Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0412U000854

Особливі позначки: відкрита

Дата реєстрації: 17-04-2012

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Якименко Ігор Зіновійович
2. Iakymenko Igor Zinoviyovych

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: 22-03-2012

Спеціальність за освітою: 6.040201

Місце роботи здобувача: Тернопільський національний економічний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: 46020, м. Тернопіль, вул. Львівська, 11

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): К58.082.02

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Тернопільський національний економічний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: 46020, м. Тернопіль, вул. Львівська, 11

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 81.14.11.05

Тема дисертації:

1. Методи та алгоритми опрацювання інформаційних потоків в комп'ютерних мережах за умови застосування еліптичних кривих

2. Methods and Algorithms for Processing of Information Flow in Computer Networks with using Elliptic curves

Реферат:

1. В дисертаційній роботі вперше розроблено методи, отримано аналітичні вирази характеристик часової складності та розроблено високопродуктивні алгоритми опрацювання ІП у КМ за умови застосування ЕК на основі модульно-матричних операцій в ТЧБ Радемахера-Крестенсона, які склали теоретичну основу зменшення часової складності компонентів алгоритму Шуфа, що на відмінно від існуючих дозволили зменшити часову складність з експоненційної до лінійної або лінійно-логарифмічної. Отримали подальший розвиток методи захисту ІП з використанням ЕК на основі генерування їх параметрів, що дозволило зменшити часову складність алгоритмів пошуку залишків чисел великої розрядності, знаходження НСД, модулярного множення, експоненціювання та пошуку оберненого елементу за модулем за рахунок використання ТЧБ Радемахера - Крестенсона, що дозволило зменшити на 1-2 порядки часову складність базових операцій алгоритму Шуфа. Розроблено високопродуктивні програмно-апаратні засоби реалізації модульних операцій над числами великої розрядності та розроблено схемотехнічні рішення відповідних

спеціалізованих процесорів. Результати досліджень використані в навчальному процесі на кафедрах комп'ютерної інженерії та спеціалізованих комп'ютерних систем при викладанні дисциплін: "Комп'ютерні системи", "Захист інформації в комп'ютерних системах", "Проектування спеціалізованих комп'ютерних систем", а також впроваджені на ТОВ ТКБР "Стріла" для захисту інформаційних потоків в дистрибутивних та корпоративних комп'ютерних мережах.

2. In the dissertation paper presents theoretical justification and new solutions of development and improvement scientific problems of efficiency increasing methods and time complexity reducing of software and hardware implementation of processing data flows algorithms in case, when used EC. In first proposed methods, derived analytical expressions of temporal characteristics of complexity and processing algorithms, which developed high information flow in computer networks, in case of elliptic curves using based on modular-matrix operations in TDB Rademacher-Krestenson, which passed the theoretical basis for reducing time complexity of Schoof algorithm components and allowed to reduce the time complexity from exponential to linear or quadratic. Information providing of computerized system for the stability measurement of EC Schoof algorithm, based on parallelization process subtasks optimization had been improved, thus improving the assessment accuracy of resistance level of information flow in existing and created computer networks. The methods of protecting information flows using the EC, based on generation of their parameters, received further development, thus allowing to reduce the time complexity of search algorithms remains large numbers, finding the greatest common divisor, modular multiplication, exponentiation and finding the inverse element for the module by using TDB Rademacher-Krestenson which allowed to reduce by 1-2 orders of time complexity of Schoof algorithm basic operations. A high-performance software and hardware implementations of modular operations realisation on large numbers had been developed and designed circuit solution of the corresponding processors. Results of the research used in the educational process at Department of Computer Engineering and Specialized Computer System at teaching subjects: "Computer Systems", "Research and design of computer systems and networks", "Information protection in computer systems", "Design of specialized computer systems and implemented on Ltd. TKBR "Strila" for the information flow protecting in distributed and corporate computer networks.

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. Николайчук Ярослав Миколайович
2. Nykolaychuk Yaroslav Mykolayovych

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Бєссалов Анатолій Володимирович
2. Бєссалов Анатолій Володимирович

Кваліфікація: д.т.н., 20.02.14

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. Головко Володимир Адамович
2. Головко Володимир Адамович

Кваліфікація: д.т.н., 05.13.01

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