ВІДГУК

офіційного опонента, члена-кореспондента
Національної академії наук України
Корченка Олександра Григоровича
на дисертаційну роботу Баранова Ігоря Анатолійовича
«Паралельні алгоритми симетричної криптографії»,
подану на здобуття ступеня доктора філософії
за спеціальністю 113 «Прикладна математика»
у галузі знань 11 «Математика та статистика»

1. Актуальність теми дисертації

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням обсягів цифрових даних, розширенням глобальних комунікаційних мереж, активним впровадженням хмарних сервісів, технологій штучного інтелекту та цифрових платформ у державному, корпоративному й приватному секторах. Одночасно з цим зростає кількість і складність кіберзагроз, що висуває підвищені вимоги до засобів захисту інформації. За таких умов забезпечення конфіденційності, цілісності та доступності даних стає одним із ключових завдань сучасної кібербезпеки.

Одним із найбільш ефективних механізмів захисту інформації залишається криптографія. Проте постійне збільшення обсягів інформації, що підлягає шифруванню, потребує не лише підвищення криптографічної стійкості алгоритмів, а й забезпечення їх високої продуктивності. Особливої актуальності набуває створення нових криптографічних рішень, орієнтованих на ефективне використання сучасних багатоядерних процесорів та графічних прискорювачів, що дозволяє значно скоротити час обробки великих масивів даних без зниження рівня безпеки.

Додатковим фактором актуальності є розвиток квантових обчислювальних технологій, які потенційно можуть вплинути на ефективність традиційних криптографічних механізмів. Це зумовлює необхідність пошуку нових підходів до побудови криптографічних примітивів, здатних забезпечити високий рівень стійкості та водночас підтримувати ефективну реалізацію на сучасних паралельних обчислювальних платформах.

Тема дисертаційної роботи Баранова Ігоря Анатолійовича знаходиться на стику двох важливих наукових напрямів – криптографії та паралельних обчислень. Особливу наукову цінність становить дослідження можливості побудови блочних симетричних шифрів, архітектура яких орієнтована на паралельне виконання та масштабування без втрати криптографічних властивостей. Розв'язання такого завдання є складною науковою проблемою, що має як фундаментальне, так і прикладне значення.

У цьому контексті дисертаційна робота, присвячена розробці та дослідженню нових алгоритмів симетричної криптографії та їх паралельних

модифікацій, є своєчасною, актуальною та відповідає сучасним тенденціям розвитку інформаційних технологій. Отримані результати мають вагоме наукове значення та можуть бути використані при створенні перспективних систем криптографічного захисту інформації, орієнтованих на високопродуктивну обробку даних.

2. Зв'язок дослідження з науковими програмами та темами

Дисертаційна робота виконана в рамках двох науково-дослідних тем 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 квартал 2022 р. – IV квартал 2023 р.) та 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. Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни

Наукові результати дисертаційної роботи є обґрунтованими та відповідають меті дослідження. Для розроблених криптографічних алгоритмів наведено математичний опис, виконано оцінку їх обчислювальної складності, досліджено властивості криптографічних перетворень та проаналізовано особливості їх реалізації в умовах паралельних обчислень. Логіка викладу матеріалу є послідовною, а сформульовані висновки випливають із проведених теоретичних та експериментальних досліджень.

Достовірність отриманих результатів підтверджується їх програмною реалізацією, комплексним експериментальним тестуванням, узгодженістю з теоретичними оцінками обчислювальної складності та криптографічних властивостей, а також відтворюваністю наведених результатів.

Наукова новизна дисертаційної роботи полягає у створенні нового сімейства блочних симетричних криптографічних алгоритмів, побудованих на основі ключозалежних тривимірних перестановок типу «кубик Рубіка». Запропонований підхід відрізняється від традиційних схем симетричного шифрування та формує оригінальну криптографічну конструкцію. У роботі вперше розроблено алгоритми WBC1 та WBC2, а також їх паралельні модифікації PWBC1, PWBC1.1, PWBC2, PWBC2.1 і GPU-реалізацію PWBCCuda. Новими є також підходи до організації ключозалежних перетворень, паралельної обробки даних та підвищення криптографічної стійкості за рахунок ускладнення внутрішньої структури алгоритмів.

Практична цінність дисертаційної роботи полягає у розробці та програмній реалізації нових криптографічних алгоритмів, які пройшли експериментальну апробацію. Запропоновані рішення можуть бути використані в системах захисту інформації, що потребують високої продуктивності при обробці великих обсягів

даних. Особливу практичну значущість мають паралельні модифікації алгоритмів, орієнтовані на ефективне використання багатоядерних процесорів і графічних прискорювачів.

4. Огляд змісту дисертації та відповідності вимогам до оформлення

Дисертаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних літературних джерел, який містить 165 найменувань. Загальний обсяг дисертації викладено на 229 сторінках друкованого тексту, де обсяг основного тексту – 146 сторінок.

У вступі обґрунтовано актуальність теми дослідження, сформульовано мету, завдання, об'єкт і предмет дослідження, визначено наукову новизну та практичне значення отриманих результатів.

У першому розділі виконано аналіз сучасного стану досліджень у галузі симетричної криптографії, розглянуто відомі блочні криптографічні алгоритми, методи їх побудови та підходи до паралельної реалізації, а також обґрунтовано вибір напрямку досліджень.

У другому розділі розроблено нові блочні симетричні криптографічні алгоритми WBC1 та WBC2 на основі ключозалежних перестановок типу «кубик Рубіка», наведено їх математичний опис, виконано аналіз криптографічних властивостей, обчислювальної складності та результати тестування.

У третьому розділі запропоновано паралельні модифікації алгоритмів PWBC1, PWBC1.1, PWBC2, PWBC2.1 та GPU-реалізацію PWBCCuda. Проведено аналіз їх складності, досліджено масштабованість, ефективність паралельних реалізацій та наведено результати експериментальних досліджень продуктивності.

У висновках узагальнено основні результати дисертаційної роботи, сформульовано наукові та практичні результати дослідження, а також визначено перспективні напрями подальших досліджень.

Дисертація викладена логічно та послідовно, оформлена відповідно до встановлених вимог, містить необхідну кількість рисунків, таблиць, додатків і списку використаних джерел.

5. Повнота викладення результатів дослідження в публікаціях

Результати дисертації опубліковано в 15 наукових публікаціях, з яких чотири статті опубліковано у наукових фахових виданнях України. Одна стаття опублікована в колективній монографії Springer за матеріалами конференції, що індексуються в наукометричних базах Scopus/Web of Science. Отримано два авторські свідоцтва на комп'ютерні програми. Результати дисертації доповідалися здобувачем на семи міжнародних наукових та науково-практичних конференціях, а також на фаховому семінарі відділу чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України.

6. Відсутність порушення академічної доброчесності

У дисертації І.А. Баранова відсутні порушення академічної доброчесності.

Усі використані ідеї, результати та тексти інших авторів належним чином супроводжуються посиланнями на відповідні джерела.

7. Зауваження та рекомендації

1. Мета дослідження сформульована переважно через створення нових алгоритмів, тоді як її доцільно було б більшою мірою орієнтувати на отримання нового наукового результату, що відображав би методологічний аспект проведеного дослідження, наприклад, через розроблення методу, моделі, принципу тощо для забезпечення бажаного ефекту, а створення алгоритмів виступало засобом досягнення цієї мети.

2. При описі «Практична значущість дисертації…» автор зазначив що вона полягає у «розробці … нових…алгоритмів», але це все було заявлено як наукова новизна, а не практична цінність.

3. Актуальність дослідження обґрунтована зростанням вимог до швидкодії та безпеки оброблення даних у високопродуктивних обчислювальних середовищах. Разом із тим у вступі доцільно було б більш детально показати, які саме обмеження сучасних стандартизованих симетричних криптографічних алгоритмів не дозволяють ефективно розв'язувати поставлені задачі та чому запропонований підхід, що передбачає створення нового криптографічного алгоритму, є більш доцільним порівняно з удосконаленням існуючих рішень.

4. У першому розділі наведено достатньо широкий історичний огляд розвитку криптографії, однак аналіз сучасних наукових праць не повною мірою відповідає предмету дисертаційного дослідження. Зокрема, недостатньо розглянуто сучасні роботи, присвячені паралельній реалізації симетричних блочних криптографічних алгоритмів на багатоядерних процесорах і GPU, а також не проведено критичного аналізу існуючих підходів, що дозволило б чіткіше обґрунтувати вибір запропонованого напряму досліджень.

5. Недостатньо обґрунтовано вибір запропонованої архітектури криптографічних алгоритмів, побудованої на перетвореннях типу «кубик Рубіка». Було б доцільно детальніше показати її концептуальні переваги та відмінності від класичних структур блокових шифрів (SPN, мереж Фейстеля та інших), а також пояснити, які саме властивості цієї архітектури забезпечують заявлене підвищення криптографічної стійкості й ефективності.

6. Автором проведено значний обсяг експериментальних досліджень, однак висновки щодо криптографічної стійкості запропонованих алгоритмів ґрунтуються переважно на статистичних тестах та експериментальних оцінках. У роботі недостатньо наведено теоретичний аналіз стійкості алгоритмів до сучасних методів криптоаналізу, що дозволило б більш переконливо підтвердити заявлені переваги розроблених криптографічних алгоритмів.

7. Практична цінність запропонованих алгоритмів підтверджена програмною реалізацією та експериментальними дослідженнями, однак було б доцільно розширити практичну апробацію шляхом інтеграції розроблених алгоритмів у реальні програмні або програмно-апаратні системи, а також дослідити їх функціонування в умовах практичних навантажень, що дозволило б більш повно оцінити перспективи їх практичного застосування.

8. Висновки

Дисертаційна робота Баранова Ігоря Анатолійовича «Паралельні алгоритми симетричної криптографії» є завершеною науковою роботою. За актуальністю, обсягом, науковою новизною та практичною значимістю вона відповідає вимогам постанови Кабінету Міністрів України №44 від 12 січня 2022 року «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», а її автор, Баранов Ігор Анатолійович, заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю 113 «Прикладна математика» в галузі знань 11–«Математика та статистика».

Офіційний опонент:
Перший проректор Державного університету
інформаційно-комунікаційних технологій,
член-кореспондент НАН України,
доктор технічних наук, професор,
лауреат Державної премії України
в галузі науки і техніки,
Заслужений діяч
науки і техніки України
Олександр КОРЧЕНКО

14.07.2026 р.