Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U002880

Особливі позначки: відкрита

Дата реєстрації: 25-06-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Халявка Віктор Володимирович
2. Viktor V. Khaliavka

Кваліфікація:

Ідентифікатор ORCID ID: 0009-0009-0811-7282

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'ютерні системи та мережі

Дата захисту: 08-07-2026

Спеціальність за освітою: Автомобільний транспорт

Місце роботи здобувача: Черкаський науково-дослідний експертно-криміналістичний центр МВС України

Код за ЄДРПОУ: 25574009

Місцезнаходження: вул. Пастерівська, Черкаси, Черкаський р-н., 18009, Україна

Форма власності:

Сфера управління: Міністерство внутрішніх справ України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 14116

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

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

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.55.01, 20.56.01

Тема дисертації:

1. Методи вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для криптографічних застосувань у комп'ютерних системах і мережах

2. Methods for Selecting the Parameters of Finite Fields of Matrices of Order 2 and Their Primitive Elements for Cryptographic Applications in Computer Systems and Networks

Реферат:

1. Дисертацію присвячено розв'язанню актуального науково-прикладного завдання - розробленню методів вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для використання в криптографічних протоколах комп'ютерних систем і мереж. Актуальність роботи зумовлена зростанням обсягів електронної інформації, розвитком розподілених обчислювальних середовищ, хмарних сервісів, мобільних мереж, вбудованих систем та Інтернету речей, а також підвищенням вимог до криптографічної стійкості засобів захисту даних. У сучасній комп'ютерній криптографії скінченні поля є основою багатьох алгоритмів узгодження ключів, електронного цифрового підпису, шифрування та автентифікації. Водночас подальший розвиток криптографічних засобів потребує нових алгебраїчних конструкцій, які розширюють простір криптографічних параметрів без втрати математичної строгості. Одним із перспективних напрямів є використання матричних структур над простими полями, практична цінність яких визначається можливістю

конструктивного вибору параметрів матричного середовища та примітивних елементів. Об'єктом дослідження є процеси вибору параметрів скінченних полів матриць другого порядку та примітивних елементів у цих полях для криптографічного використання в комп'ютерних системах і мережах. Предметом дослідження є методи, моделі та алгоритми вибору параметрів таких полів, пошуку їх примітивних елементів і застосування отриманих результатів у протоколах узгодження ключів та електронного цифрового підпису. Метою дисертаційної роботи є підвищення криптографічної стійкості засобів захисту інформації за рахунок розроблення методів вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів. Для досягнення мети проаналізовано сучасний стан використання скінченних полів і матричних структур у криптографії; визначено умови практичного застосування матричних полів; розроблено метод вибору примітивних елементів; запропоновано метод одночасного вибору параметрів матричного поля та примітивного елемента; удосконалено реалізацію протоколів Діффі-Хеллмана та Ель-Гамаля шляхом перенесення операцій у матричне середовище; досліджено статистичні властивості й обчислювальну складність запропонованих рішень. У роботі показано, що повний перебір елементів скінченних полів матриць другого порядку є обчислювально витратним і малопридатним для практичних криптографічних застосувань. Тому розроблено метод вибору примітивних елементів, який ґрунтується на аналізі характеристик матриці-кандидата, її характеристичного полінома, умов досягнення максимального періоду та порядку визначника в базовому полі. Такий підхід дає змогу конструктивно формувати множину примітивних елементів без прямого перебору всіх можливих матриць. Запропоновано метод одночасного вибору параметрів матричного поля та примітивного елемента в ньому. На відміну від традиційного підходу, коли параметри поля фіксуються окремо від пошуку генератора, цей метод поєднує обидві процедури в єдиній конструктивній схемі. Він базується на властивостях квадратичних лишків і нелишків у простому полі, аналізі нерозкладності характеристичного полінома та врахуванні зв'язку між параметрами матриці й властивостями її власних значень. Наукова новизна полягає в тому, що вперше розроблено та теоретично обґрунтовано методи вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для криптографічних застосувань у комп'ютерних системах і мережах. Запропоновано цілісний підхід, у межах якого задача вибору параметрів матричного поля поєднується із задачею вибору генератора його мультиплікативної групи. Представлено підходи до використання матричних алгебраїчних структур у протоколах узгодження ключів Діффі-Хеллмана та електронного цифрового підпису Ель-Гамаля. Практичне значення результатів полягає в можливості їх використання під час створення програмних і апаратних засобів криптографічного захисту інформації. Запропоновані алгоритмічні процедури дають змогу формувати параметри матричного поля та відповідні примітивні елементи для протоколів узгодження ключів, схем електронного цифрового підпису та інших механізмів, що базуються на складності дискретного логарифмування. Перенесення обчислень із класичного скалярного середовища до матричного розширює множину допустимих криптографічних параметрів і створює передумови для підвищення стійкості криптографічних засобів. Основні результати дисертаційної роботи оприлюднено в 5 наукових публікаціях, серед яких 2 статті у виданнях, що індексуються в Scopus та/або Web of Science, зокрема одна стаття у квартилі Q2, а також 3 доповіді на міжнародних науково-практичних конференціях.

