Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0413U004830

Особливі позначки: відкрита

Дата реєстрації: 18-07-2013

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Кулага Анатолій Анатолійович
2. Kulaga Anatolij Anatolijovych

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: 27-06-2013

Спеціальність за освітою: 7.04030201

Місце роботи здобувача: Служба безпеки України

Код за ЄДРПОУ: 00034074

Місцезнаходження: 01601, м. Київ, вул. Володимирська, 33

Форма власності:

Сфера управління: Секретаріат президента 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, 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: 01033, м. Київ, вул. Володимирська, 64

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.41.25

Тема дисертації:

1. Розробка білінійних протоколів захисту інформації.

2. Information Protection Bilinear Protocols Development.

Реферат:

1. Дисертацію присвячено розробці моделей білінійних математичних протоколів, які можуть бути використані при створенні розподілених інформаційних систем та забезпечують взаємодію розподілених систем за умов взаємної недовіри сторін інформаційного обміну. За результатами досліджень запропоновані багатобічні мультилінійні протоколи одночасного підпису та шифрування; показано можливість побудови за допомогою GDH груп Ель-Гамаля - подібних схем цифрового підпису з відкритим індивідуальним ключем та запропоновано білінійні схеми цифрового підпису з їх пороговими варіантами та схеми засліпленого підпису; розроблено ітеративний білінійний протокол доведення знання розв'язку задачі Діффі-Хеллмана з нульовим розголошенням. На підставі проведеного дослідження запропоновано програмну реалізацію розроблених білінійних схем цифрового підпису.

2. The aim of the thesis is analysis and development of bilinear mathematics protocols to be applied for building of distributed information systems and providing distributed system interactions under mutual distrust of information exchange parties. According to the research results multilinear SignCryption protocols for n-parties were proposed; building of identity-based ElGamal-type signature schemes with the GDH groups was demonstrated; bilinear digital signature schemes with their threshold variants and blind signature schemes were proposed as well as iterative bilinear protocol of zero-knowledge proof of Diffie-Hellman problem solution was developed. The bilinear digital signature schemes protocol was developed on the bases of the research performed.

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 Anatolij Vasylijovych

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. Савчук Михайло Миколайович

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. Фаль Олексій Михайлович

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 Редько Володимир Никифорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Редько Володимир Никифорович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.