Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0415U001795

Особливі позначки: відкрита

Дата реєстрації: 21-04-2015

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Мордвінов Руслан Ігорович
2. Mordvinov Ruslan Irogovych

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: 24-03-2015

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. Моделі, методи та засоби дослідження режимів роботи блокових симетричних шифрів по критеріям стійкість - складність.

2. Models, methods and tools for the study of symmetric modes of the block cipher criteria for stability - complexity

Реферат:

1. У дисертаційній роботі запропоновано та обґрунтовано методи дослідження статистичних властивостей випадкових послідовностей. Запропоновано метод статистичного тестування, який заснований на наборі тестів NIST STS, але відрізняється тим, що враховує похибки вихідних послідовностей та дає оцінку не тільки послідовності зокрема, а й джерелу послідовності в цілому. Це стало можливим завдяки використанню теорії ймовірності та проходженню тестів на великій кількості (100 шт.) послідовностей для одного джерела даних. Отримано результати статистичного тестування для БСШ ДСТУ ГОСТ 28147:2009, AES, Belt, Camellia, та БСП "Калина". Отримані результати показали високі статистичні властивості з точки зору випадковості, що є гарним показником для БСШ. Крім того тестування показало, що отримана оцінка є дуже точною, оскільки під час повторного тестування з іншими вхідними даними отримано майже таку саму оцінку. Розроблено прискорену математичну модель, яка дозволяє значно підвищити швидкодію БСП "Калина" за рахунок

використання таблиці передобчислень, яка замінює елементи, що часто використовуються у алгоритмі.

2. In the thesis proposed and proved methods of statistical properties of random sequences. The method of statistical testing, which is based on a set of tests NIST STS, but differs in that takes into account the error output sequences and evaluates not only the sequence in particular, but also the source of a whole sequence. This is made possible through the use of probability theory and testing on a large number (100 pcs.) Sequences for a data source. The results of statistical tests for SBC GOST 28147:2009, AES, Belt, Camellia, and SBC "Kalina". The results showed high statistical properties in terms of cases, which is a good indicator for SBC. Besides testing has shown that the resulting score is very accurate, because retest with other inputs received nearly the same assessment in testing. Developed accelerated mathematical model that can significantly accelerate the speed of the SBC "Kalina" by using the precomputing table which replaces often usable elements of the algorithm.

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. Толюпа Сергій Васильович

2. Толюпа Сергій Васильович

Кваліфікація: д.т.н., 05.12.02

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. Неласа Ганна Вікторівна

2. Неласа Ганна Вікторівна

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 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.