**ВІДГУК**

офіційного опонента - член-кореспондента НАН України

Кудіна Антона Михайловича

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

**1. Актуальність теми дисертації**

Стрімкий розвиток інформаційних технологій, хмарних сервісів, систем штучного інтелекту, високопродуктивних обчислень та обробки великих масивів даних обумовлює постійне зростання вимог до криптографічного захисту інформації. У сучасних умовах криптографічні механізми повинні забезпечувати не лише конфіденційність і цілісність даних, а і високу пропускну здатність, масштабованість, придатність до роботи на багатоядерних процесорах, GPU-прискорювачах і кластерних системах.

Дисертаційна робота Баранова Ігоря Анатолійовича присвячена розробленню нових симетричних блочних криптографічних алгоритмів та їх паралельних модифікацій. Запропоновані алгоритми WBC1, WBC2, PWBC1, PWBC1.1, PWBC2, PWBC2.1 та PWBCCuda базуються на оригінальній ідеї автора щодо використання тривимірних перестановок типу «кубик Рубіка» та для частини модифікацій, нелінійних S-блоків і дифузійних перетворень.

Актуальність теми не викликає сумніву, оскільки вона знаходиться на перетині прикладної математики, симетричної криптографії та паралельних обчислень. Разом з тим саме криптографічна складова таких алгоритмів потребує особливо суворої перевірки. Для нових шифрів недостатньо продемонструвати високу швидкодію, лавинний ефект або успішне

проходження статистичних тестів; необхідним є також ґрунтовний аналіз стійкості до сучасних структурних атак.

Отже, тема дисертаційного дослідження є актуальною, має наукову новизну та практичну спрямованість, однак прикладне використання запропонованих криптографічних конструкцій має розглядатися у взаємозв'язку з комплексним дослідженням усіх аспектів стійкості запропонованих криптосистем.

**2. Зв'язок дослідження з науковими програмами та темами**

Дисертаційна робота виконана відповідно до тем науково-дослідних робіт Інституту кібернетики імені В.М. Глушкова НАН України, зокрема ВФ 150.3.1230 «Розроблення моделей та методів високопродуктивних обчислень та їх застосування» і В.П.150.4.1230 «Розробити платформу високопродуктивних обчислень на базі суперкомп'ютера СКІТ для задач кібербезпеки, математичного моделювання, інженерії». Тематика дисертації узгоджується з цими напрямами, оскільки робота спрямована на створення та програмну реалізацію алгоритмів, придатних для високопродуктивної криптографічної обробки даних.

**3. Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни**

У дисертації наведено формальні описи запропонованих алгоритмів, схеми їх шифрування та розшифрування, аналіз обчислювальної складності, оцінки продуктивності, а також результати програмної апробації. Позитивною рисою роботи є те, що автор не обмежився лише теоретичною ідеєю, а реалізував алгоритми мовами Python та C/C++, дослідив різні режими роботи та виконав експериментальну перевірку на обчислювальній інфраструктурі.

Наукова новизна дисертації полягає у запропонованому сімействі симетричних блочних криптографічних алгоритмів на основі тривимірних

перестановок, а також у розробленні їх паралельних модифікацій для багатоядерних систем і GPU-орієнтованої реалізації. З погляду прикладної математики та високопродуктивних обчислень робота містить нові результати, пов'язані з побудовою паралельних процедур шифрування, оцінюванням складності та експериментальною апробацією.

Рівень обґрунтованості наукових результатів відповідає вимогам до дисертаційних робіт.

Практична значущість роботи полягає у створенні програмних прототипів і демонстрації можливості високошвидкісної паралельної обробки.

**4. Огляд змісту дисертації та відповідності вимогам до оформлення**

Дисертаційна робота має логічну структуру і складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Обсяг і структура дисертації загалом відповідають вимогам до кваліфікаційних наукових робіт на здобуття ступеня доктора філософії.

У першому розділі здійснено огляд розвитку симетричної криптографії, паралельних криптографічних алгоритмів, постквантових підходів, режимів роботи блочних шифрів та методів статистичного тестування. Розділ формує необхідне тло для постановки задачі.

Другий розділ присвячено базовим алгоритмам WBC1 та WBC2. У ньому наведено опис операцій, режимів роботи, програмної реалізації, продуктивності та статистичних випробувань.

Третій розділ містить паралельні модифікації PWBC1, PWBC1.1, PWBC2, PWBC2.1 та PWBCCuda. Розділ добре демонструє обчислювальний аспект роботи: розбиття даних на блоки, розподіл між процесорами, оцінку складності, розгляд MPI/GPU-реалізацій.

Дисертацію оформлено відповідно до чинних вимог. Список використаних джерел є репрезентативним і охоплює фундаментальні та сучасні публікації. Порушень академічної доброчесності не виявлено.

**5. Повнота викладення результатів дослідження в публікаціях**

Основні результати дисертації відображено у публікаціях здобувача, серед яких статті у наукових фахових виданнях України, публікація у виданні, що індексується наукометричною базою Scopus, тези доповідей на наукових конференціях та авторські свідоцтва на програмні засоби. Наукові результати дисертаційної роботи достатньо повно викладено в 15 наукових публікаціях, з яких серед яких 4 – статті у наукових фахових виданнях України, 1 – публікація, що індексуються в наукометричній базі Scopus (1 публікація у колективній монографії Scopus), 2 авторські свідоцтва, 7 – тез доповідей на міжнародних наукових конференціях.

Апробація результатів дисертації здійснена на 7 міжнародних наукових та науково-практичних конференціях, зокрема Computing Conference (London, United Kingdom), ПОО- XLII (Київ, Україна), XIII Міжнародна науково-практична конференція «Глушковські читання. Сучасна кібернетика 2024» (Київ, Україна). Також отримані результати доповідались здобувачем на засіданні відділу чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України 14 травня 2026 року.

Публікації охоплюють основні теоретичні та прикладні результати роботи і дозволяють однозначно ідентифікувати авторський внесок здобувача. Повнота висвітлення результатів у публікаціях відповідає вимогам до кваліфікаційних наукових робіт.

**6. Зауваження та рекомендації**

Основні зауваження до дисертаційної роботи стосуються не актуальності теми, наукової новизни, аспектів реалізації запропонованих криптосистем в паралельної моделі обчислень, а саме рекомендацій щодо повноти та строгості оцінювання криптографічної стійкості запропонованого сімейства алгоритмів.

1. При аналізі стійкості нових шифрів до криптоаналізу у роботі значну роль відведено NIST STS, аналізу ентропії, лавинному ефекту, рівномірності

розподілу байтів, кореляціям між відкритим і зашифрованим текстом та чутливості до зміни ключа. Такі перевірки є необхідними, проте не достатніми умовами доведення стійкості до сучасного криптоаналізу. Статистична випадковість шифртексту не замінює аналізу диференціальних характеристик, лінійних апроксимацій, алгебраїчних властивостей S-блоків, атак з вибраним відкритим текстом, пов'язаних ключів, інтегральних, атак типу «бумеранг», «meet-in-the-middle», «biclique», «invariant-subspace», SAT/MILP- та інших структурних атак. Тому у висновках слід чітко розмежувати «статистичну псевдовипадковість шифртексту» і «доведену або переконливо оцінену криптографічну стійкість».

2. Для алгоритму WBC1 та його базових паралельних модифікацій ключові операції фактично зводяться до перестановок і циклічних зсувів. Такі перетворення самі по собі є лінійними або «майже лінійними» над GF(2) і не забезпечують повноцінної нелінійності, характерної для сучасних блокових шифрів. У разі фіксованого ключа результат може бути еквівалентний певній глобальній перестановці бітів. У роботі недостатньо розглянуто можливість відновлення такої еквівалентної перестановки за допомогою атак з вибраним відкритим текстом.

3. При аналізі стійкості до диференціального та лінійного криптоаналізу не наведено таблиць різниць (DDT) та лінійних апроксимацій (LAT), оцінок максимальної диференціальної імовірності, лінійного зміщення, числа активних S-блоків у декількох раундах, а також формальних меж для диференціальних та лінійних характеристик.

4. У WBC2/PWBC2 використано ключезалежні S-блоки, що є сильнішим криптографічним механізмом порівняно з WBC1. Проте сам факт генерації S-box із ключа не гарантує її криптографічної якості. У дисертації доцільно було б навести для згенерованих S-блоків показники нелінійності, диференціальної рівномірності, алгебраїчного ступеня, кількості фіксованих точок, властивості

SAC/BIC, розподіли DDT/LAT, а також оцінити ймовірність появи слабких S-блоків для різних ключів.

5. Кількість раундів алгоритмів (6) суттєво менша, ніж у загальновизнаних стандартах (AES — 10–14, «Калина» — 10–18 раундів). Рекомендується навести більш детальне теоретичне обґрунтування достатності такої кількості раундів, зокрема оцінки числа активних нелінійних компонент.

6. Проведений аналіз стійкості до атак з відомим або вибраним відкритим текстом не є достатнім, оскільки необхідно оцінити, скільки пар «відкритий текст - шифртекст» потрібно для відновлення еквівалентного ключа, відновлення S-box, відновлення таблиці операцій або побудови розрізнювача від випадкової перестановки. Також недостатньо розкрито питання стійкості до атак із пов'язаними ключами та слабкими ключами. Для алгоритмів, які допускають блоки 32, 64, 128, 256 та 512 біт, у роботі не визначено чітких обмежень щодо обсягу даних, який можна безпечно шифрувати одним ключем (використання 32-бітних і 64-бітних блоків у сучасних системах має серйозні birthday-обмеження і не може рекомендуватися для великих масивів даних). У дисертації описано підтримку режимів ECB, CBC, CFB, OFB, CTR та WBC-CTR-HMAC. Однак для режимів роботи недостатньо розглянуто питання misuse-resistance, унікальності nonce/IV, повторного використання ключів, автентифікованого шифрування та меж безпеки при обробці великих обсягів даних. Недостатньо повно розглянуті атаки, спрямовані на реалізацію, особливо для атак, специфічних для паралельної моделі обчислень (таймінг, кешові ефекти, особливості доступу до пам'яті, залишкові дані в пам'яті пристрою, ризики multi-tenant середовищ, помилки синхронізації та копіювання між host/device, тощо). Також бажано більш детально розглянути питання криптостійкості алгоритмів у постквантовій моделі загроз.

7. Порівняння продуктивності з AES та «Калиною» здійснюється на різних апаратних платформах. Рекомендується явно фіксувати це застереження і

по можливості навести порівняння в однаковій апаратній конфігурації. Також зауважимо, що порівняння з AES, «Калиною» та іншими відомими алгоритмами повинно виконуватися не лише за швидкодією і простором ключів, а і за результатами комплексного криптоаналітичного порівняльного аналізу.

Вважаю, що вказані зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на позитивну оцінку дисертаційної роботи.

**7. Рекомендації щодо впровадження результатів дослідження**

Результати дисертації доцільно використовувати у науково-дослідних роботах з паралельної криптографії, у навчальному процесі підготовки фахівців з прикладної математики, криптографії, кібербезпеки та високопродуктивних обчислень, а також як експериментальну платформу для дослідження нових перестановочних і S-box-орієнтованих конструкцій.

Разом з тим впровадження запропонованих алгоритмів у системи, де вимагається високий рівень криптографічної стійкості, має здійснюватися після завершення повного комплексу досліджень з криптографічної стійкості алгоритмів.

**8. Висновок**

Вважаю, що дисертаційна робота Баранова Ігоря Анатолійовича на тему «Паралельні алгоритми симетричної криптографії», подана на здобуття ступеня доктора філософії за спеціальністю 113 «Прикладна математика», є завершеним самостійним науковим дослідженням, у якому отримано нові науково обґрунтовані результати, що мають важливе теоретичне та практичне значення для розвитку сучасної криптографії, методів паралельних обчислень та інформаційної безпеки. Робота не порушує принципів академічної доброчесності, а її автор продемонстрував наукову зрілість та обізнаність в області прикладної математики. Дисертація за актуальністю, практичною

цінністю та науковою новизною відповідає вимогам чинного законодавства України, а саме постанови № 44 Кабінету Міністрів України від 12 січня 2022 р. «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії». Здобувач Баранов Ігор Анатолійович заслуговує на присудження йому наукового ступеня доктора філософії у галузі знань 11 «Математика та статистика» за спеціальністю 113 «Прикладна математика».

Офіційний опонент:
професор кафедри
Математичних методів захисту інформації
Навчально-наукового
фізико-технічного інституту
НТУУ «Київський політехнічний інститут
імені Ігоря Сікорського»,
член-кореспондент НАН України
Кудін Антон Михайлович

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"
Відділ кадрів і архівної справи № 6

30.06.2026

Підпис гр. Кудіна А. М.
ЗАСВІДЧУЮ
Відділ кадрів
підпис (прізвище)