УДК 003.26.09; 519.688
С.О. Крівцов, А.М. Луцків
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ОГЛЯД СУЧАСНИХ АПАРАТНО-ПРОГРАМНИХ GPGPU ЗАСОБІВ ДЛЯ РОЗРОБКИ КРИПТОАНАЛІТИЧНИХ СИСТЕМ

S.O. Krivtsov, A.M. Lutskiv

REVIEW OF MODERN GPGPU HARDWARE AND SOFTWARE TOOLS FOR DESIGNING CRYPTANALYTIC SYSTEMS

Криптографічний аналіз шифрів є одним з найбільш важливих напрямків досліджень при створенні нових та удосконаленні вже існуючих криптографічних алгоритмів. Завдання криптоаналізу полягає у визначенні можливості злому криптошифру та передбачає застосування різних стандартних і не стандартних атак, які є достатньо ресурсоємними та трудомісткими задачами. Оскільки, складність використовуваних алгоритмів шифрування, а відповідно й методів їх криптоаналізу неухильно зростає, то визначення криптостійкості алгоритму шифрування може бути здійснено шляхом використання високопродуктивних обчислювальних систем.

На сьогодні, одні із кращих результатів, при розв'язанні криптоаналітичних задач показують системи на базі програмованих логічних інтегральних схем (ПЛІС), проте у розробників програмного забезпечення на високорівневих мовах програмування виникає проблема використання таких апаратних засобів. Альтернативним вирішенням даної проблеми є використання технології виконання обчислень загального призначення на графічних процесорах — **G***eneral*-**P***urpose* **G***raphics* **P***rocessing* **U***nits (*GPGPU).

До 2013-го року, до технологій програмування GPGPU належали: OpenCL, CUDA, AMD APP, OpenACC. У зв'язку з виходом, у липні 2013 року нової версії OpenMP 4.0 [1], можливості якої включають у себе підтримку додаткових апаратних обчислювальних пристроїв, зокрема GPU, дану технологію також можна віднести до GPGPU-технологій.

У дослідженні аналізуються функціональні можливості технологій паралельного програмування орієнтованих на GPGPU.

Стандарт OpenCL [2] описує мову програмування, яка базується на мові C (стандарт C99) та прикладний інтерфейс програмування — набір функцій. Дана технологія є найбільш універсальною серед перелічених й передбачає використання гібридних обчислювальних систем на базі мікропроцесорів, графічних процесорів, цифрових сигнальних процесорів, а останнім часом і спеціалізованих обчислювальних засобів, зокрема програмованих користувачем вентильних матриць Field-Programmable Gate Array (FPGA) [3], що є однією з архітектурних різновидів ПЛІС. Також варто зазначити, що на даний момент ведуться розробки по автоматичній трансляції OpenCL-програм у програми для FPGA-пристроїв, зокрема одним із провідних виробників — Altera [4]. До недоліків даної технології можна віднести необхідність враховування особливостей різного апаратного забезпечення. Стандарт OpenCL розробляється і підтримується некомерційним консорціумом Khronos Group, в який входять багато великих компаній, включаючи Intel, Advanced Micro Devices (AMD), Nvidia, Altera, Samsung, Vivante та ARM Holdings.

Технологія CUDA — це програмний інтерфейс (API) компанії Nvidia для доступу до обчислювальних можливостей графічних процесорів і є по-суті уніфікованим програмно-апаратним вирішенням для паралельних обчислень на відеопроцесорах Nvidia (що є недоліком в порівнянні з іншими кросплатформними технологіями). Пер-

вагою даної технології є наявність великої кількості бібліотек з вже реалізованими різноманітними функціями, які значно спрощують процес розробки програмного забезпечення. Детальна інформація стосовно даної технології, з урахуванням особливостей різноманітного апаратного забезпечення, наведена на офіційному інтернет-ресурсі компанії Nvidia [5].

Стандарт OpenACC описує програмний інтерфейс для мов програмування C, C++ та Fortran [6]. Базується на наборі директив компілятора, які дають змогу задавати цикли та ділянки коду, які будуть виконані на GPU-пристроях. Дана технологія є значно простішою, в плані реалізації, але і менш продуктивною, в порівнянні з технологіями CUDA і OpenCL. Стандарт розроблено компаніями Portland Group (PGI), Cray і Nvidia за підтримки CAPS.

Технологія AMD APP — це набір апаратних і програмних засобів, які дають змогу ефективно використовувати обчислювальні потужності графічних, центральних та гібридних центральних процесорів фірми AMD, з використанням технологій програмування OpenCL (з 2011 року, спочатку використовувалась технологія Brook), Bolt, C++ AMP, Aparapi та низки інших. Повна документація по використанню технології OpenCL на програмно-апаратній платформі AMD наведена на оф-сайті [7].

Технологія OpenMP визначає програмні інтерфейси і способи застосування методів паралельного програмування на багатопроцесорних системах із спільною пам'яттю для мов C, C++ і Fortran. Ключовим нововведенням OpenMP 4.0 стала можливість залучення потужностей GPU. Тепер API OpenMP надає механізми, які дозволяють вказати, що деяка область коду і/або даних повинні бути оброблені з використанням іншого обчислювального пристрою. Дана технологія охопила досить великий спектр засобів високопродуктивного та паралельного програмування, але варто зазначити, що на даний момент є відсутніми чіткі рекомендації у стандарті щодо реалізації технології на GPU і це являється суттєвим недоліком. Розробку специфікації OpenMP веде некомерційна організація OpenMP Architecture Review Board (ARB).

Отже, серед розглянутих технологій, в аспекті вирішення задач криптоаналізу, за критерієм кросплатформовості можна виділити наступні технології: OpenCL та OpenMP 4.0. Серед них більш документованою та гнучкою в плані GPGPU програмування є технологія OpenCL.

Література

1. OpenMP4.0.0 [Електронний документ] Режим доступу: URL: http://www.openmp.org/mp-documents/OpenMP4.0.0.pdf – Заголовок з екрану.

2. Aaftab Munshi. The OpenCL Specification [Електронний ресурс] Режим доступу URL:http://developer.amd.com/wordpress/media/2012/10/opencl-1.2.pdf

3. OpenCL on FPGA [Електронний ресурс] Режим доступу: URL: http://www.fixstars.com/en/services/opencl-on-fpga/ – Назва з екрану.

4. Altera SDK for OpenCL. Optimization Guide. [Електронний документ] Режим доступу: URL: http://www.altera.com/literature/hb/opencl-sdk/aocl_optimization_guide.pdf

5. CUDA Documents [Електронний ресурс] Режим доступу: URL: http://docs.nvidia.com/cuda/index.html

6. OpenACC Home [Електронний ресурс] Режим доступу: URL: http://www.openacc-standard.org/ – Назва з екрану.

7. AMD Accelerated Parallel Processing OpenCL programming Guide August 2013 Rev.2.6. [Електронний документ] Режим доступу: URL: http://developer.amd.com/wordpress/media/2013/08/AMD_Accelerated_Parallel_Processing_OpenCL_Programming_Guide.pdf