ЕВОЛЮЦІЯ АРХІТЕКТУР БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

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

Фундаментом сучасної симетричної криптографії є принципи заплутування (confusion) та дифузії (diffusion), сформульовані К. Шенноном у 1949 р. [1]. Заплутування приховує зв'язок між ключем і шифротекстом за допомогою нелінійних перетворень (S-блоки), а дифузія розповсюджує вплив окремих біт відкритого тексту на шифротекст через лінійні операції (P-блоки). Розробка продуктивних шифрів (product ciphers) у рамках проєкту IBM Lucifer (1971–1973) заклала основу для двох ключових архітектур: мережі Фейстеля та SPN-мережі.

Метою доповіді є проведення комплексного аналітичного огляду еволюції архітектурних рішень блокових симетричних шифрів (мереж Фейстеля, SPN, схем Лея-Мессі, ARX-конструкцій), висвітлення компромісів між криптографічною стійкістю, швидкодією та апаратною складністю в обмежених у ресурсах середовищах, а також оцінка безпеки симетричних шифрів у постквантову епоху.

Мережа Фейстеля (FN). Вхідний блок ділиться на дві гілки. Раундова функція F обчислюється для однієї гілки та додається за модулем 2 (XOR) до іншої. Головна перевага FN – оборотність структури незалежно від оборотності функції F. Дослідження Люби-Ракоффа (1988) та Наора-Рейнголда (1997) довели, що 3-4 раундів із псевдовипадковими функціями достатньо для забезпечення сильної псевдовипадкової перестановки.

Мережа підстановки-перестановки (SPN) [2]. Обробляє блок як єдине ціле, послідовно застосовуючи паралельні S-блоки та шар дифузії P. На набула широкого поширення з прийняттям стандарту AES (Rijndael) у 2000 р. та рекомендацій NESSIE (Camellia, SHACAL-2). Вимагає оборотності всіх елементів раунду.

Схема Лея-Мессі (LM) [3]. Використовує операцію на основі різниці двох половин блоку (шифр IDEA, FOX). Забезпечує швидшу дифузію порівняно з FN та не вимагає бієктивності раундової функції.

Також розглядаються спеціалізовані та легковагові конструкції.

GFN та Рекурсивна FN. Узагальнені мережі Фейстеля (CAST-256, RC6) ділять блок на >2 частин. Рекурсивні структури (MISTY1, KASUMI в 3G/GSM) використовують вкладені мережі Фейстеля у раундовій функції, що спрощує математичні докази стійкості.

ARX-конструкції (Add-Rotate-XOR). Застосовують модульне додавання для забезпечення нелінійності замість класичних S-блоків (ChaCha20, Speck). Оптимізовані для 32/64-бітних процесорів, усувають вразливості до атак по сторонніх каналах (timing attacks).

Легковагова криптографія (Lightweight Cryptography). Для пристроїв IoT, RFID та WSN пріоритетом є мінімізація кількості логічних вентилів (Gate Count). Шифри на кшталт PRESENT використовують мінімалістичні S-блоки

(4x4 біти) та прості перестановки, компенсуючи слабкість раунду збільшенням кількості циклів (31 раунд) [4].

Одним із визначальних чинників криптографічної стійкості архітектур блокових симетричних шифрів є здатність протидіяти диференціальному та лінійному криптоаналізу. Для SPN-конструкцій важливу роль відіграють диференціальні характеристики S-блоків і дифузійного шару, зокрема його гілкова кількість (Branch Number). Для мереж Фейстеля стійкість залежить від властивостей раундової функції, кількості раундів та способу формування підключів. В ARX-конструкціях особливе значення має взаємодія модульного додавання, циклічних зсувів і операції XOR, що ускладнює побудову ефективних диференціальних та лінійних апроксимацій.

Важливим напрямом еволюції архітектур блокових симетричних шифрів є врахування стійкості до атак через побічні канали (Side-Channel Attacks) [5]. Табличні реалізації S-блоків можуть створювати залежність часу виконання операцій і характеру звернень до пам'яті від оброблюваних даних. Це створює передумови для cache-timing-атак. ARX-конструкції, які не використовують табличних підстановок, дозволяють зменшити ризики таких атак за умови реалізації операцій із постійним часом виконання. Для SPN-архітектур застосовують апаратні криптографічні інструкції, маскування проміжних значень (masking) та інші методи протидії побічним каналам.В доповіді приділено увагу постквантовій стійкості існуючих шифрів.

Квантовий алгоритм Гровера прискорює перебір ключа з $O(2^L)$ до $O(2^{(L/2)})$. На відміну від алгоритму Шора, який повністю компрометує асиметричні системи, квантова загроза для БСШ компенсується подвоєнням довжини ключа [6]. Таким чином, AES-256 та інші 256-бітні шифри забезпечують достатній рівень 128-бітної постквантової безпеки.

Наведені дані показують, що сучасні БСШ залишаються фундаментальним інструментом захисту інформації, еволюціонуючи у напрямку високої продуктивності в обмежених середовищах та збереження квантової стійкості.

Список літератури

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

2. NIST FIPS PUB 197: Advanced Encryption Standard (AES). USDOC, 2001.

3. Lai, X., & Massey, J. L. A Proposal for a New Block Encryption Standard. Advances in Cryptology—EUROCRYPT ’90. Springer, Berlin, Heidelberg, 1991. P. 389–404.

4. Andres C. et al. PRESENT: An Ultra-Lightweight Block Cipher. CHES 2007. Springer, 2007. P. 450–464.

5. Mouha N., Dworkin M. Report on the Block Cipher Modes of Operation in the NIST SP 800-38 Series. Gaithersburg : National Institute of Standards and Technology, 2024. (NIST Interagency/Internal Report (NISTIR) 8459). DOI: https://doi.org/10.6028/NIST.IR.8459

6. Bernstein D. J., Lange T. Post-quantum cryptography. Nature, 2017. Vol. 549. P. 188–194.