Баландіна Наталія Миколаївна
старший викладач кафедри кібербезпеки,
Національний університет «Одеська юридична академія»

СИНТЕЗ ТА АНАЛІЗ КРИПТОГРАФІЧНО СТІЙКИХ S-БЛОКІВ: АЛГЕБРАЇЧНІ, ЛОГІЧНІ ТА ЕВОЛЮЦІЙНІ ПІДХОДИ

DOI https://doi.org/10.36059/978-966-397-537-5-9

1.1. Вступ та постановка задачі

У сучасну епоху стрімкого розвитку цифрових технологій та глобальної комп'ютеризації криптографія перетворилася на критичну складову інформаційної безпеки, що забезпечує захист даних як у цивільних, так і в оборонних, фінансових, урядових та приватних системах. В епоху інтенсивного обміну інформацією та розвитку систем штучного інтелекту криптографія забезпечує основу довіри, яка дає змогу функціонувати інтернет-комунікаціям, електронній комерції, цифровим підписам, безпечному зберіганню даних, а також захищеним каналам зв'язку [1]. З розвитком обчислювальних засобів та виникненням потенційної загрози квантових обчислень традиційні підходи до криптографічного захисту мають бути суттєво переглянуті або посилені, що висуває нові вимоги до структури та якості криптографічних примітивів.

Одним із ключових елементів симетричних криптографічних алгоритмів є S-блоки (підстановчі блоки) [2], які реалізують нелінійне перетворення даних і визначають основну частину криптографічної сили багатьох блочних шифрів. S-блоки перетворюють фіксовану кількість бітів в іншу кількість бітів, як правило, збережену по довжині, із застосуванням таких властивостей, як високий рівень нелінійності, відсутність фіксованих точок, диференціальну та кореляційну стійкість. Саме ці властивості забезпечують ускладнення математичного аналізу, спрямованого на розкриття структури шифру, і роблять алгоритми стійкими до відомих атак. Якість S-блоків безпосередньо впливає на загальну безпечність криптосистеми, а отже, завдання їх ефективного проєктування залишається в центрі уваги дослідницької спільноти.

У межах цього розділу монографії висвітлюються результати, що мають як теоретичне, так і прикладне значення. У першій частині запропоновано новий підхід до синтезу S-блоків, що ґрунтується на використанні конструкцій полів Галуа. Поля Галуа вже давно застосовуються в криптографії завдяки своїй структурованості, алгебраїчним властивостям та зручності в обчисленнях. Нами було розроблено методи, що розвивають ідеї, закладені у класичній конструкції Ніберг, яка використовує обернення в полі Галуа як основу для побудови сильних, з точки зору криптоаналізу, S-блоків. Нові конструкції, запропоновані в даному розділі, дозволяють подолати низку обмежень традиційних підходів, підвищуючи ефективність синтезу та забезпечуючи більшу варіативність параметрів при збереженні або навіть підвищенні рівня криптографічної стійкості.

Окрім розглянутих підходів, далі буде проаналізовано ще два важливі напрямки, що мають велике значення для розвитку теорії та практики побудови S-блоків. Першим із них є застосування генетичних алгоритмів до задачі синтезу криптографічно стійких підстановок. Ці алгоритми, що імітують механізми природного добору та еволюційного розвитку, дозволяють ефективно здійснювати пошук S-блоків із високими показниками нелінійності в умовах величезного простору можливих відображень. Генетичний підхід особливо корисний у тих випадках, коли неможливо використати суворо аналітичну формулу для побудови потрібного S-блока, або коли необхідно знайти нетривіальні, псевдовипадкові конструкції з заданими властивостями. У роботі детально описано побудову відповідного алгоритму, наведено результати обчислювальних експериментів, а також проведено порівняльний аналіз синтезованих S-блоків за класичними криптографічними критеріями.

Наступний важливий напрямок дослідження пов’язаний з аналізом множин S-блоків, що мають задані значення періоду повернення у вихідний стан. Такий підхід має фундаментальне значення для розуміння внутрішньої структури підстановок, що використовуються в сучасних шифрах, та визначення їх здатності до відновлення вихідного стану за скінчену кількість ітерацій. Період повернення у вихідний стан може бути розглянутий як окрема метрика криптографічної якості, що характеризує довгострокову

динамічну поведінку перетворення та його придатність для використання в ітеративних або самовідновлювальних криптографічних схемах. У цій частині буде досліджено статистичні властивості періодів для множин S-блоків заданої довжини, а також окреслено їх потенційне значення для криптографічної стійкості в умовах тривалого використання.

У роботі також досліджується зміни нелінійності компонентних функцій багатозначної логіки випадкового S-блока при зростанні його довжини, що є важливим з точки зору розуміння фундаментальної природи нелінійності підстановлювальних конструкцій при вдосконаленні та побудові нових методів синтезу S-блоків.

Таким чином, у межах даної роботи представлено нові підходи до синтезу та оцінювання S-блоків на основі полів Галуа та функцій багатозначної логіки, обґрунтовано ефективність застосування евристичних еволюційних методів та проаналізовано динамічні характеристики великих множин S-блоків, що відкриває нові перспективи для створення надійних криптографічних конструкцій нового покоління.

Запропоновані підходи до синтезу та оцінювання S-блоків спрямовані на зміцнення теоретичного фундаменту криптографії та практичне посилення захисту інформації в умовах нових викликів. Розроблені методи можуть бути адаптовані до широкого спектру криптографічних алгоритмів, включаючи ті, що орієнтовані на квантову стійкість, і слугують основою для подальших досліджень у сфері математичного забезпечення інформаційної безпеки.

Метою цієї роботи є узагальнення, систематизація та подальший розвиток результатів щодо створених автором нових методів синтезу криптографічно стійких S-блоків на основі конструкцій полів Галуа, функцій багатозначної логіки та генетичних алгоритмів.

Для досягнення поставленої мети в роботі вирішуються наступні наукові та прикладні завдання:

1. Аналіз сучасних критеріїв криптографічної якості S-блоків і визначення тих з них, які є найбільш релевантними в умовах постквантових загроз, зокрема в контексті функціонального представлення підстановок як компонентних булевих функцій та функцій багатозначної логіки.

2. Розробка нових методів синтезу S-блоків на основі конструкцій полів Галуа, зокрема за рахунок використання ізоморфних представлень полів, матриць GF-перетворень та дослідження їх впливу на криптографічні характеристики побудованих підстановок.

3. Побудова та експериментальна реалізація генетичного алгоритму для синтезу S-блоків із високим рівнем нелінійності, дослідження динаміки адаптації популяції підстановок та виявлення класів структур, що демонструють найкращі криптографічні властивості.

4. Дослідження множин S-блоків із заданими значеннями періодів повернення у вихідний стан, оцінка їх поширеності та впливу даного критерію на інші показники криптографічної якості.

5. Дослідження зміни нелінійності компонентних функцій багатозначної логіки випадкового S-блока при зростанні його довжини.

6. Формування узагальненого підходу до порівняльного аналізу та відбору S-блоків, побудованих різними методами, з урахуванням практичних вимог до симетричних шифрів, хеш-функцій і генераторів псевдовипадкових послідовностей.

Об'єкт дослідження – процеси побудови та оцінювання криптографічних примітивів, зокрема S-блоків, що застосовуються у симетричних криптографічних алгоритмах.

Предмет дослідження – методи синтезу S-блоків з високими показниками криптографічної стійкості на основі конструкцій полів Галуа, функцій багатозначної логіки, генетичних алгоритмів та дослідження множин S-блоків із заданими періодами повернення у вихідний стан.

1.2. S-блоки в криптографії: типи, еволюція та сучасні підходи до синтезу

Однією з ключових складових симетричних криптографічних перетворень є так звані підстановочні блоки [2] (S-блоки або S-box, від англ. Substitution box). Їх основна функція – забезпечити нелінійність криптографічної трансформації, що є фундаментальною вимогою для стійкості до атак, зокрема диференціального та лінійного криптоаналізу.

Однією з ключових задач симетричної криптографії є руйнування статистичних залежностей між відкритим текстом та шифртекстом [3]. Це необхідно для того, щоб криптоаналітик, навіть маючи великі обсяги зашифрованих даних, не зміг відновити жодної інформації про зміст відкритого повідомлення.

S-блоки відіграють критично важливу роль у досягненні цього ефекту. Вони реалізують нелінійне перетворення бітових векторів фіксованої довжини, зазвичай у вигляді функції з n бітів на m бітів (найчастіше $n = m$). У криптографічних примітивах, таких як блокові шифри, S-блоки використовуються для того, щоб вивести вихідні біти, які не є прямолінійною функцією вхідних, і тим самим зруйнувати можливі кореляції.

При цьому, якщо в шифрі не використовується достатньої кількості нелінійних перетворень, статистичні характеристики вхідного повідомлення можуть «просочуватися» в шифртекст. Добре сконструйований S-блок повинен повністю змінювати розподіл імовірностей вхідних даних, викликаючи так званий лавинний ефект – навіть невелика зміна одного біта на вході має змінювати багато бітів на виході з імовірністю, близькою до 50 % [4].

S-блоки також сприяють запобіганню витоку інформації про структуру повідомлення – наприклад, про повторювані фрагменти або статистичні закономірності мови, на які зазвичай спираються атаки частотного аналізу. Таким чином, вони є інструментом руйнування статистичних особливостей відкритого тексту системою шифрування.

Поняття S-блоку бере свій початок з фундаментальних принципів симетричної криптографії, зокрема із реалізації підстановок у класичних шифрах. Ще в шифрі Цезаря чи шифрі Віженера [5] використовувалась концепція заміни символів з метою приховування вихідного тексту. Проте саме у XX столітті, з розвитком електронної обчислювальної техніки та переходом до бітового представлення даних, S-блоки набули сучасного формального вигляду – у вигляді нелінійних функцій, що відображають один бітовий вектор у інший.

Першу значущу роль S-блоки зіграли в контексті блочного шифру Data Encryption Standard (DES) [6], який був затверджений у 1977 році Національним інститутом стандартів і технологій США (NIST). В алгоритмі DES використовуються вісім S-блоків, кожен

з яких реалізує відображення з 6-бітового вектора у 4-бітовий, і ці блоки визначають основну нелінійність у шифрі. Саме завдяки S-блокам DES зміг протистояти лінійному аналізу упродовж десятиліть. Варто зазначити, що структура S-блоків у DES довгий час залишалась предметом суперечок через їх закритість: лише у 1994 році стало відомо, що S-блоки були спроєктовані з урахуванням стійкості до диференціального криптоаналізу, який був невідомий широкому колу дослідників на момент затвердження стандарту.

Подальший розвиток криптографії, зокрема із появою блочних шифрів наступного покоління – таких як AES (Rijndael), Camellia, Twofish, Serpent – супроводжувався формалізацією вимог до S-блоків. У AES використовується єдиний 8×8-бітовий S-блок, побудований на базі алгебраїчної інверсії у полі $GF(2^8)$ з подальшим афінним перетворенням. Цей підхід забезпечує як високу криптографічну стійкість, так і ефективність реалізації на апаратному та програмному рівнях.

