

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U004456

Особливі позначки: відкрита

Дата реєстрації: 10-08-2026

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: Наказ ВНТУ № 380 від 18.09.2026р.



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Селезньов Віталій Ігорович

2. Vitalii Seleznov

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Кібербезпека

Дата захисту: 02-09-2026

Спеціальність за освітою: Кібербезпека

Місце роботи здобувача: Організація відсутня

Код за ЄДРПОУ: 000000000

Місцезнаходження: -----, Київ, 00000, Україна

Форма власності: Змішана

Сфера управління:

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 15468

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, 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: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.53.37, 50.37.23, 50.41

Тема дисертації:

1. Методи та засоби малоресурсного гешування для пристроїв Інтернету речей
2. Lightweight Hashing Methods and Their Hardware Implementations for Internet of Things Devices

Реферат/анотація:

1. Об'єктом дослідження є процеси контролю цілісності даних та автентифікації пристроїв Інтернету речей. Предметом дослідження є методи малоресурсного гешування та моделі апаратних засобів гешування даних для пристроїв Інтернету речей. Метою дослідження є зменшення апаратної складності реалізації засобів гешування для пристроїв Інтернету речей шляхом розробки нових методів малоресурсного гешування та структурних моделей засобів, що їх реалізують. Наукова новизна полягає в тому, що вперше запропоновано метод малоресурсного гешування типу «дані-генератор», який, на відміну від відомих, передбачає формування проміжних геш-значень шляхом нагромадження байтів вхідних даних, що керуються псевдовипадковою послідовністю, сформованою генератором, що забезпечує зменшення апаратних витрат на реалізацію геш-функції на 14–24 % порівняно з відомими малоресурсними засобами. Вперше запропоновано моделі спеціалізованого процесора для гешування даних, які, на відміну від відомих, містять нагромаджувальний суматор та генератор псевдовипадкової послідовності, що забезпечує підвищення інтегрального коефіцієнта ефективності апаратної реалізації в 2,7–4,5 рази порівняно з відомими

малоресурсними апаратними засобами. Удосконалено протокол автентифікації RFID-міток, який, на відміну від відомих, використовує лише геш-функції та генерування псевдовипадкового числа як криптографічні примітиви, що забезпечує розширення функціональних можливостей шляхом одночасної взаємної автентифікації сторін і контролю цілісності даних, які зберігаються та передаються RFID-міткою. Практична цінність полягає в такому. Розроблені моделі спеціалізованих процесорів гешування даних можуть бути використані як основа для створення апаратних засобів Інтернету речей з обмеженими ресурсами, які реалізують контроль цілісності даних та автентифікацію пристроїв. Розроблена програмна бібліотека методів гешування може бути використана для дослідження характеристик методів малоресурсного гешування, а також для їх програмного застосування на універсальних мікроконтролерах. Розроблений програмний засіб для віддаленого статистичного тестування за методиками NIST STS та Dieharder може бути використаний для експериментальної перевірки статистичних властивостей геш-функцій. Запропоновані методи гешування та протокол автентифікації можуть бути використані при проектуванні засобів контролю цілісності та автентифікації даних у малоресурсних IoT-пристроях. Ступінь впровадження – результати дисертаційної роботи впроваджені у систему ідентифікації на основі RFID-міток підприємства ТОВ «Солар Стар АГРО» (Вінницька обл., Україна) та у систему IoT-моніторингу для перевірки цілісності телеметричних даних підприємства ТОВ «Каскад-Безпека» (м. Вінниця, Україна), а також використовуються в навчальному процесі кафедри захисту інформації ВНТУ у дисциплінах «Прикладна криптологія» та «Криптографічний захист інформації». Сфера (галузь) використання – малоресурсні системи Інтернету речей, зокрема пасивні RFID-мітки, автономні сенсорні вузли та вбудовані контролери, а також інші комп'ютерні системи та мережі, де необхідний контроль цілісності даних та автентифікація пристроїв в умовах обмежених апаратних ресурсів. Основні результати досліджень, виконаних у дисертаційній роботі, опубліковано в 10 наукових працях, серед яких 4 статті у фахових виданнях України, 5 тез доповідей на всеукраїнських та міжнародних конференціях, а також 1 свідоцтво про реєстрацію авторського права на твір.

2. The object of the research is the processes of data integrity control and authentication of Internet of Things devices. The subject of the research is the methods of lightweight hashing and hardware models of data hashing devices for Internet of Things applications. The goal of the research is reducing the hardware complexity of hashing devices for Internet of Things applications by developing new lightweight hashing methods and structural models of the hardware implementing them. The scientific novelty consists in the following. A lightweight hashing method of the "data-generator" type, which in contradistinction to the known ones provides the formation of intermediate hash values by accumulating input data bytes under the control of a pseudorandom sequence generated by a pseudorandom generator, thereby reducing the hardware implementation cost of the hash function by 14–24% compared with known lightweight hashing devices, is first proposed. Models of a specialized hashing processor, which in contradistinction to the known ones include an accumulative adder and a pseudorandom sequence generator, thereby providing an increase of the integral hardware implementation efficiency coefficient by 2,7–4,5 times compared with known lightweight hardware implementations, are first proposed. The RFID tag authentication protocol, which in contradistinction to the known ones uses only hash functions and pseudorandom number generation as cryptographic primitives, thereby extending its functionality by providing simultaneous mutual authentication of the communicating parties and data integrity control of the data stored and transmitted by the RFID tag, is improved. The practical value consists in the following. The developed models of specialized hashing processors can be used as the basis for designing hardware devices for resource-constrained Internet of Things applications implementing data integrity control and device authentication. The developed software library of hashing methods can be used for investigating the characteristics of lightweight hashing methods as well as for their software implementation on general-purpose microcontrollers. The developed software tool for remote statistical testing based on the NIST STS and Dieharder methodologies can be used for experimental verification of the statistical properties of hash functions. The proposed hashing methods and authentication protocol can be used in the design of data integrity control and authentication mechanisms for resource-constrained IoT devices. The degree of implementation – the results of the dissertation are implemented in the RFID-based identification system of Solar Star AGRO LLC (Vinnytsia

