Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0413U004093

Особливі позначки: відкрита

Дата реєстрації: 11-06-2013

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Ісаєв Сергій Олександрович

2. Isaev Sergii Oleksandrovich

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: 14-05-2013

Спеціальність за освітою: 8.080401

Місце роботи здобувача: Харківський національний університет імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: Україна, 61022, м. Харків, майдан Свободи,4

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 імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: Україна, 61022, м. Харків, майдан Свободи,4

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. Обчислювальні методи синтезу нелінійних вузлів замін для підвищення ефективності симетричних криптоперетворень

2. Computational synthesis methods of nonlinear substitution blocks to improve the efficiency of symmetric crypto transformations

Реферат:

1. Об'єкт - процес синтезу нелінійних вузлів замін симетричних криптоперетворень. Мета - підвищення ефективності симетричних криптоперетворень на основі синтезу нелінійних вузлів замін з покращеними властивостями. Методи - методи математичного моделювання, теорії захисту інформації, математичний апарат булевої алгебри, теорії скінченних полей, теорії ймовірностей і математичної статистики. Апаратура - персональний комп'ютер. Теоретичні і практичні результати - розв'язано низку актуальних наукових і практичних задач, які стосуються розвитку та вдосконаленню математичної моделі та обчислювальних методів синтезу нелінійних вузлів замін з покращеними властивостями з використанням математичного апарату недвійкових криптографічних функцій. Розроблено та програмно реалізовано низку обчислювальних алгоритмів, які дозволяють формувати регулярні вузли заміни з покращеними криптографічними властивостями, а також оцінювати ефективність зменшених версій сучасних блокових

шифрів. Наукова новизна - набула подальшого розвитку математична модель регулярних нелінійних вузлів замін симетричних криптоперетворень з використанням недвійкових криптографічних функцій в арифметиці скінчених полів; удосконалено обчислювальний метод синтезу нелінійних вузлів замін (метод імітації відпалу) шляхом розробки критеріїв пошуку з використанням спектральних та кореляційних властивостей недвійкових криптографічних функцій та динамічних вагових коефіцієнтів; набув подальшого розвитку обчислювальний метод прогнозування оцінок ефективності симетричних криптоперетворень на основі дослідження диференційних і лінійних властивостей зменшених моделей шифрів з урахуванням показників нелінійності та автокореляції використовуваних нелінійних вузлів замін; набули подальшого розвитку методи оцінки обчислювальної ефективності ймовірнісного (побітового) синтезу регулярних нелінійних вузлів замін із заданими криптографічними показниками. Отримано акти реалізації результатів досліджень на виробництві у діяльності ТОВ "Мікрокрипт Текнолоджіс" та у навчальному процесі Харківського національного університету ім. В.Н. Каразіна. Результати дисертаційної роботи рекомендується використовувати при проведенні науково-дослідних та дослідно-конструкторських робіт зі створення нових криптографічних засобів захисту інформації, для підготовки спеціалістів у вищих навчальних закладах Міністерства освіти і науки України при вивченні учбових дисциплін з теорії захисту інформації.

2. Object - the process of synthesis of nonlinear substitution boxes of symmetric crypto transformations. Purpose - improvement of the efficiency of symmetric crypto transformations based on the synthesis of nonlinear substitution boxes with improved properties. Methods - methods of mathematical modeling, information security theory, the mathematical apparatus of Boolean algebra, the theory of finite fields, the theory of probability and mathematical statistics. Theoretical and practical results - solved a number of relevant scientific and technical issues related to the development and improvement of mathematical model and computational methods of synthesis of substitution boxes with improved properties using a mathematical apparatus of non-binary cryptographic functions. A number of computing algorithms that form regular substitution blocks with improved cryptographic properties, and also evaluate the effectiveness of the reduced models of modern block ciphers are designed and impleneted. Scientific novelty - the mathematical model of regular nonlinear boxes of cryptotransformations using symmetric non-binary cryptographic functions in arithmetic of finite fields is developed, method for the synthesis of nonlinear substitution boxes (the method of simulated annealing) through the development of search criterions using spectral and correlation properties of non-binary cryptographic functions and dynamic weights is improved; computational method for forecasting efficiency evaluations of symmetric cryptotransformations based on the study of differential and linear properties of the reduced cipher models with accounting of nonlinearity and autocorrelation properties of used nonlinear substitution boxes is developed, computational methods for evaluating the computational effectiveness of probabilistic (bit-to-bit) synthesis of regular nonlinear substitution boxes with given cryptographic properties are developed. The acts of the realization of the research results in the production of JSC "Microcrypt Technologies", and in the educational process of Kharkiv National University named after V.N. Karazin are received. The results of the thesis are recommended to use when carrying out scientific-research and research-constructional works on development of new cryptographic means of protection information, in higher educational institutions of the Ministry of Education and Science of Ukraine in the study of subjects on information protection theory.

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. Сорока Леонід Степанович

2. Soroka Leonid Stepanovich

Кваліфікація: д.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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Олексійчук Антон Миколайович

2. Олексійчук Антон Миколайович

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

Власне Прізвище Ім'я По-батькові:

1. Потій Олександр Володимирович

2. Потій Олександр Володимирович

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 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.