Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0413U005662

Особливі позначки: відкрита

Дата реєстрації: 17-10-2013

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Мельничук Євген Дмитрович
2. Melnychuk Ievgen Dmytrovych

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: 24-09-2013

Спеціальність за освітою: 8.160101

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: 20.51.35

Тема дисертації:

1. Методи оцінки криптографічної придатності вузлів нелінійних замін блокових симетричних шифрів

2. Cryptographic suitability assessing methods for substitution units of symmetric block ciphers

Реферат/анотація:

1. Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 - системи захисту інформації. - Харківський національний університет радіоелектроніки МОН України, Харків, 2013. Дисертаційна робота присвячена додатковому обґрунтуванню одного з центральних положень нового методу, який полягає в тому, що показники стійкості сучасних шифрів на відміну від існуючих підходів від властивостей застосованих S-блоків практично не залежать. У роботі виконано комплекс досліджень з малими та повномасштабними моделями шифрів, зокрема досліджень диференціальних та лінійних показників шифрів при застосуванні в них різних, у тому числі й випадкових S-блоків, що ґрунтовно свідчать про справедливість вихідного положення. Запропоновано та випробувано для застосування в сучасних шифрах (Rijndael, Калина, Мухомор, Лабіринт) S-блоки випадкового типу, які не знижують показників стійкості цих шифрів до атак диференціального і лінійного криптоаналізу. В процесі досліджень обґрунтована вдосконалена модель випадкової підстановки, яка будується на основі використання відомих та додатково введених критеріїв відбору. Зокрема, встановлено що підстановки що пройшли ці критерії (за

інверсіями, зростаннями і циклами, а також додаткові критерії з використанням показників близькості законів розподілу переходів XOR таблиць та зміщень таблиць лінійних апроксимацій не є суттєво конструктивними для відбору підстановок з покращеними властивостями. У якості практичної доцільності підходу відбору випадкових підстановок сформульовано та теоретично обґрунтовано метод що ґрунтується на використанні властивостей вибірки випадкових підстановок який є узагальненням додатково введених критеріїв то дозволяє з високою ймовірністю отримувати підстановки, для яких значення максимумів диференціальних таблиць й максимумів зміщень таблиць лінійних апроксимацій співпадають з теоретичними значеннями максимумів таблиць випадкових підстановок. Ключові слова: блоковий симетричний шифр, диференціальний криптоаналіз, лінійний криптоаналіз, доказова стійкість, максимальна диференціальна ймовірність.

2. Thesis for a Ph.D. science degree by specialty 05.13.21 - information security systems. - Kharkiv National University of Radioelectronics of the MESYouthsport of Ukraine, Kharkiv, 2013. The thesis is devoted to additional justification of one of the central positions of the new method that in contrast to existing approaches is based on the following idea: the stability indices of modern ciphers do not depend on the properties of used S-blocks. The thesis represents a complex of research with small and full-scale cipher models, in particular the study of differential and linear parameters for ciphers using different types of substitutions, including random S-boxes. The research results indicate the validity of the original point. Keywords: the block symmetric cipher, differential cryptanalysis, linear cryptanalysis, provable security, the maximum differential probabilities.

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. Долгов Віктор Іванович

2. Dolgov Victor Ivanovych

Кваліфікація: д.т.н., 20.00.16

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. Єсін Віталій Іванович
2. Єсін Віталій Іванович

Кваліфікація: к.т.н., 20.02.12

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.