Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0417U001889

Особливі позначки: відкрита

Дата реєстрації: 28-04-2017

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Навроцький Денис Олександрович

2. Navrotskyi Denys

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: 13-04-2017

Спеціальність за освітою: 8.091003

Місце роботи здобувача: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: 03058,Україна,м.Київ,Просп.Космонавта Комарова,1

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 26.062.17

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова 1, м. Київ, Київська обл., 03058, 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: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: 03058,Україна,м.Київ,Просп.Космонавта Комарова,1

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 побудови симетричних криптографічних шифрів з використанням тривимірних керованих перетворень

2. Methods of Constructing Symmetric Cryptographic Ciphers Using Three-Dimensional Controlled Transformations

Реферат:

1. Дисертаційна робота присвячена розв'язанню актуального науково-практичного завдання розроблення і дослідження нових більш ефективних методів побудови симетричних криптосистем (блокових та потокових шифрів) для підвищення ефек-тивності захисту інформації. Отримані в дисертаційній роботі результати можуть бути використані для підвищення ефективності (захищеності, швидкості роботи, зменшення ресурсоємності) систем захисту. У роботі розроблено методи тривимірних матричних перетворень, на основі яких побудовані динамчно керовані криптографічні примітиви. Розроблені елементи узагальнених тривимірних перетворень Грея, які окрім класичних (лівосторонніх) і так званих правосторонніх та складених кодів містять рандомізовані коди Грея, на основі яких вирішені окремі проблеми побудови динамічно керованих криптографічних примітивів. Синтезовані тривимірні криптографічні примітиви перемішування, нелінійної заміни, матричного перетворення, стохастичного циклічного зсуву, «ковзного»

кодування. Удосконалено методики синтезу примітивних матриць Галуа і Фібоначчі, а також їх сполучених варіантів над простими полями Галуа характеристики 2, що дозволило як розширити множину узагальнених генераторів псевдовипадкових послідовностей, так і запропонувати нові підходи до розв'язання проблеми формування таємних ключів шифрування абонентами мережі з відкритими каналами зв'язку. Отримали подальший розвиток методи симетричного блокового криптографічного перетворення інформації з динамічно керованими параметрами шифрування (криптографічні перетворення виконуються в тривимірному простору і в алгоритмах шифрування здійснюється оперативна модифікація параметрів криптографічних примітивів під час переходу до чергового блоку тексту, що перетворюється). Розроблено криптографічний протокол для захисту командної і телеметричної інформації БПЛА. Розроблено, виготовлено і апробовано апаратно-програмні реалізації 3D шифраторів.

2. The dissertation addresses practical problems in modern cryptography by presenting new and more effective methods of constructing symmetric key cryptosystems (i.e. block and stream ciphers) in order to improve information security. Obtained results prove efficiency increase (improved quality of cryptography, increased speed, improved re-source management) of the presented cipher implementation. This work deals with the three-dimensional matrix transformation methods of building dynamically controlled cryptographic primitives. In particular, a generalization of the three-dimensional Gray transformations has been developed, which apart from the classical (left-side) and the so-called right-side and compound code, also includes randomized Gray codes, allowing to solve a number of problems related to constructing dynamically controlled cryptographic primitives. Besides, three-dimensional cryptographic shuffle primitives have been synthe-sized, as well as primitives for non-linear substitutions, matrix transformation, stochastic cyclic shift and «sliding» encoding. Furthermore, methods for a primitive Galois and Fibonacci matrices synthesis are improved, as are their jointed compounds over finite Galois fields of characteristic two, allowing to expand generalized pseudo-random se-quence generators' set, as well as to propose new approaches to a problem of providing secret encryption keys for communication network participants over open channels. A further development in the methods of symmetric block transformation with dynamically controlled parameters of encryption is provided, in particular, the cryptographic transfor-mations are performed in a three-dimensional space and the parameters of cryptographic primitives during encryption are modified each time a new block of text is being pro-cessed. Moreover, a cryptographic communication protocol is developed to encode telem-etry information of unmanned aerial vehicle. Hardware and software for 3D cipher proto-type are manufactured and successfully tested.

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. Білецький Анатолій Якович

2. Beletsky Anatoly

Кваліфікація: д.т.н., 05.12.04

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. Лужецький Володимир Андрійович

2. Лужецький Володимир Андрійович

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. Рудницький Володимир Миколайович

2. Рудницький Володимир Миколайович

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Корченко Олександр Григорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Корченко Олександр Григорович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.