МЕТОДИ ОЦІНКИ СТІЙКОСТІ ЛЕГКОВАГИХ СИМЕТРИЧНИХ ШИФРІВ ДО ДИФЕРЕНЦІЙНО-ЛІНІЙНИХ АТАК

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

Легковагова криптографія є головним інструментом, що забезпечує безпеку пристроїв з обмеженими обчислювальними ресурсами. Але, не дивлячись на її ефективність, такі шифри можуть бути вразливими до диференційно-лінійного криптоаналізу (DL-криптоаналізу), що поєднує методи лінійного та диференційного аналізу [1].

Метою доповіді є аналіз методів оцінки стійкості легковагових симетричних шифрів до диференційно-лінійного криптоаналізу та виявлення основних факторів, що впливають на їхню безпеку.

DL-криптоаналіз використовує статистичні закономірності між зашифрованими та відкритими текстами щоб зменшити простір ключів.

Аналіз стійкості легковагових шифрів, таких як Ascon, PRESENT та LED, показує, що їхня безпека залежить від структури S-Box та кількості раундів [2].

Для підвищення стійкості пропонується збільшення кількості раундів, модифікація нелінійних компонентів та використання адаптивних алгоритмів зміни ключів [3].

Рекомендовані заходи підвищення стійкості:

– використовувати S-Box з високою нелінійністю та низькою диференційною/лінійною ймовірністю;
– збільшення кількості раундів (без значної втрати продуктивності);
– проєктування раундових функцій із мінімізацією лінійних кореляцій.

Методи оцінки стійкості до диференційно-лінійних атак є важливою складовою криптографічної експертизи легковагих шифрів. Їх застосування дозволяє:

– виявити потенційні слабкі місця в дизайні;
– визначити необхідну кількість раундів для забезпечення безпеки;
– порівняти ефективність різних шифрів.

Таким чином, розробка та оцінка стійкості легковагових шифрів до DL-криптоаналізу є критично важливими для забезпечення безпеки IoT-систем та вбудованих пристроїв.

Список літератури

1. Бірюков А., Дункельман О., Келлер Н. Диференційно-лінійний криптоаналіз Serpent. Journal of Cryptographic Engineering, 2017.

2. Мендель Ф., Над Т., Шлеффер М. Диференційно-лінійний криптоаналіз спрощеного PRESENT. Fast Software Encryption, 2019.

3. Столлінгс В. Криптографія та безпека мереж: принципи та практика. Pearson, 2020.