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

1. Актуальність теми дисертації

Комп'ютерні мережі та цифрові сервіси відіграють дедалі важливішу роль у зберіганні та передачі інформації, що підвищує вимоги до забезпечення її конфіденційності та цілісності. Криптографія є одним з методів, що забезпечують найбільш безпечний спосіб передачі конфіденційної інформації від відправника до передбачуваного одержувача. Водночас стрімке зростання обсягів даних і потреба у високошвидкісній обробці інформації створюють суттєві обмеження для традиційних послідовних криптографічних алгоритмів. Особливо гостро ця проблема проявляється в умовах використання багатоядерних процесорів і графічних прискорювачів, потенціал яких не завжди може бути ефективно задіяний існуючими криптографічними рішеннями. У зв'язку з цим актуальним є створення нових симетричних криптографічних алгоритмів, орієнтованих на паралельне виконання та ефективне використання сучасних обчислювальних архітектур. Такі алгоритми дозволяють поєднати високий рівень криптографічної стійкості з підвищеною продуктивністю під час обробки великих обсягів даних.

Саме розв'язанню цієї науково-прикладної проблеми присвячена дисертаційна робота Баранова Ігоря Анатолійовича, у якій запропоновано нове сімейство паралельних алгоритмів симетричної криптографії, орієнтованих на ефективне використання багатоядерних процесорів і графічних прискорювачів.

2. Зв'язок дослідження з науковими програмами, планами та темами

Дисертаційна робота виконана згідно з планами таких науково-дослідних робіт Інституту кібернетики імені В.М. Глушкова НАН України:

- 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.,).

3. Наукова новизна одержаних результатів

Наукова новизна дисертаційної роботи полягає у розробленні нового сімейства блочних симетричних криптографічних алгоритмів на основі ключозалежних тривимірних перестановок. У межах дослідження вперше запропоновано алгоритми WBC1 та WBC2, а також їх паралельні реалізації PWBC1, PWBC1.1, PWBC2, PWBC2.1 і PWBCCuda. Новими є також підходи до організації криптографічних перетворень та їх ефективної реалізації на багатоядерних процесорах і графічних прискорювачах. Одержані результати, мають ознаки наукової новизни, належним чином обґрунтовані та підтверджені експериментально.

4. Практичне значення отриманих результатів

Практичне значення роботи полягає у доведенні запропонованих алгоритмів до рівня програмної реалізації та їх експериментальній апробації. Розроблені алгоритми можуть бути використані у програмних системах захисту інформації, де необхідне поєднання високої швидкодії та надійного криптографічного захисту під час обробки значних обсягів даних.

5. Ступінь обґрунтованості основних положень, результатів та висновків

Основні наукові положення, висновки та рекомендації дисертаційної роботи викладені структуровано та послідовно, мають належне математичне і методологічне обґрунтування. Всі розроблені методи та алгоритми програмно реалізовано. Основні положення, що виносяться на захист, обґрунтовані коректним

використанням математичного апарату для побудови алгоритмів, а також на підставі результатів тестування та обчислювальних експериментів з використанням даних з реальних практичних задач. Структура дисертаційного дослідження логічна та у повному обсязі розкриває тему.

6. Огляд змісту дисертації та відповідності вимогам до оформлення

Дисертаційна робота має логічну структуру та складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків.

У першому розділі проаналізовано сучасний стан досліджень у галузі симетричної криптографії та паралельних обчислень і обґрунтовано напрям дослідження.

У другому розділі розроблено та досліджено блочні симетричні криптографічні алгоритми WBC1 і WBC2 на основі ключозалежних перетворень типу «кубик Рубіка», а також розглянуто режими їх роботи.

У третьому розділі запропоновано паралельні модифікації PWBC1, PWBC1.1, PWBC2, PWBC2.1 та GPU-реалізацію PWBCCuda, наведено результати дослідження їх продуктивності, масштабованості та криптографічних властивостей.

Дисертацію оформлено відповідно до встановлених вимог, список використаних джерел є достатньо повним і відображає сучасний стан досліджуваної проблематики. Ознак порушення академічної доброчесності не виявлено.

7. Повнота викладення результатів дослідження в публікаціях

Сутність основних отриманих результатів виконаного дослідження та їх наукова новизна достатньо повно викладено в 6 опублікованих наукових статтях, одна з яких входить до наукометричної бази даних Scopus, а чотири опубліковано в наукових фахових виданнях України. Отримано два авторські свідоцтва та комп'ютерні програми. Крім того результати проведеного дослідження доповідалися на семи міжнародних наукових конференціях та відображені у відповідних друкованих матеріалах цих конференцій. Основні наукові положення та

висновки чітко сформульовано відповідно до поставлених задач наукової роботи.

8. Зауваження та побажання до дисертаційної роботи

Дисертаційне дослідження справляє загалом позитивне враження, однак, як будь-яке наукове дослідження, не позбавлене окремих недоліків, які можуть бути враховані у подальшій науковій діяльності автора:

1. У роботі основну увагу приділено оцінці складності процедур шифрування та розшифрування, тоді як складність побудови та аналізу обернених криптографічних перетворень могла б бути розглянута більш детально. Додаткове дослідження властивостей зворотної функції дозволило б глибше охарактеризувати криптографічну стійкість запропонованих методів.

2. Бажано доповнити дослідження аналізом накладних витрат, пов'язаних із передачею ключової інформації та синхронізацією процесів у паралельних реалізаціях алгоритмів. Це дозволило б повніше оцінити їх ефективність у практичних умовах використання.

3. Доцільно більш детально дослідити механізми генерації, передачі та синхронізації ключового матеріалу між обчислювальними процесами з урахуванням вимог безпеки та можливих загроз компрометації ключів.

9. Висновок

Дисертаційна робота Баранова Ігоря Анатолійовича «Паралельні алгоритми симетричної криптографії» є завершеним самостійним науковим дослідженням, у якому отримано нові науково обґрунтовані результати, що мають істотне теоретичне та практичне значення для розвитку симетричної криптографії, методів паралельних обчислень і засобів захисту інформації. За актуальністю, науковою новизною, теоретичною та практичною цінністю отриманих результатів дисертація відповідає вимогам «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 №44 від 12 січня 2022 року, а її автор, Баранов І.А., заслуговує

присудження ступеня доктора філософії за спеціальністю 113 Прикладна математика.

Офіційний рецензент:
старший науковий співробітник
відділу методів комбінаторної оптимізації
та інтелектуальних інформаційних технологій
Інституту кібернетики
імені В.М. Глушкова НАН України
кандидат фізико-математичних наук,
старший науковий співробітник
Ходзінський Олександр Миколайович

Національна Академія наук України
Інститут кібернетики імені В.М.Глушкова
Ідентифікаційний код 05417176
Україна * м.Київ

16.07.2026 р.

Підпис Ходзінського О.М.
ЗАСВІДЧУЮ
Зав. канц. ІК НАН України 16.07.2026