

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U002531

Особливі позначки: відкрита

Дата реєстрації: 15-06-2026

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: № НСВС/35/25 від 20 травня 2026 року



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Нікольський Сергій Сергійович

2. Serhii S. Nikolskyi

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 123

Назва наукової спеціальності: Комп'ютерна інженерія

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерна інженерія

Дата захисту: 10-07-2026

Спеціальність за освітою: Комп'ютерна інженерія

Місце роботи здобувача: 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

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 14191

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: 20.55.01

Тема дисертації:

1. Методи прискорення комп'ютерної реалізації криптографічних механізмів захисту даних на основі алгебри полів Галуа
2. Methods for acceleration of data protection cryptographic mechanisms based on the algebra of Galois fields computer implementation

Реферат/анотація:

1. Мета і завдання дослідження. Мета дослідження полягає в прискоренні комп'ютерної реалізації експоненціювання на скінчених полях Галуа – базової операції сучасних механізмів криптографічного захисту інформації з відкритим ключем в системах дистанційного управління на базі технологій IoT. Для досягнення мети дослідження поставлено і вирішено такі задачі : 1. Аналіз використання криптографічних механізмів захисту даних, в яких використовується алгебра скінчених полів Галуа, обґрунтування критеріїв ефективності засобів обчислювальної реалізації базової операції над полями Галуа, що використовується в цих механізмах – експоненціювання над числами, довжина яких значно перевищує розрядність процесора; огляд, з позицій цих критеріїв існуючих методів та алгоритмів обчислення експоненти на полях Галуа,

визначення можливостей підвищення швидкодії її обчислювальної реалізації. 2. Теоретичне обґрунтування, розробка та дослідження методу прискореного експоненціювання, який організує обробку бітів коду експоненти в напрямку від старших до молодших групами по h розрядів, при цьому всі операції множення в рамках групи замінюються однією такою операцією з використанням передобчислень, що здійснюється перед кожним експоненціювання, а група з h операцій піднесення до квадрату замінюється на одну операцію піднесення в ступінь $2h$ з використанням передобчислень, яка виконуються при зміні утворюючого поліному поля Галуа, що дозволяє зменшити кількість мультиплікативних операцій. 3. Теоретичне обґрунтування, розробка та дослідження методу прискорення обчислення експоненти на полях Галуа за рахунок організації суміщення в часі виконання двох операцій на полі Галуа – піднесення до квадрату та множення на постійне число, за рахунок чого забезпечується прискорення виконання важливої для криптографічних застосувань операції обчислення експоненти. 4. Теоретичне обґрунтування, розробка та дослідження методу прискорення обчислення експоненти на полях Галуа шляхом організації обробки коду експоненти зі старших розрядів по групам, що складаються з одиниці та передуючим їй нулям і здійснюється для кожної з них у вигляді однієї суміщеної операції множення на полях Галуа з використанням передобчислень, за рахунок чого досягається зменшення кількості операцій множення і, відповідно, прискорення обчислення експоненти на полі Галуа. 5. Теоретичне обґрунтування, розробка та дослідження методу прискорення обчислення експоненти на полях Галуа шляхом організації паралельного обчислення експоненти на кінцевих полях Галуа, яка відрізняється тим, що в рамках кожного із k обчислювальних процесів здійснюється піднесення числа в ступінь, код якої містить n/k значущих бітів експоненти, розділених $k-1$ нульовими бітами, за рахунок чого кількість операцій множення і піднесення в ступінь двійки на полі Галуа зменшується в k раз. 6. Теоретичне обґрунтування, розробка та дослідження методу прискорення обчислення експоненти на полях Галуа шляхом організації паралельного обчислення експоненти на скінчених полях Галуа, яка відрізняється тим, що в рамках кожного із k обчислювальних процесів здійснюється піднесення числа в ступінь числа два з отриманням стартового значення для обчислення часткової експоненти, що містить в собі n/k суміжних розрядів коду експоненти, що дозволяє прискорити процес обчислення експоненти на полях Галуа в k раз. 7. Теоретичне обґрунтування, розробка та дослідження методу прискорення обчислення експоненти на полях Галуа шляхом організації паралельного обчислення експоненти на скінчених полях Галуа, яка відрізняється тим, що в кожному із паралельних процесів оброблюється група фрагментів коду експоненти для яких попередньо обраховано значення експонент-шаблонів, які підносять в ступінь двійки з застосуванням інших передобчислень, за рахунок чого досягається прискорення обчислення на багатоядерних процесорних платформах експоненти на полях Галуа. 8. Створення програмних засобів для експериментального дослідження ефективності запропонованих методів та підходів до прискорення реалізації базової для криптографічних протоколів операції експоненціювання на скінчених полях Галуа.

