УДК 004.056.55

І. О. Бондаренко
М. О. Тарасюк

АНАЛІЗ КРИПТОГРАФІЧНОГО АЛГОРИТМУ TWOFISH ТА ЙОГО МІСЦЕ СЕРЕД СУЧАСНИХ СТАНДАРТІВ ШИФРУВАННЯ

Вінницький національний технічний університет

Анотація

У роботі проведено аналіз симетричного алгоритму блочного шифрування Twofish, який був одним із фіналістів конкурсу AES. Також було досліджено особливості структури алгоритму, зокрема, використання S-блоків, що залежать від ключів, 16-раундову мережу Фейстеля. MDS-матриці. Криптоалгоритм має відкритий вихідний код. Також визначено, що Twofish – один із найкращих виборів серед кандидатів на AES завдяки його швидкості та гнучкості. Результати аналізу підтверджують, що Twofish залишається одним із найбільш надійних інструментів для захисту даних у сучасних інформаційно-комунікаційних системах.

Ключові слова: криптографія, ключ, S-блоки, Twofish, блочне шифрування, захист інформації, AES.

Abstract

The paper analyzes the Twofish symmetric block cipher algorithm, which was one of the finalists in the AES competition. It also examines the algorithm's structural features, including the use of key-dependent S-boxes, a 16-round Feistel network, and MDS matrices. The cryptographic algorithm is open-source. It was also determined that Twofish is one of the best choices among the AES candidates due to its speed and flexibility. The results of the analysis confirm that Twofish remains one of the most reliable tools for data protection in modern information and communication systems.

Keywords: cryptography, key, S-blocks, Twofish, block encryption, information protection, AES.

Вступ

З розвитком цифрової економіки та зростанням кіберзагроз, вибір надійного алгоритму шифрування стає дедалі важливішим для бізнесу. Хоча стандарт AES (Rijndael) широко використовується, дослідження альтернативних рішень, таких як Twofish, дозволяє розробляти більш гнучкі системи безпеки з кращим захистом від певних атак. Проблематику стійкості Twofish та порівняння криптоалгоритмів досліджували такі відомі фахівці, як Брюс Шнайєр [1], Нільс Фергюсон [2] та Джон Келсі [3]. Метою роботи є аналіз технічних переваг Twofish та оцінка його ефективності порівняно з сучасними стандартами.

Результати дослідження

Алгоритм Twofish належить до сімейства симетричних блочних шифрів і використовує 128-бітний розмір блоку з можливістю застосування ключів довжиною 128, 192 або 256 біт. Архітектурно він базується на мережі Фейстеля з 16 раундами перетворень, що забезпечує високу стійкість до лінійного та диференційного криптоаналізу [1].

Однією з ключових переваг Twofish є використання залежних від ключа S-блоків (таблиць заміни). На відміну від алгоритму AES, де S-блоки є статичними та однаковими для будь-якого ключа, у Twofish вони генеруються на основі самого ключа шифрування . Це означає, що зловмисник не може заздалегідь проаналізувати властивості таблиць замін для пошуку вразливостей, оскільки для кожного нового ключа архітектура шифру фактично стає унікальною. Такий підхід значно підвищує теоретичний «запас міцності» алгоритму [2].

Для забезпечення швидкого розсіювання (diffusion) даних у Twofish застосовуються MDS-матриці (Maximum Distance Separable) та псевдо-перетворення Адамара (PHT). Ці математичні операції дозволяють одному вхідному біту впливати на багато вихідних бітів вже після кількох раундів, що критично важливо для захисту від статистичних методів злому [1]. При порівнянні з AES стає очевидним, що Twofish має складніший механізм розгортання ключа (key schedule). Хоча це вимагає

більше часу на підготовку до шифрування, такий підхід робить алгоритм стійкішим до атак на пов'язаних ключах (related-key attacks), які є потенційною загрозою для спрощених систем [3].

Важливим аспектом є продуктивність алгоритму на різних апаратних платформах. Twofish демонструє високу ефективність як на сучасних 32-бітних і 64-бітних процесорах, так і на мікроконтролерах з обмеженими ресурсами (наприклад, смарт-картках). Розробник має можливість обирати стратегію реалізації: або попередньо обчислювати всі підключі для максимальної швидкості, або генерувати їх «на льоту» для економії оперативної пам'яті. Така гнучкість дозволяє використовувати Twofish у широкому спектрі пристроїв – від потужних серверів до вбудованих систем інтернету речей (IoT) [4].

Незважаючи на те, що Twofish не було обрано офіційним стандартом AES через дещо нижчу швидкість у програмних реалізаціях порівняно з Rijndael, він зберігає високий рівень криптостійкості. За понад два десятиліття існування не виявлено повнораундової атаки, ефективнішою за метод повного перебору (brute force). Це підтверджує його високу репутацію серед фахівців із кібербезпеки. Станом на сьогодні алгоритм активно інтегрується в професійні інструменти захисту інформації, такі, як криптоконтейнери VeraCrypt і поштові сервіси з наскрізним шифруванням, де пріоритет надається надійності над швидкістю обробки даних [5].

Висновки

Зі швидким розвитком інформаційних технологій також зростають вимоги щодо безпеки обміну даними в цифровому світі. Результати аналізу підтверджують, що криптоалгоритм Twofish залишається одним із найбільш надійних алгоритмів шифрування та зразком криптографічної досконалості. Алгоритм підтримує 128-, 192- або 256-бітові ключі, що робить його гнучким та адаптивним до всіх вимог безпеки. Twofish забезпечує оптимальний баланс між безпекою та ефективністю, представляючи собою відповідне рішення для проблем кібербезпеки в реальних додатках.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. The Twofish Encryption Algorithm: A 128-Bit Block Cipher / Bruce Schneier та ін. Wiley, 1999. 208 с.
2. Practical Cryptography Niels Ferguson Bruce Schneier. *fullpdfword.com*. URL: https://fullpdfword.com/reviews/u3202G/244467/4968440-practical-cryptography-niels-ferguson-bruce-schneier (дата звернення: 05.04.2026).
3. Report on the development of the Advanced Encryption Standard (AES) / J. Nechvatal та ін. *Journal of Research of the National Institute of Standards and Technology*. 2001. Т. 106, № 3. С. 511. URL: https://doi.org/10.6028/jres.106.023 (дата звернення: 09.04.2026).
4. Система передачі інформації із застосуванням інтерактивного блокового криптографічного алгоритму TWOFISH / С. В. Клименко та ін. *Actual Problems of Automation and Information Technology*. URL: https://actualproblems.dp.ua/index.php/APAIT/article/view/198 (дата звернення: 09.04.2026).
5. Мельничук Є. Д. Методи оцінки криптографічної придатності вузлів нелінійних замін блокових симетричних шифрів : автореф. дис. … канд. техн. наук. Харків, 2013. 24 с. (дата звернення: 09.04.2026).

Бондаренко Ірина Олексіївна – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Тарасюк Микита Олегович – студент групи 2КІТС-23б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: nikitatarasiuk1@gmail.com

Bondarenko Iryna O. – assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua

Tarasiuk Mykyta O. - student of group 2KITS-23b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: nikitatarasiuk1@gmail.com