МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ

ВЕРБИЦЬКИЙ ІГОР ВОЛОДИМИРОВИЧ

УДК 003.26.09; 004.032.24-004.272.3

ДОСЛІДЖЕННЯ ОБЧИСЛЮВАЛЬНИХ ПРОЦЕСІВ У ВИСОКОПРОДУКТИВНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ ПРИ РОЗВ'ЯЗАННІ ЗАДАЧ КРИПТОАНАЛІЗУ

8.05010201 «Комп'ютерні системи та мережі»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2017

Роботу виконано на кафедрі комп'ютерних систем та мереж Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат технічних наук, доцент кафедри комп'ютерних систем та мереж
Луцків Андрій Мирославович,
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: кандидат технічних наук, доцент кафедри програмної інженерії
Михалик Дмитро Михайлович,
Тернопільський національний технічний університет імені Івана Пулюя,

Захист відбудеться 20 лютого 2017 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії №35 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд.1-603

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Ключовим завданням, яке необхідно розв’язувати при розробці нових та впровадженні існуючих систем криптографічного захисту є їх верифікація. Оскільки, криптостійкість більшості сучасних шифрів базується на просторовій (вимоги до об'єму пам'яті) та часовій (вимоги до процесорного часу виконання) складностях, а відповідно, неможливості розв'язання задачі криптоаналізу за розумний час на доступних обчислювальних засобах. Тому актуальною є проблема адаптації існуючого криптоаналітичного алгоритмічного забезпечення для його використання на високопродуктивних обчислювальних системах: векторних, паралельних та гібридних, тобто здійснення певної декомпозиції даної задачі. У даному аспекті доцільним є аналіз та обґрунтований вибір програмно-апаратних засобів для розв'язання задач криптоаналізу. Особливе місце в даному аспекті посідають програмні компоненти комп'ютерних систем криптоаналізу, оскільки, створення спеціалізованих апаратних засобів буває доволі нетривіальною та матеріальнозатратною задачею.

Мета роботи: Метою магістерського дослідження є обґрунтування вибору ефективних методів та засобів, які лежать в основі роботи криптоаналітичних систем. Зокрема, у дослідженні буде здійснено аналіз алгоритмічного та математичного забезпечення, яке лежить в основі сучасних криптоаналітичних методів. Відповідні обчислювальні методи реалізуються у векторних, паралельних та розподілених обчислювальних системах. Передбачається, що відповідні системи повинні враховувати широкий спектр можливих методів криптоаналізу, а також архітектурні особливості сучасних обчислювальних систем, зокрема зі спільною та розподіленою пам’яттю, GPGPU, FPGA та інших.

Об’єкт дослідження: обчислювальні процеси у векторних, паралельних та розподілених обчислювальних системах.

Предмет дослідження: математичні моделі, алгоритми, патерни паралельного програмування, методи декомпозиції обчислювальних задач, криптоаналітичні методи сучасних шифросистем, векторні, паралельні та розподілені обчислювальні системи.

Методи дослідження: моделювання комп’ютерних систем та програм, теорія алгоритмів та обчислювальних методів, криптологія, теорія побудови обчислювальних систем.

Наукова новизна отриманих результатів:

1. Вперше, на основі аналізу особливостей алгоритмів криптоаналізу, проаналізовано можливість їх реалізації на базі бібліотек MPI, CUDA, OpenCL, Java (фреймворки ThreaPoolExecutor та Fork-Join) для створення програмних компонент системи криптоаналізу на базі доступного апаратного забезпечення.
2. Вперше запропоновано використання комплексної архітектури криптоаналітичної системи на базі бібліотек OpenMPI, jCUDA, jOCL, Java (фреймворки ThreaPoolExecutor та Fork-Join).
3. Вперше обґрунтовано доцільність використання кросплатформових технологій програмування при розв'язанні задач криптоаналізу.

Практичне значення отриманих результатів.

Реалізовано програмне забезпечення для криптоаналізу хеш-функцій. Проведено обчислювальні експерименти з метою обґрунтування доцільності запропонованої архітектури програмно-апаратної системи.

Апробація результатів дипломної роботи магістра. Результати дипломної роботи магістра апробовано на двох конференціях:

- міжнародній науково-технічний конференції молодих учених та студентів «Актуальні задачі сучасних технологій» (Тернопіль, ТНТУ, 2016);
- XIX-й науковій конференції Тернопільського національного технічного університету імені Івана Пулюя (2016).

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 9 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 115 арк. формату А4, графічна частина – 10 аркушів формату А1

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність дослідження та здійснено короткий огляд сучасного стану проблем у галузі високопродуктивних обчислювальних систем для розв'язання задач криптоаналізу. Охарактеризовано основні завдання, які необхідно вирішити у дипломній роботі магістра.

В розділі 1 «Аналіз предметної області високопродуктивних криптоаналітичних комп'ютерних систем» проведено аналіз предметної області криптоаналізу, апаратного та програмного забезпечення криптоаналітичних комп'ютерних систем. Сформульовано основні задачі дипломної роботи магістра.

