Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U002106

Особливі позначки: відкрита

Дата реєстрації: 01-06-2026

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: Наказ Чернівецького національного університету від 17.07.2026 № 48-асп

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Дячук Ростислав Любомирович
2. Rostyslav L. Diachuk

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0002-6259-3302

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 121

Назва наукової спеціальності: Інженерія програмного забезпечення

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Інженерія програмного забезпечення

Дата захисту: 18-06-2026

Спеціальність за освітою: Інженерія програмного забезпечення

Місце роботи здобувача: Чернівецький національний університет імені Юрія Федьковича

Код за ЄДРПОУ: 02071240

Місцезнаходження: вул. Коцюбинського, Чернівці, 58012, 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 13280

Повне найменування юридичної особи: Чернівецький національний університет імені Юрія Федьковича

Код за ЄДРПОУ: 02071240

Місцезнаходження: вул. Коцюбинського, Чернівці, 58012, 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: Чернівецький національний університет імені Юрія Федьковича

Код за ЄДРПОУ: 02071240

Місцезнаходження: вул. Коцюбинського, Чернівці, 58012, 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, 20.54.07

Тема дисертації:

1. Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел

2. Information System for Generating a High-Entropy Random Number Sequence

Реферат/анотація:

1. Дячук Р.Л. Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 121 – «Інженерія програмного забезпечення» – Чернівецький національний університет імені Юрія Федьковича, Чернівці, 2026. Дисертаційна робота присвячена створенню та дослідженню інформаційної системи для генерування високоентропійної послідовності випадкових чисел (ПВЧ) на основі сучасних технологій та методів програмної інженерії, а також використання фотоелектричних явищ в якості джерела ентропії. Створена система і її програмне забезпечення побудована на основі технології екстракції хаосу з стохастичних фізичних явищ: інтенсивності пікселів зображення з веб-камери, або цифрової відеокамери, фото- та темнового струму фотодіода.

Отримані ПВЧ також можуть оброблятися за допомогою клітинних автоматів, що збільшує рівень хаотичності випадкової послідовності. Система містить модуль статистичної оцінки послідовностей та забезпечує криптостійкість при шифруванні й кодуванні. Проведено порівняльне дослідження статистичних і робочих характеристик аналогічних відомих генераторів ПВЧ, яке показало перевагу створеної системи за рядом показників. Система має базові внутрішні перевірки, регулювання співвідношення якості та швидкості потоку і постобробку клітинними автоматами. Окрім того система має відкритість апаратури та програмного забезпечення Open-hardware та open-source (GPLv3) в тому числі для застосування у нейронних мережах. Для роботи з крипто-примітивами на основі клітинних автоматів створено бібліотеку на мові програмування Java. Експериментально підтверджено ефективність клітинних автоматів правил 30, 90, 105. Забезпечено неперервну генерацію ПВЧ заданої продуктивності та якості. Перший розділ містить ключові відомості з теорії генерації високоентропійних ПВЧ, а також відомості про апаратні генератори ПВЧ в системах інформаційної безпеки. Розглянуто різні підходи до джерела ентропії та програмно-конструкторського оточення. Проаналізовано їх значення у системах на основі криптокодових та шифрувальних конструкцій. Обґрунтовано доцільність дослідження фото-електричних явищ (ФЕЯ) та квантових як джерела ентропії для генерації ПВЧ. У другому розділі дисертаційного дослідження описано дослідження інтенсивності пікселів зображення з веб-камери, або цифрової відеокамери, фото- та темнового струму фотодіода з високою квантовою ефективністю як природних джерел для генерації ПВЧ. Показано, що послідовність випадкових чисел, згенерована на основі інтенсивності пікселів зображення відеокамери має продуктивність 85–288 Мбіт/сек. Проведено дослідження гібридного генератора послідовностей випадкових чисел, який поєднує у собі генератор на основі веб-камери і клітинних автоматів. Третій розділ присвячено створенню інформаційної системи генерування послідовності випадкових чисел на основі усіх трьох генераторів із обробкою отриманих ПВЧ за допомогою клітинних автоматів. Інтерфейс системи дозволяє керувати параметрами генерації числових послідовностей; регулювати баланс між швидкістю та рівнем безпеки. У четвертому розділі висвітлено результати застосування розробленої системи при формування вхідного вектора для хеш-функції, для стеганографічних систем а також для формування криптографічних ключів. Результати роботи впроваджені та використовується у ТДВ ЗАВОД «Кварц», Kaskad Developers Group та компанії «Datawiz» для підвищення криптостійкості програмного забезпечення. У висновках підсумовано основні результати дисертаційного дослідження. У додатках подано наукові публікації, в яких відображено основні наукові результати роботи, відомості про апробацію результатів дисертації, акти та довідки про впровадження результатів роботи, лістинг частини коду програми. Теоретичне значення. Результати теоретичних досліджень можуть застосовуватись для досліджень у галузі програмної інженерії, а також у навчальних курсах кафедри програмного забезпечення комп'ютерних систем Чернівецького національного університету імені Юрія Федьковича (та інших ЗВО). Практичне значення. Розроблена у дисертаційній роботі інформаційна система для генерації послідовностей випадкових чисел може в подальшому використовуватися для практичної реалізації. Запропоновані підходи до генерації вхідного вектора хеш-функцій із використанням клітинних автоматів та послідовностей випадкових чисел, стеганографічні алгоритми та алгоритми генерації криптографічних ключів, використовуються у компанії ТДВ ЗАВОД «Кварц», Kaskad Developers Group та компанії «Datawiz» – для розробки власного програмного забезпечення підвищеної криптостійкості. Ключові слова: програмне забезпечення, випадкові числа, джерела ентропії, хаотична система, кібербезпека, крипто-кодування, інформаційна система, шифрування, генератор, відеокамера, зображення, фотодіод, квантова ефективність, хеш-функція, нейромережа.

