DOI: 10.18372/2225-5036.31.21162

КВАНТОВИЙ РОЗПОДІЛ КЛЮЧІВ (QKD) У ПРОТОКОЛІ TLS 1.3

Олексій Шайна

Київський національний університет імені Тараса Шевченка, м. Київ, Україна

ШАЙНА Олексій Максимович, асп.
Рік та місце народження: 30.03.2000 м.Енергодар
Освіта: Київський національний університет імені Тараса Шевченка,
Посада: Senior Application Security Engineer
Наукові інтереси: кіберфізичні системи, кібербезпека, квантові технології
Публікації: 3 наукові публікації
E-mail: p.papyge@gmail.com
ORCID: 0009-0003-5707-0544

Анотація. *У статті розглядається архітектурна модель інтеграції квантового розподілу ключів (QKD) у протокол TLS 1.3 з метою підвищення стійкості до квантових атак. Автори аналізують криптографічні обмеження традиційних асиметричних алгоритмів, таких як RSA та ECC, у контексті появи квантових обчислень, а також обґрунтовують доцільність використання QKD як фізично захищеного джерела симетричних ключів. Запропонована модель дозволяє мінімізувати зміни в структурі TLS 1.3, використовуючи механізми PSK або заміни DH, і підтримує fallback-сумісність із наявними TLS-бібліотеками. Стаття описує технічні передумови, модифікації протоколу, логіку обміну повідомленнями, а також переваги та виклики, пов'язані з впровадженням QKD у класичні мережеві середовища. Зокрема, наголошується на фізичному рівні forward secrecy, складностях масштабування QKD та необхідності стандартизації. Представлене рішення позиціонується як практичний крок до побудови квантово-стійкої цифрової інфраструктури з високим рівнем безпеки для критичних систем зв'язку.*
Ключові слова: *квантовий розподіл, TLS, критографічний протокол, інтеграція.*

Вступ

У сучасному цифровому середовищі захист інформації є критично важливим завданням. Протокол TLS (Transport Layer Security) є домінуючим стандартом криптографічного захисту трафіку в Інтернеті. Його остання версія — TLS 1.3 — була розроблена з урахуванням найновіших криптографічних досягнень і забезпечує високий рівень конфіденційності, цілісності та автентичності переданих даних. TLS 1.3 усуває низку вразливостей попередніх версій, скорочує кількість раундів обміну повідомленнями та запроваджує обов'язкове використання алгоритмів з преференцією до проскладності. Однак з появою квантових комп'ютерів виникає серйозна загроза для безпеки класичних криптографічних алгоритмів, зокрема алгоритмів асиметричного шифрування, таких як RSA та ECC. Завдяки алгоритму Шора квантовий комп'ютер з достатньою кількістю кубітів зможе ефективно розв'язати задачі факторизації та дискретного логарифмування, на яких базується безпека цих алгоритмів. Це означає, що більшість сучасних криптопротоколів втратять стійкість, щойно з'явиться достатньо потужний квантовий комп'ютер. Квантова криптографія, і зокрема квантовий розподіл ключів (Quantum Key Distribution, QKD), пропонує радикально новий підхід до забезпечення безпеки. На відміну від класичних методів, QKD не покладається на складність математичних задач, а використовує фундаментальні закони квантової фізики для розподілу симетричних ключів. Будь-яка спроба перехоплення квантового каналу призводить до зміни стану фотонів, що може бути виявлено сторонами зв'язку, а отже — канал вважається скомпрометованим. Інтеграція QKD у сучасні криптографічні протоколи є актуальною темою досліджень. Одним із перспективних напрямів є створення гібридних протоколів, які поєднують переваги TLS 1.3 та квантової безпеки. У цій статті пропонується архітектурна модель інтеграції QKD у протокол TLS 1.3 з урахуванням поточних технологічних можливостей та обмежень. Метою моделі є збереження структури TLS 1.3 з мінімальними модифікаціями та забезпечення повної або часткової стійкості до квантових атак за допомогою квантово згенерованих ключів.

В ході дослідження була запропонована архітектура, яка передбачає використання окремого квантового каналу між комунікуючими сторонами для реалізації QKD. Передбачається наявність фізичної QKD-лінії (наприклад, оптоволоконного каналу з підтримкою однофотонної передачі) між сервером і клієнтом або між вузлами мережі (наприклад, у межах дата-центру або національної критичної інфраструктури). У моделі TLS 1.3 ключові обміни зазвичай реалізуються за допомогою протоколів Diffie–Hellman або PSK. У пропонованому підході QKD виступає джерелом симетричного ключа, який використовується на етапі розрахунку секрету (early_secret, handshake_secret, master_secret). Цей ключ

генерується незалежно від TLS-обміну, а перед його використанням QKD-модулі клієнта і сервера повинні здійснити аутентифікацію один одного за допомогою класичного каналу, наприклад, з використанням сертифікатів X.509.

Також передбачається наявність шару керування ключами (Key Management Layer), відповідального за буферизацію QKD-ключів, синхронізацію їх між сторонами, контроль унікальності та знищення використаних ключів. Цей шар повинен мати інтерфейс до TLS-бібліотеки (наприклад, OpenSSL), забезпечуючи передачу ключа в tls13_key_schedule() у вигляді Pre-Shared Key або внутрішньої заміни секрету після фази Hello. З технічного боку, модель вимагає реалізації API згідно з рекомендаціями ETSI GS QKD 014 або аналогічними. Також потрібна точна синхронізація часу для QKD-сесій, що може бути складно реалізувати в мобільних або високозатримкових середовищах. Нарешті, враховується, що повноцінне розгортання QKD можливе лише в умовах керованого середовища з фізично захищеним квантовим каналом. У відкритих мережах або при наявності проміжних вузлів довіра до кінцевих точок QKD є критичною вимогою [1].

Мета статті: дослідження та розробка архітектурної моделі інтеграції квантового розподілу ключів (QKD) у протокол TLS 1.3 з урахуванням сучасних технологічних можливостей та обмежень. Основна увага приділяється забезпеченню стійкості TLS 1.3 до квантових атак шляхом використання симетричних ключів, згенерованих за допомогою квантових каналів, замість класичних алгоритмів обміну (RSA, ECC, DH). Автори ставлять за мету зберегти сумісність із чинними реалізаціями TLS, мінімізуючи зміни в структурі протоколу через механізми PSK або заміни DH. У статті також розглядаються технічні вимоги до інтеграції, переваги фізичної безпеки (forward secrecy), виклики масштабованості, синхронізації та стандартизації. Запропонована модель позиціонується як практичний крок до побудови квантово-стійкої цифрової інфраструктури, придатної для застосування у критичних системах зв'язку, зокрема в дата-центрах, урядових мережах та телекомунікаційних структурах.

Архітектурна модель

QKD дозволяє двом сторонам безпечно обмінятися секретним ключем, навіть якщо комунікаційний канал контролюється зловмисником. Гарантія безпеки тут заснована на тому, що квантові стани не можна виміряти або клонувати без порушення — це фундаментальна властивість квантової механіки (принцип невизначеності Гейзенберга, теорема про заборону клонування). В запропонованій моделі використовуються наступні компоненти:

1. QKD-модулі (сервер/клієнт) створюють захищений секрет через квантовий канал. TLS 1.3 стек з додатковою підтримкою QKD-ключів у процесі key_schedule.
2. Рівень керування ключами (Key Management Layer): зберігає і буферизує QKD-ключі.

Протокол з використанням, модифікації TLS 1.3, передбачає два можливі варіанти A та B. Кожен з яких має свою особливість побудови.

Варіант A: **QKD як PSK**

У цьому сценарії TLS 1.3 розглядає QKD-ключ як попередньо узгоджений ключ (Pre-Shared Key, PSK), що використовується замість класичного обміну Diffie–Hellman. Обмін ключами в TLS 1.3 відбувається в таких етапах:

Генерація квантового ключа: клієнт і сервер ініціюють QKD-сесію через квантовий канал. Після проходження процесу постобробки (sifting, error correction, privacy amplification) обидві сторони отримують однаковий симетричний ключ K_QKD довжини n біт. Використання K_QKD як PSK: перед початком TLS-з'єднання обидві сторони мають K_QKD і ідентифікатор psk_identity. У повідомленні ClientHello клієнт додає розширення pre_shared_key з psk_identity (Формула 1). *Формула 1. Обчислення handshake_secret*

$$handshake\_secret = HKDF\_Extract(0, K\_QKD) \quad (1)$$

Подальша процедура TLS 1.3. Відповідно до RFC 8446, з early_secret обчислюються handshake_secret (Формула 2), де x – приватний ключ клієнта, Y = yG, як публічний ключ, y – приватний ключ сервера, G – базова точка на еліптичній кривій, а HMAC (Keyed-Hash Message Authentication Code) формується із формули 3, де H - хеш-функція (наприклад, SHA-256), K - секретний ключ, M – повідомлення, K' – ключ відповідно до блоку байтів B, в якому ipad – 0x36 байтів повторений B раз, а opad – 0x5c, повторений B раз. *Формула 2. Обчислення handshake_secret та Формула 3. Обчислення HMAC.*

$$handshake\_secret = HMAC_{earlysecret}(x * y = x * y * G). \quad (2)$$

$$HMAC = H((K' \oplus opad) \parallel H((K' \oplus ipad) \parallel M)). \quad (3)$$

Відповідно разом із handshake_secret ми обчислюємо master_secret (Формула 4). *Формула 4. Обчислення master_secret*

$$master_{secret} = HKDF\_Extract\,(handshake\_secret, empty) \quad (4)$$

У випадку режиму psk_ke значення ECDHE не додається, тому handshake базується повністю на K_QKD. Завершення handshake: всі наступні ключі шифрування (client_traffic_secret, server_traffic_secret) виводяться згідно з деревом TLS-ключів. Такий підхід

дозволяє інтегрувати QKD у TLS 1.3 без зміни базової структури протоколу, використовуючи вже визначені механізми PSK [5].

Варіант B: **QKD замість DH**

У цьому підході квантово згенерований ключ K_QKD безпосередньо замінює результат класичного обміну Diffie–Hellman (DH). Це означає, що під час фази обміну ClientHello / ServerHello у TLS 1.3 сторони погоджуються використовувати QKD як джерело спільного секрету. Послідовність кроків така:

QKD-розподіл ключа:

1. Клієнт і сервер встановлюють QKD-сесію.

2. Отримують спільний симетричний ключ K_QKD, який буде використовуватись як shared_secret в TLS 1.3.

TLS 1.3: Ініціація handshake:

У ClientHello клієнт включає спеціальне розширення, яке позначає підтримку QKD. Сервер відповідає в ServerHello, підтверджуючи використання QKD. У полі key_share сторони не передають DH-параметри, або використовують зарезервовану мітку. Використання K_QKD як shared_secret - класичний обмін DH пропускається, TLS 1.3 виконує обчислення (Формула 5) [6]. *Формула 5. Обчислення handshake_secret, де QKD замість DH*

$$handshake\_secret = HKDF\_Extract(0, K\_QKD) \quad (5)$$

Обчислення трафікових ключів:

Як і в класичному TLS 1.3, далі виконується виведення ключів шифрування для клієнта і сервера, де HKDF_Expand формується як зазначено у формулі 6, де PRK – псевдовипадковий ключ, info – контекст, L – бажана довжина результату, T1 - $HMAC_{PRK}(info \parallel 0x01)$, T2 - $HMAC_{PRK}(T1 \parallel info \parallel 0x02)$, і так далі поки не отримуємо L байт. *Формула 6. Обчислення HKDF_Expand*

$$HKDF\_Expand(PRK, info, L) = T1 \parallel T2 \parallel \cdots \parallel Tn \quad (6)$$

Надалі виконуємо обчислення ключів шифрування зпочатку для клієнта (client_application_traffic_secret*)* як зазначено на формулі 7. *Формула 7. Обчислення клієнтського ключа шифрування – client_application_traffic_secret*

$$client\_application\_traffic\_secret = HKDF\_Expand(master\_secret, "captraffic") \quad (7)$$

Після цього робимо обчислення ключа шифрування для сервера, зазначеного у формулі 8. *Формула 8. Обчислення серверного ключа шифрування server_application_traffic_secret*

$$server\_application\_traffic\_secret = HKDF\_Expand(master\_secret, "saptraffic", \dots) \quad (8)$$

Аутентифікація

Застосовується стандартна TLS-аутентифікація на основі сертифікатів або попередньо встановлених довірчих ключів. Цей варіант вимагає незначних змін у реалізації TLS 1.3, здебільшого на рівні інтерпретації полів обміну. QKD-ключ відіграє роль основного матеріалу замість DH та не потребує передачі відкритих параметрів. Перевагою є виключення обчислювального навантаження на генерацію ключа, що важливо для пристроїв з обмеженими ресурсами. Крім того, канал забезпечує forward secrecy завдяки фізичній неможливості дублювання квантового стану [7].

Схема обміну

У цьому розділі наведено покрокову схему обміну повідомленнями між клієнтом і сервером у модифікованому протоколі TLS 1.3 з інтегрованим квантовим розподілом ключів. Нижче подано як логічний опис, так і відповідні математичні формули. Ініціація з'єднання. Клієнт ініціює встановлення TLS-з'єднання з сервером через класичний TCP/IP канал. Встановлення QKD-сесії: Через окремий квантовий канал сторони (QKD-модулі клієнта і сервера) проводять протокол квантового розподілу ключа (наприклад, BB84). Після квантового обміну виконується класична постобробка: усічення (sifting), виправлення помилок (error correction), підсилення конфіденційності (privacy amplification) [2]. У результаті формується загальний симетричний ключ $K_{QKD} \in \{0,1\}n$, що означає квантово згенерований ключ – це бітовий вектор довжини n, тобто - $K_{QKD} = (k1, k2, \dots, kn)$, де $ki \in \{0,1\}, \forall i \in \{1,2,\dots,n\}$

Передача ідентифікатора ключа. Клієнт у ClientHello передає psk_identity (для варіанту PSK) або маркер підтримки QKD (для варіанту B). Handshake з використанням K_QKD. TLS використовує K_QKD на місці shared_secret для генерації початкових ключів – early_secret (Формула 5), handshake_secret (Формула 9), де hello_hash це $Transcript - Hash(ClientHello \,||\, ServerHello)$ та master_secret (Формула 10). Формула 9. Обчислення handshake_secret в схемі з використання QKD та Формула 10. Обчислення master_secret зі схемою QKD.

$$handshake\_secret = HKDF\_Extract(early\_secret, hello\_hash) \quad (9)$$

$$master\_secret = HKDF\_Extract(handshake\_secret, empty) \quad (10)$$

Генерація ключів шифрування. На основі master_secret формуються трафікові ключі за формулою 7 та формулою 8, де saptraffic та captraffic -

це позначки (labels), які використовуються у протоколі TLS 1.3 при розширенні ключів через HKDF_Expand_Label [8].

Завершення handshake

Клієнт і сервер аутентифікують один одного, обмінюються повідомленнями Finished, після чого починається захищений сеанс. Схематичне представлення зображене на рисунку 1.

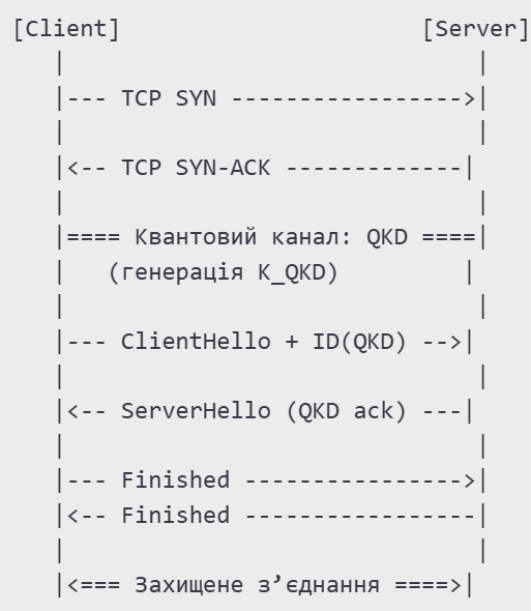

Рис. 1. Схематичне зображення захищенного з'єднання протоколу TLS з використанням квантового розподілу ключів

Схема на рисунку 1, демонструє гібридний характер протоколу: TLS 1.3 реалізується у класичному середовищі, але з використанням ключів, згенерованих у квантовому каналі. Ключова відмінність полягає в джерелі shared_secret, яке формується фізично захищеним способом.

Переваги та недоліки

Квантовий розподіл ключів (QKD) забезпечує стійкість до квантових атак, оскільки не базується на обчислювальній складності, як традиційні криптографічні алгоритми RSA або ECC. Натомість він використовує фундаментальні закони квантової фізики. Завдяки цьому QKD забезпечує інформаційно-теоретичну безпеку, яка не залежить від потужності обчислювальних пристроїв, включно з квантовими комп'ютерами. Ще однією ключовою перевагою є те, що QKD працює на повністю фізичному рівні секретності. Через принцип неможливості клонування квантових станів (no-cloning theorem), будь-яка спроба перехопити квантовий сигнал вносить помилки, які можуть бути виявлені сторонами, що комунікують. Це дозволяє одразу помітити присутність зловмисника та припинити сесію для уникнення компрометації. Навіть якщо класична криптографія буде скомпрометована в майбутньому, ключі, згенеровані за допомогою QKD, залишаться захищеними, оскільки вони не передавались у відкритому вигляді. QKD також може бути інтегровано як додатковий рівень безпеки до існуючих реалізацій протоколу TLS 1.3, зокрема в режимі попередньо спільного ключа (PSK). Це відкриває можливості для гібридного підходу до захисту даних у майбутньому постквантовому світі.

Квантовий розподіл ключів (QKD) потребує використання спеціалізованого обладнання, зокрема джерел однофотонних імпульсів, детекторів, модуляторів, а також оптоволоконного з'єднання або іншого захищеного фізичного каналу. Станом на сьогодні ефективна передача квантових ключів має обмеження по відстані — зазвичай до 100–150 км без використання ретрансляторів або квантових повторювачів. Крім того, для успішного встановлення сесії необхідна висока точність синхронізації між сторонами. Також важливою умовою є наявність механізмів буферизації ключів, правильне управління їхнім життєвим циклом і гарантія того, що жоден ключ не буде використано повторно. З точки зору масштабованості та мобільності, впровадження QKD значно складніше порівняно з програмною криптографією. Реалізувати таку технологію на мобільних пристроях або в хмарних сервісах наразі проблематично. Ще одним обмеженням є висока вартість обладнання, необхідного для побудови QKD-систем, що наразі робить цю технологію доступною переважно для урядових структур та великих корпорацій. Попри те, що вже існують перші технічні рекомендації від організацій на кшталт ETSI та ITU-T, глобальні стандарти QKD досі перебувають на стадії розробки.

Висновки

Запропонована архітектурна модель демонструє реалістичну можливість інтеграції квантового розподілу ключів (QKD) у протокол TLS 1.3 без радикального перепроектування стандарту. Завдяки використанню існуючих механізмів TLS, зокрема режиму PSK або заміни DH, стає можливою побудова гібридних рішень, які підвищують криптографічну стійкість без порушення сумісності. Інтеграція QKD у TLS 1.3 дозволяє реалізувати новий клас криптографічних протоколів з фізичним рівнем безпеки, що базується не на обчислювальній складності, а на фундаментальних властивостях квантової механіки. Це забезпечує forward secrecy, а також захист від майбутніх квантових атак, включно з тими, що стануть можливими за допомогою повноцінних квантових комп'ютерів. З технічної точки зору модель є масштабованою для інфраструктур з фіксованими каналами зв'язку, зокрема для дата-центрів, урядових мереж, телекомунікаційних операторів та критичних об'єктів національного

значення. Її реалізація вимагає належної підтримки на рівні обладнання та програмного забезпечення, включаючи QKD-сумісні пристрої, стандартні API та ключову інфраструктуру. Незважаючи на ряд технічних і економічних викликів, запропонована модель є перспективним кроком до побудови квантово-стійкої цифрової екосистеми. Подальші дослідження мають бути зосереджені на стандартизації інтерфейсів, розробці універсальних протоколів узгодження ключів, а також на оптимізації вартості і надійності QKD-компонентів. Таким чином, інтеграція QKD у TLS 1.3 — це не лише інженерне завдання, а й стратегічна відповідь на майбутні загрози цифровій безпеці. Вона відкриває шлях до побудови нових типів захищених систем, у яких класична криптографія підсилюється законами квантової фізики.

Список використаних джерел

[1] Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, Internet Engineering Task Force (IETF).

[2] Krawczyk, H., Eronen, P. (2010). HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869, IETF.

[3] NIST (2015). Recommendation for Key Derivation Using Pseudorandom Functions (SP 800-108). National Institute of Standards and Technology.

[4] ETSI GS QKD 014 V1.1.1 (2020). Quantum Key Distribution (QKD); API for QKD integration. European Telecommunications Standards Institute.

[5] ETSI GR QSC 001 V1.1.1 (2018). Quantum Safe Cryptography (QSC); Quantum-safe algorithm requirements. ETSI White Paper.

[6] Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P. (2016). Post-quantum key exchange—NewHope. In USENIX Security Symposium, pp. 327–343.

[7] ITU-T Y.3800 (2019). Framework for Networks Supporting Quantum Key Distribution. International Telecommunication Union.

[8] Bindel, N., Brendel, J., Fischlin, M., Goncalves, B. (2018). Hybrid Key Exchange Protocols for the TLS Protocol. In: Cryptographers' Track at the RSA Conference. Springer, pp. 206–226.

Shaina O. Quantum key distribution (QKD) in TLS protocol

Abstract. *The paper discusses an architectural model for integrating quantum key distribution (QKD) into the TLS 1.3 protocol to improve its resistance to quantum attacks. The authors analyze the cryptographic limitations of traditional asymmetric algorithms, such as RSA and ECC, in the context of the emergence of quantum computing, and justify the feasibility of using QKD as a physically secure source of symmetric keys. The proposed model allows for minimizing changes to the TLS 1.3 structure using PSK or DH replacement mechanisms, and supports fallback compatibility with existing TLS libraries. The paper describes the technical prerequisites, protocol modifications, messaging logic, and the benefits and challenges associated with implementing QKD in classical network environments. In particular, it emphasizes the physical level of forward secrecy, the complexities of QKD scaling, and the need for standardization. The presented solution is positioned as a practical step towards building a quantum-resistant digital infrastructure with a high level of security for critical communication systems.*

Keywords*: quantum distribution, TLS, cryptographic protocol, integration.*

Шайна Олексій Максимович, аспірант, Київський національний університет імені Тараса Шевченка.

Shaina Oleksii Maksymovych, PhD Student, Taras Shevchenko National University of Kyiv.