Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0514U000223

Особливі позначки: відкрита

Дата реєстрації: 14-04-2014

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Олійников Роман Васильович

2. Oliynykov Roman Vasylyovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.05

Назва наукової спеціальності: Комп'ютерні системи та компоненти

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 26-03-2014

Спеціальність за освітою: 7.05010201

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): Д 64.052.01

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 аналізу і синтезу перспективних симетричних криптографічних перетворень

2. Methods for analysis and synthesis of perspective symmetric cryptographic transformations

Реферат/анотація:

1. Дисертаційна робота присвячена вирішенню актуальної науково-технічної проблеми синтезу симетричних криптографічних перетворень, які забезпечують високий рівень стійкості та швидкодії. Для основних типів криптоаналітичних атак на основі таблиці передобчислень вперше запропоновано методи оцінки складності виконання етапу побудови таблиць в умовах, коли потужність множини врахованих унікальних елементів близька до потужності множини значень невідомого стану криптографічного перетворення. Вперше запропонований метод порівняння високорівневих конструкцій симетричних блокових шифрів дозволяє визначити найкращу конструкцію на основі співвідношення стійкості до кількості раундів перетворення. Вперше запропонований метод синтезу блокових шифрів на основі таємних несюр'єктивних S-блоків дозволяє безключове читання криптограм для сторони, яка авторизована, і забезпечує стійкість щодо розкриття для інших сторін. Запропонований метод синтезу схем генерації циклових ключів блокових алгоритмів забезпечує небієктивну відповідність множин циклових ключів і ключів шифрування, захист від атак на зв'язаних ключах та підвищення стійкості до атак на реалізацію, зберігаючи стійкість до переборних

атак. Запропоновані методи дозволили розробити блоковий шифр "Калина" та ґеш-функцію "Купина", які мають високий та надвисокий рівень криптографічної стійкості та швидкодію, що перевищує іноземні аналоги на сучасних 64-бітових програмних платформах, і використані під час розробки проектів специфікацій національних стандартів України.

2. The thesis is dedicated to solving of the important scientific problem of symmetric cryptographic transformations synthesis providing high level strength and performance. For main types of cryptanalytic attacks based on precomputed tables methods of table computation stage complexity estimation in conditions where the set cardinality of accounted unique elements is near to unknown state values set cardinality of cryptographic transformation are proposed for the first time. Comparison method of block cipher high level constructions allows selection of the best construction based on strength to number of encryption rounds ratio is proposed for the first time. Method of block ciphers synthesis based on secret non-surjective S-boxes allows keyless decryption for authorized party and provides security to encrypted message compromising to any other unauthorized party is proposed for the first time. Proposed synthesis method of block cipher key schedule provides non-bijective correspondence of round key and encryption key sets, protection from related keys attacks and improving strength to side-channel attacks, keeping security against brute force attacks. Proposed methods allow development of block cipher "Kalyna" and hash function "Kupyna" providing high level of cryptographic strength and performance exceeding international standards on 64-bit software implementations. These cryptographic transformations were used during Ukrainian national cryptographic standards project development.

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. Gorbenko Ivan Dmytrovych

Кваліфікація: д.т.н., 20.01.09

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. Корченко Олександр Григорович
2. Корченко Олександр Григорович

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. 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. Харченко В'ячеслав Сергійович

2. Харченко В'ячеслав Сергійович

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Машталір Володимир Петрович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Машталір Володимир Петрович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.