

МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ
ГО “ВСЕУКРАЇНСЬКА АСАМБЛЕЯ ДОКТОРІВ НАУК
З ДЕРЖАВНОГО УПРАВЛІННЯ”
МІЖНАРОДНА КАДРОВА АКАДЕМІЯ
UNIVERSIDAD CENTRAL DEL ECUADOR
UNIVERSIDAD TECNOLÓGICA ISRAEL (REPÚBLICA DE ECUADOR)
“ANANIA SHIRAKATSI” UNIVERSITY OF INTERNATIONAL RELATION (ARMENIA)



ПРОБЛЕМИ МОДЕРНІЗАЦІЇ УКРАЇНИ

Випуск 8

Матеріали

*Міжнародної науково-практичної конференції
присвяченої 30-річчю МАУП*

*“Актуальні проблеми модернізації
недержавного сектору освіти в Україні
у контексті світових тенденцій і національної практики”*

м. Київ, МАУП, 11 квітня 2019 р.

Київ
ДП “Видавничий дім “Персонал”
2019

*Схвалено Вченою радою Міжрегіональної Академії управління персоналом
(протокол № 3 від 27.03.19)*

Редакційна колегія:

М. Н. Курко (голова), д-р юрид. наук, проф.;
Є. О. Романенко (заступник голови), д-р наук з держ. упр., проф.;
А. А. Ігнатченко (відповідальний редактор), канд. техн. наук;
І. П. Бідзюра, д-р політ. наук, проф.;
В. М. Воронін, д-р іст. наук;
М. Ф. Головатий, д-р політ. наук, проф.;
А. М. Кислий, д-р юрид. наук., проф.;
О. Л. Фещенко, канд. екон. наук, доц.;
Л. В. Янюк (виконавчий редактор)

*Матеріали подано в авторській редакції.
Відповідальність за зміст та орфографію матеріалів несуть автори.*

Проблеми модернізації України : [зб. наук. пр.] / МАУП. — К.: ДП
“Видавничий дім “Персонал”, 2008 —

С76 Вип. 8: Матеріали Міжнар. наук. конф. “Актуальні проблеми модернізації недержавного сектору освіти в Україні у контексті світових тенденцій і національної практики”, 11 квітня 2019 р. / редкол. : М. Н. Курко (голова) [та ін.]. — 2019. — 460 с. : іл. — Бібліогр. у кінці ст.

У пропонованому збірнику подано тези учасників науково-практичних конференцій з проблематики широкого кола аспектів процесу системної модернізації України.

Для науковців, громадсько-політичних діячів, студентів, а також усіх, хто цікавиться розвитком Української держави і світовим досвідом проведення модернізаційних процесів.

ББК 63.3(4УКР)я43+67.9(4УКР)301я43

Сарабун О. Б. Екзистенційний вимір освітнього самоздійснення як спосіб протистояння безособовості людини	261
Чолишкіна О. Г., Домків Т. С. Алгоритм пошуку пароля до PDF файла із застосуванням технології CUDA.....	264
Ліскін В. О. Система моніторингу навчального процесу в системі Moodle на основі чанк-орієнтованого підходу	266
Бацуровська І. В., Грубань В. А. Проблеми розвитку STEM-освіти: педагогічний аспект.....	271
Дяченко М. П., Людвиченко В. О. Про розробку веб-застосунку “моніторинг і обчислення вартості продовольчого кошика в Україні”	274
Яворська В. Г. Історія та перспективи вдосконалення приватних навчальних закладів в Україні: правові та практичні тенденції	277
Магас Н. В. Стан недержавної вищої освіти в сучасній Україні	280
Дмишко О. С., Гудиш В. Г. Психологія управління недержавними ЗВО.....	283
Стівакова Н. О. Сучасні ризики розвитку недержавної вищої освіти в Україні	287
Кривоберець М. М. Особливості надання недержавних освітніх послуг у сфері туризму в Україні	290
Вейнгард К. О. Інноваційний характер недержавної системи вищої освіти як одна з важливіших її ознак і пріоритетів	292
Черкаська В. В. Підтримка розвитку недержавної освіти в аграрній сфері.....	294
Негода Ю. В. Особливості трансформації аграрних комплексів у контексті розвитку недержавної освіти	296
Миколаєць А. П. Вплив комерційних і неприбуткових організацій на формування соціального партнерства з органами влади у сфері освіти.....	298
Доносо Варгас Дієго Хосе Формування нової моделі підготовки фахівців поліції в Україні та Еквадорі на основі компетенцій тісного підходу	300
Rosero L. M., Cobos A. R., Calahorrano C. R. Transformational leadership of teachers as competition race police sciences and safety of quito in the period 2018–2020	304
Cobos A. R., Rosero L. M. Technology as a fundamental tool in the formation of police officers of Ecuador in the period 2018–2020	307

АЛГОРИТМ ПОШУКУ ПАРОЛЯ ДО PDF ФАЙЛА ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЇ CUDA

Обчислення на GPU зробили великий крок вперед, привносячи високопродуктивні обчислення в звичайне апаратне забезпечення. Багатофункціональні паралельні мови, такі як CUDA і OpenCL, зменшили складність програмування. Однак, щоб повною мірою скористатися їх обчислювальною потужністю, потрібно власноруч програмувати криптоалгоритми тому, що бібліотек, які допомагають працювати з CUDA у сфері криптоаналізу немає. Більш того, складна ієрархія пам'яті графічного процесора і багатопотокова архітектура роблять програмування складним завданням навіть для досвідчених програмістів.

