qChat - Post Quantum P2P Chat

Miles Strässle, Svenja Sutter

December 20, 2023

OST – Ostschweizer Fachhochschule

Table of Content

OST
Ostschweizer
Fachhochschule

Motivation

Ensure secure messaging in post-quantum era ...

OST
Ostschweizer
Fachhochschule

State of the Art

Briar

Pros:

- P2P
- Tor
- Offline communication

Cons:

- No PQC

Signal

Pros:

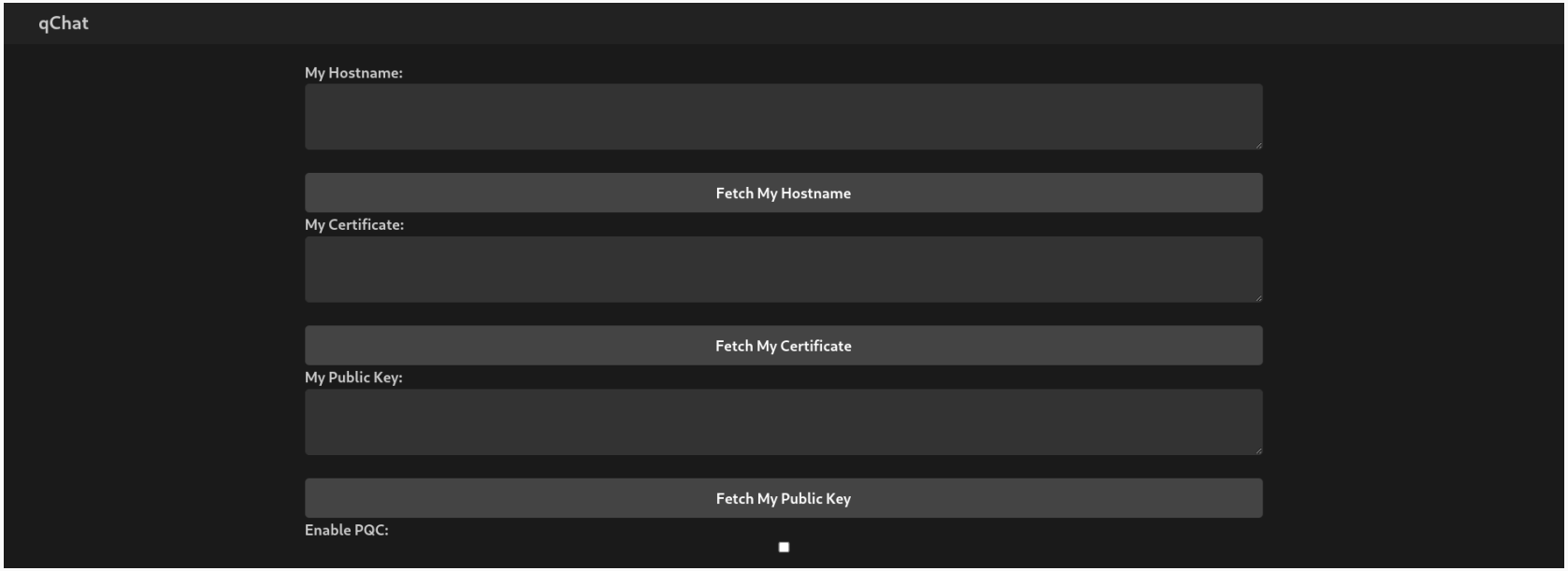
- P2P
- PQC

Cons:

