Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0421U103996

Особливі позначки: відкрита

Дата реєстрації: 14-12-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Пустовіт Олександр Сергійович
2. Pustovit Oleksandr S.

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.06

Назва наукової спеціальності: Інформаційні технології

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 09-12-2021

Спеціальність за освітою: математика

Місце роботи здобувача: Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України

Код за ЄДРПОУ: 26022051

Місцезнаходження: Чоколовский бул., 13, м. Київ, 03186, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.255.01

Повне найменування юридичної особи: Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України

Код за ЄДРПОУ: 26022051

Місцезнаходження: Чоколовский бул., 13, м. Київ, 03186, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

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

Повне найменування юридичної особи: Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України

Код за ЄДРПОУ: 26022051

Місцезнаходження: Чоколовский бул., 13, м. Київ, 03186, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 27.45, 27.47.17

Тема дисертації:

1. Застосування теорії екстремальних графів до сучасних проблем інформаційної безпеки

2. Application of theories of extreme graphs to modern problems of information security

Реферат:

1. Об’єктом дослідження є Марковський процес блукання на алгебраїчних графах та задач дослідження його криптографічних властивостей. Метою дисертаційної роботи є розв’язання нових постквантових задач захисту інформації. Методи дослідження. При вирішенні поставлених задач у дисертаційній роботі було використано методи Екстремальної теорії графів, Теорії скінченних геометрій та Теорії символьних обчислень разом із методами некомутативної криптографії та прикладної алгебраїчної геометрії. Для задач симетричної криптографії (потокове шифрування та створення дайджестів електронних документів) використовувались обчислювальні методи. При дослідженні властивостей (швидкодія, степені змішування) вживались статистичні методи. Новизна: вперше в термінах теорії алгебраїчних графів та графів-експандерів створено криптографічно стійкі постквантові швидкі алгоритми для хешування великих файлів у дайджесту заданих розмірів, який буде чутливим до будь-яких змін символів у файлі; вперше розроблені алгоритми

створення чутливих дайджестів електронних файлів для виявлення кібератак на віртуальні організації з покращеним на 45% показником аваланч ефекту; вперше в термінах Алгебраїчної Геометрії запропоновано нову парадигму, в якій теорія алгебраїчних графів та некомутативна алгебра використовується для розробки та впровадження нових несиметричних інструментів криптографії (протоколи, криптосистеми, інструмент контролю доступу), стійких до кібератак супротивника у постквантову епоху; вперше в термінах теорії алгебраїчних графів створено алгоритми використання напівгрупи над скінченними комутативними кільцями для розробки швидких потокових алгоритмів шифрування зі зростаючим простором відкритих текстів; вперше теорію скінченних геометрій використано для створення алгоритмів електронного підпису криптографії від багатьох змінних, які замість публічних ключів використовують протоколи некомутативної криптографії. Впровадження в: Київському університеті імені Бориса Грінченка в рамках навчальних дисциплін «Методи побудови та аналізу криптосистем», «Математичні методи криптографії» та впроваджені в програмно-апаратне забезпечення «Центру технологій захисту інформаційних активів» при розгортанні Лабораторії криптографічного та технічного захисту інформації. ТОВ «Алгорітм –Х» у програмно-апаратне забезпечення при створенні алгоритмів захисту мереж ситуаційних центрів та алгоритмів виявлення кібератак. Сфера використання – кібербезпека.

2. The dissertation, devoted to the solution of a topical scientific and practical problem, reveals the methods of data protection involved in the Big Data call and the first samples of a quantum computer appear. A new class of groups and semigroups of transformations of the affine space K^n is considered, which satisfy the properties of superposition, ie, the possibility of calculating the product of n elements for the polynomial time T (n). These algebraic objects are defined in terms of special graphs defined by the commutative ring K. They are the tool for constructing cryptographic algorithms in the cases K=F_q (finite field), Z_m (arithmetic ring of surpluses modulo m), K=B(m,2) (Boolean ring of size 2^n). The paper describes in detail a new flow symmetric encryption algorithm for the known family of graphs A (n, K) and the corresponding group of cubic transformations of the open text space K^n. The encoding speed O (n) is comparable to the file read speed. With a certain length restriction, different slogans correspond to different ciphers. The properties of mixing were investigated based on the results of computer simulation. It is shown that linearization attacks require O(n^3) plaintext / corresponding ciphertext interceptions. The complexity of the linearization attack is O(n^10). The algorithm is supported by a secure post-quantum protocol, the safety of which is determined by the task of scheduling the transformation of the Cremona group into the product of known generators. Fast, post-quantum stable algorithms for creating digests of electronic documents are offered. New algorithms with a public key defined by transformations from many variables of unlimited degree are described. The properties of new asymmetric El Gamal-type encryption algorithms defined by post-quantum protocols are investigated. New digital signature algorithms are proposed, the security of which is also determined by post quantum protocols of non-commutative cryptography, defined in terms of cryptography from many variables.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Устименко Василь Олександрович

2. Ustymenko Vasyl O.

Кваліфікація: д. ф.-м. н., 01.01.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Петравчук Анатолій Петрович

2. Petravchuk Anatolii P.

Кваліфікація: д.ф.-м.н., 01.01.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Семко Віктор Володимирович

2. Semko Victor V.

Кваліфікація: д.т.н., 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Миронцов Микита Леонідович
2. Myroncov Mykyta L.

Кваліфікація: д.ф.-м.н., 04.00.22

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Довгий Станіслав Олексійович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Довгий Станіслав Олексійович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.