Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0821U102352

Особливі позначки: відкрита

Дата реєстрації: 29-09-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Родінко Марія Юріївна

2. Rodinko Mariia Yuriivna

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп'ютерні науки

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 14-09-2021

Спеціальність за освітою: Безпека інформаційних і комунікаційних систем

Місце роботи здобувача: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, м. Харків, Харківський р-н., Харківська обл., 61022, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 64.051.019

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

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, м. Харків, Харківський р-н., Харківська обл., 61022, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

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

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

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, м. Харків, Харківський р-н., Харківська обл., 61022, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.41.25, 81.14.11.05

Тема дисертації:

1. Методи побудови та дослідження властивостей малоресурсних блокових шифрів та їх компонентів

2. Methods of construction and research of properties of lightweight block ciphers and their components

Реферат:

1. Дисертація присвячена розробці та удосконаленню методів аналізу криптографічних властивостей компонентів симетричних блокових шифрів та побудові перспективних криптографічних перетворень. Метою дисертаційної роботи є підвищення продуктивності симетричних криптографічних перетворень і удосконалення методів аналізу їх стійкості. У дисертації удосконалено метод градієнтного спуску для генерації нелінійних таблиць заміни, що дозволяє суттєво знизити складність генерації оптимальних S-блоків. Отримав подальший розвиток математичний метод оцінки колізійних властивостей неін'єктивних схем розгортання ключів блокових шифрів, що відрізняється застосуванням вдосконаленої математичної моделі та більш ефективного математичного апарату та дозволяє отримати уточнену оцінку ймовірності колізії двох послідовностей циклових ключів. У дисертації вперше запропоновано два методи пошуку одноциклових диференційних характеристик для визначеного класу ARX-шифрів, що дозволяють з низькою обчислювальною складністю отримувати оцінки стійкості циклової функції блокового шифру визначеного класу до диференційного криптоаналізу. Крім того, отримали подальший розвиток методи пошуку

багатоциклових диференційних характеристик для визначеного класу ARX-шифрів, що відрізняються вдосконаленим механізмом відбору вхідних різниць та формуванням початкової множини одноциклових диференційних характеристик, що дозволяє отримати оцінку щодо стійкості повномасштабного блокового шифру визначеного класу до диференційного криптоаналізу. Розроблений перспективний постквантовий малоресурсний блоковий шифр «Кипарис», що забезпечує високий та надвисокий рівні стійкості та перевершує за швидкодією відомі малоресурсні блокові шифри на процесорах загального призначення та мобільних платформах, а також обґрунтована стійкість блокового шифру «Кипарис-256» до диференційного криптоаналізу згідно з вимогами практичного критерію.

2. The dissertation is devoted to the development and improvement of methods on cryptographic properties analysis of block ciphers components and construction of perspective cryptographic transformations. The aim of the dissertation is to increase performance of symmetric cryptographic transformations and improve methods of analysis of their strength. In the dissertation it is improved the gradient descent method for generating nonlinear substitution tables, which significantly reduces the complexity of optimal S-boxes generation. It is further developed the mathematical method of estimating the collision properties of non-injective key schedules of block ciphers, which differs in the application of an improved mathematical model and more efficient mathematical apparatus and allows to obtain an accurate estimate of the collision probability of two round key sequences. In the dissertation for the first time two methods of searching for one-round differential characteristics for a certain class of ARX-ciphers are proposed, which allow to obtain estimates of the strength of the round function of a block cipher of the certain class to differential cryptanalysis with low computational complexity. Moreover, methods of searching for multi-round differential characteristics for a certain class of ARX-ciphers have been further developed, which differ by an improved mechanism for selecting input differences and forming an initial set of one-round differential characteristics, which allows to estimate the strength of a full-scale block cipher of the certain class to differential cryptanalysis. A perspective post-quantum lightweight block cipher Cypress is developed, which provides high and ultra-high levels of security and exceeds the performance of known lightweight block ciphers on general-purpose processors and mobile platforms, and also the strength of the block cipher Cypress-256 to the differential cryptanalysis in accordance with the requirements of the practical criterion is proven.

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. Олійников Роман Васильович

2. Oliynykov Roman Vasylovych

Кваліфікація: д. т. н., 05.13.05

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. Семенов Сергій Геннадійович
2. Semenov Serhii Hennadiiovych

Кваліфікація: д. т. н., 05.13.05

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. Яковлєв Сергій Володимирович
2. Yakovliev Serhii Volodymyrovych

Кваліфікація: к. т. н., 05.13.21

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. Єсін Віталій Іванович

2. Yesin Vitalii Ivanovych

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

Власне Прізвище Ім'я По-батькові:

1. Нарєжній Олексій Павлович

2. Nariezhnii Oleksii Pavlovych

Кваліфікація: к. т. н., 05.12.17

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 Лазурик Валентин Тимофійович

Власне Прізвище Ім'я По-батькові головуючого на засіданні

Лазурик Валентин Тимофійович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.