ДОСЛІДЖЕННЯ ВІДОМИХ ЛЕГКОВАГОВИХ АЛГОРИТМІВ БЛОЧНОГО СИМЕТРИЧНОГО ШИФРУВАННЯ

Товма О.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток Інтернету речей, промислового Інтернету речей та вбудованих інформаційно-комунікаційних систем зумовлює потребу в криптографічному захисті даних за умов обмежених обчислювальних, апаратних та енергетичних ресурсів. Вибір легковагових алгоритмів блочного шифрування потребує комплексного оцінювання їхньої криптографічної стійкості, продуктивності та ресурсомісткості програмної й апаратної реалізації [1].

Метою доповіді є аналіз відомих легковагових алгоритмів блочного симетричного шифрування, узагальнення критеріїв їх порівняльного оцінювання та визначення обґрунтованого напряму подальших досліджень із використанням алгебраїчних властивостей розширених полів Галуа.

У легковагових блочних шифрах застосовують різні принципи організації раундових перетворень. Мережі підстановок і перестановок (SPN) поєднують нелінійні підстановки та операції перемішування бітів, мережі Фейстеля реалізують послідовне перетворення частин блока, конструкції ARX використовують додавання за модулем степеня двійки, циклічні зсуви та XOR.

Алгоритм PRESENT побудовано за принципом SPN з 64-бітовим блоком і варіантами ключа довжиною 80 або 128 біт. Його раундові перетворення поєднують компактні 4-бітові S-блоки з бітовою перестановкою, що сприяє апаратній компактності [2]. GIFT також належить до SPN-конструкцій, сімейство охоплює GIFT-64 та GIFT-128 і орієнтоване на ефективне поєднання нелінійних підстановок із перестановками бітів [3].

Сімейство SKINNY використовує концепцію tweakey, яка передбачає спільне оброблення ключового матеріалу та додаткового параметра налаштування (tweak) у процесі раундових перетворень. Для SKINNY розробники окремо розглядали властивості стійкості до диференціальних і лінійних атак, зокрема для моделей пов’язаних ключів або налаштувань [4]. SIMON реалізує модифіковану мережу Фейстеля з простими побітовими операціями, тоді як SPECK поєднує структуру Фейстеля з ARX-перетвореннями. Різні принципи їх побудови пов’язані з різними профілями ефективності апаратного та програмного виконання [5].

Для коректного порівняння доцільно використовувати сукупність взаємопов’язаних критеріїв: стійкість до відомих класів криптоаналізу за конкретних параметрів шифру; час шифрування й розшифрування та пропускну здатність; обсяг оперативної пам’яті і програмного коду; апаратну площу та затримку; енергію, витрачену на оброблення визначеного обсягу даних. Для зіставлення програмних реалізацій необхідно фіксувати мікроконтролер, тактову частоту, компілятор, параметри оптимізації та спосіб вимірювання. Для апаратних реалізацій слід зазначати технологічну бібліотеку, архітектуру ядра, частоту і правила оцінювання площі.

Окремою методологічною вимогою є врахування безпекових обмежень, зумовлених розміром блока та ключа, а також розмежування властивостей самого блочного шифру і протоколу його застосування. Наприклад, для шифрів із 64-бітовим блоком необхідно враховувати обмеження на обсяг даних, що обробляються одним ключем у відповідному режимі роботи.

Одним із можливих напрямів є використання арифметики розширених полів Галуа $GF(2^m)$ для побудови нелінійних підстановок і лінійних перетворень дифузії. Ефективність використання операцій у розширених полях Галуа залежить від способу представлення елементів поля, вибору незвідного полінома, структури криптографічних перетворень та особливостей цільової платформи.

Для оцінювання запропонованого напряму доцільно дослідити нелінійність і диференціальну рівномірність підстановок, лінійні та диференціальні характеристики багатораундової конструкції, властивості дифузії, алгоритм формування раундових ключів і вартість основних операцій. Лише після визначення конкретної конструкції та проведення криптоаналітичних і реалізаційних досліджень можна робити висновок про її переваги порівняно з відомими легковаговими шифрами.

Отже, проведений огляд показує, що PRESENT, GIFT, SKINNY, SIMON і SPECK відображають різні підходи до побудови легковагових блокових шифрів, а їх вибір має визначатися узгодженим аналізом криптографічних властивостей та ресурсних обмежень цільової системи. Науково обґрунтованим продовженням дослідження є проєктування й аналіз раундових перетворень із використанням розширених полів Галуа та їх порівняння з відомими алгоритмами за єдиною методикою. Подальша робота передбачає теоретичне оцінювання властивостей запропонованої конструкції та експериментальне дослідження її швидкодії, обсягу пам’яті й енергетичних витрат на ресурсно-обмежених пристроях.

Список літератури

1. Lightweight block ciphers for resource-constrained environments: A comprehensive survey. Future Generation Computer Systems. 2024. DOI: https://doi.org/10.1016/j.future.2024.03.054.

2. Bogdanov A., Knudsen L. R., Leander G., et al. PRESENT: An Ultra-Lightweight Block Cipher. Cryptographic Hardware and Embedded Systems – CHES 2007. LNCS. 2007. Vol. 4727. P. 450–466. DOI: https://doi.org/10.1007/978-3-540-74735-2_31.

3. Banik S., Pandey S. K., Peyrin T., Sasaki Y., Sim S. M., Todo Y. GIFT: A Small Present – Towards Reaching the Limit of Lightweight Encryption. CHES 2017. LNCS. 2017. Vol. 10529. P. 321–345. DOI: https://doi.org/10.1007/978-3-319-66787-4_16.

4. Beierle C., Jean J., Kölbl S., et al. The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. Advances in Cryptology – CRYPTO 2016. LNCS. 2016. Vol. 9815. P. 123–153. DOI: https://doi.org/10.1007/978-3-662-53008-5_5.

5. Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L. The SIMON and SPECK Lightweight Block Ciphers. Proceedings of the 52nd Annual Design Automation Conference. 2015. Article 175. P. 1–6. DOI: https://doi.org/10.1145/2744769.2747946.