УДК 004.056:004.89:623.746.4-519

Лисицька І. В.

д.т.н., професор кафедри кібербезпеки інформаційних систем, мереж і технологій, Навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна; професор кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки

Лисицький К. Є.

PhD, доцент кафедри математичного моделювання і аналізу даних Навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна

ЕВОЛЮЦІЯ АРХІТЕКТУР БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

Анотація. У роботі проведено аналіз еволюції архітектурних рішень у галузі побудови блокових симетричних шифрів (БСШ) від витоків криптографічної теорії до сучасних постквантових вимог. Проаналізовано принципи заплутування та дифузії,

запропоновані К. Шенноном, розкрито особливості функціонування Мережі Фейстеля, SPN-мереж та конструкції Лея-Мессі. Окремо розглянуто актуальні підходи легковагової криптографії (ARX-структури, мінімалізм S-блоків) та оцінено стійкість симетричних шифрів проти квантових атак на основі алгоритму Гровера.

Ключові слова: блокові симетричні шифри, мережа Фейстеля, SPN, Лей-Мессі, ARX, легковагова криптографія, алгоритм Гровера, постквантова криптографія.

Стрімкий розвиток сучасних інформаційно-комунікаційних систем, бездротових сенсорних мереж та пристроїв Інтернету речей (IoT) сформував нові вимоги до засобів криптографічного захисту інформації [1]. Історія сучасних симетричних блокових шифрів (БСШ) є процесом постійного пошуку оптимального поєднання двох фундаментальних принципів, сформульованих Клодом Шенноном: заплутування (confusion) та дифузії (diffusion) [1]. Для досягнення нелінійності використовуються S-блоки підстановки, а для розсіювання бітів – лінійні P-блоки або матричні перетворення. По послідовній концепції «product ciphers» Шеннона було створено дві базові класичні структури – Мережу Фейстеля та Мережу Підстановки-Перестановки (SPN), вперше детально опрацьовані в рамках проєкту IBM «Lucifer» (1971–1973) [2].

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. У ході дослідження проаналізовано класичні та альтернативні типові структури БСШ.

Мережа Фейстеля (DES, Blowfish, CAST-128, RC5, RC6). Дослідження М. Люби, Ч. Ракоффа, М. Наора та О. Рейнгольда довели теоретичну стійкість цієї конструкції (3–4 раунди гарантують сильну псевдовипадкову перестановку). Головною перевагою мережі Фейстеля є її структурна оборотність – відсутність вимоги щодо інвертованості

раундової функції.

На противагу їй, SPN-мережа (AES, Camellia) обробляє весь блок паралельно, забезпечуючи значно швидшу дифузію за рахунок суворого дотримання бієктивності всіх внутрішніх шарів [3]. Альтернативна схема Лея-Мессі (IDEA, FOX) вдало поєднує переваги обох підходів: вона забезпечує високу швидкість дифузії та не вимагає інвертивності раундової функції.

Окрему увагу приділено еволюції шифрів під впливом нових обчислювальних платформ. Для подолання обмежень класичних моделей розроблено узагальнені Мережі Фейстеля (CAST-256, RC6) [4], Рекурсивні Мережі Фейстеля (MISTY1, KASUMI) та ARX-конструкції (ChaCha20, Speck), де заплутування досягається нелінійністю модульного додавання [5]. ARX-структури усувають затримки через кеш-промахи та захищають від атак по сторонніх каналах (timing attacks).

В умовах жорстких апаратних обмежень IoT (RFID-мітки, датчики) сформувався напрям мінімалізму раундової функції (шифр PRESENT): використання малих S-блоків 4×4 та простих перестановок мінімізує кількість логічних вентилів (Gate Count), що компенсується більшою кількістю раундів.

Проаналізовано стійкість БСШ проти квантових загроз. На відміну від асиметричних систем, що ламаються алгоритмом Шора, симетричні шифри піддаються впливу квантового алгоритму Гровера, який знижує складність перебору ключа довжиною L біт з $O(2^L)$ до $O(2^{L/2})$ [6]. Для збереження стандартного рівня безпеки у 128 біт достатньо подвоїти довжину секретного ключа до 256 біт (наприклад, AES-256), завдяки чому блокові симетричні шифри залишаються надійним фундаментом захисту даних у постквантову еру.

Список використаних джерел

1. Shannon C. E. A communication theory of secrecy systems. Bell System Technical Journal. 1949. Vol. 28, № 4. P. 656–715.

2. Feistel H. Cryptography and computer privacy. Scientific American. 1973. Vol. 228, № 5. P. 15–23.

3. FIPS PUB 197: Advanced Encryption Standard (AES) / NIST. U.S. Department of Commerce, 2001. 51 p.

4. Schneier B., Whiting D. A performance comparison of the AES submissions. AES Conference Proceedings. NIST, 1999.

5. Beaulieu S., Shors J. The SIMON and SPECK families of lightweight block ciphers. IACR Cryptology ePrint Archive. 2013.

6. Grover L. K. A fast quantum mechanical algorithm for database search. Proc. of the 28th ACM STOC. 1996. P. 212–219.