Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0420U102445

Особливі позначки: відкрита

Дата реєстрації: 29-12-2020

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Новокшонов Андрій Костянтинович
2. Novokshonov Andrii Kostiantynovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 01.05.03

Назва наукової спеціальності: Математичне та програмне забезпечення обчислювальних машин і систем

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 17-12-2020

Спеціальність за освітою: Інформатика

Місце роботи здобувача: Міжнародний науково-навчальний центр інформаційних технологій та систем НАН та МОН України

Код за ЄДРПОУ: 24741741

Місцезнаходження: пр.Академіка Глушкова,40, м. Київ, Київська обл., 03187, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.001.09

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, буд. 60, м. Київ, Київська обл., 01033, 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: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, буд. 60, м. Київ, Київська обл., 01033, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.41, 50.07

Тема дисертації:

1. Методи контролю цілісності делегованих обчислень

2. Methods for controlling integrity of delegated computations

Реферат:

1. Дисертаційну роботу присвячено проблемі перевірки правильності виконання обчислень віддаленим пристроєм, який не є довіреним для користувача. Розроблено систему алгоритмів контролю цілісності обчислень для обмеженого класу функцій над цілими числами довільної, заздалегідь не фіксованої довжини. У дисертаційній роботі побудовано нову адитивно гомоморфну схему автентифікації цілочисельних даних довільної довжини, яка дозволяє контролювати процес виконання операцій додавання та віднімання над ними. Розроблено нове для галузі перевірки цілісності обчислень застосування моделі обчислень додавальної машини. Сформульовано та доведено практично важливі умови цілісності обчислень для конструкцій умовних розгалужень та циклів із заздалегідь не фіксованою кількістю ітерацій. Побудовано алгоритми контролю цілісності для варіанту моделі обчислень додавальної машини з цілочисельними регістрами довільної довжини. На основі розроблених алгоритмів програмно реалізовано прототип системи

перевірки цілісності обчислень.

2. The dissertation is devoted to the problem of verifying correctness of computations performed by a remote device that is not trusted by the user. A system of algorithms for checking integrity of computations has been developed for a limited class of functions over integers of arbitrary length. A new additively homomorphic authentication scheme for integer data of arbitrary length is constructed, which allows controlling the process of performing addition and subtraction operations on them. A new application of the addition machine model of computation is developed for the industry of controlling computation integrity. Practically important conditions for checking integrity of conditional statements and general loops are formulated and proved. Algorithms for checking integrity of computations are constructed for a variant of the addition machine model of computation with integer registers of arbitrary length. Using developed algorithms, a prototype of the software system for controlling integrity of computations is implemented.

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. Анісімов Анатолій Васильович
2. Anisimov Anatolii Vasylovych

Кваліфікація: д. ф.-м. н., 01.05.01

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. Савчук Михайло Миколайович
2. Savchuk Mykhailo Mykolaiovych

Кваліфікація: д.ф.-м.н., 01.05.01

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. Фаль Олексій Михайлович
2. Fal Oleksii Mykhailovych

Кваліфікація: к. ф.-м. н., 01.01.05

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 Анісімов Анатолій Васильович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Погорілий Сергій Дем’янович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.