Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0416U000737

Особливі позначки: відкрита

Дата реєстрації: 29-03-2016

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Кайдалов Дмитро Сергійович
2. Kaidalov Dmytro Serhiyovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.21

Назва наукової спеціальності: Системи захисту інформації

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 01-03-2016

Спеціальність за освітою: 8.17010101

Місце роботи здобувача: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: 61166, м. Харків, пр. Науки, 14

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): К 64.052.05

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, 14, м. Харків, Харківський р-н., Харківська обл., 61166, 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 радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: 61166, м. Харків, пр. Науки, 14

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 20.51.19

Тема дисертації:

1. Методи аналізу властивостей високорівневих конструкцій та схем формування циклових ключів блокових симетричних шифрів

2. Methods for analyzing properties of high-level constructions and key-expansion schemes of block symmetric ciphers

Реферат:

1. Дисертаційна робота присвячена аналізу властивостей сучасних блокових симетричних шифрів, зокрема проводиться оцінка ефективності основних високорівневих конструкцій блокових шифрів, а також аналізується стійкість блокового шифру Калина до атак на зв'язаних ключах. У роботі отримано оцінки ефективності трьох високорівневих конструкцій блокових шифрів: ланцюга Фейстеля, схеми Лей-Месі та SPN структури. Встановлено, що SPN-структура є найбільш ефективною конструкцією за критерієм розрізнювання із випадковою функцією/ перестановкою. Запропонований метод оцінки стійкості блокових шифрів на основі SPN-конструкції до атак на зв'язаних ключах (практичний критерій). Застосування методу показало захищеність цього перетворення до розглянутого класу атак.

2. The thesis is devoted to the analysis of properties of modern block symmetric ciphers. In particular the efficiency of basic high-level constructions for block ciphers is being analyzed. Security of block SPN-structure

against related-key attacks has also been researched. The thesis represents a complex of researches with the main three high-level constructions: Feistel scheme, Lai-Massey scheme and SPN-structure. Research results confirm that the SPN-structure is the most efficient high-level construction according to the criteria of distinguishing with the random function. Research on security analysis of the block ciphers on the base of SPN-structure against related-key attacks was also made (practical criteria). The developed method proved that this cipher is secure against such attacks.

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 Vasylyovych

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. Олексійчук Антон Миколайович

2. Олексійчук Антон Миколайович

Кваліфікація: д.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

Власне Прізвище Ім'я По-батькові:

1. Петренко Ольга Євгенівна

2. Петренко Ольга Євгенівна

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

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Халімов Геннадій Зайдулович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Халімов Геннадій Зайдулович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.