Алгоритм пошуку пароля до PDF файлу із застосуванням технології CUDA

- 1) Створюємо файл з розширення *.cu (вихідний текст модуля, що використовуватиметься на CUDA). В ньому запрограмовані всі криптоалгоритми, які необхідні для аналізу та розшифрування pdf файлів.
 - 2) Створений файл компілюємо і збираємо під CUDA. Розширення файлу після компіляції *.ptx.
 - 3) Зкомпільований файл завантажуюмо в глобальну пам'ять GPU з використанням технології CUDA.
 - 4) Передаємо крипто-параметри PDF файлу на відеокарту.
 - 5) Передаємо масив, що складається з першого і останнього на цей блок ядер паролів, а також кількість цих паролів (N), що залежить від використовуваних на даний момент ядер GPU (один пароль — один потік).
 - 6) Потоки паролів передаються на загальну пам'ять відеокарти, в окремі банки
 - 8) В реєстрі формується новий пароль з заданого діапазону та знову передається в загальну пам'ять.
 - 9) Якщо за 1 такт GPU вірний пароль не знайдено, то повторюємо пункти 5–7 поки не знайдемо вірний.
 - 10) Після знаходження пароля його значення знову передається на глобальну пам'ять, звідки і відбувається зчитування його програмою.
- Процедуру пошуку пароля відображено на рисунку нижче (рис. 1).
- 11) Перевірка результатів роботи алгоритму.
 - 12) Вивільнення використовуваних ресурсів.
 - 13) Розшифрування PDF-файлу.

Оптимізація алгоритму: Оскільки передача всього робочого масиву паролів займає досить тривалий час, щоб не було відчутної паузи після початку роботи алгоритму, відбувається поступовий “розгін” відеокарти до робочого режиму, шляхом поступового нарощування потоків GPU циклами зі значенням $N = 1$. Після виходу відеокарти на робоче значення потоків, значенням N (кількість ітерацій в циклі перевірки паролів) досягається стабілізація роботи відеокарти таким чином, щоб час виконання ядра CUDA не перевищувало 1–2 сек.

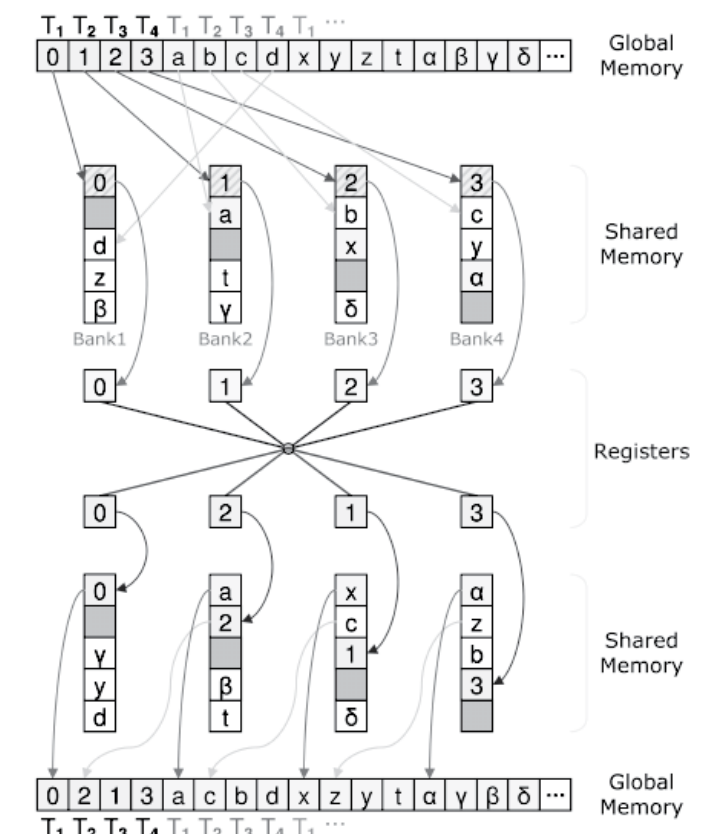


Рис. 1. Процедура пошуку пароля на GPU з використанням технології CUDA

Висновок: Тестування даного алгоритму на реальних даних показало прискорення в часі, порівняно з виконанням обчислень на CPU, в 8.5 разів. Отже, пошук багатосимвольних паролів відбувається за дуже малий час, що дає можливість обробляти більшу кількість інформації.

Джерела

1. Andreas Klckner, Nicolas Pinto, Yunsup Lee, B. Catanzaro, Paul Ivanov, and Ahmed Fasih. PyCUDA and PyOpenCL: A Scripting-Based Approach to GPU Run-Time Code Generation. *Parallel Computing*, 38(3):157{174, 2012.
2. Боресков А. В., Харламов А. А. Основы работы с технологией CUDA. — Москва: ДМК Пресс, 2010. — 232 с.
3. Параллельные вычисления на GPU. Архитектура и программная модель CUDA / Боресков А. В., Харламов А.А., Марковский Н., Микушин Д. Н., Мортиков Е. В., Мыльцев А. А., Сахарных Н. А., Фролов В. А. — М.: МГУ имени М. В. Ломоносова, 2015 — 336 с.