Додаток 1
Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

Авторська довідка

(кваліфікаційної роботи магістра)

Назва кваліфікаційної роботи магістра Розроблення алгоритмів несиметричного шифрування: схема Мак-Еліса на еліптичних кодах для мобільних засобів зв'язку
назви записувати нижнім регістром (як у реченні)

Назва (англ.): Development of Asymmetric Encryption Algorithms: Elliptic Curve MacEliece Scheme for Mobile Communication Devices
переклад англійською

Освітній ступінь : магістр

Шифр та назва спеціальності: 125 «Кібербезпека»
напр.:151 Автоматизація та комп'ютерно-інтегровані технології

Екзаменаційна комісія: Екзаменаційна комісія № 41
напр.: Екзаменаційна комісія №1

Установа захисту: Тернопільський національний технічний університет імені Івана Пулюя
напр.: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 28 грудня 2023 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 64

УДК: 004.48:004.94

Автор роботи
Прізвище, ім'я, по батькові (укр.): Сава Лука Михайлович
розкривати ініціали

Прізвище, ім'я (англ.): Luka Sava
використовувати паспортну транслітерацію (КМУ 2010)

Місце навчання (установа, факультет, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра кібербезпеки, м.Тернопіль, Україна

Керівник
Прізвище, ім'я, по батькові (укр.): Александер Марек Богуслав
повністю

Прізвище, ім'я (англ.): Aleksander Marek Bohuslav
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Україна

Вчене звання, науковий ступінь, посада: д.т.н., професор кафедри кібербезпеки

Рецензент
Прізвище, ім'я, по батькові (укр.): Млинко Богдана Богданівна
повністю

Прізвище, ім'я (англ.): Bodana Mlynko
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра комп'ютерних наук, м.Тернопіль, Україна
Вчене звання, науковий ступінь, посада: к.т.н, доцент кафедри

Ключові слова

українською мак-еліс, теоретико-кодові схеми, алгебро-геометричні коди, достовірність, скритність, еліптичні криві. *до 10 слів*

англійською mc-elice, theoretical code schemes, algebra-geometric codes, reliability, skills, elliptic curves. *до 10 слів*

Анотація

українською:

Об’єкт дослідження – процес підвищення вірогідності та конфіденційності переданих даних за допомогою несиметричної крипто-кодової системи Мак-Еліса.

Предмет дослідження – алгоритми підвищення вірогідності та конфіденційності переданих даних за допомогою несиметричної крипто-кодової системи Мак-Еліса та їх дослідження.

Мета дослідження – підвищення вірогідності та конфіденційності переданих даних за допомогою несиметричної крипто-кодової системи Мак-Еліса на еліптичних кодах у мобільних каналах зв’язку.

Розроблено програмний продукт який дозволяє інтегровано забезпечити вимоги щодо достовірності та інформаційної скритності в протоколах з автоперезапитом або з прямим виправленням помилок.

Результати можуть бути впроваджені в комп’ютерних мережах в протоколи з автоперезапитом на основі використання теоретико кодової схеми Мак-Еліса.

англійською:

The object of the study is the process of increasing the reliability and confidentiality of transmitted data using the asymmetric crypto-code system of McElis.

The subject of the study is algorithms for increasing the reliability and confidentiality of transmitted data using the asymmetric crypto-code system of McElice and their research.

The purpose of the study is to increase the reliability and confidentiality of transmitted data using the asymmetric McElice crypto-code system on elliptic codes in mobile communication channels.

A software product has been developed that allows for the integrated provision of requirements for reliability and information secrecy in protocols with autorequest or with direct error correction.

The results can be implemented in computer networks in protocols with auto-request based on the use of the theoretical code scheme of McElice.

Бібліографічний опис:

Сава Л.М. Розроблення алгоритмів несиметричного шифрування: схема Мак-Еліса на еліптичних кодах для мобільних засобів зв’язку: кваліфікаційна робота магістра за спеціальністю 125 — Кібербезпека / Сава Лука Михайлович. – Тернопіль : ТНТУ, 2023. – 64 с.