Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0823U101907

Особливі позначки: відкрита

Дата реєстрації: 20-12-2023

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Александров Микита Олександрович

2. Mykyta Aleksandrov

Кваліфікація: 122

Ідентифікатор ORCID ID: ORCID 0000-0002-275

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп’ютерні науки

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерні науки

Дата захисту: 22-12-2023

Спеціальність за освітою: Спеціальність "Комп'ютерні науки"

Місце роботи здобувача: Державний вищий навчальний заклад "Донецький національний технічний університет"

Код за ЄДРПОУ: 02070826

Місцезнаходження: пл. Шибанкова, буд. 2, Покровськ, Покровський р-н., 85300, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 11.052.009

Повне найменування юридичної особи: Державний вищий навчальний заклад "Донецький національний технічний університет"

Код за ЄДРПОУ: 02070826

Місцезнаходження: пл. Шибанкова, буд. 2, Покровськ, Покровський р-н., 85300, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Державний вищий навчальний заклад "Донецький національний технічний університет"

Код за ЄДРПОУ: 02070826

Місцезнаходження: пл. Шибанкова, буд. 2, Покровськ, Покровський р-н., 85300, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. НЕЙРОМЕРЕЖЕВЕ СИНХРОННЕ ГЕНЕРУВАННЯ КЛЮЧІВ ПІДВИЩЕНОЇ НАДІЙНОСТІ ДЛЯ СИМЕТРИЧНИХ СИСТЕМ ШИФРУВАННЯ

2. Neural network synchronous generation of highly reliable keys for symmetrical encryption systems

Реферат:

1. Дисертаційна робота присвячена підвищенню криптографічної стійкості у протоколах обміну ключами за рахунок розробки та модифікації методів синхронізації ключів з використанням нейронних мереж. У першому розділі проведено аналіз існуючих методів криптографічного захисту інформації. Наведені основні поняття криптографії та протоколів обміну ключами. Розглянуті сучасні симетричні криптографічні системи, асиметричні криптографічні системи, протоколи обміну ключами та їх застосування, а також хеш функції. Розглянуті атаки на криптографічні протоколи, та інші причини зниження стійкості сучасних криптографічних алгоритмів. У другому розділі проведений аналіз використання явища взаємної синхронізації нейронних мереж для генерації ідентичних абонентських ключів шифрування, без необхідності їх передачі по мережі. Наведені основні поняття нейронних мереж та процесу їх взаємного

навчання. Проведений аналіз використання явища повної взаємної синхронізації у деревоподібних машинах парності, при якому синапси двох синхронізованих мереж стають ідентичними в результаті паралельного навчання. Визначено, що використання взаємної синхронізації деревоподібних машин парності може стати альтернативою існуючим системам обміну ключами. Наведено можливі способи формування ключа на соснові взаємно синхронізованих деревоподібних машин парності. У третьому розділі розроблена експериментальна система для запропонованого методу обміну ключами з можливостями тонкого та варіативного налаштування архітектури, правил навчання, а також затримки в мережі. Досліджені фактори, що впливають на час взаємної синхронізації двох деревоподібних машин парності. Досліджено вплив правил навчання нейромереж на стабільність часу синхронізації. Експериментально змоделювано атаки на систему методом паралельної синхронізації. Визначено напрямки подальшого дослідження методу з метою його удосконалення. У четвертому розділі було виконано удосконалення методу обміну ключами з використанням взаємно синхронізованих нейронних мереж для забезпечення більшої крипостійкості порівняно з існуючими методами. Запропоновано використання хеш функцій для підтвердження завершення взаємної синхронізації нейронних мереж. Виконано дослідження підтвердження завершення взаємної синхронізації нейронних мереж. Виконано модифікацію методу використанням часткових даних при синхронізації деревоподібних машин парності для додаткового підвищення крипостійкості. Запропонована модифікація дозволила приховати частину даних від передачі по мережі навіть у зашифрованому вигляді. Виконано аналіз використання групової синхронізації нейронних мереж. Запропоновано використання серверної архітектури з пулом нейронних мереж кожна з яких відповідає мережі користувача, даний підхід суттєво зменшує час взаємної синхронізації нейронних мереж, але потребує наявності серверу та пропорційного підвищення його розрахункової потужності, також такий підхід додатково створює загрозу зламу серверу.

2. The dissertation is devoted to improving cryptographic security in key exchange protocols by developing and modifying key synchronization methods using neural networks. The first chapter analyzes the existing methods of cryptographic information protection. The basic concepts of cryptography and key exchange protocols are presented. Modern symmetric cryptographic systems, asymmetric cryptographic systems, key exchange protocols and their application, as well as hash functions are considered. Attacks on cryptographic protocols and other reasons for reducing the stability of modern cryptographic algorithms are considered. The second chapter analyzes the use of the phenomenon of neural networks mutual synchronization to generate identical subscriber encryption keys without the need to transmit them over the network. The basic concepts of neural networks and the process of their mutual learning are presented. An analysis of the use of the complete mutual synchronization phenomenon in tree parity machines, in which the synapses of two synchronized networks become identical as a result of parallel learning, is carried out. It is determined that the use of mutual synchronization of tree parity machines can be an alternative to existing key exchange systems. Possible ways of forming a key on a pine tree of mutually synchronized tree parity machines are presented. In the third chapter, an experimental system for the proposed key exchange method with the ability to accurate and variable architecture customization, learning rules, and network delay is developed. The factors affecting the time of mutual synchronization of two tree parity machines are investigated. The influence of neural network learning rules on the stability of synchronization time is investigated. Attacks on the system by the method of parallel synchronization are experimentally modeled. The directions of further research of the method are determined in order to improve it. In the fourth chapter, an improvement of the key exchange method using mutually synchronized neural networks was made to provide greater cryptographic security than existing methods. It is proposed to use hash functions to confirm the completion of mutual synchronization of neural networks. The study of confirming the completion of mutual synchronization of neural networks is carried out. A modification of the method using partial data in the synchronization of tree parity machines is performed to further increase cryptographic resistance. The proposed modification made it possible to hide part of the data from transmission over the network even in encrypted form. An analysis of the use of group synchronization of neural networks is performed. The use of a server architecture with a pool of neural networks, each of which corresponds to the user's network, is proposed, this approach

