УДК 004.056.5

О. В. Салієва
В. О. Максимець

ПОРІВНЯЛЬНИЙ АНАЛІЗ ТЕХНОЛОГІЙ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ ДЛЯ ПІДВИЩЕННЯ ШВИДКОДІЇ МАТЕМАТИЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ ВІДЕОПОТОКУ

Вінницький національний технічний університет

Анотація

У доповіді розглянуто сучасні технології паралельних обчислень, проаналізовано їхні переваги та недоліки, створено порівняльну таблицю даних технологій, що ґрунтуються на виборі архітектури цільового апаратного забезпечення та характері задач, що розпаралелюються.

Ключові слова: криптографія, захист, шифрування, відеопотоки, API, OpenCL, MPI, CUDA, OpenMP, Pthreads, паралельне обчислення, математичні алгоритми.

Annotation

The report considers modern parallel computing technologies, analyzes their advantages and disadvantages, and creates a comparative table of these technologies based on the choice of target hardware architecture and the nature of parallelized tasks.

Keywords: cryptography, security, encryption, video streams, APIs, OpenCL, MPI, CUDA, OpenMP, Pthreads, parallel computing, mathematical algorithms.

Вступ

Відеопотік представляє собою послідовну та безперервну передачу відеоданих у реальному часі через мережу з мінімальним затриманням, що дозволяє відтворювати відео без необхідності повного завантаження відеофайлу перед відтворенням [1]. Цей процес вимагає стійкого та неперервного потоку даних для забезпечення плавності відтворення відео на приймачі. Одна з особливостей відеопотоку полягає в тому, що він дозволяє користувачам переглядати відеоконтент миттєво, без заздалегідь завантаженого відеофайлу.

Розуміючи важливість безпеки при передачі відеопотоків у режимі реального часу, особливо в контексті веб-сервісів та мобільних додатків, виникає необхідність в застосуванні ефективного та швидкого шифрування відеопотоків.

Шифрування відеопотоків полягає в застосуванні спеціальних криптографічних алгоритмів для перетворення відеоданих у нерозбірливий вигляд, який може бути розшифрований лише з використанням відповідного ключа. Однак шифрування відеопотоку має свої особливості: великий обсяг даних, що потребує обробки у реальному часі та потреба в стійких алгоритмах передачі даних через мережу. У зв’язку із цим шифрування відеопотоку вимагає значних обчислювальних ресурсів, особливо при високій роздільній здатності відео й шифруванню великого обсягу даних, та тонкого балансу між забезпеченням надійних заходів безпеки та підтриманням низької затримки.

Для подолання даних обмежень обчислювальних ресурсів при виконанні складних завдань шифрування відеопотоків ключовою стратегією є використання методів паралельних обчислень. Паралельні обчислення можуть допомогти значно полегшити обчислювальне навантаження при шифруванні великих обсягів даних, таких як відеопотік. Проте для реалізації даної задачі необхідно підібрати правильну та оптимізовану обчислювану технологію.

Метою даної роботи є здійснення порівняльного аналізу відомих технологій паралельних обчислень задля підвищення швидкості математичних алгоритмів шифрування відеопотоку.

Результати дослідження

Паралельні обчислення передбачають одночасне виконання декількох обчислень, розбиваючи складні завдання на менші, більш керовані блоки, які можна обробляти одночасно. Цей підхід є ключовим для шифрування відеопотоків, оскільки він використовує розпаралелювання математичних операцій, що застосовуються в алгоритмах шифрування [2].

У найпростішому розумінні паралельні обчислення для математичного алгоритму передбачають одночасне використання декількох обчислювальних ресурсів для вирішення конкретної обчислювальної задачі [3]:

1. Математичний алгоритм деконструюється на окремі компоненти або операції, які можуть бути вирішені одночасно.
2. Кожен компонент далі поділяється на серію інструкцій або обчислювальних кроків.
3. Інструкції з кожного компонента виконуються одночасно на окремих процесорах або обчислювальних блоках.

Для забезпечення синхронізації та узгодженості виконання розпаралелених інструкцій існує загальний механізм контролю та координації, що сприяє ефективному та прискореному процесу обчислень.

Паралельні обчислення є потужним інструментом для підвищення швидкості математичних алгоритмів. Вони можуть розділити обчислювальну роботу між кількома обчислювальними ресурсами, такими як процесори або ядра графічного процесора. Основною перевагою паралельних обчислень є здатність до виконання багатьох операцій одночасно, що призводить до значного прискорення розрахунків.

Використовуючи потужність паралельних обчислень, процес шифрування можна розподілити між декількома процесорами, що значно прискорює загальну швидкість шифрування [4]. Таке розпаралелювання особливо вигідне для алгоритмів з симетричним ключем, де один і той самий ключ використовується як для шифрування, так і для дешифрування. Однак використання паралельних обчислень також має свої труднощі: необхідно окремо розділити обчислювальну роботу між великими ресурсами, а також вирішити проблеми синхронізації та доступу до спільних ресурсів. Крім того, не всі математичні алгоритми підходять для паралельного виконання, деякі з них мають «покрокову» природу та залежать від результатів попередніх кроків [5].

Враховуючи ці особливості, необхідно аналізувати алгоритми та їхні вимоги до обчислювальної потужності, перед тим як використовувати паралельні обчислення. Правильно підібрані та оптимізовані паралельні обчислення можуть суттєво підвищити швидкість математичних алгоритмів та допомогти в обробці складних обчислювальних задач.