2. Diachuk R. Information System for Generating a High-Entropy Random Number Sequence. – Qualification scientific work as a manuscript. Thesis for the degree of Doctor of Philosophy in Specialty 121 – "Software Engineering" – Yuriy Fedkovych Chernivtsi National University, Chernivtsi, 2026. The proceeding is devoted to the development and investigation of an information system for generating high-entropy random number sequences (RNS) based on modern technologies and software engineering methods, as well as the use of photoelectric phenomena as entropy sources. The developed system and its software are based on the technology of chaos extraction from stochastic physical phenomena: image pixel intensity obtained from a webcam or digital video

camera, as well as the photo-current and dark current of a photodiode. The generated RNS can additionally be processed using cellular automata, which increases the chaoticity of the generated sequences. The system includes a statistical evaluation module and provides cryptographic strength for encryption and encoding. A comparative study of statistical and operational characteristics of known random number generators has been carried out, demonstrating the advantages of the proposed system across several indicators. The system includes internal validation mechanisms, regulation of the balance between output quality and generation speed, and post-processing using cellular automata. Furthermore, the system is characterized by open hardware and open-source software (GPLv3), including applicability in neural network systems. In addition, a Java-based library has been developed for working with cryptographic primitives based on cellular automata. The effectiveness of chaotic cellular automata Rules 30, 90, and 105 has been experimentally confirmed. Continuous generation of RNS with specified performance and quality parameters has been achieved. The first chapter contains key information on the theory of high-entropy random number generation, as well as hardware random number generators in information security systems. Various approaches to entropy sources and software–hardware environments were investigated. Their role in systems based on cryptographic coding and encryption schemes is analyzed. The feasibility of investigating photoelectric phenomena (PhEPh), as well as quantum phenomena, as entropy sources for random number generation has been substantiated. The main research tasks have been formulated. The second chapter presents a study of pixel intensity from webcam or digital video camera images, as well as the photo-current and dark current of a high-quantum-efficiency photodiode, as entropy sources for generating RNS. It is demonstrated that sequences generated from video camera pixel intensity achieve throughput ranging from 85 Mbit/s to 288 Mbit/s. A hybrid random number generator combining a webcam-based generator with cellular automata has also been investigated. The third chapter is devoted to the development of an information system for generating random number sequences based on all three generators with post-processing using cellular automata. The interface of the system enables control over generation parameters and adjustment of the balance between generation speed and security level. The fourth chapter presents the application of the developed system for forming input vectors for hash functions, steganographic systems, and cryptographic key generation. The obtained results have been implemented and are being used at Kvarts Plant, Kaskad Developers Group, and Datawiz to improve software cryptographic strength. The Conclusions summarize the main results of the dissertation research. The Appendices include scientific publications reflecting the principal research findings, information on the approbation of the dissertation results, certificates and reports on the implementation of the research outcomes, and listings of parts of the program code. Theoretical significance. The obtained results may be applied in software engineering research, as well as in educational courses at Yuriy Fedkovych Chernivtsi National University and other higher education institutions. Practical significance. The information system for generating random number sequences developed in this dissertation can be further employed for practical implementation. The proposed approaches to generating input vectors for hash functions using cellular automata and random number sequences, as well as the developed steganographic algorithms and cryptographic key generation algorithms, are being utilized at ZAVOD Kvarts, Kaskad Developers Group, and Datawiz for the development of proprietary software systems with enhanced cryptographic strength. Keywords: software, random numbers, entropy sources, chaotic system, cybersecurity, cryptographic encoding, information system, encryption, generator, video camera, image, photodiode, quantum efficiency, hash function, neural network.

