

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U004706

Особливі позначки: відкрита

Дата реєстрації: 20-08-2026

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу:



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Баранов Ігор Анатолійович

2. Igor Baranov

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 113

Назва наукової спеціальності: Прикладна математика

Галузь / галузі знань: математика та статистика

Освітньо-наукова програма зі спеціальності: Прикладна математика

Дата захисту: 12-08-2026

Спеціальність за освітою: Програмне забезпечення автоматизованих систем

Місце роботи здобувача: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, Київ, 03187, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 14597

Повне найменування юридичної особи: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, Київ, 03187, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, Київ, 03187, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 28.31.01, 28.31.03

Тема дисертації:

1. Паралельні алгоритми симетричної криптографії
2. Parallel Algorithms of Symmetric Cryptography

Реферат/анотація:

1. Стрімкий розвиток інформаційних технологій, зростання обсягів даних, що передаються та зберігаються, а також поява квантових обчислювальних систем зумовлюють підвищені вимоги до криптографічних алгоритмів захисту інформації. Це визначає актуальність розробки нових блочних симетричних алгоритмів, архітектурно орієнтованих на паралельні обчислювальні платформи класу MIMD з підтримкою MPI та GPU. Дисертаційна робота присвячена розробці та дослідженню нових блочних симетричних криптографічних алгоритмів, в тому числі для паралельних комп'ютерів, що базуються на оригінальних криптографічних перетвореннях типу "кубик Рубіка" з ключозалежним вибором операцій. Основна увага приділялася підвищенню продуктивності за рахунок розпаралелювання обчислень, в тому числі на багатоядерних процесорах (з використанням MPI) та графічних прискорювачах (CUDA), а також покращенню криптографічної стійкості шляхом ускладнення внутрішньої структури алгоритмів. У роботі вперше

розроблено блочний симетричний криптографічний алгоритм WBC1 на основі обертань кубика Рубіка, у якому шифрування реалізується через тривимірні перестановки та циклічні побітові зсуви. Такий підхід забезпечує високий рівень дифузії, нелінійності та значний простір перестановок, що підвищує стійкість алгоритму до brute-force, диференціального та лінійного криптоаналізу. Вперше розроблено модифікацію алгоритму WBC2, у якій використано ключезалежні таблиці перестановок, динамічну S-box та раундові ключі. Це дозволило підвищити лавинний ефект, збільшити ентропію шифртексту та забезпечити додаткову стійкість у white-box моделі. Вперше розроблено паралельні модифікації блочно-симетричних криптографічних алгоритмів PWBC1, PWBC1.1, PWBC2 та PWBC2.1 для багатоядерних систем, а також GPU-орієнтовану реалізацію PWBCcuda. Запропонований підхід забезпечує незалежну паралельну обробку блоків даних, ефективне масштабування в MPI- та CUDA-середовищах і дозволяє поєднати високий рівень криптографічної стійкості з підвищеною продуктивністю при обробці великих обсягів інформації. В ході дослідження розроблено програмні реалізації всіх алгоритмів мовами Python та C/C++ з використанням технологій MPI і CUDA. Реалізації протестовано та апробовано на суперкомп'ютерному кластері SKIT-5 Інституту кібернетики НАН України. Запропоновані алгоритми забезпечують високий рівень криптографічної стійкості, підтверджений статистичними тестами, аналізом ентропії, лавинного ефекту та тестуванням NIST STS. Розроблені алгоритми можуть бути застосовані для захисту мультимедійних даних, шифрування у блокчейн-системах, системах обробки великих даних та інших задачах, що потребують високопродуктивного шифрування у паралельних і GPU-орієнтованих середовищах, а також можуть бути впроваджені в навчальний процес.

