Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0821U102360

Особливі позначки: відкрита

Дата реєстрації: 30-09-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Лисицький Костянтин Євгенійович
2. Lysytskyi Kostiantyn Yevgeniyovych

Кваліфікація:

Ідентифікатор ORCHID ID: Не застосовується

Вид дисертації: доктор філософії

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп'ютерні науки

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 15-09-2021

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

Сектор науки: Не застосовується

III. Відомості про дисертацію

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 64.051.020

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

Сектор науки: 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

Сектор науки: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 81.14.11.05

Тема дисертації:

1. Методи та засоби побудови блокових симетричних шифрів з підвищеною стійкістю та швидкодією
2. Methods and means of constructing block symmetric ciphers with increased stability and speed

Реферат:

1. Дисертацію присвячено обґрунтуванню нової методології оцінки стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу і подальшому її розвитку в напрямку створення і розробки нової концепції проєктування блокових симетричних шифрів.. Проведено великий комплекс теоретичних і експериментальних досліджень показників випадковості сучасних блокових симетричних шифрів і випадкових підстановок. Запропоновано нову концепцію проектування блокових симетричних шифрів, основою реалізації якої стало використання окремо або спільно трьох методів, спрямованих на збільшення числа S-блоків, які активізуються на першому циклі шифрування. Вперше запропоновано методи побудови шифрів Шуп-1М і Шуп-2М з 256-бітовим входом, з поліпшеними показниками стійкості і швидкодії, орієнтованих на використання в постквантовом періоді розвитку криптографії. Розроблені підходи та методи

також були використані для порівняльного аналізу шифрів, представлених в свій час на український конкурс з вибору національного стандарту блокового симетричного шифрування України, а пізніше при дослідженнях шифру Калина-2, який став стандартом. Розробки останнього часу визначають напрямок подальшого вдосконалення властивостей і показників доказової стійкості блокових симетричних шифрів, орієнтованих на застосування в постквантовом періоді розвитку криптографії. В результаті виконаних досліджень, вирішена важлива науково-технічна задача, яка має практичне значення для вдосконалення технологій блокового симетричного шифрування і складається в розробці методів поліпшення динамічних показників приходу блокових симетричних шифрів до стану випадкової підстановки на основі збільшення числа S-блоків, які активізуються на перших циклах шифрування.

2. The dissertation is devoted to substantiation of a new methodology for assessing the resistance of block symmetric ciphers to attacks of differential and linear cryptanalysis and its further development in the direction of creating and developing a new concept of designing block symmetric ciphers. A large set of theoretical and experimental studies of the indicators of randomness of modern block symmetric ciphers and random substitutions. A new concept of designing block symmetric ciphers is proposed, the basis of which was the use separately or jointly of three methods aimed at increasing the number of S-blocks that are activated in the first cycle of encryption. For the first time, methods for constructing Shup-1M and Shup-2M ciphers with 256-bit input, with improved stability and speed indicators, focused on use in the post-quantum period of cryptography development, have been proposed. The developed approaches and methods were also used for comparative analysis of ciphers submitted at one time to the Ukrainian competition for the selection of the national standard of block symmetric encryption of Ukraine, and later in the study of the cipher Kalyna-2, which became the standard. Recent developments determine the direction of further improvement of the properties and indicators of evidence-based stability of block symmetric ciphers, focused on the use in the postquantum period of cryptography. As a result of the performed researches, the important scientific and technical problem which has practical value for improvement of technologies of block symmetric encryption is solved and consists in development of methods of improvement of dynamic indicators of arrival of block symmetric ciphers to a condition of random substitution on the basis of increase in number of S-blocks. encryption cycles.

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. Горбенко Іван Дмитрович

2. Horbenko Ivan Dmytrovych

Кваліфікація: 05.13.21

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Ковальчук Людмила Василівна

2. Kovalchuk Liudmyla Vasylyvna

Кваліфікація: 05.13.21

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Харченко Вячеслав Сергійович

2. Kharchenko Viacheslav Sergiyovych

Кваліфікація: 20.02.14

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Єсін Віталій Іванович

2. Yesin Vitalii Ivanovych

Кваліфікація: 05.13.06

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Нарєжній Олексій Павлович

2. Nariezhnii Oleksii Pavlovich

Кваліфікація: 05.12.17

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: 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.