НЕЛІНІЙНІ ПЕРЕТВОРЕННЯ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

Лисицький К.Є., Лисицька І.В.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна
Харківський національний університет радіоелектроніки, Харків, Україна

Нелінійність є життєво важливою для криптографічної стійкості блокових симетричних шифрів (БСШ), оскільки вона ускладнює лінійні та алгебраїчні атаки. Основою нелінійних перетворень є S-блоки (Substitution-boxes), що забезпечують властивість заплутування (confusion) за Шенноном [1]. Еволюція S-блоків пройшла шлях від класичного шифру DES та стандарту AES до сучасних динамічних і хаотичних конструкцій.

Метою доповіді є аналітичний огляд методів побудови S-блоків БСШ, оцінка компромісів між криптографічною стійкістю, апаратною складністю та продуктивністю, а також аналіз їхньої поведінки в умовах постквантової ери.

В доповіді наводяться криптографічні вимоги до S-блоків. Для забезпечення протидії криптоаналізу S-блоки повинні відповідати низці суворих математичних критеріїв [2, 3]:

1) висока нелінійність (High Non-linearity) — для протидії лінійному криптоаналізу Мацуї;

2) низька диференціальна однорідність (Low Differential Uniformity) – протидія диференціальному криптоаналізу Біхама-Шаміра;

3) бієктивність та збалансованість – забезпечення оборотності дешифрування та відсутності статистичного зсуву;

4) строгий лавинний ефект (Avalanche Effect) та високий алгебраїчний ступінь – захист від алгебраїчних атак.

Детерміновані (фіксовані) S-блоки (AES, Camellia, DES). Мають постійну таблицю підстановки, побудовану на основі складних алгебраїчних конструкцій.

Переваги: висока швидкість, оптимальні гарантовані криптопоказники та легкість стандартизації. Недоліки: потенційна вразливість до атак по сторонніх каналах (cache-timing attacks) та алгебраїчного аналізу у разі наявності прихованих математичних структур [2].

Динамічні (ключозалежні) S-блоки (Blowfish, Twofish). Генеруються під час ініціалізації алгоритму на основі секретного ключа. Переваги: високий захист від криптоаналізу «білої скриньки» та усунення ризику вбудованих «бекдорів». Недоліки: високі обчислювальні витрати на ініціалізацію та складність доведення відсутності «слабких» ключів [3].

Хаотично згенеровані S-блоки. Використовують детермінований хаос (Логістичне відображення, системи Чуа та Хенона). Забезпечують високу нелінійність, ергодичність та гнучкість, проте залишаються складними для гарантування параметрів та стандартизації [3].

Випадкові S-блоки. Формуються з виходу генератора випадкових підстановок із проходженням перевірки за критеріями відбору. Доведено, що

для випадкової булевої функції більшість параметрів близькі до оптимальних, що усуває можливість вбудовування бекдорів [3].

Окремим аспектом оцінювання нелінійних перетворень є стійкість їхньої реалізації до атак через побічні канали [4]. Використання табличних S-блоків може створювати залежність часу виконання операцій від значень оброблюваних даних, що потенційно дозволяє здійснювати cache-timing-атаки. Для зменшення такого ризику застосовують реалізації з постійним часом виконання (constant-time), обчислення S-блоків без табличного доступу, а також апаратні інструкції, що забезпечують захищене виконання криптографічних операцій.

Також обговорюється постквантовий аспект. В умовах квантових обчислень основна загроза для БСШ полягає у застосуванні алгоритму Гровера, який забезпечує квадратичне прискорення пошуку ключа (зменшуючи складність з $O(2^n)$ до $O(2^{(n/2)})$ [1, 3]. Вимоги до самих S-блоків у постквантову епоху залишаються аналогічними класичним, а захист досягається подвоєнням довжини ключа (наприклад, AES-256). У практичних постквантових БСШ перевага надається ретельно дослідженим фіксованим S-блокам через їхню передбачуваність та відсутність додаткових витрат на генерацію.

Постквантова стійкість блокових симетричних шифрів визначається не лише довжиною ключа, а й властивостями всієї криптографічної конструкції. Алгоритм Гровера створює загрозу для симетричних алгоритмів через квадратичне прискорення перебору ключів, тоді як класичні критерії оцінювання S-блоків залишаються важливими для протидії диференціальному, лінійному та алгебраїчному криптоаналізу. Таким чином, використання AES-256 є одним із практичних підходів до підвищення стійкості симетричного шифрування в постквантовій перспективі.

Наведені дані аналізу показують, що вибір структури S-блоку є компромісом між безпекою, швидкістю та апаратною складністю. Попри активне дослідження динамічних та хаотичних S-блоків, у практичних та постквантових стандартах домінують алгебраїчно обґрунтовані фіксовані S-блоки у поєднанні з 256-бітними ключами.

Список літератури

1. Shannon C. E. A communication theory of secrecy systems. Bell Syst. Tech. J., 1949. Vol. 28, № 4. P. 656–715.

2. Daemen J., Rijmen V. The Design of Rijndael - The Advanced Encryption Standard. Springer-Verlag, 2002.

3. Лисицька І. В., Лисицький К. Є., Гальцева І. М., Колованова Є. П. Особливості побудови нелінійних перетворень блокових симетричних шифрів // Радіотехніка. 2025. № 222. С. 62–68.

4. Singha T. B., Palathinkal R. P., Ahamed S. R. Securing AES Designs Against Power Analysis Attacks: A Survey. IEEE Internet of Things Journal. 2023. Vol. 10, No. 16. P. 14332–14356. DOI: https://doi.org/10.1109/JIOT.2023.3265683