Oblast, Ukraine), in the IoT monitoring system for telemetry data integrity verification of Kaskad-Bezpeka LLC (Vinnytsia, Ukraine), and are also used in the educational process of the Information Security Department of Vinnytsia National Technical University in the courses "Applied Cryptology" and "Cryptographic Information Protection." The field of application – resource-constrained Internet of Things systems, in particular passive RFID tags, autonomous sensor nodes, and embedded controllers, as well as other computer systems and networks where data integrity control and device authentication are required under conditions of limited hardware resources. The main results of the dissertation are published in 10 scientific publications, including 4 papers in Ukrainian peer-reviewed scientific journals, 5 conference proceedings, and 1 certificate of copyright registration for a software work.

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. Селезньов В. І., Лужецький В. А. Метод малоресурсного гешування типу «Дані – Генератор». Кібербезпека: освіта, наука, техніка, 2023. Т. 2, № 22. С. 84–95.
2. Лужецький В. А., Селезньов В. І. Огляд підходів та методів малоресурсного гешування даних. Вісник Вінницького політехнічного інституту, 2025. № 6. С. 99–112.
3. Luzhetskyi V., Seleznev V. Hardware implementation of the HDG hash function. Bulletin of Cherkasy State Technological University. 2025. Т. 30, № 2, С. 10–21.
4. Лужецький В., Селезньов В., Хохлачова Ю. Протокол автентифікації засобів інтернету речей з використанням RFID-міток. Кібербезпека: освіта, наука, техніка. 2026. Т. 4, № 32. С. 987–1001.
5. Селезньов В. І. Аналіз методів малоресурсного гешування. Матеріали LII науково-технічної конференції підрозділів ВНТУ. Вінниця, 21–23 червня 2023 р
6. Селезньов В. І. Програмний засіб для віддаленого статистичного тестування методів малоресурсного гешування за допомогою пакету NIST STS 822. Матеріали LIII науково-технічної конференції підрозділів ВНТУ. Вінниця, 20–22 березня 2024 р.
7. Селезньов В. І., Лужецький В. А. Удосконалення методу малоресурсного гешування HDG. Матеріали XIII Міжнародної науково-технічної конференції «ITSec-2024 Безпека інформаційних технологій». Львів, 9–11 травня 2024 р.
8. Лужецький В. А., Селезньов В. І. Метод малоресурсного гешування типу «генератор-дані». Матеріали міжнародної науково-практичної конференції «ІТКМ-2024». Івано-Франківськ, 21–24 травня 2024 р.
9. Селезньов В. І. Засіб для гешування даних методом HDG. Матеріали LIV Всеукраїнської науково-технічної конференції підрозділів ВНТУ. Вінниця, 24–27 березня 2025 р.

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

Соціально-економічна спрямованість: забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Охоронні документи на ОПІВ:

Комп'ютерні програми

Селезньов В. І., Лужецький В. А. Свідоцтво про реєстрацію авторського права на твір № 127025 «Комп'ютерна програма «Засіб для віддаленого статистичного тестування методів малоресурсного гешування за допомогою пакету NIST STS 822». Державна організація «Український національний офіс

інтелектуальної власності та інновацій». Дата реєстрації 31 липня 2024 р.

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. Лужецький Володимир Андрійович

2. Volodymyr Luzhetskyi

Кваліфікація: д.т.н., професор, 05.13.05

Ідентифікатор ORCID ID: 0009-0003-2218-1527

Додаткова інформація:

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, 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. Смірнова Тетяна Віталіївна

2. Tetiana V. Smirnova

Кваліфікація: к. т. н., доц., 05.02.01

Ідентифікатор ORCID ID: 0000-0001-6896-0612

Додаткова інформація:

Повне найменування юридичної особи: Центральнуукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, Кропивницький, Кропивницький р-н., 25006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Фесенко Андрій Олексійович
2. Andrii O. Fesenko

Кваліфікація: к. т. н., доц., 05.13.21**Ідентифікатор ORCID ID:** 0000-0001-5154-5324**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. 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:****Рецензенти****Власне Прізвище Ім'я По-батькові:**

1. Баришев Юрій Володимирович
2. Yurii V. Baryshev

Кваліфікація: к. т. н., доц., 05.13.05**Ідентифікатор ORCID ID:** 0000-0001-8324-8869**Додаткова інформація:****Повне найменування юридичної особи:** Вінницький національний технічний університет**Код за ЄДРПОУ:** 02070693**Місцезнаходження:** вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

**Власне Прізвище Ім'я По-батькові
голови ради**

Ковтун В'ячеслав Васильович

**Власне Прізвище Ім'я По-батькові
головуючого на засіданні**

Ковтун В'ячеслав Васильович

**Відповідальний за підготовку
облікових документів**

Іванчук Ярослав Володимирович

Реєстратор

Юрченко Тетяна Анатоліївна

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**



Юрченко Тетяна Анатоліївна