РЕФЕРАТ

Актуальність теми. Актуальність теми дослідження зумовлена зростанням загрози квантових атак, які потенційно здатні зламувати криптографічні механізми, що нині застосовуються у VPN-протоколах, зокрема у WireGuard, який базується на класичному алгоритмі ECDH. Поява алгоритмів постквантової криптографії (PQC), рекомендованих NIST, відкриває можливість забезпечити довготривалу криптографічну стійкість мережевих систем. У зв'язку з цим особливої актуальності набуває впровадження постквантових механізмів узгодження ключів у сучасні VPN-системи, що дозволяє підвищити безпеку корпоративних мереж, хмарних сервісів та інфраструктури критичної важливості.

Метою даного дослідження є аналіз, розробка та впровадження механізму постквантового оновлення ключів для WireGuard на основі алгоритму Kyber-768, що забезпечує захищене узгодження спільного секрету та регулярну ротацію ключового матеріалу без переривання VPN-тунелю.

Об'єктом дослідження є постквантові алгоритми та процеси обміну криптографічними ключами і їх оновлення в тунельних VPN-протоколах.

Предметом дослідження є методи інтеграції постквантових KEM-алгоритмів у процедури встановлення й підтримки VPN-з'єднання, а також оцінка впливу PQC-ротації ключів на продуктивність та стабільність тунелю.

Наукова новизна полягає в наступному:

1. Розроблено прототип механізму PQC-рукостискання для WireGuard, що використовує Kyber-768 для формування спільного секрету та автоматичного оновлення PresharedKey у процесі роботи тунелю.

2. Запропоновано архітектуру клієнт–серверної системи, яка дозволяє виконувати постквантовий обмін ключами паралельно з транспортним рівнем WireGuard, без модифікації базового протоколу.

Проведено криптографічну валідацію ключового матеріалу Kyber-768 (NTT-структури, статистичні та ентропійні характеристики) та показано його повну несумісність із класичними ECDH-ключами, що підтверджує постквантову природу реалізованого механізму.

Практична цінність роботи полягає в тому, що розроблений механізм постквантової ротації ключів може бути інтегрований у сучасні VPN-інфраструктури без змін на стороні серверів WireGuard. Це дозволяє суттєво підвищити криптографічну стійкість корпоративних та хмарних систем, забезпечити forward secrecy навіть при тривалих VPN-сесіях та мінімізувати ризики компрометації даних у випадку появи квантових обчислювальних засобів. Запропоноване рішення може застосовуватися у сфері кібербезпеки, у сервісах віддаленого доступу, у хмарних середовищах та інфраструктурі критичної важливості, де забезпечення довгострокової стійкості до квантових атак є ключовою вимогою.

Апробація результатів роботи. Положення роботи та проміжні результати доповідались і обговорювались на таких наукових заходах:

1. VIII Всеукраїнська студентська наукова конференція «Формування сучасної науки: методика та практика», м. Львів, 2025.
2. Прикладна математика та комп'ютинг 2025, м. Київ, 2025.

Публікації.

Ільчук О. О., Загрози квантових обчислень для класичної криптографії у віртуальних приватних мережах та шляхи переходу до постквантової криптографіїобчислень” // Матеріали Конференції: VIII Всеукраїнська студентська наукова конференція «Формування сучасної науки: методика та практика», 2025. – С. 247 – 249.

Ільчук О. О., Постквантові підходи до захисту тунельних протоколів мережевого рівня // Прикладна математика та комп'ютинг 2025, 2025. – С. <сторінки>.

Структура та обсяг роботи. Магістерська дисертація складається зі вступу, чотирьох розділів, висновків до кожного розділу, загальних висновків, списку використаних джерел та додатків.

У *вступі* наведено актуальність теми, мету, завдання, об’єкт і предмет дослідження.

У *першому розділі* викладено теоретичні основи постквантової криптографії та проаналізовано сучасні загрози для класичних алгоритмів обміну ключами.

У *другому розділі* обґрунтовано загальну архітектуру системи та її основні компоненти.

У *третьому розділі* описано реалізацію клієнтської, серверної частин та механізму PQC-рукостискання.

У *четвертому розділі* наведено результати тестування, включаючи часові характеристики Kyber-768, продуктивність PQC-ротації та аналіз стабільності VPN-тунелю.

У *висновках* підсумовано результати дослідження.

Повний обсяг дисертації — 154 сторінок, у тому числі 118 сторінок основного тексту, 20 рисунків, 1 таблиця, список використаних джерел із 51 найменувань, 20 слайдів презентації.

Ключові слова: постквантова криптографія, Kyber-768, VPN, WireGuard, ротація ключів, KEM, криптостійкість, квантові загрози.

ABSTRACT

Topic relevance. The relevance of the research topic is driven by the growing threat of quantum attacks, which could potentially compromise the cryptographic mechanisms currently used in VPN protocols, in particular WireGuard, which relies on the classical ECDH algorithm. The emergence of post-quantum cryptographic (PQC) algorithms recommended by NIST opens up the possibility of ensuring long-term cryptographic resilience of network systems. In this regard, the implementation of post-quantum key-agreement mechanisms in modern VPN systems becomes especially relevant, as it enables enhanced security of corporate networks, cloud services, and critical infrastructure.

The purpose of this research is the analysis, development, and implementation of a post-quantum key-update mechanism for WireGuard based on the Kyber-768 algorithm, which ensures secure shared secret agreement and regular rotation of key material without interruption of the VPN tunnel.

The object of the research is the postquantum algorithms and the processes of cryptographic key exchange and their updates in tunneling VPN protocols.

The subject of the research is the methods of integrating post-quantum KEM algorithms into the procedures of VPN connection establishment and maintenance, as well as the assessment of the impact of PQC key rotation on the performance and stability of the tunnel.

The scientific novelty is as follows:

A prototype of a PQC handshake mechanism for WireGuard has been developed, which uses Kyber-768 for generating a shared secret and automatic updating of the PresharedKey during tunnel operation.

An architecture of a client-server system is proposed, enabling post-quantum key exchange to run in parallel with the WireGuard transport layer, without modifying the base protocol.

Cryptographic validation of Kyber-768 key material has been conducted (NTT-structures, statistical and entropy characteristics), demonstrating its complete incompatibility with classical ECDH keys, which confirms the post-quantum nature of the implemented mechanism.

The practical value of the work lies in the fact that the developed mechanism of post-quantum key rotation can be integrated into modern VPN infrastructures without changes on the WireGuard server side. This significantly enhances the cryptographic resilience of corporate and cloud systems, ensures forward secrecy even during long-lasting VPN sessions, and minimizes the risk of data compromise in the event of the emergence of quantum computing capabilities. The proposed solution can be used in cybersecurity, remote-access services, cloud environments, and critical infrastructure, where long-term resistance to quantum attacks is a key requirement.

Approval of the research results. The main statements and interim results of the work were reported and discussed at the following scientific events:

VIII All-Ukrainian Student Scientific Conference “Formation of Modern Science: Methodology and Practice”, Lviv, 2025.

Applied Mathematics and Computing 2025, Kyiv, 2025.

Publications.

Ilchuk O. O., Threats of Quantum Computing to Classical Cryptography in Virtual Private Networks and the Pathways to Post-Quantum Cryptography // Conference Proceedings: VIII All-Ukrainian Student Scientific Conference “Formation of Modern Science: Methodology and Practice”, 2025. – pp. 247 – 249.

Ilchuk O. O., Post-Quantum Approaches to Protection of Layer-3 Tunneling Protocols // Applied Mathematics and Computing 2025, 2025. – pp. <pages>.

Structure and volume of the work. The Master's thesis consists of the introduction, four chapters, conclusions to each chapter, general conclusions, references, and appendices.

The *introduction* presents the relevance of the topic, purpose, objectives, object, and subject of the research.

The *first section* covers the theoretical foundations of post-quantum cryptography and analyzes modern threats to classical key-exchange algorithms.

The *second section* substantiates the overall system architecture and its main components.

The *third section* describes the implementation of the client part, the server part, and the PQC-handshake mechanism.

The *fourth section* presents the testing results, including timing characteristics of Kyber-768, PQC-rotation performance, and analysis of VPN-tunnel stability.

The *conclusions* summarize the research results.

The total volume of the thesis is 154 pages, including 118 pages of the main text, 20 figures, 1 table, a list of 51 references, and 20 presentation slides.

Keywords: post-quantum cryptography, Kyber-768, VPN, WireGuard, key rotation, KEM, cryptographic resistance, quantum threats.