УДК 003.26.09; 004.032.24-004.272.3
А.М. Луцків (канд.техн.наук; доц.), І.В. Вербицький
Тернопільський національний технічний університет імені Івана Пулюя, Україна

АНАЛІЗ ТЕХНОЛОГІЙ РОЗПАРАЛЕЛЕННЯ У ВИСОКОПРОДУКТИВНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ ДЛЯ ЗАДАЧ КРИПТОАНАЛІЗУ

A.M. Lutskiv (Ph.D.; Assoc. Prof.), I.V. Verbytskyi

ANALYSIS OF PARALLELIZATION TECHNOLOGIES IN HIGH-PERFORMANCE COMPUTER SYSTEMS FOR THE CRYPTANALYSIS

Криптоаналіз – це розділ криптології, у рамках якого здійснюється аналіз надійності шифрів. Надійність сучасних алгоритмів шифрування базується на проблемах надвеликих алгоритмічних складностей задач їх криптоаналізу (дешифрування без наявного ключа), тому створення ефективного математичного, алгоритмічного, програмного та апаратного забезпечення є актуальною задачею.

Створення спеціалізованого апаратного забезпечення для реалізації певних криптоаналітичних методів є доволі трудомісткою задачею. Враховуючи наявність універсальних обчислювальних засобів з різними конструктивними особливостями, які можуть бути ефективно використані в ході криптоаналізу, власну їх реалізацію можна вважати недоцільною. Водночас наявні спеціалізовані та універсальні компілятори, бібліотеки, фреймворки та інше програмне забезпечення, яке орієнтоване на відповідні апаратні засоби. Таким чином, доцільним є створення програмно-апаратних криптоаналітичних комплексів на базі доступних апаратних та програмних засобів [1].

Ключовою задачею криптоаналітика є ефективне використання математичного та алгоритмічного забезпечення, яке лежить в основі сучасних криптоаналітичних методів, що може бути забезпечене шляхом:

1. Зменшення обчислювальної складності криптоаналітичної задачі шляхом її декомпозиції до меншої кількості підзадач різної складності. При виборі методу декомпозиції, варто керуватись обчислювальною складністю даного методу та його адаптивністю до заданого типу вхідних даних (зашифрованої послідовності): потоку вхідних даних чи певних сукупностей збережених блоків даних.

2. Зменшення обчислювальної складності алгоритмів криптоаналітичних підзадач шляхом використання методів векторизації та розпаралелення. У даному контексті векторизація — це одна з форм розпаралелення, яка полягає у перетворенні скалярної програми в векторну, а векторні обчислення варто розглядати як один із видів паралельних обчислень на рівні даних (SIMD).

3. Вибору таких апаратних та програмних засобів, які б давали змогу максимально ефективно реалізувати відповідні алгоритми (п.1 і п.2) та були б універсальними й доступними.

4. Ефективної реалізації алгоритмів (п.1 і п.2) з урахуванням можливостей програмного забезпечення.

На сьогодні до доступних та універсальних високопродуктивних обчислювальних апаратних засобів можна віднести кластерні системи, які об'єднують SMP- та GPGPU-вузли. Універсальність та доступність апаратного забезпечення

визначається не лише ціновим фактором, але й фактором документованості та доступності засобів їх програмування (компіляторів, бібліотек, фреймворків тощо).

При виборі бібліотек та технологій програмування варто звертати увагу на зручність та звичність для розробника, а саме — на скільки простою є модифікація послідовної програми до паралельного (векторизованого) виду. Тому, на думку авторів, хоча на ринку наявна велика кількість бібліотек паралельного програмування і вони доволі часто використовуються у системному та прикладному програмуванні, проте процес перетворення послідовної програми у векторну і/або паралельну буде відносно трудомістким.

До доступних апаратних SMP-платформ належать сучасні багатоядерні та багатопроцесорні системи з наборами векторних інструкцій (SIMD) x86, x86_64 та ARM-архітектури, які можуть бути обладнані спеціалізованими графічними співпроцесорами. За наведеними критеріями оптимальними є технології програмування — OpenMP та OpenCL. Зокрема, технологія OpenMP версії 4.0 і 4.5.

Для GPGPU-платформ, які обладнані графічними процесорами (сучасні відеокарти або спеціалізовані GPU-обчислювачі такі як nVidia Tesla та AMD FirePro) доцільним є використання технологій OpenCL або OpenACC.

Високопродуктивні обчислювальні системи на базі FPGA та DSP хоча й не належать до типових та універсальних обчислювальних засобів, проте підтримка технологій програмування OpenCL[2] та OpenMP[3], яка реалізована відносно нещодавно, дає змогу використовувати дану платформу не лише фахівцям знайомим з мовами AHDL, VHDL, Verilog та засобами низькорівневого програмування, а й C/C++ розробникам (компілятор GCC та його розширення).

Таким чином у результаті крупнозернистої декомпозиції криптоаналітичної задачі великі фрагменти обчислювальної задачі надсилаються вузлам або групам вузлів кластера багатомашинних систем (технологія MPI), а їх дрібніші фрагменти розподіляються у рамках окремого обчислювального вузла й опрацьовуються центральними, графічними або спеціалізованими (DSP, FPGA) процесорами обчислювальних систем. На даному рівні найпростішою та найдоступнішою технологією програмування є OpenMP версії 4.5. Аналіз асемблерного коду криптоаналітичного програмного забезпечення вказує на прийнятний рівень розпаралелення за даними (векторизації) та розпаралелення на рівні інструкцій. Конкуруючою технологією є OpenACC, проте вона ще не є доволі зрілою. Авторами аналізувались результати роботи компілятора GCC версії 6.1.

Література

1. Загородна Н. В., Лупенко С. А. Луцків А. М. Обґрунтування вибору доступних програмно-апаратних засобів високопродуктивних обчислювальних систем для задач криптоаналізу. // Електроніка та системи управління. 2011. №1(27). - К.: НАУ, 2011. - с.42-50.
2. TI OpenCL v01.01.xx - TI OpenCL Runtime Documentation [Електронний документ] Режим доступу: URL: http://downloads.ti.com/mctools/esd/docs/opencl/index.html
3. Hahn T. Demystifying digital signal processing (DSP) programming: The ease in realizing implementations with TI DSPs / Todd Hahn, Jonathan Humphreys, Andy Fritsch, Debbie Greenstreet // Texas Instruments [Електронний документ] Режим доступу: URL: http://www.ti.com/lit/wp/spry281/spry281.pdf