РЕЦЕНЗІЯ

офіційного рецензента – кандидата фізико-математичних наук,
старшого наукового співробітника
Швідченко Інни Віталіївни
на дисертаційну роботу Баранова Ігоря Анатолійовича
на тему «Паралельні алгоритми симетричної криптографії»,
подану на здобуття ступеня доктора філософії
у галузі знань 11 «Математика та статистика»
за спеціальністю 113 «Прикладна математика»

Актуальність теми дисертації

У сучасному цифровому суспільстві інформаційно-комунікаційні технології стали невід'ємною складовою практично всіх сфер діяльності людини. Постійне зростання обсягів даних, що передаються та зберігаються в електронному вигляді, зумовлює необхідність забезпечення їх надійного захисту від несанкціонованого доступу. Одним із найбільш ефективних засобів розв'язання цього завдання є криптографічні методи захисту інформації, які забезпечують конфіденційність, цілісність та автентичність даних. Разом із тим збільшення інтенсивності інформаційних потоків та вимог до швидкодії систем обробки даних висуває нові вимоги до криптографічних алгоритмів. Традиційні послідовні підходи не завжди забезпечують необхідний рівень продуктивності під час роботи з великими обсягами інформації та не дозволяють повною мірою використовувати обчислювальні можливості сучасних багатоядерних процесорів і графічних прискорювачів. У зв'язку з цим актуальним науковим завданням є розробка нових криптографічних рішень, орієнтованих на паралельну обробку даних і ефективне використання сучасних обчислювальних архітектур.

Дисертаційна робота Баранова Ігоря Анатолійовича, присвячена розробці та дослідженню нових симетричних блочних криптографічних алгоритмів та їх паралельних модифікацій, які поєднують високий рівень криптографічної стійкості з можливістю ефективного виконання на багатоядерних процесорах і графічних прискорювачах.

Наукова новизна отриманих результатів

Наукова новизна дисертаційної роботи полягає у створенні оригінального підходу до побудови блочних симетричних криптографічних алгоритмів, який базується на використанні ключозалежних тривимірних перестановок. У роботі вперше запропоновано нові алгоритми WBC1 та WBC2, а також вперше розроблено їх паралельні модифікації PWBC1, PWBC1.1, PWBC2, PWBC2.1 і GPU-орієнтовану реалізацію PWBCCuda. Наукова новизна отриманих результатів є достатньо обґрунтованою та експериментально підтвердженою.

Практичне значення отриманих результатів

Практична цінність дисертаційної роботи визначається створенням програмних реалізацій запропонованих криптографічних алгоритмів та підтвердженням їх працездатності в ході експериментальних досліджень. Отримані результати можуть бути використані при розробці програмних засобів захисту інформації, орієнтованих на забезпечення високої продуктивності та належного рівня криптографічної стійкості під час обробки великих масивів даних.

Ступінь обґрунтованості основних положень, результатів та висновків

Наукові результати, висновки та рекомендації дисертаційної роботи викладені послідовно й логічно, належним чином обґрунтовані з теоретичної та методичної точок зору. Розроблені алгоритми доведено до рівня програмної реалізації та перевірено в ході експериментальних досліджень. Обґрунтованість положень, винесених на захист, забезпечується використанням сучасного математичного апарату, результатами тестування та проведених обчислювальних експериментів. Структура дисертації є цілісною, логічно побудованою та повною мірою відповідає поставленій меті й завданням дослідження.

Зв'язок дослідження з науковими програмами, планами та темами

Дисертаційну роботу виконано відповідно до планів науково-дослідних робіт Інституту кібернетики імені В. М. Глушкова НАН України, а саме у межах НДР: ВФ 150.3.1230 «Розроблення моделей та методів високопродуктивних обчислень та їх застосування» (Державний реєстраційний номер 0122U200449; I кв. 2022 р. – IV кв. 2023 р.), В.П.150.4.1230 «Розробити платформу високопродуктивних обчислень на базі суперкомп'ютера СКІТ для задач кібербезпеки, математичного

моделювання, інженерії» (Державний реєстраційний номер 0123U101573; 0124U003282; I кв. 2023 р. – IV кв. 2024 р.).

Огляд змісту дисертації та відповідності вимогам до оформлення

Дисертаційна робота має логічну структуру та складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел і додатків. Загальний обсяг роботи становить 229 сторінок, з яких 146 сторінок становить основний текст.

У першому розділі проаналізовано сучасний стан досліджень у галузі симетричної криптографії та паралельних обчислень. У другому розділі розроблено та досліджено нові алгоритми WBC1 і WBC2 та режими їх роботи. У третьому розділі запропоновано паралельні модифікації алгоритмів PWBC1, PWBC1.1, PWBC2, PWBC2.1 і GPU-реалізацію PWBCCuda, а також наведено результати їх експериментального дослідження.

Список використаних джерел є достатньо повним і відображає сучасний стан досліджуваної проблематики. Ознак порушення академічної доброчесності не виявлено.

Повнота викладення результатів дослідження в публікаціях

Основні результати дисертаційної роботи повною мірою висвітлено у 15 наукових публікаціях, із яких 4 опубліковано у наукових фахових виданнях. Ще 1 публікацію представлено в колективній монографії видавництва Springer, підготовленій за матеріалами міжнародної конференції та проіндексованій у наукометричних базах Scopus і Web of Science. Публікації відповідають вимогам до наукових статей, установленим МОН України на момент їх опублікування. Результати проведених досліджень доповідалися на 7 міжнародних наукових і науково-практичних конференціях.

Зауваження та побажання до дисертаційної роботи

Дисертаційна робота виконана на високому науковому рівні та загалом відповідає встановленим вимогам. Разом з тим окремі положення дослідження можуть бути предметом подальшого розвитку, уточнення та наукової дискусії:

– потребує подальшого дослідження стійкість запропонованих алгоритмів до атак на основі пов'язаних ключів (related-key attacks), а також атак, пов'язаних із витоком побічної інформації (side-channel attacks);

– доцільно більш детально розглянути особливості безпечного розподілу та управління криптографічними ключами в умовах паралельного виконання алгоритмів;

– перспективним є подальше дослідження квантово-стійких властивостей запропонованих алгоритмів та можливості створення їх постквантових модифікацій.

Висновок

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Баранова Ігоря Анатолійовича на тему «Паралельні алгоритми симетричної криптографії» виконана на високому науковому рівні, не містить порушень принципів академічної доброчесності та є завершеним самостійним науковим дослідженням, сукупність теоретичних і практичних результатів якого забезпечує розв'язання важливого наукового завдання, що має істотне значення для галузі знань 11 «Математика та статистика» за спеціальністю 113 «Прикладна математика».

За актуальністю, науковою новизною, теоретичним значенням і практичною цінністю дисертаційна робота повністю відповідає вимогам чинного законодавства України, передбаченим пунктами 6–9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44.

Здобувач ступеня доктора філософії Баранов Ігор Анатолійович заслуговує на присудження ступеня доктора філософії в галузі знань 11 «Математика та статистика» за спеціальністю 113 «Прикладна математика».

Офіційний рецензент:

провідний науковий співробітник
відділу оптимізації чисельних методів
Інституту кібернетики
імені В. М. Глушкова НАН України
кандидат фізико-математичних наук,
старший науковий співробітник _____ Інна ШВІДЧЕНКО

«16» січня 2026 р.

Підпис І. Швідченко
ЗАСВІДЧУЮ
Зав. канц. _____
ІК НАН України