В розділі 2 «Математичне забезпечення комп'ютерних систем криптоаналізу» проведено аналіз алгоритмічної складності криптоаналітичних задач, належність їх до відповідних класів складностей.

Обґрунтовано доцільність використання у SMP-системах патернів паралельних обчислень у рамках багатопоточності технології Java. Зокрема, ThreadPool та Fork-Join. Наведено методи оцінювання ефективності використання обчислювальних ресурсів шляхом створення пулів потоків певного розміру. Відповідні методи дають змогу реалізувати програмне забезпечення, яке буде адаптуватись до типу обчислювальної системи.

В розділі 3 «Засоби та методи розробки програмного забезпечення комп'ютерних систем криптоаналізу» здійснено огляд, вибір та обґрунтування апаратного забезпечення для розв'язання задач криптоаналізу з урахування парадигм та концепцій паралельного програмування. Проаналізовані парадигми забезпечують максимальну ефективність роботи обчислювальних систем й дають змогу реалізувати паралельні алгоритми криптоаналізу.

Також у даному розділі здійснено огляд, вибір і обґрунтування можливих засобів розробки програмного забезпечення криптоаналізу в паралельних та розподілених комп’ютерних системах, це технології CUDA, OpenCL для GPGPU-платформ; технологія MPI для систем з розподіленою пам’яттю (кластерних систем). Водночас, технологією програмування обрано технологію Java. Взаємодія з

бібліотеками CUDA та OpenCL забезпечена за допомогою бібліотек-оболонок jCUDA та jOCL. Важливою є робота з підсистемою MPI, для чого розглянуто спеціалізовані бібліотеки. Наведено процедуру розгортання середовища розробки та виконання MPI-програм, оскільки, вона доволі нетривіальна.

Для використання можливостей центральних процесорів та їх ядер використано фреймворки паралельного програмування технології Java, це ThreadPool та Fork-Join. Проведено їх апробацію й проаналізовано результати обчислювальних експериментів, зокрема, оцінено час виконання за різних умов (з введенням-виведенням і без нього, з різною кількістю потоків). Зроблені висновки стосовно використання відповідних патернів паралельного програмування на наявній обчислювальній базі.

В розділі 4 «Обґрунтування економічної ефективності» показано доцільність проведення науково-дослідних робіт за даною тематикою і економічно обґрунтовано доцільність застосування запропонованих засобів. Показано економічну доцільність використання відкритого програмного забезпечення, зокрема засобів розробки, операційних систем та типових апаратних засобів.

В розділі 5 «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто вимоги до охорони праці користувачів ВДТ, до яких належать науковці, розробники криптоаналітичного програмного забезпечення, користувачі, а також розглянуті вимоги до організації серверних кімнат у яких може розташовуватись високопотужні системи опрацювання даних. Це дало змогу забезпечити належний рівень умов праці.

В розділі 6 «Екологія» проаналізовано сучасні програмні продукти для опрацювання великих масивів екологічної інформації, а також розглянуто методи узагальнення екологічної інформації у комп’ютерних системах.

У загальних висновках щодо дипломної роботи описано прийняті в роботі технічні рішення і організаційно-технічні заходи, які забезпечують виконання завдання на проектування; оригінальні технічні рішення, прийняті автором в процесі роботи.

В додатках до пояснювальної записки наведено фрагменти вихідного коду програм для здійснення криптоаналізу хеш-функцій на мові програмування Java.

В графічній частині наведено характеристики досліджуваних хеш-функцій, особливості їх криптоаналізу, архітектурні особливості високопродуктивної системи криптоаналізу. Показано взаємодію програмних компонент й процес формування виконуваних файлів-ядер для GPU.

ВИСНОВКИ

1. Проаналізовано предметну область криптоаналізу й високопродуктивних обчислювальних систем й сформульовано рекомендації по вибору доступних апаратних та програмних компонентів високопродуктивних обчислювальних систем за критерієм вартості та доступності.

2. Проведено аналітичне оцінювання продуктивності апаратних засобів для реалізації декількох криптоаналітичних алгоритмів. А також, проаналізовано підходи до формування архітектур ПРКС для певних видів криптоаналізу. Зокрема, з можливістю інтеграції спеціалізованих апаратних засобів на базі FPGA та DSP для

реалізації криптоаналітичних алгоритмів, та спряження їх з існуючими ПРКС, системами моніторингу та керування завданнями.

3. Запропоновано використовувати технологію Java для створення програмного забезпечення розподіленої обчислювальної системи та розглянуто практичні аспекти її впровадження, а саме інтегрування з системою з розподіленою пам'яттю на базі OpenMPI, програмними засобами для роботи з GPU-прискорювачами: OpenCL - JOCL та Nvidia CUDA — JCUDA.

4. Обґрунтовано використання фреймворку Fork-Join технології Java для виконання багатопотокових програм на системах зі спільною пам'яттю.

5. Запропоновано програмно-апаратну архітектуру, яка базується на доступних апаратних (багатоядерні x86_64 SMP-системи, які обладнані GPU-відеокартами та об'єднані Gigabit-ethernet мережею) та програмних (ОС Linux, Java, MPI, CUDA або OpenCL) засобах.

6. Розроблено розподілену кросплатформову програму для криптоаналізу хеш-функцій. Система орієнтована на 2 вузли і реалізує поставлене завдання, а саме: найпростіший метод криптоаналізу хеш-функцій — метод повного перебору з використанням багатьох потоків. Для реалізації поставленого завдання використано технології MPI, JAVA та GPGPU. Програму реалізовано на мові програмування JAVA. З метою спрощення роботи з GPGPU та MPI використано бібліотеку jCUDA та середовище OpenMPI. Як апаратне забезпечення використано відеокарту ZOTAC NVIDIA GeForce GTX 465 та типові x86_64 процесор - Intel Core i5-2300 CPU 2.80GHz.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Луцків А.М. Аналіз технологій розпаралелення у високопродуктивних комп’ютерних системах для задач криптоаналізу / А.М. Луцків, І.В. Вербицький// Матеріали XIX наукової конференції Тернопільського національного технічного університету імені Івана Пулюя. – Тернопіль: ТНТУ ім. І. Пулюя (м. Тернопіль, 18-19 травня 2016 року), 2016. – 95-96 С. [Електронний ресурс] Режим доступу: URL: http://elartu.tntu.edu.ua/handle/123456789/16496.

2. Луцків А.М. Створення програмного забезпечення для високопродуктивних обчислювальних систем при розв’язанні задач криптоаналізу / А.М. Луцків, І.В. Вербицький // Актуальні задачі сучасних технологій : зб. тез доповідей міжнар. наук.-техн. Конф. Молодих учених та студентів, (Тернопіль, 17–18 листоп. 2016.) / М-во освіти і науки України, Терн. націон. техн. ун-т ім. І. Пулюя [та ін]. – Тернопіль : ТНТУ, 2016. – 73-75С.

АНОТАЦІЯ

Вербицький І.В. Дослідження обчислювальних процесів у високопродуктивних обчислювальних системах при розв’язанні задач криптоаналізу

Дипломна робота магістра, 8.05010201 – Комп’ютерні системи та мережі. – Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, 2017.

В дипломній роботі виконано дослідження обчислювальних процесів у високопродуктивних обчислювальних системах при розв’язанні задач криптоаналізу. Аналізувався криптоаналіз хеш-функцій, а саме виникнення колізій, методи повного перебору, парадокс днів народження. Для реалізації криптоаналітичних алгоритмів використано програмні та апаратні засоби. У роботі обґрунтована архітектура паралельної та розподіленої комп'ютерної системи на базі доступних компонентів: графічних плат nVidia та багатоядерних x86_64 процесорів. Графічні процесори забезпечують дрібнозернистий паралелелізм, а ядра центральних процесорів крупнозернистий. Обчислювальні системи об’єднані комунікаційним каналом GigabitEthernet. Технологією програмування графічних процесорів nVidia використано CUDA (бібліотека jCUDA для роботи з Java), ефективне використання ядер центрального процесора забезпечується використанням Java Fork-Join фреймворку, а робота по мережі в рамках технології MPI забезпечується програмною системою OpenMPI з відповідною Java-оболонкою. Таким чином досліджуване програмне забезпечення реалізоване з використання технології Java.

У роботі наведені результати оцінювання ефективності використання відповідних технологій. Застосування технології Java дало змогу використати усі конкурентні переваги даної мови програмування, зокрема простоту, надійність та високу ефективність. Використано Java 8 фреймворк Fork-Join.

Ключові слова: високопродуктивні обчислення, криптоаналіз, Java, CUDA, OpenCL, MPI

ANNOTATION

Verbytskyi I. Investigation of computing processes in highly efficient computing systems for cryptanalysis problems solving

Master diploma thesis, 8.05010201 – Computer systems and networks - Ternopil Ivan Puluj National Technical University, Ternopil, 2017.

Master diploma thesis deals with the study of computational processes in high-performance computing systems for solving cryptanalysis problems. Hash functions cryptanalysis, such as collisions, brute-force methods, birthday paradox problem are analyzed. Cryptanalytic algorithms, software and hardware implementations are analyzed. The work proved architecture of parallel and distributed computer systems based on the low-cost components: nVidia graphics cards and multi-core x86_64 processors. GPUs provide small parallelism and coarse parallelism is provided by CPU cores. Computing systems combined by GigabitEthernet communication channel. Programming techniques used in investigation: for nVidia GPUs - CUDA (jCUDA wrapper library for working with Java), efficient usage of CPU cores is provided by Java Fork-Join framework, and network communication provided by MPI especially by OpenMPI with Java-wrappers. Thus studied software technology implemented by Java. The results of computational experiments prove effectiveness of appropriate technologies usage. The use of Java technology enabled to use all the competitive advantages of this programming language: simplicity, reliability and high efficiency. Java 8 Fork-Join framework was used to carry out computations.

Key words: HPC, cryptanalysis, Java, CUDA, OpenCL, MPI