Державний реєстраційний номер ДіР: 0121U109232

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:

- Diachuk R., Dmytrashchuk K., Mazurets A., Prokhorov H., Yanushevskyi S. Photosensitive matrix as a source of entropy. Proceedings of SPIE. 13813, Seventeenth International Conference on Correlation Optics. 2025. 138132C. ISSN:0277-786X (Scopus) DOI: 10.1117/12.3092587
- Diachuk R., Dobrovolsky Y., Hanzhelo D., Prokhorov H., Trembach D. Research the Level of Chaotic and Reliability in Webcam-generated Random Number Sequences, Security of infocommunication systems and Internet of things. 2024. Vol. 2, №. 1. P. 01004. DOI: 10.31861/sisiot2024.1.01004
- Добровольський, Ю., Дячук, Р. Дослідження зворотного струму фотодіода для генерації надійної випадкової послідовності чисел. Вісник Хмельницького національного університету. Серія: Технічні науки. 2025. Том 357, № 5.1. С. 126-132. DOI: 10.31891/2307-5732-2025-357-15
- Prokhorov H., Hanzhelo M., Diachuk R., Yanushevskyi S. Investigation of statistical characteristics of random number sequences generated by a webcam using cellular automata functionality and NIST patterns. Security of infocommunication systems and Internet of things. 2025. Vol 3, № 1. P. 01007. DOI: 10.31861/sisiot2025.1.01007
- Добровольський Ю., Дячук Р. Дослідження генерації випадкової послідовності чисел на основі темнового струм фотодіода при різних температурах. Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки. 2025. Том 36 (75), № 4. Частина 2. С. 119-126. DOI: 10.32782/2663-5941/2025.4.2/16
- Дячук Р.Л., Павлюченко О.С., Прохоров П.А., Прохоров Г.В., Добровольський Ю.Г. Клітинні автомати як генератори Хаосу в криптографічних алгоритмах. Проблеми інформатики та комп'ютерної техніки : матеріали XI міжнар. наук.-практ. конф., м. Чернівці, 10–13 лист. 2022 р. Черн. нац. ун-т ім. Ю Федьковича, Чернівці, 2022. – С. 44-46.
- Prokhorov G., Dobrovolsky Y., Dyachuk R. Hash-Function Algorithms Balanced on Reliability and Data Processing Speed. IEEE 4th International Conference on Advanced Trends in Information Theory, 15-16 December, 2022, Kyiv, UKRAINE. P.111-114. (Scopus). DOI: 10.1109/ATIT58178.2022.10024181
- Дячук Р.Л., Добровольський Ю.Г. Алгоритм хеш-функції з підвищеною криптостійкістю. Покращення лавинного ефекту. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXXI міжнар. наук.-практ. конф., MicroCAD-2023, 17-20 травня 2023. Харків: НТУ «ХПІ». С. 1113.
- Дячук Р.Л., Комісарчук В.В., Прохоров П.А., Прохоров Г.В., Добровольський Ю.Г. Вдосконалення функції стискання хеш-функції з застосуванням клітинних автоматів. Проблеми інформатики та комп'ютерної техніки: матеріали XII міжнар. наук.-практ. конф., м. Чернівці, 10–12 лист. 2023. Чернівці: Черн. нац. ун-т, 2023. - С. 82-83.
- Добровольський Ю.Г, Прохоров Г.В., Янушевський С.В., Прохоров П.А, Дячук Р.Л., Трембач Д. В. Оцінка надійності програмного забезпечення з точки зору його довговічності. Проблеми інформатики та комп'ютерної техніки: матеріали XII міжнар. наук.-практ. конф., м. Чернівці, 01–03 лист. 2024. Чернівці: Черн. нац. ун-т, С. 36-37.
- Добровольський Ю.Г., Прохоров Г.В., Дячук Р.Л. Генерація послідовності випадкових чисел на основі темнового струму фотодіода. Current trends in scientific research development. Proceedings of the 13th International scientific and practical conference. BoScience Publisher. Boston, USA. 2025. P. 65-67.
- Prokhorov G.V., Diachuk R.L., Hanzhelo M.G,, Yanushevskyi S.V. New approaches to the design of a hybrid random sequence generator. Physical and technological problems of transmission, processing and storage of information in infocommunication systems: Proceedings of Xth International Scientific-Practical Conference. Chernivtsi : Yuriy Fedkovych Chernivtsi National University, 2025. P. 134-136.

Наукова (науково-технічна) продукція: програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0121U109232

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Добровольський Юрій Георгійович

2. Yurii H. Dobrovolskyi

Кваліфікація: д. т. н., професор, 05.09.07

Ідентифікатор ORCID ID: 0000-0003-0626-0594

Додаткова інформація:

Повне найменування юридичної особи: Чернівецький національний університет імені Юрія Федьковича

Код за ЄДРПОУ: 02071240

Місцезнаходження: вул. Коцюбинського, Чернівці, 58012, 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. Євсеєв Сергій Петрович

2. Serhii P. Yevseiev

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCID ID: 0000-0003-1647-6444

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Бараннік Володимир Вікторович

2. Vladimir V. Barannik

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

Ідентифікатор ORCID ID: 0000-0002-2848-4524

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. 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. Шпатар Петро Михайлович

2. Petro M. Shpatar

Кваліфікація: к. т. н., доц., 05.27.01

Ідентифікатор ORCID ID: 0000-0003-4088-1458

Додаткова інформація:

Повне найменування юридичної особи: Чернівецький національний університет імені Юрія Федьковича

Код за ЄДРПОУ: 02071240

Місцезнаходження: вул. Коцюбинського, Чернівці, 58012, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Баловсяк Сергій Васильович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Баловсяк Сергій Васильович
Відповідальний за підготовку облікових документів	Дячук Ростислав Любомирович
Реєстратор	Юрченко Тетяна Анатоліївна
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна