АНАЛІТИЧНА ОЦІНКА ЗАТРИМКИ ВСТАНОВЛЕННЯ З'ЄДНАННЯ TLS 1.3 ПРИ ВИКОРИСТАННІ ПОСТКВАНТОВИХ АЛГОРИТМІВ

Запорожець Д.І.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна

E-mail: diana.zaporozhets@nure.ua

Abstract

The paper presents an analytical model for evaluating TLS 1.3 handshake latency utilizing post-quantum (PQ) digital signature schemes standardized in 2024. The model explicitly incorporates cryptographic processing overhead, network round-trip time (RTT), and transmission constraints imposed by the TCP Initial Congestion Window (IW). Based on parameter sizes defined in NIST FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA), we identify scenarios where PQ authentication data fit within a single TCP congestion window, thereby avoiding additional round-trips. The results provide guidelines for selecting PQ signature schemes suitable for latency-sensitive telecommunications systems.

Із появою квантових комп'ютерів виникла загроза для традиційних криптографічних алгоритмів, що використовуються в протоколі TLS 1.3 [1]. Це призвело до розробки постквантової криптографії (PQC) – нового покоління алгоритмів, стійких до квантових атак. У 2024 році NIST стандартизував перші постквантові алгоритми цифрового підпису: ML-DSA на основі модульних решіток (FIPS 204) та SLH-DSA на основі хеш-функцій (FIPS 205) [2, 3]. Однак впровадження цих алгоритмів у TLS 1.3 призводить до суттєвого збільшення обсягу автентифікаційних даних, що критично впливає на час встановлення з'єднання – ключовий параметр для телекомунікаційних систем [4]. Зважаючи на це, метою роботи є розробка аналітичної моделі для оцінки затримки встановлення з'єднання TLS 1.3 при використанні постквантових алгоритмів та надання рекомендацій щодо їх вибору.

Постквантові алгоритми характеризуються значно більшими розмірами цифрових підписів порівняно з традиційними криптографічними схемами. Класичні алгоритми, такі як Ed25519 та ECDSA, що базуються на математиці еліптичних кривих, генерують компактні підписи розміром до 64 байт. Натомість постквантові схеми вимагають суттєво більших обсягів даних для забезпечення еквівалентного рівня безпеки: алгоритми сімейства ML-DSA створюють підписи обсягом від 2,4 до 4,6 КБ залежно від рівня безпеки, а алгоритм SLH-DSA-128s генерує підписи розміром від 7,9 КБ. У протоколі TLS 1.3 ці підписи передаються як частина повідомлення CertificateVerify разом із ланцюгом сертифікатів X.509 у повідомленні Certificate, що формують другий етап обміну під час процесу встановлення з'єднання [5]. Таке збільшення обсягу автентифікаційних даних безпосередньо впливає на мережеві характеристики протоколу та може призвести до виникнення додаткових затримок.

Для оцінки впливу постквантових алгоритмів на продуктивність TLS 1.3 запропоновано аналітичну модель, що враховує мережеві та криптографічні компоненти затримки. Час встановлення з'єднання (T_{HS}) для стандартного процесу рукостискання визначається за формулою, що враховує можливість передачі автентифікаційних даних за один або кілька циклів обміну (Round-Trip Time, RTT):

$$T_{HS} = RTT \times \left\lceil \frac{S_{auth}}{MSS \times IW_{seg}} \right\rceil + T_{sign} + T_{verify}, \quad (1)$$

де S_{auth} – сумарний розмір автентифікаційних даних, що включає ланцюг сертифікатів та цифровий підпис;

MSS – максимальний розмір TCP-сегмента;

IW_{seg} – початкове вікно перевантаження TCP у сегментах;

T_{sign} – час генерації підпису на сервері;

T_{verify} – час перевірки підписів на клієнті.

Ключовим параметром моделі є кількість циклів обміну (N_{RTT}), необхідних для передачі автентифікаційних даних, яка визначається співвідношенням їх розміру до початкового вікна перевантаження TCP:

$$N_{RTT} = \left\lceil \frac{S_{auth}}{MSS \times IW_{seg}} \right\rceil. \quad (2)$$

Якщо сумарний обсяг автентифікаційних даних не перевищує початкове вікно перевантаження, всі дані передаються за один цикл обміну. При перевищенні цього порогу кількість необхідних циклів визначається формулою (2), що призводить до пропорційного збільшення затримки встановлення з'єднання.

У стандартних реалізаціях TCP згідно з RFC 6928 [6] початкове вікно перевантаження дорівнює десяти сегментам максимального розміру. За типового значення максимального розміру сегмента 1460 байт це дозволяє передати близько 14,6 КБ даних без очікування підтвердження. Якщо сумарний обсяг повідомлень сервера перевищує цей поріг, виникає необхідність у додаткових циклах обміну, що фактично подвоює мережеву затримку рукостискання.

Для подальшого аналізу було розраховано сумарні обсяги автентифікаційних даних, що передаються у другому обміні сервера під час встановлення з'єднання TLS 1.3. Розрахунок виконано на основі експериментально виміряних розмірів повідомлень Certificate та CertificateVerify, а також параметрів постквантових цифрових підписів, визначених стандартами FIPS 204/205. Розглянуто гібридний сценарій перехідного періоду, коли сертифікат кінцевого вузла використовує постквантовий алгоритм, тоді як проміжні сертифікати залишаються класичними (RSA або ECDSA), що дозволяє врахувати накладні витрати структур X.509.

Таблиця 1. Обсяги автентифікаційних даних TLS 1.3 (гібридний сценарій)

Алгоритм	Підпис, байт	S_{auth}, байт	N_{RTT}
ECDSA-384	48	1593	1
ML-DSA-44	2420	10253	1
ML-DSA-65	3309	16136	2
SLH-DSA-128f	17000	52674	4

Показники таблиці 1 демонструють істотну різницю у мережевій поведінці алгоритмів залежно від їхнього криптографічного профілю. Для класичних схем, сумарний обсяг автентифікаційних даних вміщується у початкове вікно перевантаження TCP, забезпечуючи один цикл обміну.

Особливо критичною ситуація стає у випадку повністю постквантових сертифікаційних ієрархій. У такому сценарії застосування SLH-DSA гарантовано призводить до необхідності додаткових циклів передачі даних, що збільшує мережеву складову затримки встановлення з'єднання вдвічі або більше [7]. Це робить алгоритми сімейства ML-DSA, що базуються на математичних задачах теорії решіток, більш придатними для телекомунікаційних систем з жорсткими вимогами до затримок.

Отже, на підставі проведеного аналізу встановлено, що вибір постквантового алгоритму цифрового підпису безпосередньо впливає на продуктивність TLS 1.3. Для критичних додатків реального часу рекомендується використовувати ML-DSA-44 [8], для систем з підвищеними вимогами до безпеки – ML-DSA-65 за умови прийнятного рівня затримок. Використання SLH-DSA доцільне для випадків, де затримки не є критичним фактором. Запропонована модель може бути використана для прогнозування продуктивності TLS 1.3 у різних мережних сценаріях з урахуванням параметрів каналу зв'язку та вимог до рівня безпеки.

Література

1. RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3 / E. Rescorla. 2018. 160 p. URL : https://www.rfc-editor.org/rfc/rfc8446 (дата звернення: 06.11.2025).

2. FIPS 204. Module-Lattice-Based Digital Signature Standard. National Institute of Standards and Technology (NIST). Gaithersburg, USA, 2024. 94 p.

3. FIPS 205. Stateless Hash-Based Digital Signature Standard (SLH-DSA). National Institute of Standards and Technology (NIST). Gaithersburg, USA, 2024. 88 p.

4. Горбенко І. Д., Потій О. В., Кузнєцов О. О. Постквантова криптографія та механізми її реалізації. Радіотехніка. 2016. Вип. 184. С. 4-16.с.

5. Sikeridis D., Kampanakis P., Devetsikiotis M. Post-Quantum Authentication in TLS 1.3: A Performance Study. NDSS Symposium, 2020. 18 p. URL : https://eprint.iacr.org/2020/071.pdf (дата звернення: 08.11.2025).

6. RFC 6928. Increasing TCP's Initial Window / J. Chu, N. Dukkipati, Y. Cheng, M. Mathis. 2013. URL : https://www.rfc-editor.org/rfc/rfc6928 (дата звернення: 08.11.2025).

7. Paquin C., Stebila D., Tamvada G. Benchmarking Post-Quantum Cryptography in TLS. Cryptology ePrint Archive. 2019. 34 p. URL : https://eprint.iacr.org/2019/1447 (дата звернення: 08.11.2025).

8. Горбенко І. Д. та ін. Обґрунтування та пропозиції щодо вибору, удосконалення та стандартизації механізму постквантового електронного підпису на національному та міжнародному рівнях. Радіотехніка. 2021. Вип. 207. С. 5-25с.