2. The rapid development of information technologies, the growing volume of transmitted and stored data, and the emergence of quantum computing systems impose increasing requirements on cryptographic algorithms for information protection. This determines the relevance of developing new block symmetric algorithms architecturally oriented toward parallel computing platforms of the MIMD class with MPI and GPU support. The dissertation is devoted to the development and investigation of new block symmetric cryptographic algorithms, including algorithms for parallel computers, based on original “Rubik’s Cube”-type cryptographic transformations with key-dependent operation selection. The main focus was placed on increasing performance through parallelization of computations, including on multi-core processors (using MPI) and graphics accelerators (CUDA), as well as on improving cryptographic strength by increasing the complexity of the internal algorithmic structure. Within the framework of this work, the block symmetric cryptographic algorithm WBC1 was developed for the first time. The algorithm is based on Rubik’s Cube rotations, where encryption is implemented through three-dimensional permutations and cyclic bitwise shifts. Such an approach provides a high level of diffusion, nonlinearity, and a large permutation space, thereby increasing resistance against brute-force, differential, and linear cryptanalysis attacks. For the first time, a modification of the algorithm, WBC2, was developed, incorporating key-dependent permutation tables, a dynamic S-box, and round keys. This made it possible to improve the avalanche effect, increase ciphertext entropy, and provide additional resistance in the white-box model. Furthermore, parallel modifications of the block symmetric cryptographic algorithms PWBC1, PWBC1.1, PWBC2, and PWBC2.1 for multi-core systems, as well as the GPU-oriented implementation PWBCcuda, were developed for the first time. The proposed approach ensures independent parallel processing of data blocks, efficient scalability in MPI and CUDA environments, and enables the combination of high cryptographic strength with increased performance when processing large volumes of information. During the research, software implementations of all algorithms were developed in Python and C/C++ using MPI and CUDA technologies. The implementations were tested and validated on the SKIT-5 supercomputer cluster of the V.M. Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine. The proposed algorithms provide a high level of cryptographic strength confirmed by statistical testing, entropy analysis, avalanche effect analysis, and NIST STS testing. The developed algorithms can be applied to the protection of multimedia data, encryption in blockchain systems, big data processing systems, and other applications requiring high-performance encryption in parallel and GPU-oriented environments. In addition, the developed algorithms and their implementations can be integrated into the educational process for teaching modern cryptographic protection methods and parallel

computing technologies.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Баранов І.А. Параллельный алгоритм PWBC1. Компьютерная математика. 2010. № 2. С. 96–101.
- Баранов І.А. Криптографічний аналіз складності симетричного блочного алгоритму WBC1. Кібернетика та комп'ютерні технології. 2025. № 1. С. 64–73.
- Баранов І.А. Криптографічний аналіз складності та апробація симетричного блочного алгоритму WBC2. Кібернетика та комп'ютерні технології. 2026. № 1. С. 94–107.
- Баранов І.А. Некоторые подходы к эффективной реализации блочных матричных алгоритмов на MIMD – компьютерах. Проблемы програмування. 2008. №3. С. 103–110.
- Baranov I. Implementations of Block Symmetric Cryptography Algorithm WBC1 for Computers with Parallel Architecture. Lecture Notes in Networks and Systems. Springer, Cham. 2025. Vol 1426. P. 291–305.

Наукова (науково-технічна) продукція: методи, теорії, гіпотези; програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість: забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Планується до впровадження

Зв'язок з науковими темами: 0122U200449, 0123U101573, 0124U003282

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Хіміч Олександр Миколайович

2. Oleksandr M. Khimich

Кваліфікація: д.ф.-м.н., професор, академік НАН України, 01.05.02

Ідентифікатор ORCID ID: 0000-0002-8103-4223

Додаткова інформація: <https://www.scopus.com/authid/detail.uri?authorId=6602740665>

Повне найменування юридичної особи: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, Київ, 03187, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Кудін Антон Михайлович

2. Антон М. Кудін

Кваліфікація: д.т.н., професор, член-кор. НАН України, 05.13.21

Ідентифікатор ORCID ID: 0000-0002-3966-6489

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Корченко Олександр Григорович

2. Oleksandr Korchenko

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: 0000-0003-3376-0631

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Ходзінський Олександр Миколайович

2. Oleksandr Khodzinskyi

Кваліфікація: к. ф.-м. н., старший науковий співробітник, 01.05.01

Ідентифікатор ORCID ID: 0000-0003-4574-3628

Додаткова інформація:

Повне найменування юридичної особи: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, Київ, 03187, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Швідченко Інна Віталіївна

2. Inna V. Shvidchenko

Кваліфікація: к. ф.-м. н., с.н.с., 01.05.01

Ідентифікатор ORCID ID: 0000-0002-5434-2845

Додаткова інформація: <https://www.scopus.com/authid/detail.uri?authorId=23394005400>

Повне найменування юридичної особи: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, Київ, 03187, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

VIII. Заключні відомості

**Власне Прізвище Ім'я По-батькові
голови ради**

Задірака Валерій Костянтинович

**Власне Прізвище Ім'я По-батькові
головуючого на засіданні**

Задірака Валерій Костянтинович

**Відповідальний за підготовку
облікових документів**

Стовба Віктор Олександрович

Реєстратор

Юрченко Тетяна Анатоліївна

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**



Юрченко Тетяна Анатоліївна