

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U004237

Особливі позначки: відкрита

Дата реєстрації: 03-08-2026

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: № НСВС/67/26 від 29.09.2026



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Якимчук Олексій Петрович

2. Oleksii Yakymchuk

Кваліфікація:

Ідентифікатор ORCID ID: 0009-0000-6911-0708

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: 08-09-2026

Спеціальність за освітою: Прикладна математика

Місце роботи здобувача: Товариство з обмеженою відповідальністю "Сіменс Медицина"

Код за ЄДРПОУ: 40321110

Місцезнаходження: вул. Миколи Грінченка, Київ, 03038, Україна

Форма власності: Приватна/недержавна

Сфера управління:

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 16666

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

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

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

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 28.31.01

Тема дисертації:

1. Методи формалізованого оцінювання стійкості блокових шифрів до сучасних криптоаналітичних атак
2. Security formalized evaluation methods of block ciphers against modern cryptanalytic attacks

Реферат/анотація:

1. Якимчук О. П. Методи формалізованого оцінювання стійкості блокових шифрів до сучасних криптоаналітичних атак. — Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 113 Прикладна математика (галузь знань 11 Математика та статистика). — НТУУ «Київський політехнічний інститут імені Ігоря Сікорського», Київ, 2026. Диференціальний криптоаналіз — один з основних методів аналізу стійкості симетричних примітивів, а стійкість до нього є ключовою вимогою до сучасних блокових шифрів. Підходи на основі усічених диференціалів розроблені для слово-орієнтованих шифрів, але недостатньо для біт-орієнтованих шифрів легковагової криптографії. Для немарковських структур, на відміну від марковських, відомі методи оцінювання верхніх меж ймовірностей диференціалів неінформативні. Метою дисертаційної роботи є уточнення та аналіз формалізованих методів диференціального криптоаналізу та методів оцінювання

стійкості симетричних шифрів до диференціального криптоаналізу, що дозволить розширити сферу його застосування на нові класи блокових шифрів для різних прикладних задач. У першому розділі окреслено місце блокових шифрів серед примітивів систем захисту інформації. Розглянуто блокчейн-технології, де стійкість геш-функцій є критичною, а методи криптоаналізу блокових шифрів і геш-функцій взаємно застосовні. Проаналізовано відомі результати диференціального криптоаналізу, підходи усіченого криптоаналізу до реальних шифрів та методи оцінювання верхніх меж ймовірностей диференціалів. У другому розділі запропоновано формалізований підхід до усіченого диференціального криптоаналізу на основі трійкових шаблонів різниць. Введено параметри стійкості та досліджено їхні алгебраїчні властивості. Підхід дозволяє описувати усічені диференціали, переходи між різницями у біт-орієнтованих шифрах та їх ймовірнісні характеристики. Проаналізовано поширення шаблонів через компоненти раундових перетворень; підхід продемонстровано на модельних і реальних шифрах. У третьому розділі запропоновано аналітичні алгоритмічні методи побудови оцінок верхніх меж ймовірностей диференціалів для немарковських слово-орієнтованих фейстель-подібних шифрів. Для схеми Фейстеля, L-схеми та R-схеми отримано рекурентні формули обчислення матриці верхніх меж ймовірностей та відповідні алгоритми. Проведено експериментальні дослідження та порівняльний аналіз оцінок для модельних шифрів. Наукова новизна отриманих результатів полягає в розвитку методів формального оцінювання стійкості симетричних блокових шифрів до диференціального криптоаналізу, зокрема, в уточненні формалізованих методів аналізу усічених диференціалів для біт-орієнтованих блокових шифрів та побудові аналітичних алгоритмічних методів оцінки ймовірностей диференціалів для немарковських криптографічних схем з фейстель-подібною структурою. 1) Запропоновано формалізований підхід до опису усічених диференціалів, зокрема, у біт-орієнтованих блокових шифрах, на основі трійкових шаблонів різниць, який дозволяє описувати переходи між класами різниць та досліджувати їх ймовірнісні характеристики. 2) Вперше запропоновано параметр, який дозволяє обґрунтовувати нестійкість біт-орієнтованих шифрів до усіченого диференціального криптоаналізу. 3) Вперше запропоновано алгоритмічні методи побудови та обчислення оцінок стійкості до диференціального криптоаналізу для немарковських L-схеми та R-схеми блокового шифрування. Показано, що запропоновані методи дозволяють одержувати кращі оцінки стійкості, ніж відомі теоретичні аналоги. 4) Уточнено алгоритмічні методи побудови та обчислення матриць оцінок стійкості до диференціального криптоаналізу для немарковських схем Фейстеля. Практичне значення одержаних результатів полягає в можливості застосування розроблених методів для аналізу криптографічної стійкості сучасних блокових шифрів до диференціального криптоаналізу. Результати дисертаційного дослідження дозволяють розширити можливості застосування диференціального криптоаналізу на основі усічених диференціалів, зокрема, для оцінювання криптографічної стійкості біт-орієнтованих блокових шифрів. Окрім цього, одержані результати дозволяють покращувати існуючі оцінки верхніх меж ймовірностей диференціалів для немарковських слово-орієнтованих фейстель-подібних шифрів, що суттєво розширює клас блокових шифрів із обґрунтованою криптографічною стійкістю, придатних для практичного використання. Запропоновані методи можуть бути використані при аналізі та проектуванні нових симетричних криптографічних примітивів, а також при оцінюванні стійкості існуючих блокових шифрів до сучасних криптоаналітичних атак. Ключові слова: криптографічний захист інформації, симетрична криптографія, блокові шифри, криптографічний алгоритм, легковагова криптографія, диференціальний криптоаналіз, криптографічна стійкість, обґрунтування стійкості, аналіз стійкості, усічені диференціали, Фейстель-подібні схеми, L-схема, R-схема, блокчейн, кібербезпека

2. Yakymchuk O. Security formalized evaluation methods of block ciphers against modern cryptanalytic attacks. — Qualifying scientific work, the manuscript. Dissertation for obtaining the degree of Doctor of Philosophy in specialty 113 Applied Mathematics (field of knowledge 11 Mathematics and Statistics). — Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, 2026. Differential cryptanalysis is a main method for analyzing symmetric-cipher security and a key requirement for modern block ciphers. Truncated-differential approaches are developed for word-oriented ciphers but insufficient for bit-oriented lightweight ones; for non-Markov structures, existing methods for estimating upper bounds on differential probabilities are uninformative. The aim of the dissertation is:

to develop a formalized approach to truncated differential cryptanalysis, in particular for bit-oriented ciphers, and to demonstrate the possibility of practical application of the developed approach; to develop efficient algorithmic approaches for calculating upper bounds on differential probabilities for non-Markov ciphers with Feistel-like structure, and to compare the results of applying the developed algorithms to ciphers of different structures and with different components of round function. The first chapter outlines the place of block ciphers among the primitives of modern security systems, including blockchain, where hash function security is critical and tied to block cipher cryptanalysis. It reviews known results in differential and truncated differential cryptanalysis of real ciphers and methods for estimating upper bounds on differential probabilities for Markov and non-Markov ciphers. The second chapter develops a formalized approach based on difference ternary patterns; security parameters are introduced and their algebraic properties studied. It describes truncated differences and transitions between them in bit-oriented ciphers and their probability metrics, analyzes propagation through round-transformation components and the branch-and-bound method, and is demonstrated on real ciphers. The third chapter develops analytical algorithmic methods for estimating upper bounds on differential probabilities of non-Markov Feistel-like ciphers. For the Feistel, L- and R-schemes, structures are analyzed and recurrence formulas and algorithms constructed for the matrix of upper bounds. Model ciphers of different structures are built and compared. The scientific novelty of the obtained results consists of the development of formalized methods for the truncated differential cryptanalysis for bit-oriented block ciphers and in the construction of analytical algorithmic methods for evaluating differential probabilities for non-Markov cryptographic schemes with Feistel-like structure. 1) A formalized approach to describing truncated differentials, in particular in bit-oriented block ciphers, based on ternary difference patterns was proposed; it allows transitions between classes of differences to be described and their probability characteristics to be studied. 2) For the first time, a parameter was proposed that makes it possible to justify the insecurity of bit-oriented ciphers against truncated differential cryptanalysis. 3) For the first time, algorithmic methods have been proposed for constructing and computing estimates of security against differential cryptanalysis for the non-Markov L-scheme and R-scheme of block ciphers. It is shown that the proposed methods yield better security estimates than the known theoretical analogues. 4) Algorithmic methods for constructing and computing matrices of estimates of security against differential cryptanalysis for non-Markov Feistel schemes were refined. The practical significance of the obtained results lies in the possibility of applying the developed methods to analyze the cryptographic security of modern block ciphers against differential cryptanalysis. The proposed approaches expand the possibilities of applying differential cryptanalysis based on truncated differentials, in particular enabling its application to bit-oriented block ciphers. In addition, the developed algorithms make it possible to improve existing estimates of upper bounds on differential probabilities for non-Markov Feistel-like ciphers. And this enables a more accurate evaluation of the theoretical security of such ciphers against differential cryptanalysis. The developed algorithms can be used in the study and design of new symmetric cryptographic primitives, as well as in evaluating the security of existing block ciphers against modern cryptanalytic attacks. Keywords: cryptographic information security, symmetric cryptography, block ciphers, cryptographic algorithm, lightweight cryptography, differential cryptanalysis, cryptographic security, security justification, security analysis, truncated differentials, Feistel-like schemes, L-Feistel scheme, R-Feistel scheme, blockchain, cybersecurity

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:

- Yakymchuk O., Yakovliev S. One Formalized Approach to Truncated Differential Cryptanalysis of Block Ciphers. Tatra Mountains Mathematical Publications, vol. 87, no. 2, Slovak Academy of Sciences, 2024, pp. 43-54.
- Yakymchuk O., Medvedtskiy K. Application of Ternary Pattern-based Truncated Differential Cryptanalysis to Specific Block Ciphers. Theoretical and Applied Cybersecurity, vol. 6, no. 2, 2024, pp. 16-24.
- Yakymchuk O., Lopatetskiy M. Method of Security Evaluation of the LBlock-like Ciphers against Differential Cryptanalysis. Theoretical and Applied Cybersecurity, vol. 7, no.2, 2025, pp. 13-23.
- S. Yakovliev, Y. Dobronohov and O. Yakymchuk. A Method of Security Evaluation of Non-Markov Feistel Networks Against Differential Cryptanalysis, 2024 IEEE 5th International Conference on Advanced Trends in Information Theory (ATIT), Lviv, Ukraine, 2024, pp. 240-246.
- Yakymchuk O., Yakovliev S. On a formalized approach to truncated differential cryptanalysis of block ciphers. Central European Conference on Cryptology CECC '22, Smolenice, Slovakia. Mathematical institute of Slovak academy of sciences, 2022. pp. 104-106.
- Медведцький К. А., Якимчук О. П. Аналіз підходів до пошуку високоїмовірнісних усічених диференціалів спеціального вигляду. Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XXII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених, Київ, Україна, 13-17 трав. 2024. Київ : КПІ ім. Ігоря Сікорського, 2024. С. 224-227.
- Якимчук О. П., Медведцький К. А. Пошук усічених диференціальних характеристик спеціального виду для шифру LBlock. Theoretical and Applied Cybersecurity: Матеріали II Всеукраїнської науково-практичної конференції (TACS-2024). Київ, 2024. С. 98-101.
- Лопатецький М. В., Якимчук О. П. Оцінка стійкості модифікації шифру LBlock до диференціального криптоаналізу. Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XXIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених, Київ, Україна, 14-17 трав. 2025. Київ : КПІ ім. Ігоря Сікорського, 2025. С. 447-450.

Наукова (науково-технічна) продукція: методи, теорії, гіпотези

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Яковлев Сергій Володимирович
2. Serhii Yakovliev

Кваліфікація: к. т. н., 05.13.21

Ідентифікатор ORCID ID: 0000-0002-5647-5043

Додаткова інформація: <https://scholar.google.com/citations?hl=uk&user=40BUMd0AAAAJ>

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Родінко Марія Юріївна

2. Mariia Rodinko

Кваліфікація: д.філософ, 122

Ідентифікатор ORCID ID: 0000-0003-4692-9811

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Чевардін Владислав Євгенович

2. Vladyslav Chevardin

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

Ідентифікатор ORCID ID: 0000-0002-1070-4568

Додаткова інформація:

Повне найменування юридичної особи: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Код за ЄДРПОУ: 24978555

Місцезнаходження: вул. Московська, Київ, 01011, Україна

Форма власності: Державна

Сфера управління: Міністерство оборони України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Конюшок Сергій Миколайович

2. Serhii Koniushok

Кваліфікація: к. т. н., доцент, 05.13.21

Ідентифікатор ORCID ID: 0000-0003-4121-1464

Додаткова інформація: <https://scholar.google.com/citations?user=Pr75GyMAAAAJ&hl=uk>

Повне найменування юридичної особи: Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 34979237

Місцезнаходження: вул. Верхньоключова, буд. 4, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Державна служба спеціального зв'язку та захисту інформації України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Фесенко Андрій В'ячеславович

2. Andriy Fsenko

Кваліфікація: к. ф.-м. н., 01.05.01

Ідентифікатор ORCID ID: 000-0002-4489-3256

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

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові
голови ради

Олексійчук Антон Миколайович

Власне Прізвище Ім'я По-батькові
головуючого на засіданні

Олексійчук Антон Миколайович

Відповідальний за підготовку
облікових документів

Якимчук Олексій Петрович

Реєстратор

Юрченко Тетяна Анатоліївна

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



Юрченко Тетяна Анатоліївна