Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U003395

Особливі позначки: відкрита

Дата реєстрації: 12-08-2025

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Горячий Олег Ярославович
2. Horiachyi Oleh Ya.

Кваліфікація:

Ідентифікатор ORCHID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: кібербезпека

Дата захисту: 29-08-2025

Спеціальність за освітою: кібербезпека

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 10511

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:

Сектор науки: Університетський

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

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:

Сектор науки: Університетський

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56.01

Тема дисертації:

1. Розроблення генераторів псевдовипадкових чисел на основі покращених методів обчислення елементарних функцій для задач кібербезпеки

2. Design of pseudorandom number generators based on improved methods for elementary function computation for cybersecurity applications.

Реферат:

1. Робота присвячена розробці та дослідженню генераторів псевдовипадкових послідовностей для кібербезпеки та захисту інформації, побудованих на основі вдосконалених методів наближеного обчислення елементарних функцій в арифметиці з рухомою комою (FP) і таких, що задовольняють вимогам статистичних тестів NIST. Розглядаються універсальні програмні та програмно-апаратні способи обчислення ділення (DIV), оберненої до аргументу функції (RCP), квадратного (SQRT) та зворотного квадратного кореня (RSQRT), кубічного (CBRT) та зворотного кубічного кореня (RCBRT) тощо. Основна ідея роботи полягає в проектуванні покращених методів, зокрема на основі алгоритму FISR, та дослідженні їх використання для генерації

псевдовипадкових чисел (ПВЧ) та послідовностей (ПВП), придатних для різноманітних задач у сфері інформаційної безпеки (ІБ). У першому розділі «Огляд відомих методів обчислення елементарних функцій та генерації псевдовипадкових послідовностей» проведено огляд літератури; здійснено аналіз, класифікацію та порівняння відомих методів, визначено способи підвищення точності та швидкодії алгоритмів; здійснено аналіз методів оцінки якості генераторів ПВП; сформульовано вимоги до проєктування та розробки вдосконалених алгоритмів для задач інформаційної та кібербезпеки. Досліджено теоретичні основи класичного алгоритму FISR, його модифікації та узагальнення, модифікації методу Хаусхолдера. Проведено аналіз відомих способів генерації та оцінювання якості ПВП. Досліджено застосування чисельних методів та FP арифметики для задач кібербезпеки, зокрема для генерації ПВП. Встановлено, що недоліками відомих методів є їхні статистичні та криптографічні вразливості, та низька швидкодія. У другому розділі «Вибір методів і розроблення методики дослідження» розроблено основну методику проєктування вдосконалених алгоритмів обчислення елементарних функцій в FP арифметиці; сформульовано методи оцінки похибок та точності, вимірювання швидкодії та аналізу збіжності; розглянуто методи проєктування та дослідження ГПВЧ на основі FP арифметики для застосувань у сфері захисту інформації, методику дослідження статистичних характеристик, швидкодії та періоду повторення сформованих ПВП. Для визначення оптимальних значень коефіцієнтів розроблено набір алгоритмів рандомізованої чисельної багатовимірної оптимізації. Запропоновано новий підхід до генерації ПВП, що використовує рекурентне рівняння та чисельні методи в FP арифметиці. Розроблено методи автоматизації їх статистичного тестування для задач кібербезпеки на основі тестів NIST та визначення періоду повторення для різних початкових значень та параметрів генерації ПВП. У третьому розділі «Проєктування генераторів псевдовипадкових чисел на основі вдосконалених алгоритмів обчислення елементарних функцій» представлено результати розробки модифікованих алгоритмів обчислення елементарних функцій та проєктування ГПВЧ на їх основі, актуальних для застосувань у сфері захисту інформації. Запропоновані ефективні алгоритми забезпечують підвищену точність і швидкодію завдяки використанню методу МС, ітераційних методів Ньютона-Рафсона (NR) та Хаусхолдера (H) вищих порядків в спеціальних формах, а також адаптивному вибору параметрів залежно від вхідних даних з метою мінімізації відносної похибки. Запропоновано метод швидкого обчислення функції RCP на основі тотожності з поліномами найкращого рівномірного наближення 3 го порядку, методи на основі модифікованої ітерації Хаусхолдера 2-го порядку (Ho2) для RCP та RSQRT, методи переключення магічних констант (DC та 8DC) для обчислення RSQRT та SQRT на основі розбиття інтервалу визначення функції та оптимізації параметрів. У четвертому розділі «Практичне тестування та аналіз ефективності запропонованих алгоритмів та генераторів псевдовипадкових чисел на ПК, міні-комп'ютері та МК для задач у сфері кібербезпеки та захисту інформації» здійснено тестування та дослідження ефективності для задач інформаційної та кібербезпеки запропонованих алгоритмів на різноманітних пристроях, що підтримують FP обчислення, зокрема на Intel, Raspberry Pi та ESP-32. Наведено результати дослідження та тестування запропонованих ГПВЧ, а саме: статистичних характеристик з використанням тестів NIST, графічних тестів та ентропії; періоду повторення; обчислювальної складності; швидкодії; параметрів генерації та діапазонів початкових значень. У висновках дисертаційної роботи узагальнено основні наукові та практичні результати, наведено порівняння ефективності методів, окреслено сфери їх застосування для кібербезпеки та захисту інформації, сформульовано рекомендації щодо впровадження та подальших досліджень.