Історично розвиток S-блоків можна умовно поділити на кілька етапів:

1. Класична епоха – використання підстановок у вигляді таблиць або ручних схем у класичних шифрах.

2. Епоха стандартів – фіксовані S-блоки у DES, IDEA, GOST 28147-89.

3. Алгебраїчний підхід – побудова S-блоків на основі операцій у скінченних полях, наприклад, S-блок криптоалгоритма AES.

4. Керовані та хаотичні S-блоки – побудова адаптивних S-блоків з використанням складних математичних структур, випадковості, біоінспірованих моделей.

Таким чином, історія S-блоків демонструє постійний рух від простих табличних підстановок до складних, адаптивних та математично вивірених конструкцій, що відіграють центральну роль у забезпеченні нелінійності, дифузії та стійкості до сучасних типів криптоаналізу.

Існує кілька підходів до класифікації S-блоків, серед яких можна виділити такі:

1. За принципом побудови:

1.1. табличні (статичні) S-блоки, які реалізуються у вигляді фіксованих таблиць підстановок;

1.2. генеративні (динамічні) S-блоки, які обчислюються під час виконання шифрування.

2. За структурою:

2.1. бієктивні (однозначні та взаємно однозначні) – часто використовуються в AES;

2.2. часткові підстановки (небієктивні) – можуть використовуватись у поточних шифрах чи хеш-функціях.

3. За способом формування:

3.1. аналітичні (на основі алгебраїчних функцій, обернення в полі $GF(2^n)$;

3.2. псевдовипадкові (з використанням генераторів псевдовипадкових або випадкових чисел);

3.3. еволюційні (генетичні алгоритми, нейромережі);

3.4. керовані (керування параметрами або ключовою інформацією).

У традиційних схемах, як-от у DES, S-блоки фіксовані та однакові для всіх ключів. Проте сучасні потреби кібербезпеки, зокрема в умовах постійного вдосконалення атак, вимагають більшої гнучкості та адаптивності криптографічних примітивів. Це спонукало дослідників до створення так званих керованих параметрами або ключем S-блоків, які формуються динамічно на основі ключової інформації, часу, стану системи тощо.

Як було вказано раніше, історично перші S-блоки були статичними – тобто заданими фіксованими таблицями заміни, які не змінювалися ані між сеансами шифрування, ані між раундами. Однак у міру розвитку атак, зокрема диференціального й лінійного криптоаналізу, з'явилася ідея створення залежних від ключа S-блоків. У таких схемах таблиці заміни генеруються на основі ключа шифрування, завдяки чому стає набагато складніше здійснити попередній аналіз структури S-блоку або застосувати універсальні шаблони атак.

У 2000-х роках почали з'являтись концепції генерованих та динамічних S-блоків, які залежать від секретного ключа або від параметрів середовища. Такі S-блоки отримали назву керовані S-блоки (key-dependent, dynamic, або controlled S-boxes) [7]. Наприклад, у шифрі Twofish [8] використовуються чотири динамічних S-блоки, які залежать від ключа, що підвищує ентропію та ускладнює атаки за відомим текстом. У багатьох сучасних розробках розглядається

створення S-блоків з використанням хаотичних відображень, алгебраїчних кривих, нейромережевих моделей, що дозволяє зменшити передбачуваність та підвищити адаптивність шифру до різних сценаріїв використання.

У таких підходах S-блоки можуть змінюватися не тільки залежно від ключа, а й динамічно – на кожному раунді шифрування, що ускладнює побудову моделей для атаки. Адаптивні S-блоки сьогодні активно досліджуються в контексті постквантових шифрів, де класичні принципи шифрування доповнюються новими ідеями гнучкості та динамічності.

Ідея залежних від ключа S-блоків реалізується в сучасній криптографії як засіб посилення криптостійкості за рахунок динамічної модифікації перетворень на основі секретного ключа. Такий підхід дозволяє зруйнувати фіксованість структури підстановки, що властива класичним S-блокам, і ускладнює проведення криптоаналітичних атак, зокрема диференціального та лінійного аналізу, атак на основі бумеранга, квадратного аналізу тощо. Формально, залежні від ключа S-блоки є функціями, які будуються динамічно під час ініціалізації шифру або навіть під час кожного раунду, враховуючи ключ або інші секретні параметри, що робить шифр непередбачуваним.

Існує низка криптографічних алгоритмів, у яких ця концепція вже реалізована на практиці. Наприклад, у шифрі Blowfish підстановочна таблиця генерується на основі ключа і відрізняється для кожної сесії. У ще більш гнучкому алгоритмі Twofish застосовано ідею ключового розкладу, в якому частини ключа використовуються для генерації модифікованих S-блоків через застосування максимально нелінійних функцій. В обох випадках метою є зробити кожен екземпляр шифру індивідуальним, що перешкоджає використанню універсальних таблиць або статистичних методів атак.

Сучасні дослідження в напрямку постквантової криптографії також демонструють інтерес до управління S-блоками за допомогою змінних параметрів. Зокрема, в деяких проєктних прототипах, що використовують симетричні схеми на основі дерев Гротендіка або у конструкціях з вузькими блоками, ключ впливає не лише на структуру розкладу, але й безпосередньо формує S-блоки для кожного

раунду. Це дозволяє досягати високого ступеня криптографічної диференціації при незначному збільшенні обчислювальних витрат.

Управління S-блоками в динамічному режимі дозволяє шифрам адаптуватися до умов середовища – зокрема, змінювати поведінку при зміні політик безпеки, алгоритмів або навіть типу пристрою. Це відкриває нові горизонти для створення криптографічних примітивів із властивостями самоналаштування, що є особливо актуальним у контексті обчислень у хмарних середовищах.

Зазначимо окремо, що збільшення розміру S-блока призводить до суттєвого покращення його криптографічних властивостей за рахунок значного розширення простору можливих відображень. У великих S-блоках зростає дистанційна нелінійність, що ускладнює лінійний криптоаналіз, а також алгебраїчна нелінійність, яка робить їх стійкішими до алгебраїчних атак. Лавинні властивості покращуються за рахунок більш рівномірного розподілу впливу вхідних бітів на вихідні, що забезпечує швидке «розповсюдження» змін. Крім того, збільшення розміру S-блока сприяє покращенню кореляційних властивостей, зменшуючи статистичні зв'язки між входами та виходами, а також збільшує періоди повернення у вихідний стан, що ускладнює атаки, засновані на циклічності.

Однак таке покращення якості досягається ціною значного зростання обчислювальної складності. Великі S-блоки вимагають більших обчислювальних ресурсів для реалізації, оскільки збільшується обсяг пам'яті для зберігання таблиць замін, а також кількість операцій, необхідних для їх обробки. Це особливо критично в низькоресурсних системах, де швидкодія є ключовим фактором. Таким чином, при проєктуванні шифрів необхідно знаходити баланс між криптографічною стійкістю, яка залежить від розміру S-блока, та ефективністю його реалізації. Оптимальний вибір розмірності визначається конкретними вимогами до безпеки та продуктивності криптосистеми.

Таким чином, S-блоки не є лише елементом заміни в схемі шифрування – вони є ядром забезпечення нелінійності та криптографічної складності, що визначають опір шифру до цілого ряду атак. Їх еволюція від статичних таблиць до складних керованих конструкцій свідчить про зростаючі вимоги до безпеки та адаптивність сучасної криптографії до нових викликів.

1.3. S-блоки на основі GF-перетворень

Основним компонентом практично будь-якої системи захисту інформації сьогодні є криптографічний компонент, який унеможливлює читання зашифрованої інформації без криптографічного ключа. Водночас, хоча асиметричні криптографічні алгоритми, через їх значну обчислювальну складність, використовуються на практиці здебільшого для вирішення задачі розподілу ключів та цифрового підпису, симетричні шифри залишаються основним компонентом, який використовується для шифрування великих обсягів захищених даних. Блокові та потокові симетричні шифри характеризуються як швидкі, перевірені на криптографічну стійкість та прості в реалізації алгоритми. У свою чергу, основним компонентом сучасних шифрів, який значною мірою визначає рівень дифузії та конфузії [3], який вони забезпечують, є криптографічний S-блок. На сьогоднішній день для оцінки ступеня реалізації концепції дифузії та конфузії криптографічним S-блоком, а також ступеня його стійкості до основних атак криптоаналізу використовується підхід, заснований на представленні S-блока у вигляді його компонентних булевих функцій, до яких застосовується набір критеріїв криптографічної якості. Основними критеріями криптографічної якості S-блока є наступні: критерій максимізації алгебраїчної нелінійності, критерій максимізації відстані нелінійності, суворий лавинний критерій та критерій мінімізації кореляції вихідних та вхідних векторів.

Важливим завданням є синтез криптографічних S-блоків, які б гармонійно відповідали переліченим критеріям криптографічної якості, чого можна досягти, використовуючи конструкції полів Галуа. Прикладом такого відомого методу є конструкція Ніберг, проте цей метод дозволяє отримати лише малі потужності високоякісних S-блоків, що робить актуальним завдання розробки нових методів синтезу S-блоків на основі конструкцій полів Галуа [9].

На сьогоднішній день існує кілька підходів до оцінки криптографічної якості S-блоків, зокрема, на основі їх представлення за допомогою компонентних булевих функцій [10], а також з використанням компонентних функцій багатозначної логіки, для

яких застосовуються спеціальні криптографічні критерії якості, наприклад, [11]. Далі для оцінки криптографічної якості синтезованих S-блоків ми використовуємо загальноприйнятий підхід, який базується на представленні S-блоків у вигляді їх компонентних булевих функцій. Оскільки довжина запропонованих S-блоків становить $N = 256$, їх можна представити як вісім компонентних булевих функції, тоді як загальна криптографічна якість S-блока визначається найслабшою з них. Серед багатьох існуючих критеріїв криптографічної якості компонентних булевих функцій ми вибрали наступний набір основних критеріїв:

1. Алгебраїчний степінь нелінійності, який визначається як найбільша кількість кон'юнкцій в термах алгебраїчної нормальної форми компонентної булевої функції [12]. У цьому випадку вектор коефіцієнтів при термах алгебраїчної нормальної форми булевої функції можна побудувати за допомогою перетворення Ріда – Маллера як

$$A = f \cdot L_N A, \tag{1}$$

де f – таблиця істинності булевої функції над алфавітом $\{0,1\}$, L_N – матриця перетворення Ріда – Маллера, яку можна побудувати відповідно до наступної рекурентної формули:

$$L_1 = [1], \quad L_{2N} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes L_N = \begin{bmatrix} L_N & 0 \\ L_N & L_N \end{bmatrix}, \tag{2}$$

де $\otimes$ позначає добуток Кронекера.

2. Відстань нелінійності булевої функції, яку можна визначити як мінімум відстані Хеммінга між її компонентними булевими функціями та всіма кодовими словами афінного коду [13]:

$$N_S = \min\left\{\text{dist}(f_i, \varphi_j)\right\}, \; i = 1,...,k, \; j = 1,...,2^{k+1}, \tag{3}$$

де f_i – компонентна булева функція; φ_j – кодові слова афінного $A(N,k)$-коду, $\text{dist}(\circ)$ – оператор для обчислення відстані Хеммінга.

3. Відповідність критерію поширення помилки [13], для оцінки якого використовуються мінімальне та максимальне значення ваги похідних компонентних булевих функцій:

$$D_u f(x) = f(x) \oplus f(x \oplus u), \quad (4)$$

за усіма напрямками $\forall u \in V_k$, $wt(u) = 1$, де V_k – лінійний векторний простір векторів довжини k, $wt(\circ)$ – оператор для обчислення ваги Хеммінга. Ідеальний випадок, коли всі похідні (4) збалансовані, тобто їхні ваги Хеммінга дорівнюють $N/2$, означає, що компонентна булева функція відповідає суворому лавинному критерію, тобто ймовірність зміни її виходу при зміні значення будь-якого з її вхідних бітів дорівнює 0,5.

4. Критерій мінімізації кореляції вихідних та вхідних векторів [13]. Для оцінки відповідності S-блока цьому критерію використовується максимум серед абсолютних значень коефіцієнтів кореляції $\max\left\{\left|r_{i,j}\right|\right\}$ матриці $R = \left\|r_{i,j}\right\|$, який визначає ступінь лінійного зв'язку між вихідними y та вхідними x векторами S-блока:

$$r_{i,j} = 1 - \frac{\sum_{m=1}^{N} (x_{m,i} \oplus y_{m,j})}{N/2}, i, j = 0,...,k-1, \quad (5)$$

де символ $\oplus$ позначає підсумовування по mod2.

Досить багато сучасних публікацій присвячено питанням синтезу S-блоків заданої довжини, які б відповідали заданим критеріям криптографічної якості, де для їх побудови використовується найрізноманітніші алгоритми: починаючи від алгоритмів їх синтезу на основі послідовностей де Брейна, як, наприклад, запропоновано в [14], закінчуючи методами синтезу S-блоків на основі теорії динамічного хаосу [15–19]. Тим не менш, на практиці для побудови криптографічних алгоритмів найбільш важливими є S-блоки, які мали б збалансований набір показників криптографічної якості, що найлегше досягається за допомогою конструкцій полів Галуа. Наприклад, у криптографічному алгоритмі AES [20], який на сьогоднішній день є де-факто найпопулярнішим та найширше використовуваним криптографічним алгоритмом у світі, використовується конструкція Ніберг, заснована на операції знаходження оберненого елемента в розширеному полі Галуа. Багато досліджень присвячено криптографічним властивостям S-блоків конструкції Ніберг, зокрема [21], тоді як стаття [11] присвячена дослідженню криптографічних

властивостей S-блоків конструкції Ніберг у випадку їх представлення за допомогою функцій багатозначної логіки.

У будь-якому разі, конструкція Ніберг характеризується малою потужністю множин S-блоків, які можна синтезувати, що не дозволяє використовувати їх як довгостроковий ключ, що важливо в низці криптографічних застосувань.

Ми показуємо, що можливості синтезу S-блоків над розширеними полями Галуа не вичерпуються, і потужність наборів синтезованих S-блоків з використанням розширених полів Галуа можна збільшити шляхом розробки нових конструкцій криптографічно високоякісних S-блоків на основі матриць GF-перетворення для розширеного поля Галуа.

Теорія та практика синтезу алгебраїчної нормальної форми (АНФ) функцій багатозначної логіки (q-функцій) або так званих GF-перетворень [14] динамічно розвиваються в сучасній криптографії.

Визначення 1 [22]. Функція q-значної логіки k змінних є відображенням $\{0,1,2,...,q-1\}^k \to \{0,1,2,...,q-1\}$.

Коли $q=2$, ми отримуємо булеві функції.

Далі, з точки зору практики побудови S-блоків, ми розглянемо функції багатозначної логіки зі значеннями $q=2^k$.

У [22] показано, що будь-яку функцію багатозначної логіки можна однозначно (з точністю до ізоморфізму) представити над полем Галуа $GF(2^k)$ за допомогою полінома, що містить операції «Додавання в полі Галуа», «Множення в полі Галуа».

Специфічні аспекти знаходження АНФ для випадку розширених полів Галуа розглядаються в [23].

Перехід до простору GF-перетворень можна виконати за такою формулою

$$: \begin{cases} A = g \cdot L_N, \\ g = A \cdot L_N^{-1}, \end{cases} \tag{6}$$

де g – таблиця істинності булевої функції, $A \in GF(2^k)$ – вектор значень GF-перетворення.

Відомо [22], що для випадку функцій багатозначної логіки $k=1$ змінної, побудова матриці оберненого GF-перетворення L_N^{-1}, $N=q^k$ над полем $GF(2^k)$ може бути виконана відповідно до наступної конструкції:

$$L_1^{-1} = \begin{bmatrix} \alpha_0^0 & \alpha_0^1 & \dots & \alpha_0^{q-1} \\ \alpha_1^0 & \alpha_1^1 & \cdots & \alpha_1^{q-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{q-1}^0 & \alpha_{q-1}^1 & \cdots & \alpha_{q-1}^{q-1} \end{bmatrix}, \quad (7)$$

де $\alpha_i \in GF(2^k), i = 0,1,...,q-1$ – елементи розширеного поля Галуа. Для випадку функцій багатозначної логіки, на відміну від випадку матриці перетворення Ріда – Маллера для булевих функцій (2), пряма та обернена матриці GF-перетворення не збігаються, тобто $L_N \neq L_N^{-1}$, тому пряму матрицю GF-перетворення можна знайти за допомогою одного з алгоритмів знаходження обернених матриць над розширеними полями Галуа [24].

Зауважимо, однак, що різні ізоморфні представлення полів Галуа $GF(2^k)$ означають різні реалізації операції множення (а також операцій піднесення до степеню та ділення, похідних від неї) відповідно до правила, що визначається незвідним поліномом $\psi(z)$, на основі якого побудовано поле Галуа $GF(2^k)$.

Таким чином, для поля Галуа $GF(2^k)$ функція багатозначної логіки може мати певну кількість різних ізоморфних відображень в області АНФ, що відповідає кількості незвідних поліномів степеню k, на основі яких можна побудувати арифметику поля Галуа.

У цьому випадку кількість існуючих незвідних поліномів степеню k, коефіцієнти яких належать полю Галуа $GF(2^k)$, визначається відповідно до формули [25]:

$$\left|\Psi_k\right| = \frac{1}{k} \sum_{d \,//\, k} \mu(d) 2^{(k/d)}, \quad (8)$$

де d – дільники значення степеню k; $\mu(d)$ – функція Мебіуса; позначення $d // k$ означає, що d ділить k націло.

Отже, для випадку поля Галуа $GF(2^k)$, який ми розглядаємо, відповідно до (8), кількість незвідних поліномів дорівнює $\left|\Psi_8\right| = 30$, тоді як десяткові еквіваленти цих поліномів мають наступний вигляд:

$$\Psi_8 = \{283,285,299,301,313,319,333,351,355,357,361,369,375,379,391, \\ 395,397,415,419,425,433,445,451,463,471,477,487,499,501,505\}. \quad (9)$$

Як приклад, на рис. 1 представлено у вигляді зображень у градаціях сірого (де колір кожного пікселя відповідає значенню елемента матриці в полі Галуа $GF(2^8)$ в діапазоні від 0 – чорний, до 255 – білий) перші шість матриць GF-перетворення для ізоморфних представлень поля Галуа $GF(2^8)$, побудованих на основі незвідних поліномів:

$$\begin{aligned}
\psi_1(z) &= 283_{10} = z^8 + z^4 + z^3 + z + 1, \\
\psi_2(z) &= 285_{10} = z^8 + z^4 + z^3 + z^2 + 1, \\
\psi_3(z) &= 299_{10} = z^8 + z^5 + z^3 + z + 1, \\
\psi_4(z) &= 301_{10} = z^8 + z^5 + z^3 + z^2 + 1, \\
\psi_5(z) &= 313_{10} = z^8 + z^5 + z^4 + z^3 + 1, \\
\psi_6(z) &= 319_{10} = z^8 + z^5 + z^4 + z^3 + z^2 + z + 1.
\end{aligned} \tag{10}$$

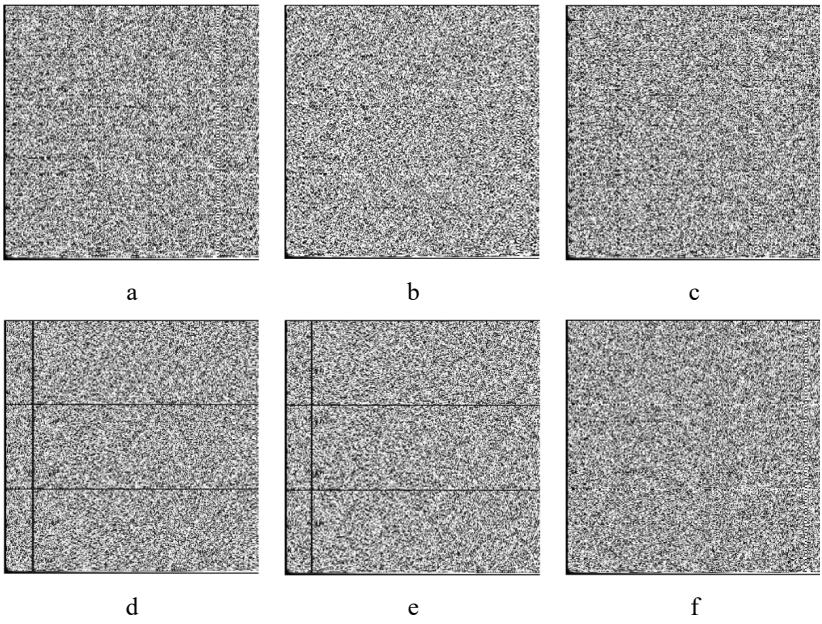


Рисунок 1 – Приклади матриць GF-перетворення для поліномів: ψ_1 (a), ψ_2 (b), ψ_3 (c), ψ_4 (d), ψ_5 (e) і ψ_6 (f)

Проведені дослідження показали, що рядки матриці GF-перетворення характеризуються достатньо високими значеннями основних показників криптографічної якості, тому їх можна використовувати для задач побудови високоякісних S-блоків. Детальне дослідження структури матриць GF-перетворення порядку $N=256$ над усіма ізоморфними представленнями поля Галуа $GF(2^8)$ дозволило встановити, що лише половина рядків цих матриць містить усі елементи поля Галуа $GF(2^8)$, що означає, що вона придатна для побудови бієктивних S-блоків. Номери цих рядків інваріантні до ізоморфізму поля Галуа $GF(2^8)$ та задаються у вигляді наступного виразу:

$$\begin{gathered}\Upsilon' = \{2,3,5,8,9,12,14,15,17,20,23,24,27,29,30,32,33,38,39,42,44,\\ 45,47,48,50,53,54,57,59,60,62,63,65,68,72,74,75,77,78,80,83,84,\\ 87,89,90,92,93,95,98,99,102,104,105,107,108,110,113,114,117,\\ 119,122,123,125,128,129,132,134,135,138,140,143,144,147,149,150,\\ 152,153,155,158,159,162,164,165,167,168,170,173,174,177,179,\\ 180,182,183,185,189,192,194,195,197,198,200,203,204,207,209,\\ 210,212,213,215,218,219,224,225,227,228,230,233,234,237,240,\\ 242,243,245,248,249,252,254,255\}.\end{gathered} \tag{11}$$

Однак, не всі рядки з (11) матриць GF-перетворення мають однаковий рівень криптографічної якості. Проведені дослідження дозволили визначити 24 номери рядків, які, незалежно від ізоморфізму, забезпечують побудову S-блоків з найкращим рівнем криптографічної якості:

$$\begin{gathered}\Upsilon = \{2,3,5,8,9,15,17,29,33,38,42,57,65,74,75,83,113,\\ 129,132,147,149,165,194,225\}.\end{gathered} \tag{12}$$

При використанні набору рядків (12) для завдання побудови S-блоків, їхня криптографічна якість є стабільною незалежно від ізоморфізму. Таким чином, ми можемо записати запропонований метод побудови криптографічних S-блоків на основі матриць GF-перетворення у вигляді конкретних кроків:

Крок 1. Оберіть початкові параметри методу, якими є: довжина S-блока N та відповідне розширене поле Галуа $GF(2^k)$, $k = \log_2 N$;

конкретний незвідний поліном, що визначає правила арифметики в розширеному полі $GF(2^k)$.

Крок 2. На основі (7) побудувати обернену матрицю GF-перетворення L_N^{-1}.

Крок 3. Використовуючи один з відомих алгоритмів інверсії матриць у розширених полях Галуа [24] на основі оберненої матриці GF-перетворення L_N^{-1} знайти пряму матрицю GF-перетворення L_N.

Крок 4. Вибрати рядки матриці GF-перетворення, що містять усі елементи розширеного поля Галуа $GF(2^k)$.

Крок 5. Представивши рядки матриці GF-перетворення, вибраної на Кроці 4, у вигляді S-блоків довжини N, оцінити рівень їх відповідності основним критеріям криптографічної якості, в результаті чого вибрати S-блоки, які найкраще відповідають критеріям, що вважаються вирішальними при модернізації або проєктуванні криптографічного алгоритму.

З огляду на практичну значущість та затребуваність використання в сучасних симетричних шифрах та хеш-функціях криптографічних S-блоків, що виконують побайтове перетворення вхідних даних, для експерименту було обрано такі параметри методу: довжина S-блока $N = 256$, всі можливі ізоморфні представлення основного поля Галуа $GF(2^8)$ на основі незвідних поліномів (9).

У табл. 1 наведено результати експериментального дослідження відповідності S-блоків, побудованих на основі запропонованого методу, основним критеріям криптографічної якості. При цьому в табл. 1 прийнято такі позначення: ψ позначає десятковий еквівалент незвідного полінома, що використовується для побудови матриці GF-перетворення; $\deg(S)$ позначає значення алгебраїчного степеню нелінійності S-блоків, побудованих у заданому ізоморфному представленні поля Галуа $GF(2^8)$; N_S позначає відстань нелінійності S-блоків, побудованих у заданому ізоморфному представленні поля Галуа $GF(2^8)$; $wt(D_u f)$ позначає значення ваг похідних за напрямком компонентних булевих функцій S-блоків для заданого ізоморфного представлення поля Галуа $GF(2^8)$; $\left|r_{i,j}\right|$ позначає значення матриць коефіцієнтів кореляції для S-блоків для заданого ізоморфного представлення поля Галуа $GF(2^8)$.

Таблиця 1 – Значення показників криптографічної якості для побудованих S-блоків

ψ	deg(*S*)	N_S	$wt(D_u f)$	$\lvert r_{i,j} \rvert$
283	5–7	112	108–156	0–0,1250
285	5–7	112	108–156	0–0,1250
299	5–7	112	108–156	0–0,1250
301	5–7	112	108–156	0,0156–0,1250
313	5–7	112	108–156	0–0,1250
319	5–7	112	108–156	0,0156–0,1250
333	5–7	112	108–156	0–0,1250
351	5–7	112	108–156	0–0,1250
355	5–7	112	108–156	0–0,1250
357	5–7	112	108–156	0–0,1250
361	5–7	112	108–156	0–0,1250
369	5–7	112	108–156	0–0,1250
375	5–7	112	108–156	0–0,1250
379	5–7	112	108–156	0–0,1250
391	5–7	112	108–156	0–0,1250
395	5–7	112	108–156	0–0,1250
397	5–7	112	108–156	0–0,1250
415	5–7	112	108–152	0,0156–0,1250
419	5–7	112	108–156	0–0,1250
425	5–7	112	108–156	0,0156–0,1250
433	5–7	112	108–156	0,0156–0,1250
445	5–7	112	108–156	0–0,1250
451	5–7	112	108–156	0–0,1250
463	5–7	112	108–156	0–0,1250
471	5–7	112	108–156	0–0,1250
477	5–7	112	108–156	0–0,1250
487	5–7	112	108–156	0,0156–0,1250
499	5–7	112	108–156	0–0,1250
501	5–7	112	108–156	0–0,1250
505	5–7	112	108–156	0–0,1250

Аналіз даних, представлених у табл. 1, дозволяє зробити висновок, що криптографічна якість S-блоків на основі рядків матриць GF-перетворення є високою та стабільною. За криптографічною якістю своїх компонентних булевих функцій побудовані S-блоки не поступаються S-блокам конструкції Ніберг. Більше того, загальна

кількість S-блоків для всіх ізоморфних представлень $GF(2^8)$ дорівнює $J = |\Upsilon| \cdot |\Psi| = 24 \cdot 30 = 720$, що в 24 рази більше, ніж кількість S-блоків конструкції Ніберг в тому ж розширеному полі Галуа.

Також зазначимо, що алгебраїчний степінь нелінійності S-блоків на основі матриць GF-перетворення залежить від вибраного номера рядка матриці, на основі якої побудовано S-блок. У табл. 2 наведено значення алгебраїчних степенів нелінійності залежно від номера рядка (12).

Таблиця 2 – Значення алгебраїчного степеня нелінійності залежно від номера рядка матриці GF-перетворення

$\upsilon_i \in \Upsilon$	2	3	5	8	9	15	17	29	33	38	42	57
deg(S)	7	7	7	5	7	5	7	5	7	5	5	5
$\upsilon_i \in \Upsilon$	65	74	75	83	113	129	132	147	149	165	194	225
deg(S)	7	5	5	5	5	7	5	5	5	5	5	5

Розглянемо приклад S-блока на основі другого рядка матриці GF-перетворення в полі Галуа $GF(2^8)$, арифметика якого визначається незвідним поліномом $\psi_1(z) = 283_{10} = z^8 + z^4 + z^3 + z + 1$, який ми представляємо як наступну алгебраїчну конструкцію:

S_1	0	1	2	3	4	5	6	7	8	9	*A*	*B*	*C*	*D*	*E*	*F*
0	00	01	8E	F4	47	A7	7A	BA	AD	9D	DD	98	3D	AA	5D	96
1	D8	72	C0	58	E0	3E	4C	66	90	DE	55	80	A0	83	4B	2A
2	6C	ED	39	51	60	56	2C	8A	70	D0	1F	4A	26	8B	33	6E
3	48	89	6F	2E	A4	C3	40	5E	50	22	CF	A9	AB	0C	15	E1
4	36	5F	F8	D5	92	4E	A6	04	30	88	2B	1E	16	67	45	93
5	38	23	68	8C	81	1A	25	61	13	C1	CB	63	97	0E	37	41
6	24	57	CA	5B	B9	C4	17	4D	52	8D	EF	B3	20	EC	2F	32
7	28	D1	11	D9	E9	FB	DA	79	DB	77	06	BB	84	CD	FE	FC
8	1B	54	A1	1D	7C	CC	E4	B0	49	31	27	2D	53	69	02	F5
9	18	DF	44	4F	9B	BC	0F	5C	0B	DC	BD	94	AC	09	C7	A2
A	1C	82	9F	C6	34	C2	46	05	CE	3B	0D	3C	9C	08	BE	B7
B	87	E5	EE	6B	EB	F2	BF	AF	C5	64	07	7B	95	9A	AE	B6
C	12	59	A5	35	65	B8	A3	9E	D2	F7	62	5A	85	7D	A8	3A
D	29	71	C8	F6	F9	43	D7	D6	10	73	76	78	99	0A	19	91
E	14	3F	E6	F0	86	B1	E2	F1	FA	74	F3	B4	6D	21	B2	6A
F	E3	E7	B5	EA	03	8F	D3	C9	42	D4	E8	75	7F	FF	7E	FD

(13)

Відстань нелінійності S-блока (13) дорівнює $N_{S_1} = 112$, його значення алгебраїчного степеню нелінійності дорівнює $\deg(S_1) = 7$.

Представимо матрицю ваг похідних компонентних булевих функцій S-блока (13):

e_j	$wt(D_{1,k})$	$wt(D_{2,k})$	$wt(D_{3,k})$	$wt(D_{4,k})$	$wt(D_{5,k})$	$wt(D_{6,k})$	$wt(D_{7,k})$	$wt(D_{8,k})$
10000000	128	116	120	124	136	112	116	116
01000000	116	124	144	144	112	116	116	128
00100000	124	128	120	132	116	116	128	116
00010000	128	128	132	124	116	128	116	124
00001000	128	116	116	124	128	116	124	128
00000100	116	132	120	140	116	124	128	128
00000010	132	124	136	140	124	128	128	116
00000001	124	136	124	136	128	128	116	132

, (14)

а також його матрицю коефіцієнтів кореляції

$$R = \begin{bmatrix} 0{,}016 & 0 & -0{,}016 & 0{,}047 & 0{,}094 & 0{,}016 & 0{,}094 & 0{,}047 \\ 0 & 0{,}094 & 0{,}094 & 0{,}047 & 0{,}016 & 0{,}094 & 0{,}047 & 0{,}016 \\ -0{,}016 & 0{,}094 & 0{,}063 & 0 & -0{,}094 & 0{,}063 & -0{,}109 & 0{,}078 \\ 0{,}047 & 0{,}047 & 0 & 0{,}031 & 0{,}063 & 0{,}031 & -0{,}109 & -0{,}031 \\ 0{,}094 & 0{,}016 & -0{,}094 & 0{,}063 & -0{,}063 & -0{,}063 & 0{,}125 & 0{,}094 \\ 0{,}016 & 0{,}094 & 0{,}063 & 0{,}031 & -0{,}063 & 0{,}125 & 0{,}094 & 0{,}094 \\ 0{,}094 & 0{,}047 & -0{,}109 & -0{,}109 & 0{,}125 & 0{,}094 & 0{,}094 & 0{,}016 \\ 0{,}047 & 0{,}016 & 0{,}078 & -0{,}031 & 0{,}094 & 0{,}094 & 0{,}016 & 0{,}094 \end{bmatrix}. \quad (15)$$

Таким чином, набір побудованих S-блоків, зокрема, S-блок (13), не поступається за своєю криптографічною якістю відомим конструкціям S-блоків, таким як конструкція Ніберг, і може бути рекомендований для практичного застосування в задачах підвищення ефективності існуючих криптографічних алгоритмів, а також розробки нових перспективних шифрів.

Відзначимо основні результати:

1. Матриці GF-перетворення можуть стати вихідним матеріалом для побудови криптографічно високоякісних S-блоків. Запропоновано ефективний метод побудови криптографічно високоякісних S-блоків практично цінних довжин на основі матриць GF-перетворення.

2. Для найбільш застосовуваного на практиці значення довжини S-блоків $N = 256$, на основі запропонованого методу синтезу S-блоків на основі матриць GF-перетворення, синтезовано клас S-блоків,

показники криптографічної якості яких не поступаються відомій конструкції Ніберг, проте потужність представленого класу в 24 рази більша порівняно з потужністю класу S-блоків конструкції Ніберг.

3. З огляду на високий рівень криптографічної якості запропонованих S-блоків, їх можна рекомендувати для практичного використання з метою вдосконалення існуючих криптографічних алгоритмів (блокових та потокових симетричних шифрів, хеш-функцій, генераторів псевдовипадкових ключових послідовностей), а також для розробки перспективних шифрів.

Як можливі напрямки подальших досліджень можна виділити можливість дослідження криптографічних властивостей S-блоків при їх представленні за допомогою АНФ, побудованої за допомогою GF-перетворення для значень $q = N$, тобто з використанням однієї функції багатозначної логіки, що може бути основою для розробки нових ефективних методів синтезу великих класів криптографічно високоякісних S-блоків.

1.4. Генетичний алгоритм для побудови високонелінійних S-блоків підстановки

Генетичні алгоритми є потужним інструментом еволюційної оптимізації, натхненним принципами природного добору та генетичної еволюції. Цей клас стохастичних алгоритмів широко використовується в задачах, де простір можливих рішень є надзвичайно великим, а традиційні методи пошуку не дають ефективного результату або потребують надмірних обчислювальних ресурсів. Генетичні алгоритми довели свою ефективність у таких галузях, як оптимальне проєктування технічних систем, біоінформатика, обробка сигналів, штучний інтелект, теорія графів і, зокрема, у криптографії – там, де необхідно знаходити структури з наперед заданими або оптимальними властивостями в умовах надскладних просторових залежностей між параметрами.

У контексті криптографії однією з найбільш цікавих задач, до якої можна застосувати генетичні алгоритми, є синтез S-блоків із високим рівнем нелінійності. Оскільки пошук S-блоку – це, фактично, комбінаційна оптимізаційна задача, що вимагає знаходження такої відображувальної функції, яка задовольняє низці критеріїв (висока

нелінійність, низька кореляція, хороша диференціальна та лінійна стійкість, відсутність фіксованих точок тощо), класичні методи синтезу часто стикаються з обмеженнями через обчислювальну складність задачі та необхідність балансувати між різними, іноді суперечливими, метриками якості. Генетичні алгоритми дозволяють розглядати цю задачу в еволюційному контексті – шляхом багаторазової генерації та селекції популяцій можливих S-блоків, з використанням операцій мутації та добору, поступово наближаючись до оптимального або субоптимального рішення.

Суттєвою перевагою генетичного підходу є його здатність ефективно досліджувати великі й розріджені простори рішень, де стандартні методи вичерпуються або втрачають ефективність. У випадку синтезу S-блоків це означає, що генетичний алгоритм може виявити нетривіальні структури відображень, які задовольняють високим криптографічним вимогам, хоча формально вони не входять у добре вивчені класи конструкцій (наприклад, не є афінними перетвореннями, не ґрунтуються на зворотних функціях у полі Галуа тощо). Крім того, адаптивність і гнучкість генетичних алгоритмів дає змогу враховувати додаткові цільові функції, зокрема метрики, пов'язані з властивостями багатозначної логіки, поведінкою компонентних функцій, стійкістю до перспективних атак квантового криптоаналізу.

Ще однією важливою особливістю генетичних алгоритмів у контексті синтезу S-блоків є їхня здатність формувати паралельні рішення. Це відкриває можливість створення цілих сімейств високоякісних S-блоків, які можуть використовуватися в різних криптографічних системах із динамічним оновленням або ротацією підстановок, підвищуючи загальний рівень криптографічної гнучкості та стійкості системи до аналізу зі сторони зловмисника. До того ж, генетичні алгоритми добре масштабуються, що дозволяє їх застосування не лише для S-блоків довжини $N = 256$, які є стандартними у багатьох шифрах, а й для більших розмірів, придатних для постквантових конструкцій або криптографічних систем зі змінною структурою блоку.

Таким чином, використання генетичних алгоритмів у задачі синтезу S-блоків з високою криптографічною якістю становить сучасний і перспективний підхід, який поєднує в собі силу еволюційного пошуку з математичними критеріями, притаманними сфері криптографії. Цей

підхід не тільки доповнює класичні методи побудови, засновані на алгебраїчних структурах, а й створює міст між теорією оптимізації, теорією обчислень і криптографією, відкриваючи нові горизонти у проєктуванні стійких і ефективних криптографічних примітивів.

Генетичний алгоритм [26–27] – це метод пошуку оптимального рішення, який імітує процес природного добору в біології. Його основна ідея полягає в тому, щоб почати з випадкового набору можливих рішень (їх ще називають «особинами» або «хромосомами»), а потім поступово покращувати ці рішення, використовуючи механізми, схожі на біологічну еволюцію: відбір, схрещування та мутації.

Спочатку створюється початкова популяція – набір випадкових кандидатів на рішення задачі. Наприклад, у випадку синтезу S-блоків кожен кандидат може бути представлений у вигляді таблиці відображення або як послідовність чисел, що задає певне переставлення бітів. Для кожного з кандидатів обчислюється так звана функція пристосованості, яка показує, наскільки добре це рішення виконує поставлену ціль. У нашому випадку – це відстань нелінійності.

Далі генетичний алгоритм проводить процес селекції – вибирає ті рішення, які мають кращу пристосованість, і використовує їх для створення нової популяції. При цьому застосовуються два основних механізми: схрещування – коли двоє «батьківських» рішень об'єднуються для створення нового, яке успадковує риси обох, та мутація – невелика випадкова зміна, що допомагає вийти за межі локального оптимуму й урізноманітнює пошук.

Новостворені особини (потомки) утворюють нову популяцію, і процес повторюється: оцінка якості, відбір, схрещування, мутація – покоління за поколінням. Ідея полягає в тому, що з кожною ітерацією (тобто з кожним новим «поколінням») середній рівень якості рішень зростає, і алгоритм поступово наближається до бажаного або навіть оптимального результату.

Зупиняється алгоритм тоді, коли досягнута достатньо висока якість рішень, або коли досягнуто певну кількість поколінь. Хоча результат не завжди є абсолютним максимумом, на практиці генетичні алгоритми часто дають дуже хороші та практично корисні рішення у задачах, де немає ефективного точного методу пошуку.

Алгоритм синтезу криптографічних S-блоків викладемо у вигляді наступних конкретних кроків [28]:

Крок 1. Задати початкову популяцію з $n/2$ S-блоків довжини N, кожний з яких визначається тривіальною монотонно-зростаючою послідовністю виду $0,1,...,N-1$. Задати значення лічильника ітерацій генетичного алгоритму $i=0$.

Крок 2. На основі популяції з $n/2$ S-блоків створити ще $n/2$ S-блоків, здійснюючи перестановку двох, випадковим чином обраних елементів їх Q-послідовностей, для кожного з них.

Крок 3. Провести вимірювання дистанційної нелінійності N_S кожного з n отриманих S-блоків, згідно до (3).

Крок 4. Видалити з популяції $n/2$ S-блоків, що володіють найменшими значеннями нелінійності N_S.

Крок 5. Якщо досягнуто останньої ітерації генетичного алгоритму, тобто $i=i_0-1$, зупин, інакше – перейти на Крок 2.

Для значення довжини S-блока $N=256$, загальної кількості S-блоків у популяції $n=0$, а також кількості ітерацій генетичного алгоритму $i_0=1000$, були отримані наступні результати щодо зростання максимального значення дистанційної нелінійності серед S-блоків у популяції в залежності від номеру ітерації генетичного алгоритму (рис. 2, де продемонстровані ітерації від 0 до 400).

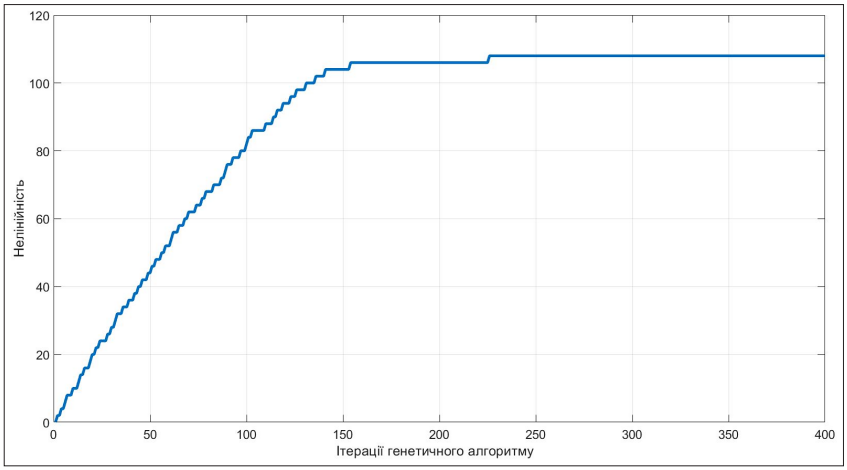


Рисунок 2 – Графік залежності максимального значення дистанційної нелінійності серед S-блоків у популяції від номера ітерації генетичного алгоритму

Аналіз даних рис. 2 показує стрімке зростання максимального значення дистанційної нелінійності серед S-блоків у популяції до 154 ітерації, після чого, на 227 ітерації максимальне значення дистанційної нелінійності стабілізується на значенні $\max(N_S) = 108$, що складає ~96.43 % від максимального значення нелінійності бієктивних S-блоків довжини $N = 256$.

Ми наводимо приклад одного із згенерованих за допомогою запропонованого генетичного алгоритму S-блоків у вигляді його Q-послідовності, що кодує.

$$
\begin{gathered}
S = \{86,150,43,44,105,93,12,107,196,206,161,138,217,13,120,59,29,\\
199,19,189,110,139,26,230,80,25,220,203,68,125,227,145,235,4,232,\\
183,42,155,211,148,253,245,201,163,84,99,66,39,210,54,90,78,100,\\
9,11,252,147,160,181,135,186,30,177,133,57,193,\ 89,55,149,27,38,136,\\
239,20,209,170,65,144,122,205,250,40,154,46,168,56,21,251,184,69,\\
95,231,248,223,187,35,104,119,101,88,60,106,204,197,36,81,126,137,\\
109,28,79,32,172,34,117,175,179,229,17,153,166,247,207,85,164,240,\\
214,\ 33,47,188,31,16,131,185,94,146,128,130,\ 18,202,58,225,75,91,71,\\
212,114,208,7,2,0,226,140,169,82,162,238,171,233,213,45,165,167,218,\\
174,37,121,190,180,127,115,123,243,64,50,151,134,6,191,158,192,73,97,\\
228,112,52,1,51,156,222,53,157,83,22,249,10,221,215,198,195,241,74,\\
113,124,132,5,159,98,254,236,224,116,62,141,194,152,176,111,182,200,\\
70,\ 15,237,118,\ 63,\ 76,173,72,178,77,108,61,96,103,129,14,102,67,\\
143,242,3,92,23,255,234,24,246,41,48,49,216,244,87,142,8,219\}.
\end{gathered}
\tag{16}
$$

Зазначений S-блок володіє дистанційною нелінійністю $N_S = 108$. Наведемо також інші показники криптографічної якості зазначеного S-блока. Його алгебраїчний степінь нелінійності складає $\deg(S) = 7$.

Наведемо матрицю ваг Хеммінга похідних компонентних булевих функцій S-блока (16):

e_j	$wt(D_{1,k})$	$wt(D_{2,k})$	$wt(D_{3,k})$	$wt(D_{4,k})$	$wt(D_{5,k})$	$wt(D_{6,k})$	$wt(D_{7,k})$	$wt(D_{8,k})$
10000000	144	132	128	120	136	124	128	128
01000000	132	128	132	120	132	140	112	116
00100000	132	136	140	120	112	120	128	116
00010000	128	128	132	136	148	116	148	136
00001000	120	120	116	136	132	108	140	112
00000100	132	116	120	136	128	124	132	124
00000010	120	132	128	124	132	132	124	124
00000001	92	124	124	116	120	132	140	132

, (17)

а також його матрицю коефіцієнтів кореляції:

$$R = \begin{bmatrix} 0,05 & 0,08 & 0,05 & 0,06 & -0,08 & 0,03 & -0,02 & -0,09 \\ 0 & 0,09 & 0 & -0,03 & 0 & -0,05 & -0,08 & 0,08 \\ 0,05 & -0,11 & -0,05 & -0,06 & 0,03 & 0,11 & 0,06 & 0,02 \\ 0,03 & 0,03 & 0,06 & -0,13 & -0,05 & -0,09 & 0,05 & -0,06 \\ -0,05 & 0,06 & -0,06 & 0,02 & 0,06 & 0 & 0 & 0 \\ -0,08 & -0,02 & -0,06 & 0 & 0,02 & 0,13 & 0,06 & -0,02 \\ -0,06 & 0,03 & 0 & 0,08 & -0,05 & -0,03 & 0,09 & 0,02 \\ 0,02 & 0,06 & 0 & 0,06 & 0,13 & -0,05 & -0,05 & 0 \end{bmatrix}. \quad (18)$$

Аналіз (17) і (18) показує, що окрім високих як алгебраїчної, так і дистанційної нелінійності, S-блок (16) володіє припустимими лавинними і кореляційними властивостями, що у поєднанні з його псевдовипадковою природою дозволяє рекомендувати його до практичного застосування.

Відзначимо основні результати:

1. Представлено генетичний алгоритм для синтезу множин довільної потужності високонелінійних (псевдо)випадкових S-блоків підстановки довільної довжини N.

2. Дослідження криптографічних властивостей синтезованих за допомогою розробленого генетичного алгоритму S-блоків довжини $N = 256$ дозволило встановити високий рівень їх криптографічної якості, зокрема, дистанційної та алгебраїчної нелінійності, а також припустимі лавинні і дистанційні властивості. У поєднані із їх псевдовипадковою природою це дозволяє рекомендувати такі S-блоки до практичного застосування.

1.5. Дослідження потужностей множин нелінійних перетворень із заданими значеннями періодів повернення у вихідний стан

К. Шенноном у 1949 р. [3] було введено концепцію криптографічного S-блока, як основного компонента для побудови захищених шифрів. Роки дослідження криптографічних конструкцій та досвід їх практичного застосування підтвердив роль S-блоків, як основних

компонентів, що визначають ефективність та швидкодію сучасних шифрів. У сьогоденні чітко визначений математичний апарат дослідження криптографічної якості S-блоків, що включає такі критерії, як нелінійність, критерій розповсюдження помилки та суворий лавинний критерій, критерій кореляційного імунітету та матриці коефіцієнтів кореляції, критерій максимізації періодів повернення у вихідний стан [29–30]. Запропоновано численні конструкції, призначені для побудови S-блоків, що відповідають зазначеним критеріям криптографічної якості.

Природньо, що у повній множині S-блоків існують обмежені кількості таких їх екземплярів, що у тій чи іншій мірі задовольняють вибраному критерію криптографічної якості. Означене встановлює певні лімітації на побудову S-блока, який був би ідеальним з точки зору кожного з зазначених критеріїв криптографічної якості. Дослідження потужностей множин S-блоків є фундаментальним з точки зору розробки практичних конструкцій S-блоків, дослідження їх криптографічної якості та розуміння основних можливостей щодо її підвищення.

Одним з основних критеріїв криптографічної якості є критерій, який було запропоновано у фундаментальній роботі [30], – повернення S-блоків у вихідний стан, який визначається як число ітерацій до повернення S-блоку в початковий стан, при тривалій вхідній дії. Для обчислення періоду повернення S-блока у вихідний стан, необхідно розкласти його на цикли, що визначаються як послідовності переходів елементів. Наприклад, для S-блока довжини $N = 8$:

$$S = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 6 & 7 & 3 & 2 & 0 & 1 & 4 & 5 \end{bmatrix}, \tag{19}$$

маємо наступні цикли:

$$S = \{C_3(6,4,0),\ C_3(1,7,5),\ C_2(2,3)\}, \tag{20}$$

тоді період повернення S-блока у вихідний стан визначатиметься як

$$T = \text{НСК}(i_1, i_2 ...). \tag{21}$$

Сформуємо алгоритм експериментальних досліджень у вигляді конкретних кроків [31].

Крок 1. Сформувати вибірку досліджуваних S-блоків Ψ заданої довжини N та потужності $|\Psi|$.

Крок 2. Провести дослідження періодів повернення для кожного S-блока, який був сформований на *Кроці 1*.

Задля дослідження взаємозв'язку періодів повернення S-блоків у вихідний стан для значення довжини $N = 8$ може бути застосований метод повного перебору, тобто сформована вибірка Ψ, що вміщуватиме всі можливі варіанти S-блоків даної довжини, оскільки загальна множина даних S-блоків включає лише $|\Psi| = 40\,320$ елементів.

У табл. 3 представлено значення періодів повернення S-блоків довжини $N = 8$ у вихідний стан.

Таблиця 3 – Значення періодів повернення у вихідний стан та відповідні їм значення нелінійності для S-блоків довжини $N = 8$

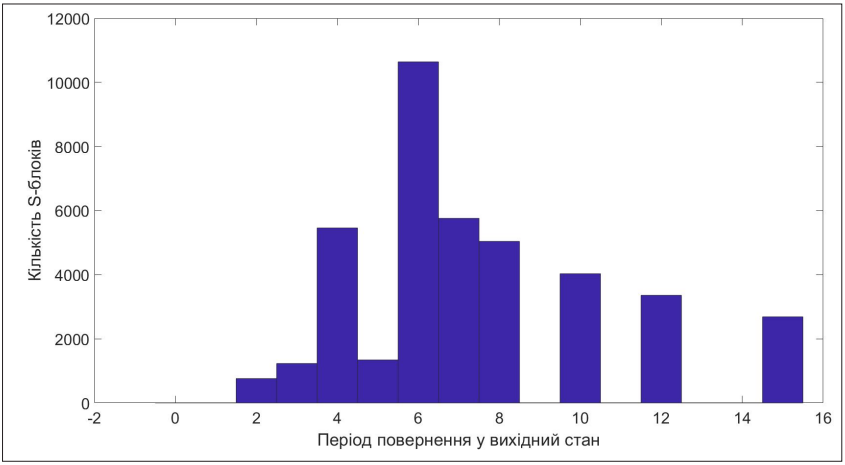
Період	1	2	3	4	5	6	7	8	10	12	15
Кількість	1	763	1232	5460	1344	10640	5760	5040	4032	3360	2688

Для дослідження S-блоків довжини $N = 16$ сформуємо вибірку з $|\Psi| = 1\,000\,000$ випадково згенерованих S-блоків, щодо яких проведемо дослідження, результати яких представлені у табл. 4.

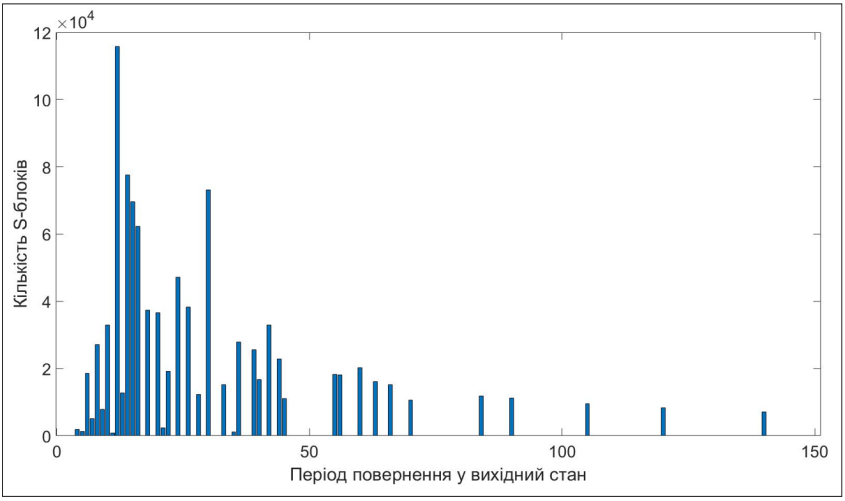
Таблиця 4 – Значення періодів повернення у вихідний стан та відповідні їм значення нелінійності для S-блоків довжини $N = 16$

Період	2	3	4	5	6	7	8
Кількість	1	52	1948	1440	18873	5034	27046
Період	9	10	11	12	13	14	15
Кількість	7580	32850	744	116719	12700	77251	69394
Період	16	18	20	21	22	24	26
Кількість	62387	37195	36889	2233	18684	47334	38474
Період	28	30	33	35	36	39	40
Кількість	12133	73450	15424	1172	27886	25781	16756
Період	42	44	45	55	56	60	63
Кількість	32804	23027	11089	18241	17764	19959	15831
Період	66	70	84	90	105	120	140
Кількість	15285	10714	11989	11031	9435	8145	7256

На рис. 3 показане графічне представлення кількостей S-блоків, що мають заданий період повернення у вихідний стан для значень довжини S-блоків $N = 8$ та $N = 16$.



a



b

Рисунок 3 – Кількості S-блоків, що мають заданий період повернення у вихідний стан для значень довжини $N = 8$ (a) та $N = 16$ (b)

Аналіз даних, що представлені у табл. 3 та табл. 4, а також даних рис. 3 дозволяє дійти висновку, що зі збільшенням значення необхідного періоду повернення, кількість S-блоків, що володіють даним періодом істотно зменшується.

