Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U003342

Особливі позначки: відкрита

Дата реєстрації: 06-11-2024

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Бондаренко Микита Олегович
2. Mykyta Bondarenko

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0002-8849-7378

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп’ютерні науки

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: ОП 25599 Комп'ютерні науки та інформаційні технології

Дата захисту: 14-11-2024

Спеціальність за освітою: 122 Комп'ютерні науки

Місце роботи здобувача: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Харківська, буд. 116, Суми, Сумський р-н., 40007, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 6941

Повне найменування юридичної особи: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Харківська, буд. 116, Суми, Сумський р-н., 40007, 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: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Харківська, буд. 116, Суми, Сумський р-н., 40007, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Повне найменування юридичної особи: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Харківська, буд. 116, Суми, Сумський р-н., 40007, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Повне найменування юридичної особи: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Харківська, буд. 116, Суми, Сумський р-н., 40007, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56.01

Тема дисертації:

1. Моделі та методи інформаційної технології створення криптосистем на основі функцій дійсних змінних

2. Models and methods of information technology for a cryptosystem based on the functions of real variables

Реферат:

1. У дисертаційній роботі розв’язано важливе науково-практичне завдання розробки нових моделей та методів криптографічних систем на основі функцій дійсної змінної. Обґрунтовано актуальність теми дисертації, зазначено зв’язок роботи з науковими темами, сформульовано мету та задачі дослідження, визначено об’єкт, предмет та методи дослідження, показано наукову новизну та практичне значення отриманих результатів, апробацію результатів та їх висвітлення у публікаціях. Актуальність дослідження зумовлена комплексом факторів, що формують сучасні виклики у сфері інформаційної безпеки та криптографії, включаючи в потенційні обмеження існуючих криптосистем на основі цілих чисел, загрозу з боку квантових обчислень, та потребу в нових підходах до захисту різних типів даних. Об'єктом дослідження є процеси криптографічного захисту даних. Предметом досліджень є моделі, методи та алгоритми криптографічних систем на основі функцій дійсної змінної. Обрані методи дослідження базуються на принципах і методах криптографії, методах розпізнавання сигналів і функціях непропорційності. У роботі поставлено та вирішено наступні завдання: 1. Проведено аналіз сучасних криптографічних систем, їх переваг та недоліків. 2. Розроблено математичну модель криптосистем на основі функцій дійсної змінної. 3. Створено метод шифрування даних з використанням суми функцій дійсної змінної як симетричних ключів. 4. Розроблено метод дешифрування даних, які зашифровані за допомогою обчислення невідомих коефіцієнтів ключових функцій. 5. Адаптовано розроблені методи для шифрування та дешифрування зображень. 6. Розроблено алгоритм використання зображення як криптографічного ключа для шифрування інших зображень. 7. Створено програмну реалізацію розроблених криптосистем та проведено експериментальні дослідження їх ефективності. Практичне значення отриманих результатів полягає в розробці програмного забезпечення для реалізації запропонованих криптографічних алгоритмів. Це програмне забезпечення може бути використане як для подальших наукових досліджень, так і для практичного застосування в різних сферах, де потрібен високий рівень захисту даних. Наукова новизна полягає в тому, що 1. Удосконалено моделі та методи створення криптосистем на основі функцій дійсної змінної, що повинно збільшити крипостійкість. 2. Уперше розроблено метод використання інтегральних функцій непропорційності для дешифрування даних, що дозволяє використовувати в криптосистемі дискретні функції-ключі. 3. Уперше розроблено криптосистему, що поєднує шифрування за допомогою суми функцій дійсної змінної та шифрування за допомогою інтегральної функції непропорційності. Відбувається двох-етапне шифрування, при якому результат першого етапу шифрується ще раз, що суттєво ускладнює злам криптосистеми. 4. Удосконалено метод шифрування даних шляхом впровадження додаткового елементу перестановки функцій-ключів, що також підвищує криптостійкість системи. 5. Вперше розроблено криптосистему для захисту зображень, де інше довільне зображення використовується в якості криптографічного ключа, шляхом використання функцій інтегральної непропорційності. Це значно спрощує передачу ключа порівняно з передачею функцій-ключів в аналітичному вигляді. Це зображення легше непомітно передати приймальній стороні при використанні симетричних криптосистем. Крім того, зловмиснику складніше виявити зображення-ключ серед багатьох зображень, до яких він отримав доступ. 6. Експериментально продемонстровано високу криптостійкість розроблених методів шифрування до атак грубої сили через необхідність підбору значень ключа з високою точністю. Також продемонстровано високу здібність до декореляції значень шифротексту. Результати досліджень дисертаційної роботи доповідалися та обговорювалися на міжнародних науково-практичних конференціях. За темою дисертаційної роботи опубліковано 10 наукових праць, з них: 4 статті у наукових фахових виданнях України, з яких 2 включені до міжнародних наукометричних баз, та 4 публікації за матеріалами конференцій.

