УДК 003.26.09; 004.032.24-004.272.3
**А. Луцків, Н. Новак**
(Тернопільський національний технічний університет імені Івана Пулюя)

# ПРОГРАМНА СИСТЕМА КРИПТОАНАЛІЗУ МЕТОДОМ НЕМОЖЛИВИХ ДИФЕРЕНЦІАЛІВ

Криптоаналіз – це розділ криптології, який займається аналізом надійності шифрів, а саме за допомогою математичних та алгоритмічних методів виконується пошук невідомого ключа, або здійснюється розшифрування без нього. Його головною задачею є визначення стійкості алгоритму шифрування до зламу. До найбільш поширених методів криптоаналізу, або «атак» на симетричні, блокові шифри відносяться: бумеранг атака, метод грубої сили (brute force attack), диференціальний криптоаналіз, лінійний криптоаналіз, сандвіч атака, алгебраїчний тощо.

Суть диференціального криптоаналізу полягає у тому, щоб зміни на вході методу шифрування могли впливати на отриманий зашифрований текст. Метод неможливих диференціалів [1] є формою диференціального криптоаналізу блокових симетричних шифрів, який у свою чергу полягає дослідженні того, як зміни у відкритому, незашифрованому тексті можуть відобразитись на результати шифрування. Особливість методу неможливих диференціалів полягає у виборі диференціалів з нульовою ймовірністю. Тобто всі варіанти ключа, які приводять до неможливих диференціалів відкидаються, і за результатом цих операцій знаходиться єдиний варіант ключа, або підмножина ключової множини. Атака неможливих диференціалів успішно показала себе із шифрами: Twofish, Zodiac, MISTY1, Camellia, ARIA, спрощених варіантах AES та інших.

Для успішного проведення криптоаналізу потрібні значні обчислювальні ресурси: процесорний час та пам’ять. Саме з цієї причини існують потреби у збільшенні обчислювальних потужностей для зменшення часу знаходження ключа.

Для систем криптоаналізу використовуються наступні технології паралельних обчислень: OpenMP (для систем зі спільною пам’яттю), MPI (для систем з розподіленою пам'яттю), GPGPU-технології (CUDA, OpenAAC, OpenCL, AMD APP SDK). Враховуючи доступність обчислювальної бази, оптимальним є використання технологій OpenMP та MPI [2].

Авторами доповіді здійснюється дослідження можливості використання технологій MPI та OpenMP для здійснення криптоаналізу неможливих диференціалів.

**Література:**

1. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999).

2. Загородна Н. В., Лупенко С. А. Луцків А. М. Обгрунтування вибору доступних програмно-апаратних засобів високопродуктивних обчислювальних систем для задач криптоаналізу. // Електроніка та системи управління. 2011. №1(27). - К.: НАУ, 2011. - с.42-50.