Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0417U004025

Особливі позначки: відкрита

Дата реєстрації: 26-10-2017

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Лавданський Артем Олександрович
2. Lavdanskyi Artem Oleksandrovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат 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: 05-10-2017

Спеціальність за освітою: 8.091501

Місце роботи здобувача: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: 18006, м. Черкаси, бульвар Шевченка, 460

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 73.052.04

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, 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: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: 18006, м. Черкаси, бульвар Шевченка, 460

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 28.21.19

Тема дисертації:

1. Методи та засоби формування псевдовипадкових послідовностей для комп'ютерної криптографії.

2. Methods and tools of forming pseudorandom sequences for computer cryptography.

Реферат/анотація:

1. Дисертаційна робота присвячена питанням розробки нових та вдосконалення існуючих методів і засобів формування та тестування псевдовипадкових послідовностей для комп'ютерної криптографії. Розроблено метод перетворення послідовності слів у рівномірно розподілену на всій області можливих значень за довільних значень параметрів генераторів на основі лінійного конгруентного методу та регістра зсуву з лінійними зворотними зв'язками. Удосконалено комбінаційний метод формування псевдовипадкових послідовностей за рахунок використання множини перестановок та комбінуючої функції підсумовування за модулем або мультиплексування. Розроблено метод чисельного оцінювання автокореляційної функції.

2. The dissertation is devoted to actual issues of developing new and improving existing methods and tools of forming and testing pseudorandom sequences for computer cryptography. The method of converting a sequence of words in a uniformly distributed one throughout the region of possible values is offered. Combination method for the formation of pseudorandom sequences has been improved by using a set of permutations using the combination with module or multiplexing function. The proposed method for evaluation of autocorrelation

function allows to determine statistical deviations by determining statistical properties of the coefficients of autocorrelation of sequence of numbers.

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. Фауре Еміль Віталійович
2. Faure Emil Vitaliiovych

Кваліфікація: к.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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Халімов Геннадій Зайдулович
2. Халімов Геннадій Зайдулович

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

Власне Прізвище Ім'я По-батькові:

1. Корченко Анна Олександрівна
2. Корченко Анна Олександрівна

Кваліфікація: к.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	Рудницький Володимир Миколайович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Рудницький Володимир Миколайович
Відповідальний за підготовку облікових документів	
Реєстратор	

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.