2. The dissertation solves an important scientific and practical task of developing new models and methods of cryptographic systems based on real variable functions. The relevance of the dissertation topic is substantiated, the connection of the work with scientific themes is indicated, the purpose and objectives of the research are formulated, the object, subject, and methods of research are defined, the scientific novelty and practical significance of the obtained results are shown, as well as the approbation of results and their coverage in publications. The relevance of the research is determined by a complex of factors that shape modern challenges in the field of information security and cryptography, including potential limitations of existing cryptosystems based on integers, the threat from quantum computing, and the need for new approaches to protecting different types of data. The object of the research is the processes of cryptographic data protection. The subject of the research is models, methods, and algorithms of cryptographic systems based on real variable functions. The chosen research methods are based on the principles and methods of cryptography, signal recognition methods, and disproportionality functions. The following tasks were set and solved in the work: 1. Analysis of modern cryptographic systems, their advantages and disadvantages. 2. Development of a mathematical model of a cryptosystem based on real variable functions. 3. Creation of a data encryption method using the sum of real variable functions as symmetric keys.4. Development of a method for decrypting data encrypted by calculating unknown coefficients of key functions. 5. Adaptation of the developed methods for encryption and decryption of images. 6. Development of an algorithm for using an image as a cryptographic key for encrypting other images. 7. Creation of a software implementation of the developed cryptosystems and conducting experimental studies of their effectiveness. The practical significance of the obtained results lies in the development of software for the implementation of the proposed cryptographic algorithms. This software can be used both for further scientific research and for practical application in various fields where a high level of data protection is required. The scientific novelty lies in the following: 1. Improved models and methods for creating cryptosystems based on real variable functions. 2. For the first time, a method of using integral disproportionality functions for data decryption has been implemented, which allows determining unknown coefficients in the sum of real variable functions. 3. For the first time, a cryptosystem has been developed that combines encryption using the sum of real variable functions and encryption using the integral disproportionality function. 4. The data encryption method has been improved by introducing an additional element of key function permutation. 5. For the first time, a cryptosystem for image protection has been developed, where another arbitrary image is used as a cryptographic key, using integral disproportionality functions. 6. High cryptographic resistance of the developed encryption methods to brute force attacks has been experimentally demonstrated, due to the need to select key values with high accuracy. High ability to decorrelate ciphertext values has also been demonstrated.

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:

- Avramenko V., Bondarenko M. Recognition of reference signals and determination of their weighting coefficients if an additive interference presents. Radio Electronics, Computer Science, Control, 2023. P. 73-82.
- Avramenko V., Bondarenko M. Encryption of messages by the sum of a real variable functions. Artificial intelligence, 2024. № 29. P. 10–19.
- Avramenko V. Bondarenko M. Encrypting images using the sum of the functions of a real variable. Transactions of Kremenchuk Mykhailo Ostrohradskyi National University, 2024. № 144(1). P. 140–147.
- Avramenko V., Bondarenko M. Image cryptosystem with image key using integral disproportion. Radioelectronic and Computer Systems, 2024. № 2(110). P. 147–159.

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

Соціально-економічна спрямованість: створення нових методів захисту даних

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Планується до впровадження

Зв'язок з науковими темами: 0118U006971

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Авраменко Віктор Васильович
2. Viktor Avramenko

Кваліфікація: к.т.н., доц., 05.13.01

Ідентифікатор ORCID ID: 0000-0003-3998-9031

Додаткова інформація:

Повне найменування юридичної особи: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Харківська, буд. 116, Суми, Сумський р-н., 40007, 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. Котух Євген Володимирович
2. Yevgen Kotukh

Кваліфікація: д. т. н., професор, 25.00.02

Ідентифікатор ORCID ID: 0000-0003-4997-620X

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Дніпровська політехніка"

Код за ЄДРПОУ: 02070743

Місцезнаходження: проспект Дмитра Яворницького, буд. 19, Дніпро, Дніпровський р-н., 49005, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Пєвнєв 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 ім. М. Є. Жуковського "Харківський авіаційний інститут"

Код за ЄДРПОУ: 02066769

Місцезнаходження: вул. Чкалова, буд. 17, Харків, Харківський р-н., 61070, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Москаленко В'ячеслав Васильович

2. Viacheslav Moskalenko

Кваліфікація: к. т. н., доц., 05.13.07

Ідентифікатор ORCID ID: 0000-0001-6275-9803

Додаткова інформація:

Повне найменування юридичної особи: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Харківська, буд. 116, Суми, Сумський р-н., 40007, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Бережна Ольга Володимирівна

2. Olha Berezhna

Кваліфікація: к. т. н., доц., 05.13.06

Ідентифікатор ORCID ID: 0000-0001-7105-1276

Додаткова інформація:

Повне найменування юридичної особи: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Харківська, буд. 116, Суми, Сумський р-н., 40007, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Довбиш Анатолій Степанович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Довбиш Анатолій Степанович
Відповідальний за підготовку облікових документів	Бойко Антон Олександрович
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна