Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0416U002068

Особливі позначки: відкрита

Дата реєстрації: 11-05-2016

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Жмурко Тетяна Олександрівна
2. Zhmurko Tetyana Oleksandrivna

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: 26-04-2016

Спеціальність за освітою: 8.17010302

Місце роботи здобувача: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: 03058,Україна,м.Київ,Просп.Космонавта Комарова,1

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: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: 03058,Україна,м.Київ,Просп.Космонавта Комарова,1

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 20.51.35

Тема дисертації:

1. Методи підвищення ефективності протоколів квантової криптографії

2. Methods for improving the efficiency of quantum cryptography protocols

Реферат:

1. Дисертаційна робота присвячена розв'язанню актуальної науково-практичної задачі розробки і дослідження нових більш ефективних методів забезпечення стійкості тритових протоколів квантової криптографії до некогерентних атак, побудови тритових генераторів псевдовипадкових послідовностей та оцінювання їх якості (можливості використання для криптографічних застосувань). Отримані в дисертаційній роботі результати можуть бути використані для підвищення ефективності (захищеності, швидкості роботи) систем захисту на базі КПБЗ і квантового розподілу ключів, а також для деяких процедур безпеки в традиційних (неквантових) криптографічних системах захисту інформації. У роботі розроблено класифікацію методів КК, яка дозволяє розширити можливості щодо вибору відповідних методів для побудови сучасних квантових систем захисту інформації (на базі КПБЗ та інших квантових технологій). Отримав подальший розвиток метод забезпечення стійкості кутритових протоколів квантової криптографії, який дозволяє звести до мінімуму кількість перемикань між режимами протоколу (передавання повідомлення та контролю підслуховування), збільшити швидкість роботи при збереженні стійкості до

некогерентних атак. Отримав подальший розвиток метод генерування псевдовипадкових послідовностей, який дозволяє формувати трійкові незбалансовані псевдовипадкові послідовності. Окрім того, отримав подальший розвиток метод оцінювання якості псевдовипадкових послідовностей, який дає можливість оцінювати статистичні параметри і закономірності тритових псевдовипадкових послідовностей.

2. Thesis is devoted to applied scientific research task to develop and study new, more efficient methods for ensuring sustainability of quantum cryptography qutrit protocols to non-coherent attacks; constructing trit generator of pseudorandom sequences and evaluation of its quality (possibility of using them in cryptographic applications). The results obtained in the thesis can be used to improve efficiency (security level and speed) of security systems based on quantum direct secure communication and quantum key distribution, and can be used for security procedures in traditional (non-quantum) cryptographic information security systems. In this work developed classification of quantum cryptography methods, which can expand opportunities for choosing appropriate methods to construct modern quantum information security systems (based on quantum direct secure communication and other quantum technologies). Was further developed a method for ensuring stability of quantum cryptography qutrit protocols, which allows to minimize the amount of switching between protocol modes (message transmission and eavesdropping control), and increase speed by a factor of 4.4, while maintaining the resistance to non-coherent attacks. Also, was further developed a method of generating pseudorandom sequences, which allows to create ternary unbalanced pseudorandom sequences. In addition, further developed a method for evaluating pseudorandom sequence quality, which enables to evaluate the statistical parameters and laws of ternary pseudorandom sequences.

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. Гнатюк Сергій Олександрович

2. Gnatyuk Sergiy Oleksandrovych

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Карпінський Микола Петрович
2. Карпінський Микола Петрович

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. Рудницький Володимир Миколайович
2. Рудницький Володимир Миколайович

Кваліфікація: д.т.н., 05.13.06

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.