінувати два чи більше правил у межах одного S-блоку.

У результаті випробувань указаних вище методів на декількох десятках знайдених нами бієктивних правил, ми дійшли деяких висновків щодо їх дієвості.

1) ЕКА радіусу 1 не здатні породити криптографічно стійкі S-блоки 8×8 у рамках описаних методів — головним чином через те, що серед автоматів цієї множини майже немає бієктивних правил.

2) Збільшення кількості ітерацій правила призводить до зменшення значень MDP та MLP, що свідчить про підвищення стійкості до диференціального та лінійного криптоаналізу.

3) За допомогою бітових зсувів між ітераціями в більшості випадків можна мінімізувати кількість нерухомих точок і 2-циклів.

4) Послідовне застосування кількох правил у межах одного S-блоку

здатне до подальшого зменшення значень MDP та MLP.

Застосувавши сукупність цих методів до знайдених нами бієктивних ECA радіусу 2, ми отримали два порівняно високих за криптографічними якостями S-блоки.

Подільші дослідження в цій області можуть виявити нові ефективні схеми комбінування правил, бітові перестановки, що можуть цілком позбавити S-блоки нерухомих точок і 2-циклів, а також провести вичерпний пошук бієктивних правил серед ECA радіусу 2.

ПЕРЕЛІК ПОСИЛАНЬ

[1] S. Amoroso та Y. Patt. “Decision Procedures for Surjectivity and Injectivity of Parallel Maps for Tessellation Structures”. в: *J. Comput. Syst. Sci.* 6 (1972), с. 448—464.

[2] Pascal Bouvry, Franciszek Seredyński та Albert Zomaya. “Application of Cellular Automata for Cryptography.” в: січ. 2003, с. 447—454.

[3] Karel Culik II та Shuangni Yu. “Yu, S.: Undecidability of CA Classification Schemes. Complex Systems 2, 177-190”. в: *Complex Systems* 2 (січ. 1988).

[4] Ashrujit Ghoshal та ін. “Lightweight and Side-channel Secure 4 × 4 S-Boxes from Cellular Automata Rules”. в: *IACR Transactions on Symmetric Cryptology* 2018.3 (вер. 2018), с. 311—334. DOI: 10.13154/tosc.v2018.i3.311-334. URL: https://tosc.iacr.org/index.php/ToSC/article/view/7305.

[5] Jegadish K J, K. Reddy та Salivahanan S. “Novel and Efficient Cellular Automata Based Symmetric Key Encryption Algorithm for Wireless Sensor Networks”. в: *International Journal of Computer Applications* 13 (січ. 2010). DOI: 10.5120/1767-2424.

[6] Jarkko Kari. “Theory of cellular automata: A survey”. в: *Theoretical Computer Science* 334.1 (2005), с. 3—33. ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2004.11.021. URL: http://www.sciencedirect.com/science/article/pii/S030439750500054X.

[7] CK Koc та AM Apohan. “Inversion of cellular automata iterations”. в: *IEE Proceedings-Computers and Digital Techniques* 144.5 (1997), с. 279—284.

[8] K. J. J. Kumar та V. Karthick. “AES S-Box Construction using One Dimensional Cellular Automata Rules”. в: *International Journal of Computer Applications* 110 (2015), с. 35—39.

[9] Moshe Sipper та Marco Tomassini. “Generating Parallel Random Number Generators By Cellular Programming”. в: *International Journal of Modern Physics C* 07 (жовт. 1996). DOI: 10.1142/S012918319600017X.

[10] Klaus Sutner. “Linear Cellular Automata and de Bruijn Automata”. в: (серп. 1998). DOI: 10.1007/978-94-015-9153-9_12.

[11] Miroslaw Szaban та Franciszek Seredynski. “Cellular Automata-Based S-Boxes vs. DES S-Boxes”. в: *Parallel Computing Technologies*. за ред. Victor Malyshkin. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, с. 269—283. ISBN: 978-3-642-03275-2.

[12] Miroslaw Szaban та Franciszek Seredyński. “Application of cellular automata to create S-box functions”. в: трав. 2008, с. 1—7. DOI: 10.1109/IPDPS.2008.4536378.

[13] S. Wolfram. *A New Kind of Science*. WOLFRAM MEDIA Incorporated, 2018. ISBN: 9781579550257. URL: https://books.google.com.ua/books?id=W0GjvgEACAAJ.

[14] Stephen Wolfram. “Cryptography with Cellular Automata”. в: *Advances in Cryptology — CRYPTO '85 Proceedings*. за ред. Hugh C. Williams. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, с. 429—432. ISBN: 978-3-540-39799-1.