2. The goal and tasks of the research. The goal of the research is to accelerate the computer implementation of exponentiation on finite Galois fields - the basic operation of modern open key cryptographic mechanisms for data protection in system for remote control based on IoT technologies. To achieve the goal of the research, the following tasks were set and solved: 1. Analysis of the application of cryptographic data protection mechanisms, which use the algebra of finite Galois fields. Substantiation of the criteria for the effectiveness of means of computational implementation of the basic operation on Galois fields used in these mechanisms - exponentiation over numbers, the length of which significantly exceeds the processor's bit capacity; a review, from the standpoint of these criteria, of the existing methods and algorithms for calculating the exponent on Galois fields, determining the possibilities of increasing the speed of its computational implementation. 2. Theoretical justification, development and research of the method of accelerated exponentiation, which organizes the processing of code bits, exponents are processed in the direction from the highest to the lowest in groups of h digits, while all multiplication operations within the group are replaced by one such operation using recalculations, which is performed before each exponentiation, and a group of h operations of raising to the square is replaced by one operation of raising to the power of $2h$ using precomputations, which are performed when changing the forming

Galois polynomial field, which allows to reduce the number of multiplicative operations. 3. Theoretical substantiation, development and research of the method of speeding up the calculation of the exponent on Galois fields due to the organization of the combination in time of the execution of two operations on the finite Galois field - squaring and multiplication by a constant number, due to which the acceleration of important for cryptographic applications operation of exponentiation on Galois fields is ensured. 4. Theoretical substantiation, development and research of the method of speeding up the calculation of the exponent on Galois fields by organizing the processing of the code of the exponent from the higher orders in groups consisting of a unit and the sequence of zeros, whose preceding it and carried out for each of them in the form of one combined operation of multiplication on Galois fields using precomputations, due to which a reduction in the number of multiplication operations and, accordingly, an acceleration of the calculation of the exponent on the finite Galois field is achieved. 5. Theoretical substantiation, development and research of the method of speeding up the calculation of the exponent on Galois fields by organizing the parallel calculation of the exponent on finite Galois fields, which is distinguished by the fact that within each of the k calculation processes, a number is raised to a power, the code of which contains n/k significant bits of the exponent, divided by $k-1$ zero bits, due to which the number of operations of multiplication and raising to the power of two on the Galois field is carried out decreases by k times. 6. Theoretical substantiation, development and research of the method of speeding up the calculation of the exponent on the Galois fields by organizing the parallel calculation of the exponent on the finite Galois fields, which is distinguished by the fact that within each of the k calculation processes, the number is raised to the power of two to obtain the starting value for the calculation of the partial exponent, which contains n/k adjacent digits of the exponent code, which allows to speed up the process of calculating the exponent on the fields Galois k times. 7. Theoretical substantiation, development and research of the method of speeding up the calculation of the exponent on Galois fields by organizing the parallel calculation of the exponent on finite Galois fields, which is distinguished by the fact that in each of the parallel processes a group of fragments of the exponent code is processed for which the value of the exponent templates, which are raised to the power of two using other recalculations, is pre-calculated, due to which the acceleration of the calculation on multi-core processor platforms of the exponent on Galois fields. 8. Creation of software tools for the experimental study of the effectiveness of the proposed methods and approaches to speeding up the implementation of the basic exponentiation operation for cryptographic protocols on finite Galois fields.

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:

- Верба О.А., Нікольський С.С., Метод експоненціювання на полях Галуа для швидкої реалізації криптографічного захисту в IoT, Проблеми інформатизації та управління 4(80), 21-31, 2025
- Марковський О.П., Нікольський С.С., Метод швидкого обчислення експоненти на полях галуа $gf(2^n)$ для криптографічних застосувань, Комп'ютерно-інтегровані технології: освіта, наука, виробництво, (58), 188-196, 2025
- Марковський О.П., Нікольський С.С., Метод розподіленого обчислення на багатоядерних процесорах експоненти на полях галуа для криптографічних застосувань, Проблеми інформатизації та управління 1(81), 59-71, 2025
- S.S. Nikolskiy, I.A. Klymenko, Designing tools for automated data collection for IoT road condition monitoring systems, "Chernihiv Polytechnic" Technical sciences and technologies 2(32), 210-223., 2023

- S.S. Nikolskiy, I.A. Klymenko, Design of data analysis means for IoT monitoring systems of the road surface condition Проблеми інформатизації та управління 1(73), 45-56, 2023
- S.S. Nikolskiy, I.A. Klymenko, Progressive IoT platform based on edge computing technology, Вісник Хмельницького Національного Університету, серія: технічні науки, 4(323), 219-225, 2023
- S.S. Nikolskiy, I.A. Klymenko, Embedded IoT platform for remote traffic control in smart city IoT infrastructure, Міжвідомчий науково-технічний збірник «Вимірювальна техніка та метрологія», 3(86), 2023
- А. В. Каплунов, А. Р. Гайдай, В. М. Гер, С. С. Нікольський Засоби моніторингу мережі в IoT інфраструктурі з гібридною архітектурою. Телекомунікаційні та інформаційні технології, 2, 2023.
- Нікольський С.С., Гуцуляк Н.А. Організація паралельного обчислення експоненти на полях Галуа для криптографічних застосувань. Тези XVIII- конференції “Прикладна математика та комп’ютинг” 19-21 листопада 2025 м.Київ.- С.87-93., 2025

Наукова (науково-технічна) продукція: технології

Соціально-економічна спрямованість: поліпшення якості життя та здоров'я населення, ефективності діагностики та лікування хворих; підвищення автоматизації виробничих процесів

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. Марковський Олександр Петрович
2. Oleksandr Markovskiy

Кваліфікація: к.т.н., доц., 05.13.05

Ідентифікатор ORCID ID: 0000-0003-3483-4233

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Певнев Володимир Яковлевич

2. Volodymyr Pevnev

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: 0000-0002-3949-3514

Додаткова інформація:

Повне найменування юридичної особи: Національний аерокосмічний університет "Харківський авіаційний інститут"

Код за ЄДРПОУ: 02066769

Місцезнаходження: вул. Манька Вадима, Харків, Харківський р-н., 61070, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Маслова Наталія Олександрівна

2. Nataliia Maslova

Кваліфікація: к.т.н., доц., 05.13.13

Ідентифікатор ORCID ID: 0000-0002-9078-0973

Додаткова інформація:

Повне найменування юридичної особи: Львівський державний університет безпеки життєдіяльності

Код за ЄДРПОУ: 08571340

Місцезнаходження: вул. Клепарівська, Львів, 79007, Україна

Форма власності: Державна

Сфера управління: Державна служба України з надзвичайних ситуацій

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Терейковський Ігор Анатолійович

2. Ihor A. Tereikovskiy

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

Ідентифікатор ORCID ID: 0000-0003-4621-9668

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. Волокита Артем Миколайович

2. Artem Volokyta

Кваліфікація: к.т.н., доц., 01.05.03

Ідентифікатор ORCID ID: 0000-0001-9069-5544

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

Дичка Іван Андрійович

Власне Прізвище Ім'я По-батькові
головуючого на засіданні

Дичка Іван Андрійович

Відповідальний за підготовку
облікових документів

Нікольський Сергій Сергійович

Реєстратор

Юрченко Тетяна Анатоліївна

Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності



Юрченко Тетяна Анатоліївна