BERGISCHE
UNIVERSITÄT
WUPPERTAL

Bachelor Thesis Proposal

Comparing Post-Quantum Instantiations of the TLS1.3 Handshake

Jonas Dinspel

November 4, 2025

Chair for IT Security and Cryptography
University of Wuppertal

First Examiner: **Prof. Dr.-Ing. Tibor Jager**

Introduction

With the continuous progress in the development of quantum computers, new challenges arise alongside of their many benefits. One, if not the biggest challenge for the field of cryptography, is the threat posed to widely used public key cryptography. These public key cryptography schemes help to ensure the integrity, confidentiality and authenticity of modern-day communications. They rely on complex mathematical problems like the factorization of large integers or the discrete logarithm problem, which, without the right information or keys, cannot be solved efficiently with today's most powerful computers. Algorithms such as shor's algorithm are able to efficiently solve these problems in polynomial time. For example, in encryption schemes, attackers would be able to derive shared secrets used in public key cryptography. Using the shared secret an attacker can easily decrypt any data encrypted using this secret, which leads to the loss of confidentiality and forward security, especially in the face of *collect now, decrypt later* attack schemes. Additionally, attackers gain the ability to fake signatures, leading to the loss of authenticity as well.

These risks underline the urgency of a fast transition to post-quantum public key cryptography to ensure the confidentiality and authenticity of transmitted data in the future.

One of the affected protocols is Transport Layer Security [TLS], which is used for a wide range of applications from simply surfing the internet or using instant messaging to voice over IP. Especially the handshake, which relies on asymmetric cryptography, is subsceptible to post quantum attacks, but the symmetric encryptions used in the following data transfer are not resistant either.

Even the most recent TLS1.3 standard itself is not inherently quantum-secure. There already are hybrid solutions which combine classical encryptions with modern post-quantum algorithms like ML-KEM, which are already included in current versions of web browsers.

As with all increases in security, the transition to post-quantum cryptography comes at a cost, as quantum-secure encryptions tend to require more computational power and produce larger cryptographic objects, thus an overall decrease in the performance of relying protocols is expected. Benchmarks for these hybrid solutions and already exist, but it is still hard to compare different cryptographic TLS configurations against each other.

To address this issue and further support the post-quantum transition of TLS, this thesis will introduce a tool to view, create and compare different TLS configurations, including classic, hybrid and post-quantum schemes. This will give a better overview of the current state of research and understanding of the implications on performance of the transition to post-quantum TLS, thus giving easier approaches for further research.

Related work

Post-quantum TLS has been studied throughout various works regarding its different implementation approaches, their individual performance and security implications. The currently used RSA or ECDSA based signatures and the ECDH based key exchange lose their security properties facing cryptographically relevant quantum computers, thus threatening the confidentiality and authenticity of network traffic. As shown by Alnahawi et al. in [AMOW24], offering a quantum safe key exchange is more challenging than simply replacing the Diffie-Hellman key exchange, as the only known alternative approach is deploying a different cryptographic concept, namely KEM algorithms.
Garcia et al. found in [RRT$^+$24] that using purely post-quantum based TLS improves Handshake performance by approximately 9% over classical configurations, however using the proposed full hybrid approach of quantum key distribution paired with post-quantum algorithms increases handshake latency by 117%.
By benchmarking post-quantum algorithms in TLS under realistic network conditions Paquin et al. found in [PST20] that the size of generated cryptographic objects, and thus the bandwidth requirements, will increase. Packet loss and fragmentation had an significant impact on the performance, emphasizing the need for size-optimized primitives.
KEM algorithms generally perform better in their post quantum versions, the overall performance is still worse than classical predecessor but already surpasses the hybrid approaches.
Current research efforts often focus on the key exchange rather than authentication, which in face of *collect now, decrypt later* attacks still leave vulnerabilities unattained . To mitigate this issue ML-KEM can be introduced to the key exchange and ML-DSA or SLH-DSA to the authentication of the handshake.[MRLC26]

Goals of this thesis

The goal of this thesis is to design and implement a formula, which calculates the expected size of the handshake for selected TLS configurations. The variables used in the formula reflect the chosen cryptographic building blocks in the handshake and the following session, and the formula's output will be a comparable performance index. The schemes used in the handshake and session can be chosen independently, and current hybrid scenarios will also be supported. For better usability, a front end will be developed where configurations can be created and compared.
The first step to achieve this will be an extensive research into the TLS 1.3 hand-

shake. This will include following research questions:

