Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0415U003148

Особливі позначки: відкрита

Дата реєстрації: 28-04-2015

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Настенко Андрій Олександрович
2. Nastenko Andrii Oleksandrovych

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: 31-03-2015

Спеціальність за освітою: 8.160105

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: 81.14.11.05

Тема дисертації:

1. Методи оцінки стійкості блокових симетричних шифрів на основі показників випадковості

2. Methods for assessing the resistance of symmetric block ciphers based on indicators of randomness

Реферат:

1. Дисертаційна робота присвячена обґрунтуванню адекватності моделювання блокових симетричних шифрів шляхом масштабування їх алгебраїчної структури для подальшої оцінки стійкості шифрів до атак диференційного та лінійного криптоаналізу на основі використання показників випадкових підстановок відповідного степеня. Вирішується науково-технічна задача з отримання аргументів і доказів того, що зменшені моделі блокових симетричних шифрів повторюють показники випадковості своїх прототипів. У роботі виконано комплекс досліджень з малими та повномасштабними моделями шифрів, зокрема, досліджені диференційні, лінійні, лавинні, кореляційні та статистичні показники шифрів. Виконані дослідження ґрунтовно свідчать про повторення малими версіями шифрів властивостей прототипів. Отримані результати впроваджено у навчальний процес Харківського національного університету радіоелектроніки, а також у діяльність Приватного акціонерного товариства "Інститут інформаційних технологій".

2. Thesis is devoted to the justification of the adequacy of the simulation block symmetric ciphers by scaling their algebraic structure for further assessing of resistance of ciphers to differential and linear cryptanalysis, using indicators of random permutations of corresponding degree. Scientific and technical challenge consists in getting arguments that the scaled models of block symmetric ciphers repeats indicators of randomness of their prototypes. The thesis represents a complex of research with small and full-scale cipher models, in particular, studies of differential and linear parameters, avalanche, correlation and statistical parameters of different block ciphers Research results confirm the adequacy of modelling symmetric block ciphers by scaling their algebraic structure. The results obtained are introduced into the learning process of the Kharkiv National University of Radioelectronics, as well as in the Private joint-stock company "Institute of Information Technologies."

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. Лисицька Ірина Вікторівна
2. Lisitskaya Irina Viktorovna

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Краснобаєв Віктор Анатолійович

2. Краснобаєв Віктор Анатолійович

Кваліфікація: д.т.н., 20.02.14

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. Рудницький Володимир Миколайович

2. Рудницький Володимир Миколайович

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

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Горбенко Іван Дмитрович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Горбенко Іван Дмитрович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.