Відзначимо основні результати:

1. Проведено дослідження кількостей S-блоків, що володіють заданим рівнем періоду повернення у вихідний стан для практично цінних довжин $N = 8,16$.

2. Встановлено, що зі збільшенням значення періоду повернення S-блоків, кількість S-блоків, що володіють даним значенням періоду повернення, зменшується. Дана обставина означає, що випадково згенерований S-блок, з великою ймовірністю, не володітиме максимальним або близьким до максимального для даної довжини S-блоків значенням періодів повернення у вихідний стан. Означене диктує необхідність розробки регулярних методів синтезу множин S-блоків, які, зокрема, відповідають критерію максимізації періоду повернення у вихідний стан.

1.6. Дослідження змін нелінійності компонентних функцій багатозначної логіки випадкового S-блока при зростанні його довжини

Дослідження змін нелінійності компонентних функцій багатозначної логіки випадкового S-блока при зростанні його довжини є надзвичайно актуальним з огляду на сучасні виклики криптографії. Класичні підходи до оцінки криптографічної стійкості S-блоків зазвичай базуються на аналізі їхніх бінарних представлень, проте розгляд всіх можливих уявлень, зокрема через функції багатозначної логіки, відкриває нові горизонти в розумінні їхньої поведінки і властивостей. Такий підхід особливо важливий в контексті розвитку квантового криптоаналізу, де класичні критерії стійкості можуть виявитися недостатніми або потребувати доопрацювання. Вивчення нелінійності через призму багатозначної логіки дозволяє глибше оцінити стійкість S-блоків до нових типів атак, а також сприяє розробці більш надійних і адаптивних криптографічних компонентів. З огляду на те, що довжина S-блока істотно впливає на його

внутрішню структуру і складність функцій, дослідження зміни нелінійності при зміні розмірності є ключовим для оптимізації дизайну сучасних шифрів.

Задля збільшення рівня якості застосовуваних математичних конструкцій, сучасними дослідниками розробляються математично обґрунтовані методи синтезу S-блоків, що мають високі значення нелінійності. Іншим підходом до синтезу ефективних S-блоків є підхід, заснований на їх випадковій генерації. Відомо, що зі збільшенням довжини S-блоку суттєво покращується його криптографічна якість, зокрема, його нелінійність. Через те, що сучасні криптографічні алгоритми характеризуються досить високою довжиною застосовуваних S-блоків (типова довжина $N=256$), якість випадково згенерованих S-блоків такої довжини проголошується як достатня.

Тим не менш, реальна динаміка змін у нелінійності S-блоків із зміною їх довжини при їх уявленні за допомогою функцій багатозначної логіки у літературі не досліджувалася.

Добре відомим є універсальне визначення нелінійності булевих функцій та функцій багатозначної логіки, яка чисельно може бути розрахована за допомогою наступної формули [32].

$$NL = \begin{cases} q^k - \max\left\{\left|\Omega(\acute{E})\right|\right\}, & q > 2; \\ 2^{k-1} - \dfrac{1}{2}\max\left\{\left|W(\acute{E})\right|\right\}, & q = 2, \end{cases} \tag{22}$$

де $\Omega(\omega)$ – коефіцієнти перетворення Віленкіна-Крестенсона досліджуваної q-функції, $W(\omega)$ – коефіцієнти перетворення Уолша – Адамара досліджуваної булевої функції, k – кількість змінних, від яких залежить компонентна q-функція.

Тим не менш, само по собі порівняння значень нелінійності (22) компонентних q-функцій різних довжин N не є показовим. Має сенс досліджувати значення нелінійності у порівнянні із максимально можливим значенням нелінійності, яке принципово можуть прийняти q-функції.

Максимальне значення нелінійності збалансованих функцій багатозначної логіки у загальному випадку відсутнє у відритих джерелах, тож для порівняння значень нелінійності зручно використовувати такі

досконалі алгебраїчні конструкції як бент-функції, які мають мінімально можливе значення максимального коефіцієнта перетворення Віленкіна-Крестенсона $q^{k/2}$, і, відповідно, максимальне значення нелінійності, що дорівнює:

$$\max\{N_{f_q}\} = q^k - q^{k/2}, \quad q > 2. \tag{23}$$

При цьому, у випадку булевих функцій, враховуючи, що мінімально можливий модуль значення максимального коефіцієнта перетворення Уолша – Адамара дорівнює $2^{\frac{k}{2}-1}$, максимальне значення нелінійності складає:

$$\max\{N_{f_2}\} = 2^{k-1} - 2^{\frac{k}{2}-1}. \tag{24}$$

Зазначимо, що вираз (24) має сенс тільки для парних значень k, тоді як при непарних k булеві бент-функції не існують.

Таким чином, коефіцієнт відносної нелінійності (виражений у відсотках) можна визначити як відношення нелінійності досліджуваної функції багатозначної логіки до максимального значення нелінійності:

$$\xi = \frac{N_{f_q} 100\%}{\max\{N_{f_q}\}}. \tag{25}$$

Коефіцієнт відносної нелінійності (25) дозволяє порівнювати рівень нелінійності криптографічних конструкцій різної довжини при їх уявленні за допомогою компонентних q-функцій для різних значень основи уявлення q.

Відзначимо при цьому, що через те, що булеві бент-функції не існують при непарних значеннях k, визначення відносної нелінійності (25) не має для них сенсу.

Відповідно до мети роботи сформуємо алгоритм експериментальних досліджень у вигляді конкретних кроків [33].

Крок 1. Сформувати перелік досліджуваних довжин S-блоків $\{N_i\}, i = 1,2,...,L$.

Крок 2. Випадково сформувати для кожного N_i J S-блоків довжини N_i.

Крок 3. Дослідити нелінійність кожного згенерованого на *Кроці* 2 S-блоку, в результаті чого сформувати для кожного N_i свою послідовність значень нелінійності $\{NL_j\}$, $j = 1,2,...,J$.

Крок 4. Усереднити значення нелінійності для кожного N_i, тобто сформувати послідовність $\{\overline{NL_i}\}, i = 1,2,...,L$.

Зазначений алгоритм досліджень був застосований до компонентних булевих функцій випадкових S-блоків довжин $\{N_i\} = \{4,16,64,256,1024,4096\}$, до компонентних 4-функцій випадкових S-блоків довжин $\{N_i\} = \{16,64,256,1024,4096\}$, а також до компонентних 16-функцій випадкових S-блоків довжин $\{N_i\} = \{256,4096\}$. При цьому був обраний параметр $J = 100$ задля забезпечення показовості отриманих результатів.

Результати виконання розробленого алгоритму досліджень у вигляді графіків залежності нелінійності випадково згенерованого S-блока від його довжини при його уявленні компонентними q-функціями для різних значень q показано на рис. 4.

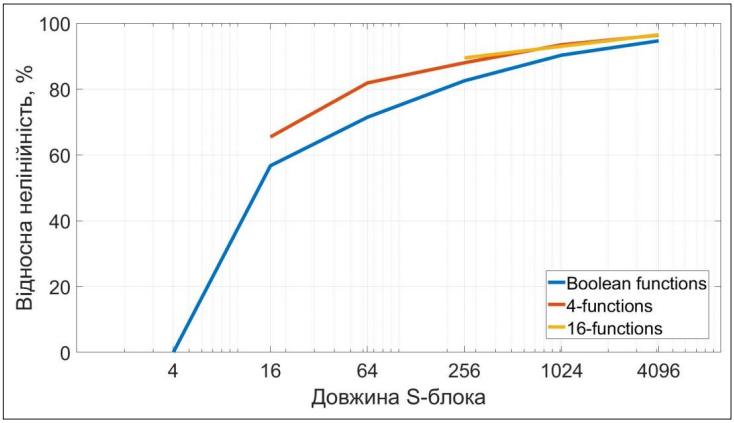


Рисунок 4 – Графік залежності нелінійності випадкового S-блока від його довжини для різних значень основи уявлення q

Аналіз рис. 4 дозволяє зробити висновок про суттєве зростання нелінійності випадково згенерованого S-блока із зростанням його довжини. При цьому, як показують дані проведеного експерименту, компонентні 4-функції та 16-функції випадкового S-блока демонструють більші значення відносної нелінійності та швидше її наближення до рівня нелінійності бент-функцій у порівнянні з компонентними булевими функціями.

Відзначимо основні результати:

1. Проведено дослідження нелінійності випадкового S-блока при його представленні компонентними булевими функціями та функціями багатозначної логіки в залежності від його довжини.

2. Встановлено, що із зростанням довжини випадкового S-блока нелінійність його компонентних q-функцій наближається до рівня нелінійності бент-функцій. При цьому, компонентні 4-функції та 16-функції, у порівнянні з компонентними булевими функціями, демонструють більші значення відносної нелінійності та швидше її наближення до рівня нелінійності бент-функцій.

3. Отримані результати показують, що при достатній довжині S-блоків ($N \geq 256$), метод їх випадкової генерації здатен забезпечити нелінійність їх компонентних q-функцій на рівні у якнайменше 80 % від нелінійності бент-функцій для основ уявлення $q = \{2, 4, 16\}$.

1.7. Перспективи подальшої роботи над вдосконаленням конструкцій підстановки

У зв'язку з постійним розвитком засобів криптоаналізу, зростанням обчислювальних можливостей, включно з появою квантових обчислювальних пристроїв, та ускладненням задач захисту даних, розробка нових підходів до побудови S-блоків залишається одним із найважливіших напрямів сучасної криптографії. Підстановки відіграють центральну роль у симетричних шифрах, забезпечуючи їхню нелінійність та здатність протистояти лінійному й диференціальному криптоаналізу. У цьому контексті можна окреслити кілька перспективних напрямів подальших досліджень, які мають потенціал суттєво посилити криптографічну стійкість алгоритмів за рахунок більш гнучких, адаптивних та математично обґрунтованих конструкцій S-блоків.

Одним із найбільш багатообіцяючих напрямів є синтез S-блоків на основі функцій багатозначної логіки. Такий підхід дозволяє розширити клас використовуваних функцій за межі традиційних булевих перетворень. Багатозначна логіка (наприклад, тризначна, чотиризначна і т. д.) дає змогу моделювати більш складні перетворення, які мають внутрішню симетрію, більш багатий спектр значень та властивостей. Завдяки цьому можна проєктувати підстановки, що

водночас мають високу булеву нелінійність, гарну кореляційну стійкість та адаптивну структуру, зручну для подальшого аналізу й оптимізації. Перспективним напрямом є розробка відповідних метрик якості таких S-блоків, урахування багатокомпонентних представлень та дослідження їхньої поведінки при спробах атак, включно з квантовими.

Не менш важливим є подальше вдосконалення конструкцій, побудованих на основі алгебраїчних структур полів Галуа. Відомі результати – зокрема, обернення в полі як базова функція в конструкції Ніберг – показали, що елементи полів Галуа здатні забезпечувати високі показники з точки зору криптографічної стійкості. Проте традиційні конструкції мають певні обмеження, пов'язані з розміром поля, обчислювальною складністю операцій та незмінністю структури. Подальші дослідження можуть бути спрямовані на створення узагальнених підстановок, які комбінують кілька операцій у полі, використовують нетривіальні автоморфізми або побудовані на злитті кількох полів у композиційні структури. Такі підходи дозволяють підвищити варіативність і непередбачуваність поведінки S-блоків, що є критичним для захисту від сучасного криптоаналізу.

Окремий клас завдань формує застосування генетичних алгоритмів для синтезу S-блоків. Як було показано раніше, генетичні алгоритми ефективні для пошуку оптимальних або близьких до оптимальних рішень у великому й складному просторі можливих відображень. Перспективним є розвиток адаптивних схем, де параметри алгоритму змінюються в процесі виконання, а також гібридизація з іншими методами – наприклад, з локальним пошуком або табу-пошуком. Особливо цікавою є можливість використання генетичних алгоритмів не лише для статичного синтезу, а й для динамічного формування S-блоків у реальному часі, наприклад, у контексті потокових шифрів або алгоритмів з обертовою структурою. Це відкриває нові горизонти в області самонавчальних або реактивних криптографічних систем, які здатні змінювати свою поведінку відповідно до умов середовища.

У ширшому контексті, застосування методів штучного інтелекту та машинного навчання у задачах побудови S-блоків відкриває абсолютно нову площину можливостей. Зокрема, нейромережеві

підходи можуть бути використані як для генерації нових S-блоків, так і для оцінювання їхньої якості або прогнозування слабких місць у структурі. Ідеї підкріпленого навчання дають змогу будувати алгоритми, які адаптують свою структуру в залежності від результатів криптоаналізу, таким чином еволюціонуючи у напрямі посилення власної стійкості. Навіть за межами класичних застосувань, штучний інтелект може бути використаний для автоматизованого доказу властивостей S-блоків, побудови моделей атак та пошуку нових принципів побудови криптографічних примітивів. Синтез таких підстановок із використанням глибоких моделей або евристичних пошуків відкриває шлях до створення інтелектуально керованих криптосистем нового покоління.

Загалом, подальше вдосконалення конструкцій S-блоків потребує поєднання глибоких математичних знань із алгоритмічною гнучкістю, властивою еволюційним і штучно-інтелектуальним підходам. Комбінація методів багатозначної логіки, алгебраїчної теорії полів, обчислювального інтелекту та криптоаналітичного моделювання утворює міждисциплінарне підґрунтя, на якому може розвиватися новий клас стійких, ефективних і адаптивних криптографічних примітивів. В умовах зростаючих викликів до безпеки інформації, особливо в еру постквантових загроз, такі дослідження мають не лише наукове, а й стратегічне значення.

Список використаних джерел

1. Sagindikovich P. Q. Modern cryptography algorithms. *American Journal of Education and Learning*. 2025. Vol. 3 (5). P. 68–73.

2. Ali R. S. et al. A comprehensive review on S-box generation methods. AIP Conference Proceedings. *AIP Publishing LLC.* 2024. Vol. 3207 (1). P. 020001.

3. Shannon C. E. Communication theory of secrecy systems. *The Bell system technical journal.* 1949. Vol. 28 (4). P. 656–715. DOI: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

4. Forrié R. The strict avalanche criterion: spectral properties of Boolean functions and an extended definition. Conference on the Theory and Application of Cryptography. New York, NY : Springer New York. 1988. P. 450–468.

5. Deepthi D. V. V., Benny B. H., Sreenu K. Various ciphers in classical cryptography. Journal of Physics: Conference Series. IOP Publishing, 2019. Vol. 1228 (1). P. 012014.

6. Hamza A., Kumar B. A review paper on DES, AES, RSA encryption standards. International Conference System Modeling and Advancement in Research Trends (SMART). IEEE, 2020. P. 333–338.

7. Krishnamurthy G. N., Ramaswamy V. Making AES stronger: AES with key dependent S-box. *IJCSNS International Journal of Computer Science and Network Security.* 2008. Vol. 8 (9). P. 388–398.

8. Schneier B. The Twofish encryption algorithm. *Dr. Dobb's Journal: Software Tools for the Professional Programmer.* 1998. Vol. 23 (12). P. 30–34.

9. Бакуніна О. В., Баландіна Н. М., Соколов А. В. Метод синтезу s-блоків на основі матриць GF-перетворення. *Український журнал інформаційних технологій.* 2023. Т. 5 (2). С. 41–48.

10. Mazurkov M. I., Sokolov A. V. Nonlinear transformations based on complete classes of isomorphic and automorphic representations of field GF (256). *Radioelectronics and Communications Systems.* 2013. Vol. 56 (11). P. 513–521. DOI: https://doi.org/10.3103/s0735272713110022

11. Sokolov A. V., Djiofack T. V.N. Nonlinear Properties of Rijndael S-boxes Represented by the Many-Valued Logic Functions. Proceedings of the International Workshop on Cyber Hygiene, Kyiv, Ukraine, 2019. P. 96–106.

12. Rostovcev A. G. Cryptography and Data Protection. Mir i Sem'ja. 2002.

13. Logachev O. A., Sal'nikov A. A., Jashhenko V. V. Boolean functions in coding theory and cryptology, USA: American Mathematical Society. 2012.

14. Mazurkov M. I., Sokolov, A. V. Constructive method for synthesis of complete classes of multilevel de Bruijn sequences. Radioelectronics and Communications Systems. 2013. Vol. 56 (1), P. 36–41. DOI: https://doi.org/10.3103/s0735272713010044

15. Wang J., Zhu Y., Zhou C., Qi Z. Construction Method and Performance Analysis of Chaotic S-Box Based on a Memorable Simulated Annealing Algorithm. *Symmetry.* 2020. No. 12, P. 2115. DOI: https://doi.org/10.3390/sym12122115

16. Lambić D. S-box design method based on improved one-dimensional discrete chaotic map. *Journal of Information and Telecommunication.* 2018. Vol. 2 (2). P. 181–191. DOI: https://doi.org/10.1080/24751839.2018.1434723

17. Lu Q., Zhu C., Wang G. (2019). A Novel S-Box Design Algorithm Based on a New Compound Chaotic System. Entropy. 2019. Vol. 21 (10). P. 1004. DOI: https://doi.org/10.3390/e21101004

18. Lai Q., Akgul A., Li C., Xu G., Çavuşoğlu U. A New Chaotic System with Multiple Attractors: Dynamic Analysis, Circuit Realization and S-Box Design. *Entropy*. 2018. Vol. 20 (1). P. 12. DOI: https://doi.org/10.3390/e20010012

19. Баландіна Н. М. Дослідження нелінійності S-блока на основі теорії динамічного хаосу при його уявленні функціями багатозначної логіки. *Кібербезпека в сучасному світі* : матер. III Всеукр. наук.-практ. конф. (м. Одеса, 19 листопада 2021 року). Одеса : ВД «Гельветика», 2021. С. 43–48. DOI: 10.32837/11300.15973

20. FIPS 197. (2001) Advanced encryption standard. URL: http://csrc.nist.gov/publications/

21. Баландіна Н. М. Алгебраїчна нелінійність S-блоків конструкції Ніберг при їх представленні функціями багатозначної логіки. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень* : матер. Міжнар. наук.-практ. конф. (м. Одеса, 19 травня 2023 року). Одеса : ВД «Гельветика», 2023. С. 627–630. ISBN 978-617-8263-37-9

22. Stankovic R. S., Astola J. T., Moraga C. Representations of Multiple-Valued Logic Functions. Morgan and Claypool Publishers, 2012.

23. Sokolov A. V., Overchuk Yu.S. On the possibility of synthesizing an algebraic normal form of quaternary functions over the field GF (4). *Problems of cyber security of information and telecommunication systems*: Proceedings of the first international scientific and practical conference. 2018. P. 384–388.

24. Grošek O., Fabšič T. Computing multiplicative inverses in finite fields by long division. *Journal of Electrical Engineering*. 2018. Vol. 69 (5). P. 400–402. DOI: https://doi.org/10.2478/jee-2018-0059

25. Berlekamp E. R. Algebraic coding theory: Revised Edition. World Scientific. 2015. DOI: https://doi.org/10.1142/9407

26. Katoch S., Chauhan S. S., Kumar V. A review on genetic algorithm: past, present, and future. *Multimedia tools and applications.* 2021. Vol. 80 (5). P. 8091–8126.

27. Haldurai L., Madhubala T., Rajalakshmi R. A study on genetic algorithm and its applications. *Int. J. Comput. Sci. Eng.* 2016. Vol. 4 (10). P. 139–143.

28. Баландіна Н. М. Розробка генетичного алгоритму для побудови високонелінійних S-блоків підстановки. *Інформаційне суспільство: проблеми та перспективи* : матер. IX Всеукр. наук.-практ. конф. (м. Одеса, 24 травня 2024 року). Одеса : НУ «ОЮА», 2024. С. 140–144. DOI: https://doi.org/10.32837/11300.27842

29. Соколов А. В. Новые методы синтеза нелинейных преобразований современных шифров. Lap Lambert Academic Publishing, Germany 2015. 100 с.

30. Зайко Ю. Н. Криптография глазами физика. Изв. Саратовского ун-та. 2009. Т. 9 (2). С. 34–48.

31. Баландіна Н. М. Дослідження потужностей множин нелінійних перетворень із заданими значеннями періодів повернення у вихідний стан. *Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика* : матер. Міжнародної наук.-практ. конференції. 2023. С. 123–127.

32. Sokolov A. V., Zhdanov O. N. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties. *Journal of Telecommunication, Electronic and Computer Engineering.* 2016. Vol. 8 (9). P. 39–43.

33. Баландіна Н. М. Дослідження змін нелінійності компонентних функцій багатозначної логіки випадкового S-блока при зростанні його довжини. *Кібербезпека в сучасному світі: актуальні виклики* : матер. IV Всеукр. наук.-практ. конф. (м. Одеса, 25 листопада 2022 року). Одеса : ВД «Гельветика», 2022. С. 24–28. ISBN 978-966-992-297-7