НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

ГЕНЕРАЦІЯ ДИНАМІЧНИХ S-БЛОКІВ (F-БЛОКІВ) НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

Роговий Іван

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

S-блоки є фундаментальним компонентом симетричних криптографічних алгоритмів, від властивостей яких безпосередньо залежить стійкість шифрів до диференціального та лінійного криптоаналізу. Використання статичних S-блоків у режимах довготривалої експлуатації супроводжується низкою обмежень, оскільки накопичення статистичної інформації та застосування адаптивних атак можуть призводити до зниження рівня криптографічного захисту. У цьому контексті особливий інтерес становлять динамічні S-блоки (F-блоки), структура яких змінюється в процесі функціонування алгоритму. Такий підхід ускладнює накопичення релевантної статистики для криптоаналізу та сприяє підвищенню загальної криптостійкості симетричних криптосистем.

Метою роботи є аналіз і обґрунтування ідеї використання еліптичних кривих для генерації динамічних S-блоків (F-блоків), а також оцінка криптографічних властивостей і перспектив застосування такого підходу в симетричних криптографічних алгоритмах.

S-блоки (substitution boxes) є ключовими нелінійними перетвореннями симетричних криптографічних алгоритмів, призначеними для забезпечення конфузії (confusion) між відкритим текстом, ключем і шифротекстом. Вони реалізують відображення вхідних бітових векторів у вихідні, формуючи основне джерело нелінійності в структурі шифру. Саме властивості S-блоків значною мірою визначають криптографічну стійкість алгоритмів до основних видів статистичного криптоаналізу, зокрема диференціального та лінійного.

До основних криптографічних характеристик S-блоків належать висока нелінійність, низька диференційна однорідність, збалансованість, відсутність фіксованих точок і лінійних апроксимацій із великою ймовірністю. Порушення цих вимог призводить до зниження стійкості шифру та створює передумови для ефективних атак. У зв’язку з цим розроблення та аналіз S-блоків із покращеними характеристиками є однією з центральних задач сучасної симетричної криптографії.

F-блоки реалізують динамічну зміну таблиці замін залежно від параметрів криптографічної сесії, секретного ключа або внутрішнього стану алгоритму, що суттєво знижує ефективність атак, заснованих на накопиченні статистичної інформації для фіксованих S-блоків. Формування таких таблиць може здійснюватися детерміністичним способом на основі ключа або початкового значення, із застосуванням генераторів псевдовипадкових

послідовностей, хаотичних відображень чи інших математичних конструкцій. Окремий інтерес становлять підходи, що використовують математичний апарат еліптичних кривих [1], у яких координати точок та результати групових операцій слугують джерелом високої ентропії для побудови перестановок. Застосування еліптичних кривих дозволяє поєднати високу криптографічну міцність із детерміністичною відтворюваністю структури F-блоку за наявності коректного ключа, що є принципово важливим для практичної реалізації симетричних криптосистем.

Алгоритм генерації F-блоків має задовольняти низку принципових вимог. Зокрема, він повинен гарантувати бієктивність відображення, тобто формування коректної перестановки значень, а також забезпечувати високий рівень нелінійності та низькі значення диференціальних і лінійних характеристик. Важливою практичною умовою є прийнятна обчислювальна складність і швидкість генерації, що визначає можливість реального впровадження алгоритму в симетричних криптосистемах. Крім того, алгоритм має бути стійким до відновлення структури F-блоку на основі часткових спостережень або побічної інформації, що є критичним для забезпечення довготривалої криптографічної безпеки. Для ілюстрації запропонованого підходу розглянемо узагальнену концептуальну схему формування динамічних S-блоків (F-блоків) із використанням операцій над еліптичними кривими. Наведена схема має ілюстративний характер і демонструє принципову можливість практичної реалізації ідеї, не претендуючи на завершену криптографічну специфікацію.

Орієнтовна схема генерації F-блоку може включати такі етапи:

1. В якості вхідних параметрів використовується симетричний ключ K та внутрішній сід S, який може формуватися як функція від ключа та випадкового вектора.
2. На основі пари $\{K, S\}$ генерується послідовність скалярів k_i, що визначають подальші операції на еліптичній кривій.
3. Для кожного значення k_i може обчислюватися відповідна точка $P_i = k_i G$ на еліптичній кривій, де G – фіксована базова точка.
4. Координати (x_i, y_i) отриманих точок перетворюються у бітові послідовності, які можуть використовуватися як джерело псевдовипадкових даних для побудови перестановки, зокрема із застосуванням алгоритму Фішера-Йетса.
5. Результатом є бієктивна перестановка значень (наприклад, множини $0...255$ для 8-бітного S-блоку), що визначає таблицю замін F-блоку.

Використання процедур перетасування гарантує бієктивність сформованого S-блоку за умови коректного контролю повторів у псевдовипадковій послідовності. У практичних реалізаціях це може

досягатися шляхом відкидання некоректних значень або повторної ініціалізації сіду.

Запропонована концептуальна схема демонструє, що операції над еліптичними кривими можуть бути ефективно використані як джерело керованої псевдовипадковості для формування динамічних S-блоків із детермінованою відтворюваністю за наявності ключа.

Побудовані S-блоки (F-блоки) підлягають обов'язковому тестуванню на відповідність базовим критеріям криптографічної якості [2], що дозволяють оцінити їхню придатність для використання в симетричних криптосистемах. До таких критеріїв належать алгебраїчна нелінійність, відстань нелінійності, диференціальна та лінійна стійкість, лавинні й кореляційні властивості. Оцінювання зазначених характеристик є необхідним для підтвердження здатності F-блоків протидіяти основним видам статистичного криптоаналізу.

Нелінійність S-блоків визначається як мінімальна відстань Хеммінга між булевими функціями, що утворюють S-блок, та множиною всіх афінних функцій. Використання послідовностей, сформованих на основі операцій над точками еліптичних кривих, дозволяє очікувати високі значення нелінійності завдяки їхній структурній непередбачуваності. Диференціальна стійкість аналізується за допомогою матриці диференціальних переходів (DDT), причому динамічний характер F-блоків призводить до розмивання статистичних залежностей між сесіями, що знижує ймовірність виявлення корисних диференціальних відмінностей.

Лавинні властивості оцінюються шляхом аналізу впливу малих змін ключа або початкового значення на структуру F-блоку, що має спричиняти суттєву реконфігурацію таблиці замін та забезпечувати як локальну, так і глобальну дифузію. Додатково аналізуються кореляційні характеристики шляхом дослідження лінійних апроксимацій, зокрема із застосуванням лінійної апроксимаційної матриці.

Методика тестування передбачає генерацію множини F-блоків для різних значень початкових параметрів, подальше обчислення їхніх криптографічних характеристик, аналіз лавинного ефекту на входах і виходах, а також дослідження поведінки F-блоків за умов часткової відомості відкритого тексту. Для розширеного аналізу можливе застосування апарату багатозначної логіки, який дозволяє узагальнено оцінювати нелінійні та кореляційні властивості криптографічних конструкцій у ширшому алгебраїчному просторі.

Питання продуктивності та оптимізації є принципово важливими для практичного застосування F-блоків, побудованих на основі еліптичних кривих. Генерація таких блоків передбачає виконання операцій множення точки на скаляр, які є обчислювально затратними порівняно з традиційними табличними S-блоками. З метою зменшення обчислювальних витрат можливе

застосування попереднього кешування F-блоків на етапі ініціалізації криптографічної сесії, використання ефективних представлень еліптичних кривих (зокрема форм Монтгомері або Едвардса), а також апаратне прискорення з використанням спеціалізованих процесорів, FPGA або ASIC. Додатковим шляхом оптимізації є обмеження частоти реконфігурації F-блоку, наприклад, на рівні сесії, а не кожного блоку повідомлення. Таким чином, ключовим завданням є балансування між частотою оновлення F-блоку та витратами обчислювальних ресурсів і пам'яті. Коректний вибір інтервалу оновлення дозволяє досягти необхідного рівня криптографічної безпеки без критичного зниження продуктивності системи, що є особливо важливим для вбудованих та високонавантажених середовищ.

Висновки та практичні рекомендації. Дослідження показує, що динамічні S-блоки на основі еліптичних кривих представляють перспективний напрямок підвищення криптостійкості симетричних шифрів, оскільки їхня зміна в процесі роботи суттєво ускладнює збір корисної статистики про заміни. Критично важливо, щоб алгоритм генерації забезпечував бієктивність та високий рівень нелінійності, що потребує обов'язкового емпіричного тестування на відповідність основним криптографічним критеріям при кожній реалізації. Для практичного застосування слід оптимізувати процес генерації F-блоків, використовуючи кешування, ефективні представлення еліптичних кривих та апаратне прискорення, а також передбачити заходи захисту від атак по сторонніх каналах. Рекомендується інтегрувати F-блоки у комплексну криптографічну стратегію, поєднуючи динамічні блоки, надійні схеми управління ключами та політики їх ротації, що забезпечує високий рівень захисту та практичну придатність симетричних систем шифрування.

Список використаної літератури:

1. Alali A.S. et al. Dynamic S-Box Construction Using Mordell Elliptic Curves over Galois Field and Its Applications in Image Encryption. Mathematics, 2024. 12(4). P. 587
2. Karpinski M., Sokolov A., Tokkuliyeva A., Radush V., Kazakova N., Shaikhanova A., Zagorodna N., Korchenko A. Development of High-Quality Cryptographic Constructions Based on Many-Valued Logic Affine Transformations. Electronics. 2025. Vol. 14, Issue 10. P. 1-22.

Ключові слова: F-блоки, динамічні S-блоки, симетричні шифри, криптостійкість, диференціальний та лінійний криптоаналіз, еліптичні криві, нелінійність, лавинні властивості, багатозначна логіка.

Keywords: F-boxes, dynamic S-boxes, symmetric ciphers, cryptoresistance, differential and linear cryptanalysis, elliptic curves, nonlinearity, avalanche properties, many-valued logic.

ЗМІСТ