МЕТОДИ АНАЛІЗУ СТІЙКОСТІ АЛГОРИТМУ ASCON ДО АЛГЕБРАЇЧНИХ АТАКА

Руженцев В.І., Куценко Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток сучасних стандартів легковагової криптографії зумовлює необхідність глибокого дослідження їхньої стійкості до алгебраїчних атак, які базуються на поданні криптографічних перетворень у вигляді систем булевих рівнянь над полем GF(2). Одним із таких алгоритмів є Ascon [1], що у 2023 році був обраний Національним інститутом стандартів і технологій США (NIST), як базовий стандарт легковагової криптографії для захисту даних у пристроях з обмеженими обчислювальними ресурсами.

Ascon ґрунтується на губчастій конструкції (sponge construction), використовує 5-бітні S-блоки, подібні до SHA-3, та лінійний шар, споріднений з SHA-2. Така структура забезпечує високу продуктивність і компактність, проте потенційно може бути вразливою до алгебраїчних і кубічних атак [2], що експлуатують низький алгебраїчний ступінь окремих компонентів алгоритму.

Доповідь присвячена методам аналізу криптостійкості алгоритму Ascon до алгебраїчних атак, а також до куб-атаки. Представлені в [3] результати демонструють, відомі оцінки криптостійкості можуть бути завищені і реальна криптостійкість алгоритму може бути нижче. Саме тому необхідно провести власний експеримент з імітації куб атаки на алгоритм Ascon та порівняти отримані характеристики з існуючими.

Метою доповіді є аналіз та оцінка стійкості багатораундового криптографічного алгоритму Ascon до алгебраїчних атак, зокрема до кубічної атаки, шляхом моделювання внутрішніх перетворень у вигляді систем булевих багаточленів, дослідження алгебраїчних властивостей S-блоків і лінійного шару, а також оцінювання алгебраїчного ступеня перетворень на різних етапах роботи алгоритму. Для досягнення поставленої мети передбачено: побудову математичної моделі криптоалгоритму Ascon, аналіз зміни алгебраїчного ступеня при різній кількості раундів, практичну реалізацію скороченого варіанту Ascon для перевірки ефективності куб-атаки та формування рекомендацій щодо підвищення його криптостійкості.

Список літератури

1. Lightweight cryptography project of the American National Institute of Standards and Technology, 2015. URL: https://csrc.nist.gov/projects/lightweight-cryptography.

2. Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, Fast Software Encryption, pp. 196–211, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg. / Режим доступу: https://doi.org/10.1007/3-540-60590-8_16

3. V. Ruzhentsev. Nonlinear degree of Ascon permutation. INTERNATIONAL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, Poland, Warsaw, 2025, VOL. 71, № 2, PP. 477-482, doi: 10.24425/ijet.2025.153594.