significantly reduces the time of mutual synchronization of neural networks, but requires a server and a proportional increase in its computing power, and this approach additionally creates a threat of server hacking.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Освоєння нових технологій виробництва матеріалів, їх оброблення і з'єднання, створення індустрії наноматеріалів та нанотехнологій

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Александров М.О., Use of interacting neural networks in cryptography. Наукові праці ДонНТУ: Всеукр. наук. зб. – Покровськ, 2020. – Серія : Інформатика, кібернетика та обчислювальна техніка. - № 1(30). – С19-24. ISSN 1996-1588
- Aleksandrov M.O. Attacks on mutual synchronization of networks in cryptography. Computer Science and Technologies, Computing and Automation Faculty Technical University of Varna, Printing: TU-Varna, 2020, No 1/2020, pp. 15-22, ISSN 1312-3335
- Aleksandrov M.O., Підходи до підтвердження взаємної синхронізації в деревоподібних машинах парності. Наукові праці ДонНТУ: Всеукр. наук. зб. – Покровськ, 2022. – Серія : Інформатика, кібернетика та обчислювальна техніка. - № 1(34). – С65-70. ISSN 1996-1588
- Aleksandrov M.O., Bashkov Y.O., Factors Affecting Synchronization Time of Tree Parity Machines in Cryptography, 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), 2020, pp. 108-112
- Aleksandrov M.O., Bashkov Y.O., Confirmation of Mutual Synchronization of the TPMs Using Hash Functions, 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT), 2021, pp. 80-83
- Aleksandrov M.O., Bashkov Y.O., "Method Using Partial Data to Confirm Completion of the Tree Parity Machines Synchronization," 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 177-180

Наукова (науково-технічна) продукція: технології

Соціально-економічна спрямованість: підвищення автоматизації виробничих процесів

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: № 0118U000295 № 0120U101843

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Башков Євген Олександрович

2. Yevhen O. Bashkov

Кваліфікація: д. т. н., професор, 05.13.05

Ідентифікатор ORCID ID: 0000-0001-6974-4882

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=6602250825; https://www.webofscience.com/wos/author/record/H-6567-2018

Повне найменування юридичної особи: Державний вищий навчальний заклад "Донецький національний технічний університет"

Код за ЄДРПОУ: 02070826

Місцезнаходження: пл. Шибанкова, буд. 2, Покровськ, Покровський р-н., 85300, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Швачич Геннадій Григорович

2. Hennadiy G. Shvachych

Кваліфікація: д.т.н., професор, 05.13.05

Ідентифікатор ORCID ID: 0000-0002-9439-5511

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет «Дніпровська політехніка»

Код за ЄДРПОУ: 2070740402

Місцезнаходження: пр. Дмитра Яворницького, 19, Дніпро, Дніпровський р-н., 49005, Україна

Форма власності: Державна

Сфера управління:

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Яцків Василь Васильович

2. Vasyl V. Yatskiv

Кваліфікація: д. т. н., 05.13.05

Ідентифікатор ORCID ID: 0000-0001-9778-6625

Додаткова інформація: https://ieeexplore.ieee.org/document/9913089; https://ieeexplore.ieee.org/document/9297052

Повне найменування юридичної особи: Західноукраїнський національний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: вул. Львівська, буд. 11, Тернопіль, Тернопільський р-н., 46009, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Давиденко Анатолій Миколайович

2. Anatolii M. Davydenko

Кваліфікація: д. т. н., професор, 05.13.05, 05.13.06

Ідентифікатор ORCID ID: 0000-0003-3848-9852

Додаткова інформація: : https://doi.org/10.1007/978-3-030-16621-2_33; https://journals.riverpublishers.com/index.php/JCSANDM/article/view/18861

Повне найменування юридичної особи: Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України

Код за ЄДРПОУ: 05516949

Місцезнаходження: вул. Генерала Наумова, буд. 15, Київ, 03164, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Масол Володимир Іванович

2. Volodymyr I. Masol

Кваліфікація: д. ф.-м. н., професор, 01.01.05

Ідентифікатор ORCID ID: 0009-0001-3852-8340

Додаткова інформація: https://www.scopus.com/record/display.uri?eid=2-s2.0-85079036560&origin=resultslist&sort=plf-f; https://www.scopus.com/record/display.uri?eid=2-s2.0-85085385398&origin=resultslist&sort=plf-f

Повне найменування юридичної особи: Державний вищий навчальний заклад "Донецький національний технічний університет"

Код за ЄДРПОУ: 02070826

Місцезнаходження: пл. Шибанкова, буд. 2, Покровськ, Покровський р-н., 85300, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Дорогий Ярослав Юрійович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Дорогий Ярослав Юрійович
Відповідальний за підготовку облікових документів	Скирда Алла Євгенівна, учений секретар
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна