Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0414U006047

Особливі позначки: відкрита

Дата реєстрації: 29-12-2014

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Яковлєв Сергій Володимирович
2. Yakovliev Serhiy Volodymyrovych

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: 22-12-2014

Спеціальність за освітою: 7.160101

Місце роботи здобувача: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: 03056, м.Київ, пр.Перемоги, 37

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): Д26.002.29

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

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

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: 03056, м.Київ, пр.Перемоги, 37

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 20.51.35

Тема дисертації:

1. Аналітичні оцінки стійкості немарковських симетричних блочних шифрів до диференціального криптоаналізу

2. Provable Security of Non-Markov Symmetric Block Ciphers against Differential Cryptanalysis

Реферат/анотація:

1. Робота присвячена розробленню та аналізу нових підходів до оцінювання теоретичної (доказової) стійкості ітеративних блочних шифрів до диференціального криптоаналізу та їх застосуванню до оцінювання стійкості схем блочного шифрування; основну увагу зосереджено на немарковських шифрах. Одержано аналітичні оцінки стійкості немарковських варіантів збалансованих та незбалансованих фейстель-подібних схем, узагальнених схем Фейстеля, SP-мереж загального та часткового виду. На основі результатів проведених досліджень створено новий алгоритм шифрування, доказово стійкий до диференціального криптоаналізу.

2. This work is dedicated to design and analysis of new approaches of provable security of iterated block ciphers against differential cryptanalysis, and to implement them for block cipher schemes' security evaluation. Non-Markov ciphers are mostly considered. Analytic evaluation of security against differential cryptanalysis was done for balanced and unbalanced Feistel-like schemes, generalized Feistel networks, SP-networks of common and

special forms. A new block cipher algorithm was created; its security against differential cryptanalysis was proven using presented theoretical results.

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. Савчук Михайло Миколайович
2. Savchuk Mykhaylo Mykolayovych

Кваліфікація: д.ф.-м.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. Кудін Антон Михайлович
2. Кудін Антон Михайлович

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. Яремчук Юрій Євгенович
2. Яремчук Юрій Євгенович

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	Новіков Олексій Миколайович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Новіков Олексій Миколайович
Відповідальний за підготовку облікових документів	
Реєстратор	

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.