Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0417U003983

Особливі позначки: відкрита

Дата реєстрації: 09-11-2017

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Шевцов Олексій Володимирович
2. Shevtsov Oleksiy Volodymyrovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

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: 12-10-2017

Спеціальність за освітою: 8.17010101

Місце роботи здобувача: Харківський національний університет імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: Україна, 61022, м. Харків, майдан Свободи,4

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 64.051.29

Повне найменування юридичної особи: Харківський національний університет імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, м. Харків, Харківський р-н., Харківська обл., 61022, 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: Харківський національний університет імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: Україна, 61022, м. Харків, майдан Свободи,4

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Моделі та методи пост-квантового електронного підпису у фактор-кільцях поліномів та на кодових конструкціях

2. Models and methods of postquantum lattice based and code based digital signatures

Реферат:

1. У дисертаційній роботі досліджено математичні моделі та обчислювальні методи електронного цифрового підпису у фактор-кільцях поліномів та на кодових конструкціях запропоновано та обґрунтовано оцінки стійкості щодо цих електронних цифрових підписів до існуючих методів криптографічного аналізу, а також розроблено рекомендацій щодо їх застосування у пост-квантовий період. В дисертаційній роботі запропонована гібридна модель порушника екзистенційної підробки, яка враховує застосування методів як класичного, так і квантового криптоаналізу. Запропоновано модель загроз електронного підпису у пост-квантовому середовищі, яка використовує метод редукції доказів безпеки, і дозволяє класифікувати загрози за додатковою складністю криптоаналізу в порівнянні до більш загальної задачі. Проведено експериментальні дослідження властивостей електронного підпису у фактор-кільцях поліномів та на кодових конструкціях та оцінена стійкість до існуючих методів криптографічного аналізу. Зокрема розроблено модель атаки підробки на електронний підпис в фактор-кільцях поліномів із посиленими

параметрами та додатковим захистом за допомогою техніки пертурбації, що дозволило отримати меншу складність підробки в порівнянні з повним перебором. Отримано оцінки стійкості від підробки та удосконалено математичні моделі атак на електронний підпис Мельхора у фактор-кільцях поліномів. Запропоновано нову атаку на електронний підпис на кодових конструкціях, яку засновано на зміні ваги Хемінга вектору-підпису шляхом додавання довільного кодового слова застосованого блокового коду, також обґрунтовано додаткові умови та процедури перевірки підпису, яка унеможливлює цю атаку. Досліджено математичні моделі та обчислювальні методи електронного підпису у фактор-кільцях поліномів та на кодових конструкціях, обґрунтовано щодо них оцінки стійкості до існуючих методів криптографічного аналізу та розроблено рекомендацій щодо практичного застосування у пост-квантовий період.

2. The thesis provides research of mathematical models and computational methods of digital signature in polynomial quotient-rings and code based signatures. For these signature schemes security estimates against existing methods of cryptographic analysis are scrutinized, and as a result there is also developed recommendations for practical implementation for post-quantum period. In the dissertation, a hybrid adversary model of existential forgery is proposed, which consider both classical and quantum cryptanalysis methods implementation. Under an assumption that adversary acts with a combination of heuristic classical and quantum computer routines, we consider strong unforgeable security model of signatures, which presumes that even legal signer can't create another valid signature for one given message. We show with experimental results that such unforgeability is unattainable for certain primitives of lattice based signatures. Also a digital signature threat model is proposed. It utilize the methods of security reductions for post-quantum environment, to classify threats by the additional complexity of cryptanalysis in comparison with a more general cryptanalysis problem. Experimental researches of digital signatures properties in polynomials quotient-ring as well as code based schemes have been carried out, and resistance to existing methods of cryptographic analysis has been estimated. In particular, an attack model against signature in the polynomial quotient-rings with enhanced parameters and additional protection by perturbation techniques was developed. This model allows to derive a lower complexity of the counterfeit compared to a brute force. Also, another approach of creating malleable signature was obtained, which gives new numerical estimates of breaking bijection between signatures and messages for relevant key sizes. This can invoke to several messages belonging to one signature derived by private key owner. New security estimates of forgery are obtained. First it has been shown that mathematical model of lattices was the reason of forgery. Finally it implies that current mathematical model of trapdoor function can't engender signature model with needed properties. Also new attack against Melchor NTRUSign signature is proposed. And new evidences that Fiat-Shamir paradigm can't provide security under flows of lattice trapdoor function have been achieved. A new attack against code based digital signature is proposed. It exploits an addition operation of arbitrary code word of the applied block code, and changes Hamming weight of signature vector. In thesis also elaborated new countermeasures against this attack as well as auxiliary conditions for verification procedure. The thesis provides research of mathematical models and computational methods of digital signature in polynomial quotient-rings and code based signatures. For these signature schemes security estimates against existing methods of cryptographic analysis are scrutinized, and as a result there is also developed recommendations for practical implementation for post-quantum period.

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. Кузнецов Олександр Олександрович
2. Kuznetsov Oleksandr Oleksandrovych

Кваліфікація: д.т.н., 20.01.12

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. Василіу Євген Вікторович
2. Василіу Євген Вікторович

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. Качко Олена Григорівна

2. Качко Олена Григорівна

Кваліфікація: к.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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Горбенко Іван Дмитрович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Горбенко Іван Дмитрович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.