Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0420U101595

Особливі позначки: відкрита

Дата реєстрації: 15-10-2020

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Коваленко Богдан Анатолійович
2. Kovalenko Bohdan

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: 17-09-2020

Спеціальність за освітою: 113 Прикладна математика

Місце роботи здобувача: Фізична особа підприємець Коваленко Богдан Анатолійович

Код за ЄДРПОУ: 3320614376

Місцезнаходження: Грушевського 17 Б, кв. 57, м. Бровари, Броварський р-н., Київська обл., 07400, Україна

Форма власності:

Сфера управління:

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, Київ, 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 технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Код за ЄДРПОУ: 21656236

Місцезнаходження: вул. акад. Янгеля, 1/37, м. Київ, Київ, 03056, Україна

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, 50.37.23

Тема дисертації:

1. Методи побудови та оцінки стійкості клептографічних механізмів у гібридних криптосистемах
2. Methods of kleptographic mechanisms implementation and security estimation in hybrid cryptosystems

Реферат/анотація:

1. У дисертації розв'язано актуальну наукову задачу розробки методу побудови криптосистем з доведеною відсутністю клептографічної модифікації. Запропоновано загальну класифікацію клептографічних систем, вперше запропоновано формалізацію для протоколів типу "запит-відповідь" у клептографічному сенсі, вперше отримані достатні умови неможливості непомітної клептографічної модифікації криптосистеми, продемонстровано метод побудови функції гешування з клептографічним механізмом. Отримані нові наукові результати дозволяють розширити аналіз існуючих та нових криптосистем та примітивів відносно атак зі сторони розробника або зловмисної модифікації реалізації криптосистем. Головним практичним результатом є можливість на практиці будувати нові криптопротоколи з доведеною стійкістю до атак зловмисної модифікації з побудовою каналу витоку секрету та підвищення рівня захищеності криптографічних систем.

2. There is science actual problem solved in the dissertation, namely the problem of creation approaches and methods for proven kleptographic modification free cryptosystem. General classification of kleptographic systems has been suggested, firstly formal model over “challenge-response” protocols in kleptographic sense has been suggested, firstly sufficient conditions of impossibility of kleptographic modifications have been obtained, the new method of implementation hash function with kleptographic mechanism has been demonstrated. These science results allow to improve analysis process of both released and being developed cryptographic systems to increase level of resistance against malicious modification. The main practical result is a capability of development of new cryptographic protocols with proved resistance against cleptographic attacks and improving security level of cryptographic systems. The dissertation consists of introduction, four sections, conclusion and list of used sources. The introduction substantiates topic’s actuality, formulates goals and tasks of research, the scientific novelty and the practical significance of the results. In the first section is overview of current state of kleptographic research, known methods and use cases of kleptographic schemes. Firstly, it’s demonstrated one of the most famous usage – symmetric encryption algorithm DES, which is designed with weakened structure to allow National Security Agency to perform practical cryptoanalysis using its huge computational resources and unknown cryptoanalysis method (namely, linear cryptoanalysis). Further, it’s described modern example – random number generator DualEC DRGB, which was standardized in 2006 and it’s a cryptographicaly secure RNG only if the development follows standard. However, if algorithm’s parameters have relation, that is known by somebody, relation’s owner is able to forecast output in practice. Next examples are russian hash function GOST Ð34-11-2012 and block ciphers GOST Ð34-12-2015 that are suspected to be designed with kleptographic trapdoor. Finally, it’s demonstrated kleptographic trapdoors based on asymmetric primitives: elliptic curves, RSA and Discrete Logarithm Problem. The second section devoted to the theory of kleptographic trapdoors. It started from classification of kleptographic mechanisms. Further, it’s introduced formal model of practical distinguisher to precise security metrics. After, formal model of “challengeresponse” protocol type is introduced with kleptographic extension of this model. The main scientific result of this section are sufficient conditions of SETUP free protocol. It allows to develop protocols without kleptographic trapdoors. The last result of the section is new kleptographic metric called “kleptographic potential”. This metric may be used for evaluation of risks of kleptographic trapdoor existence in cryptographic primitive and it may be used in crypto primitive’s design stage and for filtering of suspicious candidates on crypto competitions. The 3-rd section demonstrates sufficient conditions applying: two basic SETUP free protocols are designed – enhanced nonce generation protocol and enhanced 1-round Diffie-Hellman key agreement protocol. The main idea is usage of non randomized digital signature that is used to generate public random values that can’t be disclosed before publication but can be verified for non randomness. Theorems about absence of SETUP are formulated and proved. Also, there are two methods for hash function trapdoor development. One of them uses special transformation based on Discrete Logarithm Problem and allows Developer to recover part of message from known hash digest. Another method is Preneell’s method for generation trapdoored Feistel’s cipher which is applied to hash function basic cipher and gives Developer advantage in special use cases, here it’s blockchain Proof-of-Work consensus protocol. Thus, Developer, who knows secret in the hash function design, is able to guess message with special formatted hash digest (e.g., digest has some amount of “zero” most significant bits) with greater probability that for ideal hash function.

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. Кудін Антон Михайлович

2. Kudin Anton M.

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. Чевардін Владислав Євгенійович

2. Chevardin Vladyslav

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. Шелест Михайло Євгенович

2. Shelest Mykhailo

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

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.