2. The work is devoted to the development and research of pseudorandom sequence generators for cybersecurity and information protection, built on the basis of advanced methods for approximate calculation of elementary functions in floating-point arithmetic (FP) and those that meet the requirements of NIST statistical tests. Universal software and hardware methods for calculating division (DIV), inverse function (RCP), square (SQRT) and inverse square root (RSQRT), cubic (CBRT) and inverse cube root (RCBRT), etc. are considered. The main idea of the work is to design improved methods, in particular based on the FISR algorithm, and to study their use for generating pseudorandom numbers (PRNs) and sequences (PNRs) suitable for various tasks in the field of information security (IS). The first section, “Review of known methods for calculating elementary functions and generating

pseudorandom sequences," reviews the literature; The analysis, classification and comparison of known methods were carried out, methods for improving the accuracy and speed of algorithms were determined; methods for assessing the quality of PVP generators were analyzed; requirements for the design and development of improved algorithms for information and cybersecurity tasks were formulated. The theoretical foundations of the classical FISR algorithm, its modifications and generalizations, and modifications of the Householder method were studied. The analysis of known methods for generating and assessing the quality of PVP was carried out. The application of numerical methods and FP arithmetic for cybersecurity tasks was studied, in particular for PVP generation. It was established that the disadvantages of known methods are their statistical and cryptographic vulnerabilities and low speed. In the second section "Choice of methods and development of research methodology", the main methodology for designing improved algorithms for calculating elementary functions in FP arithmetic was developed; methods for assessing errors and accuracy, measuring speed and analyzing convergence were formulated; considered methods for designing and studying pseudorandom number generators based on FP arithmetic for applications in the field of information security, a methodology for studying statistical characteristics, speed and repetition period of generated pseudorandom number generators. To determine the optimal values of coefficients, a set of algorithms for randomized numerical multidimensional optimization was developed. A new approach to generating pseudorandom number generators using a recurrence equation and numerical methods in FP arithmetic was proposed. Methods for automating their statistical testing for cybersecurity tasks based on NIST tests and determining the repetition period for various initial values and parameters of pseudorandom number generator generation were developed. The third section, "Design of pseudorandom number generators based on improved algorithms for calculating elementary functions," presents the results of developing modified algorithms for calculating elementary functions and designing pseudorandom number generators based on them, relevant for applications in the field of information security. The proposed efficient algorithms provide increased accuracy and speed due to the use of the MC method, the iterative Newton-Raphson (NR) and Householder (H) methods of higher orders in special forms, as well as adaptive selection of parameters depending on the input data in order to minimize the relative error. A method for fast calculation of the RCP function based on the identity with the polynomials of the best uniform approximation of the 3rd order, methods based on the modified Householder iteration of the 2nd order (Ho2) for RCP and RSQRT, methods of switching magic constants (DC and 8DC) for calculating RSQRT and SQRT based on the partitioning of the function definition interval and parameter optimization are proposed. In the fourth section "Practical testing and analysis of the effectiveness of the proposed algorithms and pseudorandom number generators on a PC, minicomputer and MC for tasks in the field of cybersecurity and information protection" testing and research of the effectiveness of the proposed algorithms for information and cybersecurity tasks on various devices that support FP calculations, in particular on Intel, Raspberry Pi and ESP-32, are carried out. The results of the research and testing of the proposed GPNR are presented, namely: statistical characteristics using NIST tests, graphic tests and entropy; repetition period; computational complexity; speed; generation parameters and ranges of initial values. The conclusions of the dissertation work summarize the main scientific and practical results, compare the effectiveness of the methods, outline the areas of their application for cybersecurity and information protection, and formulate recommendations for implementation and further research.