2. The dissertation is devoted to solving a relevant scientific and applied problem: the development of methods for selecting the parameters of finite fields of matrices of order 2 and their primitive elements for use in cryptographic protocols of computer systems and networks. The relevance is determined by the growing volume of electronic information, the development of distributed computing environments, cloud services, mobile networks, embedded systems, and the Internet of Things, as well as by increasing requirements for the cryptographic strength of data protection means. In modern computer cryptography, finite fields constitute the basis of many key agreement, digital signature, encryption, and authentication algorithms. Further development of cryptographic means requires new algebraic constructions that expand the space of cryptographic parameters without loss of mathematical rigor. One promising direction is the use of matrix structures over prime fields, whose practical value is determined by the possibility of constructively selecting the parameters of the matrix environment and primitive elements. The object is the processes of selecting parameters of finite fields of matrices of order 2 and

primitive elements in these fields for cryptographic use in computer systems and networks. The subject is methods, models, and algorithms for selecting the parameters of such fields, finding their primitive elements, and applying the obtained results in key agreement protocols and digital signature schemes. The aim of the dissertation is to increase the cryptographic strength of information protection means by developing methods for selecting the parameters of finite fields of matrices of order 2 and their primitive elements. To achieve this aim, the current use of finite fields and matrix structures in cryptography was analyzed; the conditions for the practical application of matrix fields were determined; a method for selecting primitive elements was developed; a method for simultaneous selection of the matrix field parameters and a primitive element was proposed; the implementation of the Diffie-Hellman and ElGamal protocols was improved by transferring operations into the matrix environment; and the statistical properties and computational complexity of the solutions were studied. The dissertation shows that exhaustive enumeration of elements of finite fields of matrices of order 2 is computationally expensive and unsuitable for practical cryptographic applications. Therefore, a method for selecting primitive elements was developed based on analysis of the characteristics of a candidate matrix, its characteristic polynomial, the conditions for attaining the maximum period, and the order of the determinant in the base field. This approach makes it possible to constructively form the set of primitive elements without direct enumeration of all matrices. A method for simultaneous selection of the matrix field parameters and a primitive element in it is proposed. Unlike the traditional approach, in which field parameters are fixed separately from the search for a generator, this method combines both procedures within a single constructive scheme. It is based on the properties of quadratic residues and non-residues in a prime field, analysis of the irreducibility of the characteristic polynomial, and consideration of the relationship between matrix parameters and the properties of its eigenvalues. The scientific novelty lies in the fact that methods for selecting the parameters of finite fields of matrices of order 2 and their primitive elements for cryptographic applications in computer systems and networks have been developed and theoretically substantiated for the first time. An integral approach is proposed, in which the problem of selecting matrix field parameters is combined with the problem of selecting a generator of its multiplicative group. Approaches to the use of matrix algebraic structures in the Diffie-Hellman key agreement protocol and the ElGamal digital signature scheme are presented. The practical significance lies in their possible use in the development of software and hardware means for cryptographic information protection. The proposed algorithmic procedures make it possible to form matrix field parameters and corresponding primitive elements for key agreement protocols, digital signature schemes, and other mechanisms based on the difficulty of the discrete logarithm problem. Transferring computations from the classical scalar environment to the matrix one expands the set of admissible cryptographic parameters and creates prerequisites for increasing cryptographic strength. The main results of the dissertation have been published in 5 scientific publications, including 2 articles in journals indexed in Scopus and/or Web of Science, one of them in the Q2 quartile, as well as 3 papers presented at international scientific and practical conferences.

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:

- [1] A. Shcherba, E. Faure, T. Vartiainen, і V. Khaliavka, «Primitive Elements in the Finite Field of Square Matrices of Order 2 for Cryptographic Applications», Lecture Notes on Data Engineering and Communications Technologies, т. 222, Cham: Springer Nature Switzerland, 2024, С. 250–265. doi: 10.1007/978-3-031-71804-5_17.

- [2] A. Baikenov, E. Faure, A. Shcherba, V. Khaliavka, S. Tynymbayev, і O. Abramkina, «A Unified Method for Selecting Parameters and Primitive Elements in 2 × 2 Matrix Fields for Cryptographic Protocols», Symmetry, т. 17, вип. 8, 1212, 2025, doi: 10.3390/sym17081212.
- [3] Щерба А.І., Фауре Е.В., Халявка В.В. Примітивні елементи скінченного поля квадратних матриць порядку 2 для криптографічних застосувань // Тези доповідей VII Міжнародної науково-практичної конференції «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2024), (Черкаси, 23-24 травня 2024 р.) [Електронний ресурс]. Черкаси : ЧДТУ, 2024. С. 183-185. [Online]. Доступний за: https://er.chdtu.edu.ua/bitstream/ChSTU/5863/1/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA 2024_%D0%BC%D0%B0%D0%BA%D0%B5%D1%82.pdf#page=183
- [4] Фауре Е. В., Халявка В. В. Метод вибору примітивних елементів у полях матриць 2×2 для криптографічних протоколів // Збірник тез доповідей IV Міжнар. наук.-практич. конфер. «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2025)» (25 лист. 2025 р., м. Черкаси) [Електронний ресурс] / упоряд. : Т. О. Прокопенко, О. І. Підкуйко. М-во освіти і науки України, Черкас. держ. технол. ун-т. Черкаси : ЧДТУ, 2025. С. 273-275. [Online]. Доступний за: https://drive.google.com/file/d/1vfK7HzALRZHFTE8SKi6P_c-D3X4K3YPK/view
- [5] A. Baikenov, E. Faure, A. Shcherba, A. Lavdanskyi, S. Tynymbayev, V. Khaliavka, O. Abramkina. ElGamal Digital Signature Scheme in a Matrix Finite Field // 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), Paris, France, 2025. P. 1-6. DOI: 10.1109/ICECET63943.2025.11472340

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

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:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Фауре Еміль Віталійович
2. Emil V. Faure

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

Ідентифікатор ORCID ID: 0000-0002-2046-481X

Додаткова інформація:

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Одарченко Роман Сергійович

2. Roman S. Odarchenko

Кваліфікація: д. т. н., професор, 05.12.02

Ідентифікатор ORCID ID: 0000-0002-7130-1375

Додаткова інформація:

Повне найменування юридичної особи: Національний університет «Київський авіаційний інститут»

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Гарасимчук Олег Ігорович

2. Oleh I. Harasymchuk

Кваліфікація: к. т. н., доцент, 05.13.05

Ідентифікатор ORCID ID: 0000-0002-8742-8872

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Миронець Ірина Валеріївна

2. Iryna V. Myronets

Кваліфікація: к. т. н., доцент, 05.13.05

Ідентифікатор ORCID ID: 0000-0003-2007-9943

Додаткова інформація:

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Розломій Інна Олександрівна
2. Inna O. Rozlomii

Кваліфікація: к. т. н., доц., 05.13.05

Ідентифікатор ORCID ID: 0000-0001-5065-9004

Додаткова інформація:

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Бабенко Віра Григорівна
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Бабенко Віра Григорівна
Відповідальний за підготовку облікових документів	Здобувач PhD
Реєстратор	Юрченко Тетяна Анатоліївна
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна