УДК 004.7:004.056.55

Д.т.н., професор Тарасенко В.П., к.т.н., доцент Тарасенко-Клятченко О. В., магістрант Ільчук О. О.

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

ПОСТКВАНТОВІ ПІДХОДИ ДО ЗАХИСТУ ТУНЕЛЬНИХ ПРОТОКОЛІВ МЕРЕЖЕВОГО РІВНЯ

Abstract

V. Tarasenko, Professor, D.Sc., Oksana Tarasenko-Kliatchenko, Associate Professor, PhD; Ilchuk Oleksandr, student

Post-Quantum Approaches To Securing Layer 3 Tunneling Protocols

This paper addresses the issue of ensuring long-term cryptographic security of VPN and tunneling protocols in the context of emerging quantum computing. The study analyzes the vulnerability of existing key exchange mechanisms based on ECDH and RSA to Shor's algorithm and reviews the applicability of post-quantum solutions standardised by NIST, such as CRYSTALS-Kyber and Dilithium. Several integration strategies are considered, including full replacement, symmetric-based, and hybrid approaches combining classical and post-quantum algorithms. The hybrid model is emphasized as the most practical and compatible solution for implementing quantum-resistant L3 tunneling protocols like WireGuard and IPsec. Directions for further research and optimization are outlined.

Вступ

Стрімкий розвиток квантових обчислень створює новий рівень викликів для систем інформаційної безпеки. Більшість сучасних криптографічних алгоритмів, що використовуються для захисту мережевих протоколів, потенційно вразливі до атак із використанням квантових комп'ютерів, оскільки алгоритм Шора дозволяє ефективно розв'язувати задачі факторизації та дискретного логарифма, підриваючи стійкість RSA, DH і ECDH. Це безпосередньо стосується VPN-технологій, зокрема IPsec і WireGuard, які забезпечують високий рівень безпеки у класичному середовищі, але потребують модернізації в умовах квантових загроз.

Постановка задачі

Метою роботи є визначення та узагальнення постквантових підходів до захисту тунельних протоколів мережевого рівня, спрямованих на забезпечення

довготривалої криптографічної стійкості VPN-систем у контексті розвитку квантових обчислень. У межах дослідження розглядаються принципи побудови сучасних тунельних протоколів та їх криптографічна основа, а також виявляються основні загрози, що виникають із появою квантових алгоритмів. Особлива увага приділяється аналізу можливостей застосування постквантових механізмів шифрування та узгодження ключів у межах існуючих протоколів мережевого рівня.

Термінологія

Постквантова криптографія (PQC) — напрям криптографії, що розробляє алгоритми, стійкі до атак із використанням квантових комп'ютерів.

Квантові атаки — криптоаналітичні методи, які застосовують квантові алгоритми, зокрема алгоритм Шора для факторизації та алгоритм Гровера для прискореного пошуку ключів.

Тунельний протокол мережевого рівня (L3) — протокол, який забезпечує інкапсуляцію IP-пакетів у зашифровані канали зв'язку, створюючи віртуальну приватну мережу (VPN).

ECDH (Elliptic Curve Diffie–Hellman) — асиметричний алгоритм узгодження ключів, що базується на еліптичних кривих і широко використовується у VPN-протоколах, таких як IPsec і WireGuard.

KEM (Key Encapsulation Mechanism) — криптографічний механізм, який дозволяє безпечно передавати симетричний ключ через відкритий канал зв'язку; основа для більшості постквантових алгоритмів обміну ключами.

Аналіз існуючих підходів

Тунельні протоколи мережевого рівня, такі як IPsec та WireGuard, побудовані на комбінації симетричних і асиметричних криптографічних методів. Для узгодження ключів між учасниками з'єднання вони застосовують ECDH, який забезпечує ефективність і достатню безпеку в умовах класичних обчислень. Проте з розвитком квантових технологій така модель стає потенційно вразливою.

Алгоритм Шора теоретично дозволяє виконувати факторизацію великих чисел і розв'язувати задачу дискретного логарифма за поліноміальний час [1], що позбавляє криптографічної стійкості всі схеми, засновані на RSA, DH та ECDH. Відтак, усі сучасні тунельні протоколи, які використовують ці механізми під час встановлення з'єднання, опиняються під загрозою компрометації в умовах появи практично реалізованих квантових обчислювальних систем.

На відміну від цього, симетричні алгоритми шифрування, такі як AES-256 та ChaCha20-256, залишаються придатними для використання в

постквантовому середовищі. Квантовий алгоритм Гровера надає лише квадратичне прискорення повного перебору [2], тому збільшення довжини ключів до 256 біт забезпечує необхідний запас безпеки. Подовження ключа є достатнім заходом для збереження стійкості симетричних методів, тоді як основна увага має бути зосереджена на модернізації асиметричної частини протоколів.

У межах досліджень NIST Post-Quantum Cryptography (PQC) визначено нові алгоритмічні підходи, здатні забезпечити захист від квантових атак [3]. Найбільш перспективними кандидатами визнано решіткові криптосистеми, зокрема CRYSTALS-Kyber (механізм обміну ключами) та CRYSTALS-Dilithium (цифровий підпис). Ці алгоритми поєднують високу швидкодію з доказовою криптографічною стійкістю і можуть розглядатися як основа для заміни традиційних ECDH-механізмів у тунельних протоколах мережевого рівня.

Пропоновані підходи

Одним із ключових напрямів розвитку постквантової криптографії для тунельних протоколів мережевого рівня є пошук рішень, які дозволяють підвищити їх стійкість до квантових атак, зберігаючи сумісність із чинними мережевими стандартами. Такі рішення мають забезпечувати довготривалу криптографічну надійність у разі появи квантових обчислювальних систем, здатних зламати сучасні асиметричні алгоритми, не порушуючи базову архітектуру протоколів.

Першим і найбільш радикальним підходом є повна заміна класичних механізмів обміну ключами та підпису на постквантові алгоритми. У цьому випадку протокол використовує криптосистеми нового покоління — CRYSTALS-Kyber, Dilithium, BIKE, HQC, NTRU тощо замість традиційних схем ECDH і RSA [4]. Такий підхід гарантує найвищий рівень безпеки, оскільки цілком усуває залежність від математичних задач, які можуть бути розв’язані квантовими алгоритмами. Основним обмеженням є необхідність масштабного оновлення програмного забезпечення, зміни форматів службових повідомлень, підвищені вимоги до ресурсів та потреба у сертифікації нових реалізацій. Через це наразі такі рішення переважно перебувають на стадії експериментальних досліджень.

Другий підхід передбачає використання симетричних тунелів із підвищеною довжиною ключів (AES-256, ChaCha20-256) у поєднанні з безпечним каналом обміну ключами. Такий варіант відзначається простотою реалізації, однак не вирішує проблеми автентифікованого узгодження ключів, що зберігає вразливість класичних асиметричних механізмів і обмежує застосування цього підходу лише допоміжними сценаріями.

Найбільш практичним напрямом, рекомендованим, зокрема, у межах досліджень NIST PQC, є гібридний підхід, який передбачає поєднання класичних і постквантових алгоритмів у процесі узгодження ключів [5]. У такій схемі під час встановлення з'єднання сторони виконують обмін даними одразу за двома криптографічними механізмами — традиційним ECDH та постквантовим KEM (наприклад, Kyber, SABER, FrodoKEM). Отримані секрети комбінуються за допомогою функції узгодження (HKDF) у спільний сесійний ключ. Завдяки цьому, навіть у випадку зламу класичної частини обміну, постквантова компонента гарантує збереження конфіденційності даних.

Перевагою гібридного підходу є сумісність із чинними реалізаціями тунельних протоколів L3 (зокрема IPsec, WireGuard), що дозволяє поступово впроваджувати постквантові технології без зміни транспортного рівня чи формату тунельованих пакетів. Крім того, він забезпечує довготривалу криптографічну стійкість і дозволяє реалізовувати захист із мінімальними витратами на оновлення інфраструктури.

Разом із тим, постквантові підходи мають низку спільних обмежень. Найпомітнішими з них є збільшення обсягу службових даних під час handshake, що може впливати на час ініціалізації з'єднання, а також зростання обчислювального навантаження при формуванні ключів. Такі фактори особливо важливі для систем із жорсткими вимогами до затримок або для пристроїв з обмеженими ресурсами. Однак очікується, що з подальшою оптимізацією реалізацій постквантових алгоритмів та розвитком апаратних прискорювачів ці недоліки поступово втрачатимуть актуальність.

Загалом, розвиток постквантових підходів до захисту тунельних протоколів мережевого рівня відкриває можливості для створення VPN-систем нового покоління, які поєднують гнучкість, сумісність і стійкість до квантових атак, забезпечуючи поступовий перехід до стандартів безпеки майбутнього.

Висновки

Аналіз сучасних тунельних протоколів мережевого рівня показав, що їхня криптографічна безпека переважно ґрунтується на класичних асиметричних алгоритмах, які потенційно вразливі до квантових атак. Зокрема, використання схем ECDH і RSA не забезпечує довготривалої стійкості у випадку реалізації алгоритму Шора. Натомість симетричні алгоритми, такі як AES-256 і ChaCha20-256, залишаються ефективними та придатними для застосування в постквантовому середовищі.

У дослідженнях постквантової криптографії сформовано три основні підходи до захисту тунельних протоколів: повна заміна асиметричних алгоритмів на нові, використання симетричних схем із зовнішнім обміном ключами та гібридна модель, яка поєднує класичні й постквантові механізми. Порівняльний аналіз цих підходів засвідчує, що саме гібридна модель є найперспективнішим напрямом для практичного впровадження. Вона забезпечує баланс між безпекою, ефективністю та сумісністю, дозволяючи поступово адаптувати існуючу інфраструктуру до вимог квантово-стійкої криптографії.

Подальші дослідження у цій сфері мають бути спрямовані на стандартизацію гібридних рішень, оптимізацію їхніх реалізацій для пристроїв з обмеженими ресурсами та створення універсальних механізмів інтеграції у протоколи мережевого рівня, зокрема у VPN-технології нового покоління.

Література

1. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Computing. — 1997. — Vol. 26, № 5. — P. 1484–1509.
2. Grover L. K. A Fast Quantum Mechanical Algorithm for Database Search // Proceedings of the 28th Annual ACM Symposium on Theory of Computing. — 1996. — P. 212–219.
3. National Institute of Standards and Technology. Post-Quantum Cryptography: Current Status and Next Steps. — Gaithersburg, MD : NIST, 2022.
4. National Institute of Standards and Technology. NIST PQC Round 3 Report: CRYSTALS-Kyber and CRYSTALS-Dilithium Selected for Standardization. — Gaithersburg, MD : NIST, 2022.
5. Ільчук О. О. Загрози квантових обчислень для класичної криптографії у віртуальних приватних мережах та шляхи переходу до постквантової криптографії // Формування сучасної науки: методика та практика. — 2025. — С. 247–249.