Державний реєстраційний номер ДіР: № 0120U103215, № 0113U005267, № 0120U100024

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Теоретичне узагальнення і вирішення важливої наукової проблеми

Публікації:

- 1. Horyachyy O., Moroz L., Otenko V. Simple effective fast inverse square root algorithm with two magic constants // International Journal of Computing. 2019. Vol. 18, iss. 4. P. 461–470.
- 2. Moroz L., Samotyy V., Horyachyy O. Modified fast inverse square root and square root approximation algorithms: The method of switching magic constants // Computation (Basel). 2021. Vol. 9, iss. 2. P. 1–23.
- 3. Максимович В. М., Шабатура М. М., Горячий О. Я., Лужецька Н. М. Генератори псевдовипадкових бітових послідовностей на основі чисельних методів в арифметиці з рухомою комою для вирішення завдань кібербезпеки // Сучасна спеціальна техніка. 2021. 1 (64). С. 81–92.
- 4. Hrynchyshyn A., Horyachyy O., Tymoshenko O., Moroz L. An efficient algorithm for fast inverse square root // Processing, transmission and security of information : Monogrpah. Bielsko-Biała : Wydawnictwo Naukowe ATH w Bielsku-Białej, 2018. Vol. 2. P. 105–114.
- 5. Горячий О. Я., Максимович В. М., Шабатура М. М. Дослідження множини початкових значень генераторів псевдовипадкових чисел на основі арифметики з рухомою комою // Сучасний захист інформації. 2024. № 2 (58). С. 91–102.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: № 0120U103215, № 0113U005267, № 0120U100024

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Журавель Ігор Михайлович

2. Ihor M. Zhuravel

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

Ідентифікатор ORCHID ID: Не застосовується

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:

Сектор науки: Університетський

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Казакова Надія Феліксівна

2. Nadiia Kazakova

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

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Одеський національний університет імені І. І. Мечникова

Код за ЄДРПОУ: 02071091

Місцезнаходження: вул. Дворянська, буд. 2, Одеса, 65082, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

Власне Прізвище Ім'я По-батькові:

1. Єсіна Марина Віталіївна

2. Maryna V. Yesina

Кваліфікація: к.т.н., 05.13.21

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Совин Ярослав Романович

2. Yaroslav Sovyn

Кваліфікація: к. т. н., доц., 05.11.17

Ідентифікатор ORCHID ID: Не застосовується

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:

Сектор науки: Університетський

Власне Прізвище Ім'я По-батькові:

1. Гарасимчук Олег Ігорович
2. Harasymchuk Oleh I.

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

Ідентифікатор ORCHID ID: Не застосовується

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:

Сектор науки: Університетський

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Нємкова Олена Анатоліївна
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Нємкова Олена Анатоліївна
Відповідальний за підготовку облікових документів	Пархуць Любомир Теодорович
Реєстратор	УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна