Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0419U003311

Особливі позначки: відкрита

Дата реєстрації: 04-07-2019

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Козловська Світлана Григорівна
2. Kozlovska Svitlana H.

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: 27-06-2019

Спеціальність за освітою: Технологія машинобудування, металорізальні станки та інструменти

Місце роботи здобувача: Східноєвропейський університет економіки і менеджменту

Код за ЄДРПОУ: 14204539

Місцезнаходження: вул. Нечуя-Левицького, 16, м. Черкаси, Черкаський р-н., Черкаська обл., 18036, Україна

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: 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

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 20.01, 20.55.01

Тема дисертації:

1. Методи синтезу груп симетричних операцій для потокового шифрування

2. Methods of synthesis of symmetric operations groups for stream encryption

Реферат/анотація:

1. Дисертаційну роботу присвячено підвищенню якості систем потокового шифрування конфіденційної інформації за рахунок збільшення стійкості та варіативності перетворення завдяки додатковому використанню груп двохоперандних двохрозрядних операцій синтезованих на основі додавання за модулями два та чотири. Для цього розроблено метод побудови та дослідження двохоперандних операцій криптоперетворення на основі результатів обчислювального експерименту, шляхом формалізації, класифікації та математичного перетворення. Розроблено методи синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування завдяки результатам обчислювального експерименту шляхом застосування результатів реалізації розробленої технології та табличного представлення класифікації групи одноопераднних двохрозрядних операцій криптографічного перетворення, а також встановлення нових раніше невідомих взаємозв'язків між одноопераднними та двохоперандними операціями. Удосконалено метод підвищення стійкості та надійності потокового шифрування на основі додаткового застосування синтезованих груп симетричних двохоперандних операцій криптографічного

перетворення інформації, що забезпечило підвищення стійкості та варіативності потокового шифрування.

2. The thesis is devoted to the improvement of the confidential information's stream ciphering systems at the expense of increasing the stability and variability of transformation basing on the additional use of two-operand two-bit operations' groups synthesized on the bases of modulo-2 and modulo-4 addition. For this purpose, a method for constructing and investigating the two-operand operations of cryptographic transformation based on the results of a calculation experiment, through formalization, classification and mathematical transformation has been developed. The synthesizing methods of symmetric two-bit two-operand stream ciphering operations' groups based on the results of a calculation experiment are developed using the implementation results of the developed technology and the table representation of the group's classification of the one-operand two-bit operations of cryptographic transformation, as well as establishing the new previously unknown relationships between one-operand and two-operand operations. The method of increasing the stability and reliability of stream ciphering basing on the additional application of the synthesized groups of symmetric two-operand operations of cryptographic information transformation has been improved, which has provided increased stability and variation of stream ciphering.

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. Рудницький Володимир Миколайович
2. Rudnytskyi Volodymyr M.

Кваліфікація: д. т. н., 05.13.06

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. Кулик Анатолій Ярославович

2. Kulyk Anatolii Ya.

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. Пархуць Любомир Теодорович

2. Parhuts Liubomyr T.

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Рудницький Володимир Миколайович

Власне Прізвище Ім'я По-батькові головуючого на засіданні

Первунінський Станіслав Михайлович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.