Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0520U100472

Особливі позначки: відкрита

Дата реєстрації: 21-09-2020

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Касянчук Михайло Миколайович
2. Kasianchuk Mykhailo

Кваліфікація: к. ф.-м. н., 01.04.10

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор наук

Аспірантура/Докторантура: ні

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: 27-08-2020

Спеціальність за освітою: 123 Комп'ютерна інженерія

Місце роботи здобувача: Тернопільський національний економічний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: вул. Львівська, 11, м. Тернопіль, Тернопільський р-н., Тернопільська обл., 46009, 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): 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: Тернопільський національний економічний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: вул. Львівська, 11, м. Тернопіль, Тернопільський р-н., Тернопільська обл., 46009, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик:

Тема дисертації:

1. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики

2. Methods of multi-digit numbers processing in asymmetric cryptosystems based on modular arithmetic

Реферат/анотація:

1. Дисертаційна робота присвячена вирішенню актуальної науково-практичної проблеми підвищення ефективності опрацювання багаторозрядних чисел на основі використання векторно-модульних методів модулярного множення та експоненціювання, ДФ та МДФ СЗК. Розроблено методи пошуку оберненого елемента за модулем та виконання КТЗ на основі додавання модуля та додавання залишку. Розроблено метод пошуку мультистепеневої функції за модулем. Розроблено методи пошуку набору модулів СЗК, який забезпечує уникнення громіздкої операції знаходження мультиплікативного оберненого елемента за модулем. Обґрунтовано доцільність використання МДФ СЗК в асиметричних криптосистемах. Удосконалено метод Ферма для факторизації багаторозрядних чисел. Розроблено трьохмодульну криптосистему Рабіна, яка дозволила розширити блок шифрування. Розроблено методологію опрацювання багаторозрядних чисел, застосування якої дає можливість використовувати розроблені методи в єдиній стратегії опрацювання

багаторозрядних чисел в асиметричних криптосистем.

2. The thesis is devoted to solving the urgent scientific and practical problem of increasing the efficiency of multi-digit numbers processing based on the use of vector-modular operations of modular multiplication and exponentiation, the perfect (PF) and the modified perfect forms (MPF) of the residue number system (RNS) to reduce time complexity, increase speed algorithms, specific software and hardware in asymmetric cryptosystems. The methods for searching the inverse element by modulo and performing the Chinese Remainder Theorem based on adding a module and adding a remainder were developed, which make it possible to parallelize the process of searching for the inverse element by modulo and, correspondingly, reduce the time complexity of this operation when it is used in asymmetric cryptosystems by using modular operation of adding the module or remainder. A method has been developed for searching for a multi-degree function by modulo, which avoids the operation of modular exposure of multi-digit numbers due to the double use of the Euler function, performing arithmetic operations on operands, less than a given module, and switching to linear congruence. Also, the method has been proposed for exploration of a set of RNS modules, which, by calculating the coefficients of basic numbers based on analytical expressions when restoring a decimal number from a RNS, avoided the cumbersome operation of finding the multiplicative inverse element by modulo, respectively reducing the time complexity and increasing the speed of computing systems. Methods for constructing sets of PF RNS modules on the basis of fractional transformations and factorization were developed, which could reduce the time and hardware complexity when converting numbers from RNS to a decimal number system by avoiding the search for a multiplicative inverse element by modulo and multiplying by it. Also, methods for constructing a three- and multi-module MPF RNS were discovered, which, through the use of analytical expressions obtained on the basis of fractional transformations, factorization, Viet's theorem, and solutions of congruence systems, could reduce the length of operands in intermediate calculations, and avoided the operation of searching for the inverse element modulo and multiplying by it, reducing, respectively, the time complexity when restoring a decimal number from RNS. The expediency of using the MPF RNS in asymmetric cryptosystems instead of the existing integer form was substantiated. The Fermat's method for multi-digit numbers factorization has been improved, which made it possible to reduce the lengths of operands, simplify the search for factorization of digits, and increase the speed of calculations for factors of different lengths by replacing the square root extraction and squaring at each iteration with computationally simple addition and subtraction operations. A three-module Rabin's cryptosystem was developed, which allowed to increase the speed of encryption and decryption processes compared to the usual integer form and to expand the encryption block without reducing the stability of the cryptosystem due to the generalization of the methods for constructing MPF RNS and their using. Also we have discovered the methodology of multi-digit numbers processing, which, through the use of matrix and vector-modular methods for finding the remainder, modular multiplication and exponentiation, finding the inverse element by adding a module or remainder, and also using the PF and MPF RNS, allowed to reduce the computational complexity and improve performance algorithms, specialized software and hardware in asymmetric cryptosystems. The application of presented methodology makes its possible to use the developed methods in a universal strategy for multi-digit numbers processing in the field of asymmetric cryptosystems and to efficiently build of highspeed cryptographic information protection systems.

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. Nykolaichuk 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

Власне Прізвище Ім'я По-батькові:

1. Карпінський Микола Петрович
2. Karpinski Mikolay

Кваліфікація: д.т.н., 05.11.05

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. 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

Власне Прізвище Ім'я По-батькові:

1. Карпінський Микола Петрович

2. Karpinski Mikolay

Кваліфікація: д.т.н., 05.11.05

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. Казакова Надія Феліксівна

2. Kazakova Nadiia

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. Олійников Роман Васильович
2. Oliynykov Roman

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. Білецький Анатолій Якович
2. Beletskiy Anatoliy

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

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.