УДК 004.056.55

Кирилюк А. В.
Кирилащук Т. Г.

СПЕКУЛЯТИВНЕ ШИФРУВАННЯ НА GPU ДЛЯ КРИПТОГРАФІЧНИХ ФАЙЛОВИХ СИСТЕМ

Вінницький національний технічний університет

Анотація

У тезах розглядається застосування спекулятивного шифрування з використанням графічних процесорів (GPU) у криптографічних файлових системах. Досліджується використання режиму шифрування CTR, який забезпечує можливість паралельної обробки даних і попереднього формування масок шифрування. Запропонований підхід дозволяє зменшити затримки під час шифрування та підвищити продуктивність системи. Експериментальна реалізація у файловій системі EncFS++ показала покращення пропускної здатності та ефективності використання ресурсів процесора.

Ключові слова: криптографічні файлові системи, GPU, шифрування даних, режим CTR, спекулятивне шифрування, продуктивність системи.

Abstract

The theses consider the application of speculative encryption using graphics processing units (GPU) in cryptographic file systems. The study examines the use of the CTR encryption mode, which enables parallel data processing and the preliminary generation of encryption masks. The proposed approach helps reduce delays during encryption and improves overall system performance. The experimental implementation in the EncFS++ file system demonstrated increased throughput and more efficient use of CPU resources.

Keywords: cryptographic file systems, GPU, data encryption, CTR mode, speculative encryption, system performance.

Вступ

Сучасні інформаційні системи обробляють великі обсяги даних, тому питання їх захисту є важливим аспектом інформаційної безпеки. Одним із ефективних способів забезпечення конфіденційності інформації є використання криптографічних файлових систем, які виконують шифрування даних під час їх зберігання. Проте виконання криптографічних операцій може знижувати продуктивність системи, що зумовлює необхідність пошуку ефективних способів оптимізації цих процесів.

Результати дослідження

У сучасному інформаційному суспільстві обсяги цифрових даних постійно зростають, а значна частина інформації зберігається у хмарних сервісах та розподілених системах зберігання. У зв’язку з цим важливого значення набуває забезпечення конфіденційності та захисту даних від несанкціонованого доступу. Одним із ефективних способів вирішення цієї проблеми є використання криптографічних файлових систем, які виконують шифрування даних перед їх збереженням на носіях або перед передаванням через мережу. Такі системи дозволяють захистити інформацію навіть у випадку отримання доступу до фізичного носія даних сторонніми особами.

Разом з тим застосування криптографічних алгоритмів потребує значних обчислювальних ресурсів, оскільки шифрування та дешифрування великих обсягів інформації виконуються для кожного блоку даних. Це може призводити до зниження загальної продуктивності файлових систем, особливо у випадку роботи з великими масивами даних або високошвидкісними пристроями зберігання

інформації. Тому одним із актуальних напрямів досліджень є пошук способів підвищення ефективності криптографічної обробки даних.

Одним із можливих підходів до підвищення продуктивності є використання паралельних обчислень із застосуванням графічних процесорів (GPU). Сучасні GPU містять велику кількість обчислювальних ядер, що дозволяє ефективно виконувати одночасну обробку значної кількості операцій. Завдяки цьому графічні процесори можуть використовуватися не лише для обробки графіки, а й для прискорення різних обчислювальних задач, зокрема криптографічних алгоритмів. Використання GPU дає можливість значно підвищити швидкість обробки даних і зменшити навантаження на центральний процесор.

У роботі розглядається застосування режиму шифрування CTR (Counter Mode), який має ряд переваг у порівнянні з іншими режимами роботи блочних шифрів. Основною його особливістю є можливість повної паралелізації процесів шифрування та дешифрування, оскільки обробка кожного блоку даних відбувається незалежно від інших блоків. Крім того, режим CTR дозволяє виконувати попередню генерацію масок шифрування. Це означає, що частина криптографічних обчислень може бути виконана заздалегідь, ще до того, як з'являться дані, які потрібно зашифрувати або розшифрувати.

На основі цієї властивості у дослідженні запропоновано підхід спекулятивного шифрування. Його суть полягає у попередньому створенні масок шифрування за допомогою графічного процесора. Коли система отримує дані для шифрування або дешифрування, відповідні маски вже підготовлені і можуть бути використані одразу. Це дозволяє скоротити затримки під час обробки даних та підвищити загальну продуктивність файлової системи.

Запропонований підхід був реалізований у модифікованій криптографічній файловій системі EncFS++, створеній на основі системи EncFS. У процесі дослідження було проведено експериментальне тестування продуктивності системи при виконанні операцій читання та запису даних різного обсягу. Отримані результати показали суттєве зростання пропускної здатності системи та підвищення ефективності використання ресурсів центрального процесора. Це підтверджує доцільність використання графічних процесорів для прискорення криптографічних операцій у файлових системах.

Висновки

У роботі розглянуто застосування спекулятивного шифрування та використання графічних процесорів для підвищення ефективності криптографічних файлових систем. Використання режиму CTR дозволяє виконувати паралельну обробку даних і попередню генерацію масок шифрування. Запропонований підхід сприяє підвищенню продуктивності системи та більш ефективному використанню обчислювальних ресурсів. Результати дослідження підтверджують перспективність використання GPU для прискорення криптографічних операцій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Eduardo V., Erpen de Bona L. C., Zola W. M. Speculative Encryption on GPU Applied to Cryptographic File Systems // Proceedings of the 17th USENIX Conference on File and Storage Technologies (FAST'19). – Boston, USA, 2019. – P. 93–108.
2. Stallings W. Cryptography and Network Security: Principles and Practice. – 7th ed. – Boston : Pearson Education, 2017. – 766 p.
3. Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. – Indianapolis : Wiley Publishing, 2010. – 432 p.
4. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. – Berlin : Springer, 2010. – 371 p.

Кирилюк Анастасія Володимирівна – студентка групи 2БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: nastasia.kyryliuk@gmail.com

Науковий керівник: ***Кирилащук Тетяна Геннадіївна*** – асистент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: kgt0998@gmail.com

Kyryliuk Anastasiia – student of group 2BS-24B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: nastasia.kyryliuk@gmail.com

Scientific Supervisor: ***Kyrylashchuk Tatyana*** – assistant of the Information Security Department, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com