Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Institute of Information Security
Applied Cryptography Group
Prof. Dr. Kenny Paterson
Dr. Felix Günther (IBM Research - Zurich)
Shannon Veitch

Master's Project for Marc Himmelberger
Dec 20, 2024 – Jun 20, 2025

Implementing and Evaluating Quantum-Safe Fully Encrypted Protocols

1 Introduction

In an attempt to circumvent Internet censorship and strengthen privacy, Fully Encrypted Protocols (FEPs) such as obfs4 [14], Shadowsocks [2] or VMess [1] encrypt or otherwise modify the data stream, so that every byte appears to be uniformly random. These protocols often serve as tunnels for hiding specific protocol behaviour. Unlike more mainstream tunneling protocols such as SSH or IPsec, a FEP makes the tunneling more difficult to recognize by ensuring that a seemingly uniformly random sequence of bytes is sent on the wire and by changing packet sizes independent of the message sizes. A similar approach also appears in an extension to compact Transport Layer Security (cTLS) [13], although also motivated in part by a desire to counteract protocol ossification — the phenomenon where network middleboxes expect a specific protocol mode and fail to adapt to newer protocol versions. Corresponding security notions for FEPs are defined in [3, 4] to capture the goals of encrypting or obfuscating all protocol data, and thus hiding protocol behaviour from an adversary.

To ensure the confidentiality of their data, these protocols typically employ AEAD schemes such as AES-GCM or ChaCha20-Poly1305. These algorithms require a shared key between the communicating parties, which is typically set up using asymmetric cryptography like RSA or elliptic curve cryptography, but may also be supplied in the form of a pre-shared key (e.g., in the case of Shadowsocks). When using RSA or elliptic curve-based cryptography for the key exchange, the confidentiality of these protocols may be threatened by the advent of a cryptographically relevant quantum computer. Such a device, capable of employing, e.g., Shor's algorithm to factor large integers or to break the discrete-logarithm problem [8] might exist as early as 2030 [6, 5] and expose even previously recorded conversations (the so-called "Harvest Now, Decrypt Later" threat).

The general approach to safeguard against a quantum threat and to ensure a security level similar to the resistance of today's algorithms against classical computers is two-fold: Symmetric algorithms should double their key size – typically this means employing 256-bit keys which is already possible in many wide-spread AEAD schemes. Asymmetric algorithms, on the other hand, should be migrated to new, so-called "post-quantum" or "quantum-safe" algorithms to ensure the security of authentication and key exchange. In this vein, NIST has standardized [12] one key encapsulation mechanism (KEM) and two signature schemes, namely ML-KEM [9], ML-DSA [10] and SLH-DSA [11]. While current implementations of FEPs are not quantum-safe, there is a proposed quantum-safe general construction for an obfs4-like key exchange in [7].

2 Description

This thesis involves implementing the proposed pq-obfs construction from [7] (an adaptation of obfs4) in order to test the practicality and performance of the new scheme. This construction introduces, in part, a novel encoding algorithm that maps ML-KEM public keys and ciphertexts to random byte strings. This thesis pay special attention to the tradeoffs in the choice of encoding strategy and to the integration into the existing ecosystem.
We thus aim to answer the following questions:

- How well does the pq-obfs protocol integrate into the existing obfs4 implementation, and what are the main challenges in the protocol adaptation?
- What tradeoffs exist in the choice of encoding strategy for KEM public keys and ciphertexts, and how do these impact the efficiency and security of the protocol?
- How resilient is the pq-obfs protocol against censorship in regions with aggressive network filtering?

3 Tasks

The project includes the following work packages (WP) (extensions possible):

WP1: Literature Review and Protocol Familiarization

The tasks of this work package include the following:

- Reviewing the proposed construction in [7]
- Reviewing the obfs4 protocol and how it differentiates itself from VMess or Shadowsocks

This work package is planned for *January 2025*.

WP2: Implementing pq-obfs

The tasks of this work package include the following:

- Implementing pq-obfs with Kemeleon encoding as specified in [7] in order to reach a proof-of-concept stage
- Evaluating performance and traffic overhead compared to the original obfs4 protocol
- Documenting the implementation

This work package is planned for *February 2025*.

WP3: Designing and Evaluating Novel Encodings

The tasks of this work package include the following:

- Designing novel encoding algorithms for quantum-safe KEMs that map public keys and ciphertexts to random bitstrings
- Instantiating pq-obfs with several KEMs and their related encodings
- Evaluating tradeoffs of different encodings of KEM public keys/ciphertexts

This work package is planned for *March / April 2025*.

WP4: Extensions

The tasks of this work package include the following:

- Experimenting with implementing different traffic patterns, such as arbitrary fragmentation of key exchange messages and/or more flexibility in clients to send arbitrary data
- Evaluating the efficacy of the protocol against blocking in censored regions

This work package is planned for *May 2025*.

WP5: Finalization

The tasks of this work package include the following:

- Finalizing the thesis report

This work package is planned for *June 2025*.

4 Grading of the Thesis

The Master's project encompasses independent scientific research, writing a Master's thesis, and giving two presentations: a mid-way presentation (roughly, 20 minutes talk and 10 minutes Q&A) and a final presentation (30 minutes talk and 15 minutes Q&A). The evaluation of the thesis takes into account the quality of the results (understanding of the subject, contributed ideas, correctness) and the quality of the documentation (thesis and presentation).

References

[1] VMess. https://www.v2ray.com/en/configuration/protocols/vmess.html, 2019.

[2] Shadowsocks. https://shadowsocks.org/doc/what-is-shadowsocks.html, 2023.

[3] Ellis Fenske and Aaron Johnson. Security notions for fully encrypted protocols. Free and Open Communications on the Internet 2023 Workshop, Issue 1, https://www.petsymposium.org/foci/2023/foci-2023-0004.php, 2023.

[4] Ellis Fenske and Aaron Johnson. Bytes to schlep? Use a FEP: Hiding protocol metadata with fully encrypted protocols. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, CCS '24, page 1982–1996, New York, NY, USA, 2024. Association for Computing Machinery.

[5] Bundesamt für Sicherheit in der Informationstechnik. Kryptografie quantensicher gestalten — bsi.bund.de. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf, 2021. [Accessed 14-12-2024].

[6] Bundesamt für Sicherheit in der Informationstechnik. Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography — bsi.bund.de. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf, 2024. [Accessed 14-12-2024].

[7] Felix Günther, Douglas Stebila, and Shannon Veitch. Obfuscated key exchange. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, CCS '24, page 2385–2399, New York, NY, USA, 2024. Association for Computing Machinery.

[8] National Cybersecurity Center of Excellence. Migration to post-quantum cryptography. https://www.nccoe.nist.gov/sites/default/files/2022-06/Migration-to-PQC-05-16.pdf, 2022. [Accessed 14-12-2024].

[9] National Institute of Standards and Technology. Federal Information Processing Standard (FIPS) 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard. https://csrc.nist.gov/pubs/fips/203/final, 2024. [Accessed 14-12-2024].

[10] National Institute of Standards and Technology. Federal Information Processing Standard (FIPS) 204, Module-Lattice-Based Digital Signature Standard. https://csrc.nist.gov/pubs/fips/204/final, 2024. [Accessed 14-12-2024].

[11] National Institute of Standards and Technology. Federal Information Processing Standard (FIPS) 205, Stateless Hash-Based Digital Signature Standard. https://csrc.nist.gov/pubs/fips/205/final, 2024. [Accessed 14-12-2024].

[12] National Institute of Standards and Technology. Post-Quantum Cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography, 2024. [Accessed 14-12-2024].

[13] Benjamin M. Schwartz and Christopher Patton. The Pseudorandom Extension for cTLS. Internet-Draft draft-cpbs-pseudorandom-ctls-01, Internet Engineering Task Force, April 2022. Work in Progress. https://datatracker.ietf.org/doc/draft-cpbs-pseudorandom-ctls/01/.

[14] The Tor Project. obfs4 (the obfourscator), protocol specification, version c0898c2d. https://gitlab.torproject.org/tpo/anti-censorship/pluggable-transports/lyrebird/-/blob/main/doc/obfs4-spec.txt, 2019.