КРИПТОАНАЛІЗ БЛОЧНИХ СИМЕТРИЧНИХ МАЛОРЕСУРСНИХ ШИФРІВ

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

Стрімкий розвиток концепцій «розумного дому», інтернету речей (IoT), медичних імплантів та RFID-міток сформував критичну потребу в специфічних засобах захисту інформації [1]. Традиційні криптографічні стандарти (AES, RSA) розроблялися з розрахунком на потужні обчислювальні ресурси персональних комп'ютерів та серверів. Проте спроби їх інтеграції у мініатюрні пристрої виявилися неефективними через жорсткі обмеження оперативності (RAM), постійної пам'яті (ROM), енергоспоживання та площі кристала мікросхеми, яка вимірюється в еквівалентах логічних вентилів (GE). Цей технологічний виклик зумовив формування напряму малоресурсної криптографії (Lightweight Cryptography, LWC). Проєктування LWC-шифрів вимагає безперервного компромісу між криптографічною стійкістю, апаратною вартістю та продуктивністю алгоритму – концепція «криптографічного трикутника». Для оцінки реального запасу міцності LWC-систем дослідники застосовують як класичні статистичні підходи, так і новітні автоматизовані інструменти (SAT/SMT, MILP) та алгоритми машинного навчання.

Метою доповіді є комплексний аналіз архітектурних особливостей провідних малоресурсних блочних шифрів (PRESENT, CLEFIA, SIMON, SPECK) та систематизація сучасних підходів до оцінки їхньої криптографічної стійкості. Представлені в доповіді алгоритми демонструють різні підходи до вирішення задачі «криптографічного трикутника»:

PRESENT [1]. Ультралегкий шифр на основі SP-мережі (розмір блока – 64 біти, ключ – 80/128 біт, 31 раунд). Характеризується еталонною компактністю (~1570 GE) завдяки використанню 16 4-бітних S-боксів та фіксованій схемі бітових перестановок (P-layer). Недоліками є відносно низька швидкість у програмній реалізації та малий розмір блоку.

CLEFIA [2]. Розроблений компанією Sony (розмір блока – 128 біт, ключ – 128/192/256 біт, 18,22 або 26 раундів). Базується на 4-гілковій узагальненій мережі Фейстеля з двома паралельними функціями (F0 та F1), що використовують різні S-бокси та матриці дифузії. Це забезпечує рівень безпеки AES за суттєво менших апаратних витрат.

SIMON [3]. Сімейство шифрів від АНБ США, оптимізоване під апаратну реалізацію. В основі – мережа Фейстеля із побітовими операціями XOR, AND та циклічного зсуву. Використання єдиного вентиля AND як єдиного нелінійного елемента дозволяє мінімізувати площу чипа до абсолютного мінімуму.

SPECK [3]. ARX-шифр від АНБ США, оптимізований для програмного забезпечення. Захист базується на трьох операціях: модульному додаванні (+ за модулем 2^n), циклічному зсуві та XOR. Відсутність S-боксів забезпечує високу швидкість на 8 та 32-бітних мікроконтролерах.

Проведене дослідження дозволяє виділити такі ключові вектори аналізу стійкості LWC-шифрів:

Лінійний та диференціальний криптоаналіз. У шифрі PRESENT шар перестановок (P-layer) породжує потужні «лінійні оболонки» (linear hulls), роблячи його більш вразливим до лінійного аналізу (до 26 раундів), ніж до диференціального (до 16 раундів). Для CLEFIA найбільш ефективними виявилися атаки неможливих диференціалів (до 10 раундів) та лінійного аналізу з нульовою кореляцією (до 14–15 раундів).

Атаки на пов'язаних ключах (Related-Key Attacks). Прагнення розробників спростити процедуру розгортання ключів для економії вентилів створює суттєві вразливості. Лінійність та низька дифузія в Key Schedule (зокрема в PRESENT та SIMON) дозволяють будувати пов'язано-ключові диференціали, що покривають значно більше раундів, ніж у класичній single-key моделі.

Автоматизований та комбінований криптоаналіз. Застосування SAT/SMT- солверів [4] та моделей змішаного цілочисельного лінійного програмування (MILP) [5] з властивістю подільності (Division Property) дозволило точно визначати оптимальні диференціальні й лінійні траєкторії для SIMON та SPECK за мінімальний час.

Нейромережевий криптоаналіз та побічні канали. Інтеграція глибокого навчання (Deep Learning) для побудови нейронних розрізнювачів (Neural Distinguishers) дає змогу виявляти слабкі статистичні закономірності на більшій кількості раундів. Ансамблеві моделі машинного навчання у профілюючих атаках по побічних каналах (DL-SCA) здатні повністю компрометувати ключі SPECK менш ніж за 250 фізичних трас.

Головним підсумком дослідження є те, що попри значний прогрес у зламі урізаних (round-reduced) модифікацій, повні раундові варіанти шифрів PRESENT, CLEFIA [6], SIMON та SPECK залишаються практично стійкими та надійними для впровадження.

Список літератури

1. Bogdanov, A., Knudsen, at al. (2007). PRESENT: An Ultra-Lightweight Block Cipher. In: Cryptographic Hardware and Embedded Systems – CHES 2007. Lecture Notes in Computer Science, vol 4727. Springer, Heidelberg. DOI: 10.1007/978-3-540-74735-2_31

2. Katagi M., Moriai S. The CLEFIA Block Cipher Algorithm. Internet Engineering Task Force (IETF). 2011. RFC 6114. URL: https://datatracker.ietf.org/doc/html/rfc6114

3. Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L. The SIMON and SPECK families of lightweight block ciphers. IACR Cryptology ePrint Archive. 2013. Report 2013/404. URL: https://eprint.iacr.org/2013/404

4. Sun L., Liu M., Guo J., Qu L., Wang M. New integral distinguishers on SIMON and SPECK from division property. Asiacrypt 2015: Advances in Cryptology. 2015. P. 218–243. DOI: https://doi.org/10.1007/978-3-662-48800-3_9

5. Liu, F., Hu, K., & Wang, M. (2024). Differential Cryptanalysis with SAT, SMT, MILP, and CP: A Detailed Comparison for Bit-Oriented Primitives. Journal of Cryptographic Engineering, 14(3), 201–219. https://doi.org/10.1007/s13384-024-00681-z

6. ISO/IEC 29192-2:2019/Amd 1:2021. Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers. Geneva: ISO, 2021.