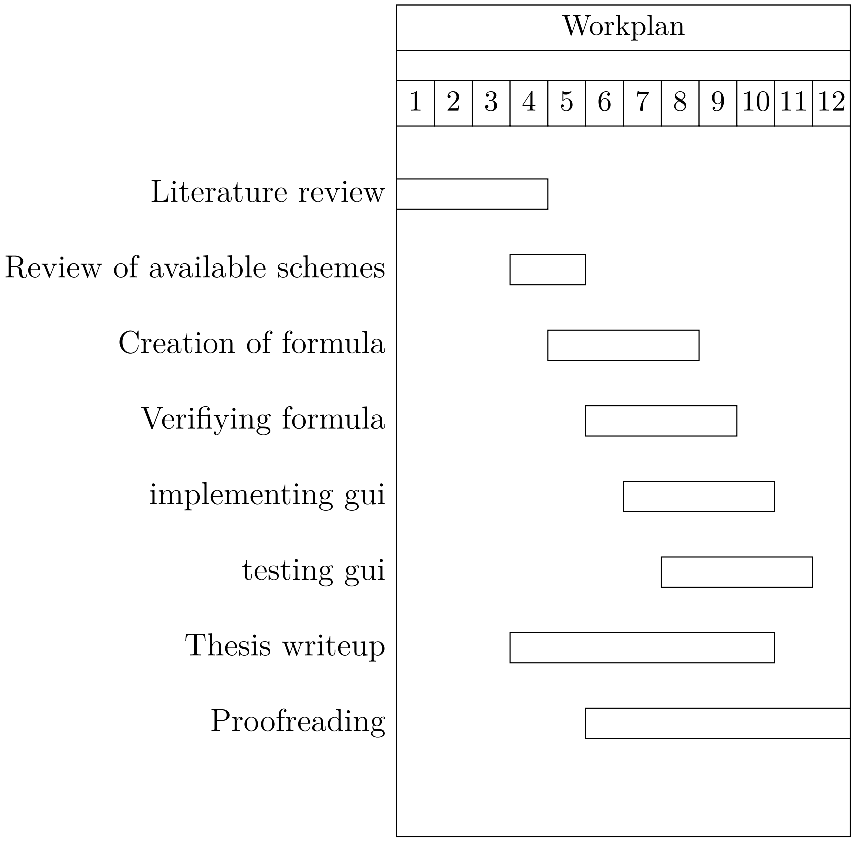
- Which cryptographic algorithms and building blocks are currently used?
- Which post-quantum alternatives are available?
- Which vulnerabilities arise in the face of CRQCs?
- How can these vulnerabilities be mitigated?

Once the research is completed, I will devise a formula that calculates the magnitude of all cryptographic components used in a selected configuration of the TLS handshake. This formula will be able to depict different possible TLS configurations using the in step one researched cryptographic algorithms. Additionally, some add-ons for the TLS handshake that require cryptographic components themselves, like OCSP-staples or CT timestamps, will be taken into account. Each cryptographic scheme offered will be assigned a weight, which will be used in the formula to calculate the overall size of the cryptographic objects.

The last step will be the creation of a website where a TLS handshake can be configured with options of classical, hybrid and post-quantum cryptography, as well as add-ons using cryptographic components . The website will then calculate the expected size of the handshake with the given configuration. If there is time to spare, additional metrics will be added.

This tool will make it easier to visualize different post quantum TLs configurations and underline the challenge posed by the transition to a quantum-safe web, as the magnitude of different classic, hybrid or post-quantum configurations can be quickly compared.

Work plan



Display of topic and name

☐ I, ______________________________ allow the working group IT Security and Cryptography to display my thesis topic as well as my full name on the webpages of the working group. I can withdraw this confirmation at any time.

☐ I, ______________________________ allow the working group IT Security and Cryptography to make my thesis available as a download in form of a pdf. I can withdraw this confirmation at any time.

Date, Place: ____________________ Signature: ____________________

Bibliography

[AMOW24] Nouri Alnahawi, Johannes Müller, Jan Oupický, and Alexander Wiesmaier. A Comprehensive Survey on Post-Quantum TLS. *IACR Communications in Cryptology*, July 2024. URL: `https://inria.hal.science/hal-04845617`, `doi:10.62056/ahee0iuc`.

[MRLC26] José A. Montenegro, Ruben Rios, and Javier Lopez-Cerezo. A performance evaluation framework for post-quantum tls. *Future Generation Computer Systems*, 175:108062, 2026. URL: `https://www.sciencedirect.com/science/article/pii/S0167739X25003577`, `doi:10.1016/j.future.2025.108062`.

[PST20] Christian Paquin, Douglas Stebila, and Goutam Tamvada. Benchmarking post-quantum cryptography in tls. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography*, pages 72–91, Cham, 2020. Springer International Publishing.

[RRT$^+$24] Carlos Rubio García, Simon Rommel, Sofiane Takarabt, Juan Jose Vegas Olmos, Sylvain Guilley, Philippe Nguyen, and Idelfonso Tafur Monroy. Quantum-resistant transport layer security. *Computer Communications*, 213:345–358, 2024. URL: `https://www.sciencedirect.com/science/article/pii/S0140366423004012`, `doi:10.1016/j.comcom.2023.11.010`.