АНОТАЦІЯ

Александров М.О. Нейромережеве синхронне генерування ключів підвищеної надійності для симетричних систем шифрування. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки». – ДВНЗ Донецький національний технічний університет, Луцьк, 2023.

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.

Наукова новизна отриманих результатів.

- Вперше запропоновано для підтвердження завершення взаємної синхронізації деревоподібних машин парності використовувати хеш функції, що забезпечує найменший час синхронізації порівняно з поліноміальною функцією та обчисленням мінімально необхідної кількості ітерацій, а також виключає хибні спрацювання.
- Удосконалено метод обміну ключами шифрування з використання взаємно синхронізованих деревоподібних машин парності, який відрізняється

використанням часткових даних, що надає можливість відмовитись від передачі 1-10% прихованих синапсів по мережі навіть у хешованому вигляді та виключає можливість розкриття ключів шифрування з використанням вразливостей алгоритмів підтвердження завершення синхронізації.

- Вперше для вирішення проблеми групової синхронізації користувачів запропоновано використання групи дублюючих деревоподібних машин парності, що дозволяє зменшити час синхронізації групи користувачів до часу синхронізації двох користувачів при відповідному збільшенні навантаження на сервер.
- Вперше експериментально підтверджено стійкість методу взаємної синхронізації деревоподібних машин парності, які мають більше 16 синапсів при діапазоні значень ваг 10^6, до атак паралельним підключенням та генетичних атак, що надає можливість подальшого використання в реальних системах.

Практичне значення отриманих результатів.

- Проведене комплексне дослідження залежності часу синхронізації нейронних мереж від архітектури, затримки в мережі та правил навчання деревоподібних машин парності дозволяє більш тонко налаштовувати параметри нейронних мереж для досягнення достатнього рівня крипостійкості при прийнятному навантаженні на систему.
- Дослідження потенційних атак на метод обміну ключами з використанням деревоподібних машин парності довело стійкість методу до атак паралельним підключенням та вразливість до атак типу «людина посередині», що в подальшому може бути використано для побудови більш криптостійких систем обміну інформацією.
- Розроблені модифікації методу з використанням часткових даних та хеш функцій для підтвердження завершення взаємної синхронізації дозволяють створювати надзахищені криптографічні системи з

використанням синхронізованих деревоподібних машин парності, та зменшують час на їх розробку.

- Запропонований метод групової синхронізації деревоподібних машин парності є альтернативним існуючим методам, та може бути використаний для розробки більш швидких але ресурсних систем групової синхронізації користувачів.

Ключові слова: нейронні мережі, деревоподібні машини парності, час синхронізації, криптографія, шифрування, розшифрування, підтвердження синхронізації, вхідні нейрони, приховані нейрони, правила навчання, хеш функції, затримка мережі, атака, криптостійкість, групова синхронізація.

ABSTRACT

Alexandrov M.O. Neural network synchronous generation of highly reliable keys for symmetrical encryption systems. Dissertation for the degree of Philosophy Doctor in specialty 122 "Computer Science." - Donetsk National Technical University, Lutsk, 2023.

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.

Scientific novelty of the results.

For the first time, it is proposed to use a hash function to confirm the completion of mutual synchronization of tree parity machines, which provides the shortest synchronization time compared to a polynomial function and the calculation of the minimum required number of iterations, and also eliminates false positives.

An improved method of encryption key exchange using mutually synchronized tree parity machines, which is characterized by the use of partial data, which makes it possible to refuse to transmit 1-10% of hidden synapses over the network even in hashed form and eliminates the possibility of disclosing encryption keys by exploiting vulnerabilities in algorithms for confirming the completion of synchronization.

For the first time, to solve the problem of group synchronization of users, it was proposed to use a group of duplicate tree parity machines, which reduces the

synchronization time of a group of users to the synchronization time of two users with a corresponding increase in the server load.

For the first time, the method of mutual synchronization of tree parity machines with more than 16 synapses and a range of weights of 10^6 is experimentally confirmed to be resistant to parallel connection and genetic attacks, which makes it possible to use it in real systems.

Practical significance of the results.

A comprehensive study of the dependence of the synchronization time of neural networks on the architecture, network delay, and training rules of tree parity machines allows us to more accurately adjust the parameters of neural networks to achieve a sufficient level of crypto-resistance at an acceptable system load.

A research on potential attacks on the key exchange method using tree parity machines proved the method's resistance to parallel connection attacks and vulnerability to man-in-the-middle attacks, which can be used in the future to build more cryptographically secure information exchange systems.

The developed modifications of the method using partial data and hash functions to confirm the completion of mutual synchronization allow creating ultra-secure cryptographic systems using synchronized tree parity machines and reduce the time for their development.

The proposed method of group synchronization of tree parity machines is an alternative to existing methods and can be used to develop faster but more resource-intensive systems for group synchronization of users.

Keywords: neural networks, tree parity machines, synchronization time, cryptography, encryption, decryption, synchronization confirmation, input neurons, received neurons, initiation rules, hash function, ping, attack, cryptographic strength, group synchronization.

Список публікацій здобувача:

1. 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.

2. 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.

3. Aleksandrov M.O., Approaches to confirming mutual synchronization in tree parity machines. Наукові праці ДонНТУ: Всеукр. наук. зб. – Покровськ, 2022. – Серія : Інформатика, кібернетика та обчислювальна техніка. - № 1(34). – С65-70. ISSN 1996-1588.

4. 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, doi: 10.1109/ATIT50783.2020.9349313. **(Scopus)**

5. 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, doi: 10.1109/ATIT54053.2021.9678779. **(Scopus)**

6. 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, doi: 10.1109/ATIT58178.2022.10024234. **(Scopus)**