Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U002957

Особливі позначки: відкрита

Дата реєстрації: 15-07-2025

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Скуцький Артем Борисович
2. Artem B. Skutskyi

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0002-8632-1176

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: 10-07-2025

Спеціальність за освітою: Комп'ютерна інженерія

Місце роботи здобувача: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, буд. 460, Черкаси, Черкаський р-н., 18006, 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 9326

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, буд. 460, 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, буд. 460, 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: 20.51.35, 20.53.23, 20.53.37, 20.55, 20.56.01

Тема дисертації:

1. Метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних

2. Method and models of a secure information exchange system with non-separable factorial fata coding

Реферат:

1. Дисертаційна робота А.Б. Скуцького "Метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних" представляє ключові аспекти дослідження, присвяченого розробці та вдосконаленню систем безпечного обміну інформацією в умовах зашумлених каналів зв'язку. Актуальність. Зростаючі обсяги передачі конфіденційних даних у відкритих каналах зв'язку вимагають постійного вдосконалення методів синхронізації та шифрування для запобігання несанкціонованому доступу, забезпечення цілісності та достовірності інформації. Особливу важливість набуває проблема синхронізації, коли сторонній вплив або атаки можуть призвести до збоїв у встановленні синхронізму. Об’єктом дослідження є процес захищеного передавання перестановок в умовах високої інтенсивності шуму в каналі зв’язку. Предметом дослідження є метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних. Метою дослідження є забезпечення захищеного інформаційного обміну в системах з нероздільним факторіальним кодуванням даних і зашумленим каналом

зв'язку. Що досягається шляхом подальшого розвитку математичної моделі та методу виявлення синхрокомбінації за невідомого початкового моменту приймання даних, а також створення імітаційних моделей системи для експериментальної оцінки теоретичних результатів. Наукова новизна отриманих результатів. – набув подальшого розвитку метод кадрової синхронізації нероздільних факторіальних кодів, що використовує як синхрокомбінацію перестановку чисел, яка має максимальне значення мінімальної відстані Хеммінга від її двійкового представлення до всіх її циклічних зсувів, а також кореляційну та мажоритарну обробку прийнятих фрагментів, де довжина фрагмента дорівнює довжині синхрокомбінації, який за рахунок використання ковзного вікна фіксованого розміру та врахування серії спрацювань підсистеми синхронізації дозволяє встановити кадрову синхронізацію приймальної та передавальної станцій системи інформаційного обміну за високої ймовірності бітової помилки та невідомого моменту початку приймання синхрокомбінацій передавача, забезпечуючи необхідні показники ймовірності правильної та хибної синхронізації; – набула подальшого розвитку математична модель процесу виявлення синхрокомбінації систем передавання інформації з нероздільним факторіальним кодуванням даних, що використовують кореляційну та мажоритарну обробку прийнятих фрагментів, яка за рахунок дослідження механізмів перетворення синхрокомбінації в її зсув в умовах застосування приймачем ковзного вікна фіксованого розміру дозволяє оцінити ймовірності правильної та хибної кадрової синхронізації. – вперше розроблено математичну модель скінченного поля квадратних матриць порядку 2 над скінченним полем простих чисел Zp, яка за рахунок збільшення порядку поля квадратних матриць до значення p^2, проте збереження порядку p поля Zp, в якому виконують операції перетворення, дозволяє підвищити стійкість криптографічних систем, які базуються на операціях у скінченому полі. Результати дисертаційної роботи підтверджують ефективність запропонованих рішень як у теоретичному, так і в експериментальному аспектах. Вони створюють підґрунтя для впровадження в практичні системи захищеного інформаційного обміну, формуючи наукову базу для подальшої розробки інтегрованих протоколів, що поєднують процеси шифрування, синхронізації та обробки даних у єдиній системі, адаптованій до роботи в умовах непередбачуваних завад та невідомого моменту початку передавання.

2. The dissertation by A.B. Skutskyi, " Method and Models of a Secure Information Exchange System with Non-Separable Factorial Data Coding" presents key aspects of research dedicated to developing and improving secure information exchange systems in noisy communication channels. Actuality. The increasing volumes of confidential data transmission over open communication channels demand continuous improvement of synchronization and encryption methods to prevent unauthorized access and ensure the integrity and authenticity of information. The problem of synchronization becomes particularly crucial when external interference or attacks can lead to failures in establishing synchronism. The object of the study is the process of secure permutation transmission under high-intensity noise in a communication channel. The subject of the study is the method and models of a secure information exchange system with inseparable factorial data encoding. The aim of the study is to ensure secure information exchange in systems with inseparable factorial data encoding and a noisy communication channel. This is achieved through the further development of a mathematical model and a method for detecting synchro-combinations when the initial data reception time is unknown, as well as the creation of system simulation models for experimental evaluation of theoretical results. Scientific novelty of the obtained results: • The frame synchronization method for inseparable factorial codes has been further developed. This method uses a permutation of numbers as a synchro-combination, which has the maximum minimum Hamming distance from its binary representation to all its cyclic shifts. It also incorporates correlation and majority processing of received fragments, where the fragment length equals the synchro-combination length. By employing a fixed-size sliding window and considering series of synchronization subsystem activations, this method allows for establishing frame synchronization between the receiving and transmitting stations of an information exchange system under high bit error probability and an unknown start time of synchro-combination reception by the transmitter, thus ensuring the required probabilities of correct and false synchronization. • The mathematical model of the synchro-combination detection process in information transmission systems using inseparable factorial data encoding has been further developed. This model utilizes correlation and majority processing of received fragments. By

investigating the mechanisms of synchro-combination transformation into its shift under the receiver's application of a fixed-size sliding window, it allows for estimating the probabilities of correct and false frame synchronization. • For the first time, a mathematical model of a finite field of square matrices of order 2 over a finite field of prime numbers Zp has been developed. By increasing the order of the field of square matrices to p^2, while maintaining the order p of the Zp field in which transformation operations are performed, this model enhances the robustness of cryptographic systems based on operations in a finite field. The results of the dissertation confirm the effectiveness of the proposed solutions in both theoretical and experimental aspects. They create a foundation for implementation in practical secure information exchange systems, forming a scientific basis for the further development of integrated protocols that combine encryption, synchronization, and data processing into a unified system adapted to operate under unpredictable interference and an unknown start time of transmission.