У сучасній сфері використання інтерфейсів паралельного програмування, пристосованих для багатоядерних процесорів, прискорювачів, таких як графічні процесори, та гібридних систем, розглянемо та порівняємо кілька рішень (табл. 1) [6-8].

Таблиця 1 – Порівняльний аналіз технологій паралельних обчислень

Технологія/API	Модель програмування	Мова програмування	Підтримуванні платформи/цільова паралельна система	Ліцензія/стандарт
OpenCL [6]	Модель OpenCL, обчислення запускаються як ядра, що виконуються декількома робочими елементами, об'єднаними в робочі групи, та об'єктами пам'яті для управління даними	C/C++	Гетерогенна платформа, що включає процесори, графічні процесори різних виробників	OpenCL – це стандарт
MPI [7]	Багатопроцесний, також багатопотоковий, якщо реалізація підтримує	C/Fortran	Кластер, сервер, робоча станція	MPI є стандартом
CUDA [6]	Модель CUDA, обчислення запускаються як ядра, що виконуються декількома потоками, згрупованими в блоки, глобальну та спільну пам'ять на графічному процесорі, а також пам'ять хоста для керування даними	C	Сервер або робоча станція з графічним процесором NVIDIA	Власне рішення NVIDIA, ліцензійна угода NVIDIA

Продовження таблиці 1

OpenMP [8]	Багатопотоковий додаток	C/C++/Fortran	Гетерогенна система з процесорами, прискорювачами, включаючи графічні процесори	OpenMP – це стандарт
Pthreads [8]	Багатопотоковий додаток, надає процедури управління потоками, механізми синхронізації, включаючи м'ютекси, умовні змінні	C	Широко доступний на платформах UNIX, реалізаціях, наприклад, NPTL	Частина стандарту POSIX

Таким чином, у таблиці наведено комплексний набір інструментів для паралельного програмування на різних обчислювальних архітектурах. Ці моделі паралельного програмування охоплюють цілий ряд стратегій розпаралелювання, від моделей зі спільною пам'яттю, таких як OpenMP і Pthreads, до моделей з розподіленою пам'яттю, таких як MPI, і спеціалізованого програмування на GPU за допомогою CUDA і OpenCL. Вибір правильної моделі залежить від таких факторів, як архітектура цільового апаратного забезпечення та характер задач, що розпаралелюються [8].

Висновки

Отже, використання паралельних обчислень суттєво впливає на швидкість та ефективність математичних алгоритмів, особливо це має велике значення для вирішення проблем, що виникають при шифруванні відеопотоку. Паралельні обчислення використовують можливості паралельної обробки даних багатоядерних процесорів, прискорювачів, таких як графічні процесори, і розподілених систем, що дозволяє одночасно виконувати обчислення. Такий підхід значно скорочує час обробки, прискорює складні математичні операції і підвищує загальну продуктивність алгоритмів шифрування.

У результаті, паралельні обчислення алгоритмів шифрування за своєю природою дозволяють ефективно використовувати ресурси, мінімізувати затримки і забезпечити обробку в реальному часі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Gillis A. S. Video streaming. TechTarget. URL: https://www.techtarget.com/searchunifiedcommunications/definition/streaming-video.
2. Introduction to Parallel Computing Tutorial | HPC @ LLNL. Home | HPC @ LLNL. URL: https://hpc.llnl.gov/documentation/tutorials/introduction-parallel-computing-tutorial.
3. CS301: Parallel Computing | Saylor Academy. Saylor Academy. URL: https://learn.saylor.org/mod/page/view.php?id=27133.
4. Kuck D. J. Parallel Computing. SpringerLink. URL: https://link.springer.com/referenceworkentry/10.1007/978-0-387-09766-4_279.
5. A Survey on Parallel Computing and its Applications in Data-Parallel Problems Using GPU Architectures | Communications in Computational Physics | Cambridge Core. Cambridge Core. URL: https://www.cambridge.org/core/journals/communications-in-computational-physics/article/survey-on-parallel-computing-and-its-applications-in-dataparallel-problems-using-gpu-architectures/879D964A36478175DEED99FB00C8D811.
6. OpenCL: A Parallel Programming Standard for Heterogeneous Computing Systems. PubMed Central (PMC). URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2964860/.
7. MPI in terms of OpenCL - StreamHPC. StreamHPC. URL: https://streamhpc.com/blog/2011-08-19/mpi-in-terms-of-opencl.
8. Swahn H. Pthreads and OpenMP. A performance and productivity study. Karlskrona Sweden, 2022. 46 p. URL: https://www.diva-portal.org/smash/get/diva2:944063/FULLTEXT02.

Салієва Ольга Володимирівна – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@gmail.com

Максимець Володимир Олександрович - студент групи 2КІТС-22м, факультет менеджменту інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: maksimec10@gmail.com

Saliieva Olha V. – Doctor of Philosophy (PhD) in specialty 125 "Cyber Security", Associate Professor of the Department of Information Systems Management and Security, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@gmail.com

Maksymets Volodymyr O. - student of the 2KITS-22m group, Faculty of Management Information Security, Vinnitsa National Technical University, Vinnitsa, email: maksimec10@gmail.com