Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0408U004786

Особливі позначки: відкрита

Дата реєстрації: 31-10-2008

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Бевз Олександр Миколайович

2. Bevz Olexander Mikolayevich

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: ні

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: 03-10-2008

Спеціальність за освітою: 7.091401

Місце роботи здобувача: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: 21021 м. Вінниця, вул. Хмельницьке шосе, 95

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 05.052.01

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, 95, м. Вінниця, Вінницький р-н., Вінницька обл., 21021, 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: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: 21021 м. Вінниця, вул. Хмельницьке шосе, 95

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.41.23

Тема дисертації:

1. Методи шифрування на основі високонелінійних бульових функцій та кодів з максимальною відстанню
2. Cipher methods based on high nonlinear boolean functions and the maximal distance codes

Реферат/анотація:

1. Об'єкт дослідження - процес обробки та перетворення даних для захисту інформації в комп'ютерних системах та мережах. Мета дослідження - підвищення ефективності захисту інформації в комп'ютерних системах та мережах на основі розробки нових методів та засобів шифрування. Методи досліджень: теорія алгебраїчного кодування, теорія ймовірності, абстрактна алгебра, лінійна алгебра. Наукова новизна одержаних результатів полягає у запропонувані нового підходу до формування максимально нелінійної бульової функції від восьми аргументів, яка, на відміну від існуючих, характеризується збалансованістю, що дозволяє покращити статистичні властивості шифру; запропонувані нового методу формування блочних шифрів в комп'ютерних системах та мережах, який, на відміну від існуючих, використовує криптографічно стійкі S-бокси, за рахунок диференційних і нелінійних властивостей яких підвищено ефективність протидії до криптаналізу і швидкість шифрування; вперше розробленому методі формування поточного шифру на основі регістру зсуву з лінійним зворотним зв'язком, який на відміну від існуючих, має низьку

обчислювальну складність, просту апаратну реалізацію і високі криптографічні властивості, за рахунок застосування в якості фільтр-функції максимально нелінійної збалансованої булевої функції; подальшому розвитку методу обчислення змісту S-боксу, який на відміну від існуючих має високу швидкість реалізації за рахунок використання табличної підстановки; удосконалені методу формування лінійного перетворення, який на відміну від існуючих забезпечує вищу ефективність шифрування в 1,5 рази за рахунок ефективного застосування конкатенації коду з максимальною відстанню на верхньому та нижньому рівні лінійного перетворення. Практичне значення одержаних результатів полягає в розробці методики захисту інформації на основі реалізації блочного шифру в комп'ютерних системах та мережах; створенні алгоритму та програмніх засобів для ефективного захисту інформації; розробці алгоритму реалізації процедури формування S-боксу; розробці алгоритмутабличної реалізації процедури формування S-боксу; розробці алгоритму табличної реалізації формування підстановочно-перестановочної мережі. Ступінь впровадження - в межах галузі. Сфера (галузь) застосування - системи управління та системи передавання інформації.

2. Object of the research - the process of handling and transforming the data for the defence information for the computing systems and networks. Aim of research - increasing the effectiveness defence information for computing system and networks, which based on design the new methods and the tools of ciphering. Methods of research: theory algebraic coding, theory probability, abstract algebra, linear algebra. Scientific novelty of the reception result - proposal the new approach to the forming eight arguments maximal nonlinear boolean function, which difference for a present, have balancing, to permit improvement the statical property cipher; proposal the new method to forming the block cipher for computing systems and networks, which difference for a present, to have cryptographic security S-boxes, due to differential and nonlinear property increasing effectiveness resistance to the cryptoanalys and the rate of the ciphering; for the first time designing the method to form the stream cipher, basedon the linear feedback shift register, which difference for a present, to have a filter-function as the maximal nonlinear balance boolean function, and to possessed of low the computational complexity, simplicity hardware and the high cryptographic property; further development of the method computation of S-box, which difference for a present, to have the high rate of work, due to use the table substitution; improving the method to forming of linear transformation, which difference for a present to have high effectiveness the ciphering to 1,5 value, due to effective use concatenation the code maximal distance on high and low level of the linear transformation. Practical sense of the received results consist of design the strategy defence guarding based on realization the block cipher for the computing systems and networks; creation the algorithm and the program tools for a effective guarding; designing the algorithm of the procedure forming S-box, the algorithm of the table substitution the procedure creation S-box; designing the algorithm of the table realization the forming the substitution-permutation network. Degree of embedding is allocation by bounding branch. Branch of application - systems of control and systems of transfer information.

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. Квєтний Роман Наумович

2. Kvetny Roman Naumovich

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. 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. Горпенюк Андрій Ярославович

2. Горпенюк Андрій Ярославович

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	Мокін Борис Іванович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Мокін Борис Іванович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.