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:

- E. Faure, A. Baikenov, A. Skutskyi, D. Faure, і O. Abramkina, «Algorithms for reliable permutation transmission protocols in noisy communication channels», CEUR Workshop Proceedings, т. 3826, с. 40-49, 2024, doi: 10.5281/zenodo.15390412 (Scopus)
- E. Faure, A. Shcherba, A. Skutskyi, і A. Lavdanskyi, «A Finite Field of Square Matrices of Order 2», CEUR Workshop Proceedings, т. 3550, с. 306-312, 2023, doi: 10.5281/zenodo.15392022 (Scopus)
- E. Faure, A. Shcherba, A. Skutskyi, і A. Lavdanskyi, «A software model to generate permutation keys through a square matrix», Вісник Черкаського державного технологічного університету, т. 29, № 2, с. 10-23, 2024, doi: 10.62660/bcstu/2.2024.10
- E. Faure, A. Skutskyi, і A. Lavdanskyi, «Algorithms and simulation model for the synchronisation subsystem of the noise-resilient communication system based on permutations», Вісник Черкаського державного технологічного університету, т. 4, № 29, с. 62-74, 2024, doi: 10.62660/bcstu/4.2024.62
- A. Lavdanskyi, E. Faure, A. Skutskyi, і C. Bazilo, «Accelerating Operations on Permutations Using Graphics Processing Units», Lecture Notes on Data Engineering and Communications Technologie, т. 178, с. 3-12, 2023, doi: 10.1007/978-3-031-35467-0_1 (Scopus)
- A. Shcherba, E. Faure, A. Skutskyi, і O. Kharin, «Families of Square Commutative 2x2 Matrices», CEUR Workshop Proceedings, т. 3550, с. 289-296, 2023, doi: 10.5281/zenodo.15391901 (Scopus)
- А. О. Лавданський, Е.В. Фауре, С. Т. Тинимбаєв, і А. Б. Скуцький, «Система захищеного інформаційного обміну текстовими даними через радіоканал ISM-діапазону», Вісник Черкаського державного технологічного університету, т. 27, № 3, с. 41-48, 2022. doi: 10.24025/2306-4412.3.2022.267786
- Е. В. Фауре, А. Б. Скуцький, і А. О. Лавданський, «Імітаційна модель передавання текстових і аудіо повідомлень з використанням нероздільного факторіального кодування в середовищі Simulink», в Challenges and threats to critical infrastructure, Detroit, Michigan, USA: NGO Institute for Cyberspace Research, 2023, с. 244-246. [Online]. Режим доступу: https://er.chdtu.edu.ua/bitstream/ChSTU/4539/1/Monograph-09-06-2023-Faure2.pdf
- Е. В. Фауре, А. Б. Скуцький, і А. О. Лавданський, «Імітаційна модель системи передавання інформації з нероздільним факторіальним кодуванням даних у середовищі Simulink», Вісник Черкаського державного технологічного університету, т. 27, № 4, с. 31-47, 2022, doi: 10.24025/2306-4412.4.2022.273385
- Е. В. Фауре і А. Б. Скуцький, «Розробка моделі трьохетапного криптографічного протоколу на основі перестановок», в Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів

управління: тези доповідей XII Міжнародної науково-технічної конференції, Баку–Харків–Жиліна, 27–28 квітня 2022 року, Харків: ХНУРЕ, 2022, с. 138. [Online]. Режим доступу: https://nure.ua/wp-content/uploads/conf-2022-akov/telecom_2022_volume_1.pdf

- Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, і О. О. Харін, «Протокол надійного передавання перестановок в умовах інтенсивних шумів у каналі зв'язку» в Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2024): тези доповідей III Міжнародної науково-практичної інтернет-конференції, Черкаси: ЧДТУ, 2024, с. 107. [Online]. Режим доступу : https://drive.google.com/file/d/15-8DffQpER_5F6TniHYNIDf2BjOPjehX/view?usp=drive_link

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

Соціально-економічна спрямованість: підвищення надійності та безпеки інформаційно-комунікаційних послуг для промисловості та населення шляхом інтеграції передових методів захисту даних та синхронізації, що сприяє цифровізації економіки та суспільства.

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Планується до впровадження

Зв'язок з науковими темами: №0125U000637, №0123U100270, №0120U102607

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, буд. 460, 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. Заліський Максим Юрійович

2. Maksym Zaliskyi

Кваліфікація: д. т. н., професор, 05.22.20

Ідентифікатор ORCID ID: 0000-0002-1535-4384

Додаткова інформація:

Повне найменування юридичної особи: Державне некомерційне підприємство "Державний університет "Київський авіаційний інститут"

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Опірський Іван Романович

2. Ivan OPIRSKYY

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

Ідентифікатор ORCID ID: 0000-0002-8461-8996

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Чепинога Анатолій Володимирович

2. Anatolii V. Chepynoha

Кваліфікація: к. т. н., доц., 01.05.02

Ідентифікатор ORCID ID: 0000-0003-3921-6557

Додаткова інформація:

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, буд. 460, 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. 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, буд. 460, 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	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна