Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0414U000121

Особливі позначки: відкрита

Дата реєстрації: 14-01-2014

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Ніколаєнко Сергій Валентинович
2. Nikolaenko Sergey Valentinovich

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: 20-12-2013

Спеціальність за освітою: 8.05020201

Місце роботи здобувача: Одеська національна академія зв'язку ім. О.С. Попова

Код за ЄДРПОУ: 01180116

Місцезнаходження: 65029, м.Одеса, вул.Кузнечна,1

Форма власності:

Сфера управління: Державний комітет зв’язку та інформатизації України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 41.816.01

Повне найменування юридичної особи: Одеська національна академія зв'язку ім. О.С. Попова

Код за ЄДРПОУ: 01180116

Місцезнаходження: Кузнечна вулиця, 1, м. Одеса, Одеська обл., 65029, 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: Одеська національна академія зв'язку ім. О.С. Попова

Код за ЄДРПОУ: 01180116

Місцезнаходження: 65029, м.Одеса, вул.Кузнечна,1

Форма власності:

Сфера управління: Державний комітет зв’язку та інформатизації України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 20.51.35

Тема дисертації:

1. Методи підвищення стійкості квантових протоколів безпечного зв’язку

2. Methods of security amplification for quantum direct communication protocols

Реферат/анотація:

1. Об'єкт дослідження є процеси передавання та перехоплення інформації в квантовому каналі зв'язку. Метою ди-сертаційної роботи є розроблення методів підвищення завадостійкості та стійкості до атак пасивного перехоплення пінг-понг протоколів квантового прямого безпечного зв'язку. Методи дослідження. Для розроблення математичних моделей некогерентної атаки пасивного перехоплення двох та більшої кількості зловмисників на пінг-понг протоколи, розроблення нового методу підвищення стійкості цих протоколів використовувалися методи квантової механіки, квантової та класичної теорії інформації, класичної криптографії та криптоаналізу. Для виконання часових оцінок реалізації методів підвищення стійкості пінг-понг протоколів використовувалися методи процедурного програмування. Для розроблення методу завадостійкого кодування при реалізації пінг-понг протоколів в деполяризуючому квантовому каналі використовувались методи квантової та класичної теорії інформації, класичного завадостійкого кодування, імітаційного моделювання. Теоретичні і практичні результати: Математичні моделі некогерентної атаки пасивного перехоплення декількох зловмисників на пінг-понг протоколи з дво- та трикубітними

переплутаними станами, які дозволяють виконувати кількісну оцінку стійкості протоколу до цієї атаки в залежності від параметрів протоколу та параметрів атакуючих систем зловмисників. Метод гамування для підвищення стійкості пінг-понг протоколів, при практичній реалізації якого підвищиться стійкість протоколів до атаки пасивного перехоплення. Імітаційні моделі та відповідне програмне забезпечення для імітаційного моделювання роботи пінг-понг протоколів з двокубітними переплутаними станами з використанням методу гамування та методу зворотнього гешування для підвищення стійкості від атак пасивного перехоплення. Результати імітаційного моделювання передавання інформації пінг-понг протоколом з парами переплутаних кубітів в деполяризуючому квантовому каналі з використанням двійкового завадостійкого коду Файра (60,44), в тому числі статистична інформація, яка підтверджує корекцією пакетів помилок, якщо ймовірність деполяризації кубіту в квантовому каналі не перевищує 7%, що відповідає сучасній експериментальній ситуації при передаванні фотонів на відстань порядку 150 км. Наукова новизна: Вперше на основі квантової та класичної теорії інформації побудовані математичні моделі послідовної некогерентної атаки пасивного перехоплення двох та більшої кількості зловмисників на оригінальний пінг-понг протокол, а також цієї ж атаки двох зловмисників на протоколи з переплутаними дво- та трикубітними станами та квантовим надщільним кодуванням, що дозволило виконати оцінки стійкості цих протоколів до такої атаки. Отримала подальший розвиток методологія квантового криптоаналізу шляхом узагальнення математичних моделей атак пасивного перехоплення одного зловмисника на пінг-понг протоколи на випадок послідовної атаки двох та більшої кількості зловмисників. Вперше на основі методів класичної криптографії запропоновано метод підвищення стійкості пінг-понг протоколів, який ґрунтується на гамуванні блоків повідомлення та придатний для використання з будь-яким з пінг-понг протоколів, що дозволило підвищити стійкість цих протоколів до атаки. Вперше на основі класичної теорії завадостійкого кодування розроблено метод виправлення помилок кодом Файра для пінг-понг протоколів, які реалізуються в деполяризуючому квантовому каналі, що дозволило підвищити завадостійкість цих протоколів. Результати роботи впроваджено в таких організаціях: Одеська національна академія зв'язку ім. О.С. Попова та Національний авіаційний університет, м. Київ.

2. An object of research is the process of transmission and interception of information in quantum communication channel. An objective is to develop of methods for improving noise immunity and security to one and more eavesdropping attacks of quantum direct communication protocols. Research methods. To develop mathematical models of non-coherent eavesdropping attack and two more attacks of eavesdropper on ping-pong protocol, to develop a new method of increasing security of these protocols used methods of quantum mechanics, quantum and classical information theory, classical cryptography and cryptanalysis. To perform time estimations implementing methods to increasing security of ping-pong protocols used methods of procedural programming. To develop a method for the implementation of error-correcting coding ping-pong protocols in depolarizing quantum channel used methods in quantum and classical information theory, classical error-correcting coding, simulation. Theoretical and practical results: Mathematical models of several eavesdropper attacks on ping-pong protocol with two-and three-qubit entangled states, which allow you to perform quantitative assessment of security to this attack protocol depending of protocol parameters and parameters of systems eavesdroppers. XOR encryption for increasing security of ping-pong protocols, the practical implementation of that increasing security of protocols to eavesdropping attacks. Simulation models and software for simulation of ping-pong protocols two-qubit entangled states using the XOR encryption and reversible hashing for increasing security to eavesdropping attacks. Simulation results information transmission ping-pong protocol with pairs of entangled qubits in quantum depolarizing channel using a binary error-correcting Fire code (60.44), including statistical information confirming the correction of error bursts, if the probability of depolarization of qubits in the quantum channel does not exceed 7 %, which corresponds to the modern experi-mental situation in the transmission of photons at a distance of about 150 km. Scientific novelty : For the first time the mathematical models of sequential incoherent eavesdropping attack of two or more eavesdroppers on the protocols with entangled two- and three-qubit states is developed on the basis of the quantum and classical information theory, which allowed to perform security estimation of these protocols to such attacks. For the first time the method of security amplification for the ping-

pong protocols based on XOR encryption of message are proposed for any of ping-pong protocol that allowed to improve the security of these protocols to eavesdropping attacks. Also the method of reversible hashing by LUP-decomposition is modified. Assessment of the computational complexity of the proposed methods of security amplification for the ping-pong protocols with entangled two-qubit states is performed, that allowed to evaluate the effect of the improving security procedures on protocols performance on the whole and to give recommendations for the choice of methods for security amplification. For the first time the method of error correction Fire Code of ping-pong protocol with two entangled qubit states is used, thus noise immunity of these protocols is improved. The results of studies are implemented in such organizations: Odessa National Academy of Telecommunications named after A.S. Popov and National Aviation University, Kiev.

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. Василіу Євген Вікторович

2. Vasiliu Yevgen Victorovich

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

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

Власне Прізвище Ім'я По-батькові:

1. Конахович Георгій Филимонович

2. Конахович Георгій Филимонович

Кваліфікація: д.т.н., 05.22.14

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 Воробієнко Петро Петрович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Воробієнко Петро Петрович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.