УДК 003.26.09; 519.688

А. Луцків, Р. Мороз
(Тернопільський національний технічний університет імені Івана Пулюя)

ОПТИМІЗАЦІЯ МЕТОДІВ КРИПТО АНАЛІЗУ БЛОКОВИХ ШИФРІВ ШЛЯХОМ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ GPGPU

Розробка нових та вдосконалення існуючих блокових алгоритмів шифрування обумовлює необхідність їх детального криптоаналітичного дослідження. На сьогодні при здійсненні криптоаналітичної експертизи алгоритмів шифрування використовуються наступні методи: повного перебору, диференціальний або його похідні, лінійний, “зустріч по середині”, алгебраїчний [1] та деякі інші [2].

Проте варто зазначити, що значна частина цих методів носить теоретичний характер або може бути використана лише до спрощених досліджуваних шифрів (меншої кількості раундів або меншій довжині ключа) у зв'язку з великими часовою та просторовою складностями. Часова складність визначається високими вимогами до процесорних ресурсів, а просторова — до оперативної та/або дискової пам'яті.

Використання засобів паралельної та розподіленої обробки даних, які стають доступнішими, дає змогу практично реалізувати атаки, які до деякого часу вважались теоретичними. На сьогодні до таких засобів належать: 1) багатоядерні та багатопроцесорні системи об'єднані в обчислювальні кластери (технології програмування OpenMP та MPI); 2) грід-мережі; 3)спеціалізовані обчислювальні пристрої на базі DSP (Digital signal processor — цифрових сигнальних процесорів) та FGPA (Field-programmable gate array — програмованих користувачем вентильних матриць); 4) технологія GPGPU (General-Purpose computation on Graphics Processing Units). Підвидами даної технології є OpenCL, AMD APP SDK та nVidia CUDA. На думку авторів технологія GPGPU є оптимальною для задач криптоаналізу, оскільки має блоки цілочисельної арифметики, а також дає змогу організовувати велику кількість (кілька тисяч) одночасно виконуваних потоків. Вибір конкретного підвиду технології визначається можливостями обчислювальних засобів.

У доповіді буде показано результати порівняльного аналізу сучасних криптоаналітичних методів з точки зору їх ефективності, функціональних можливостей та можливостей оптимізації їх виконання в паралельних та розподілених комп'ютерних системах. Також буде наведено які саме елементи криптоаналітичних методів можуть бути оптимізовані та способи їх оптимізації.

Література

1. Nicolas T. Courtois, Sean O'Neil and Jean-Jacques Quisquater: Practical Algebraic Attacks on the Hitag2 Stream Cipher, In 12th Information Security Conference, ISC 2009, Pisa, Italy 7-9 September 2009, Springer LNCS 5735, pp. 167-176.

2. Alex Biryukov and Dmitry Khovratovich. Related-key Cryptanalysis of the Full AES-192 and AES-256, University of Luxembourg 29 May 2009 [Електронний ресурс]. - Режим доступу: URL: http://eprint.iacr.org/2009/317.pdf