- Phone number for registration

OST
Ostschweizer
Fachhochschule

Application - User Information

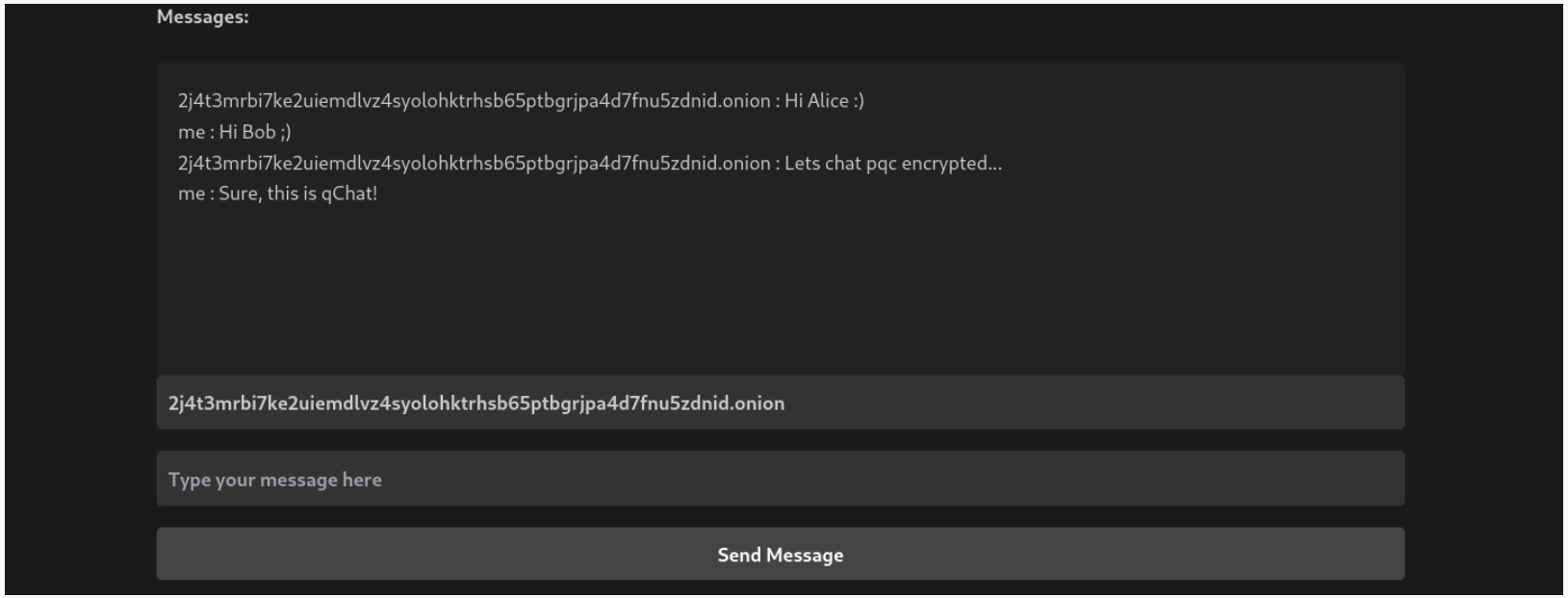


OST
Ostschweizer
Fachhochschule

Application - Registration Friend

OST
Ostschweizer
Fachhochschule

Application - Send Messages



OST
Ostschweizer
Fachhochschule

PQC: Post Quantum Cryptography

- National Institute of Standards and Technology
- Round 3 - Crystals-Kyber (KEM)
  - kyber-768 parameter set
  - shared library
  - structured lattices

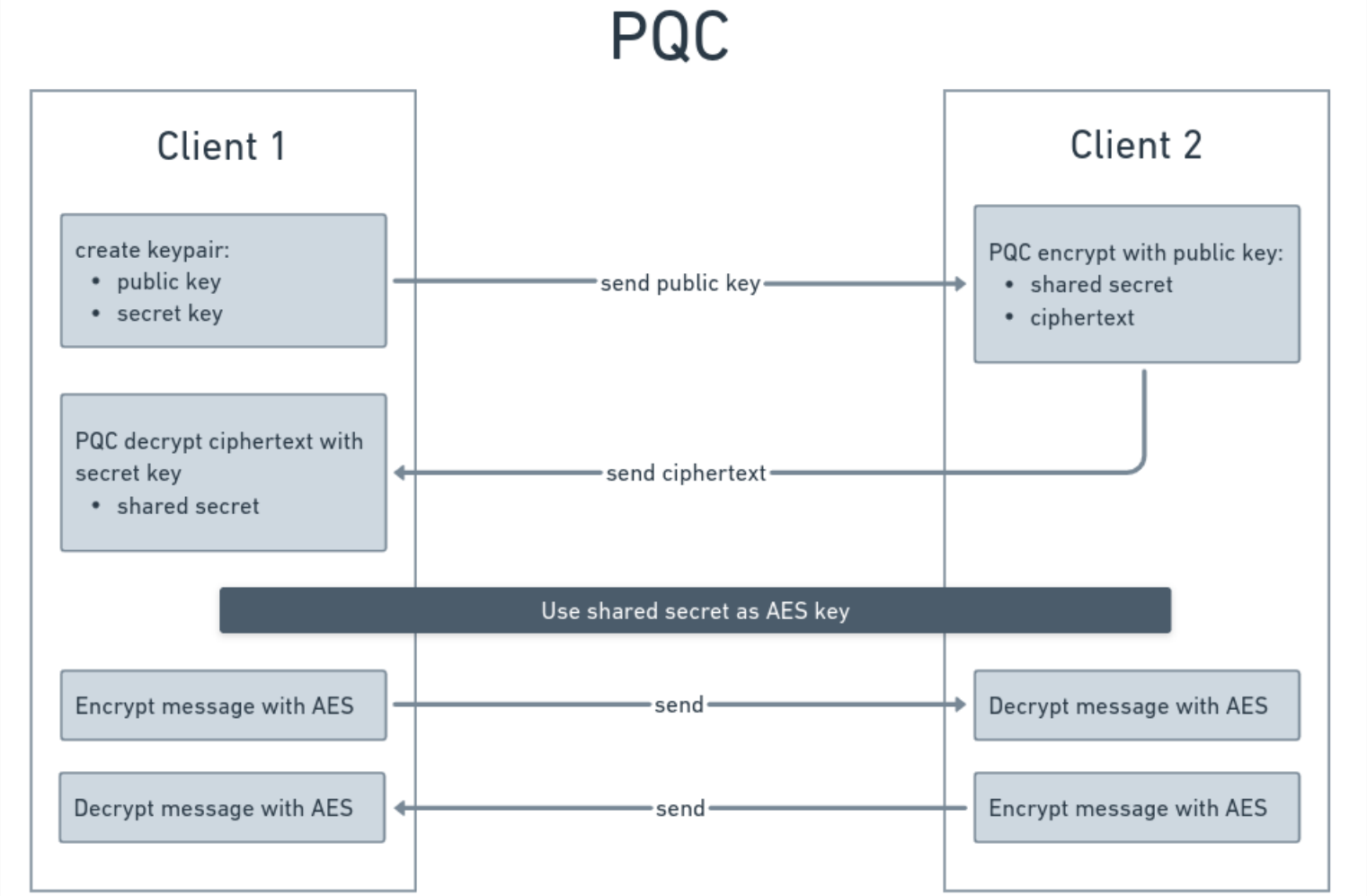
OST
Ostschweizer
Fachhochschule

Lattice-based Cryptography

- BQP (complexity)
- LWE Problem (reduction CVP/SVP Problem)
- Encapsulates symmetric AES-256 key
- Keysize
  - secret key: 2400 Bytes
  - public key: 1184 Bytes

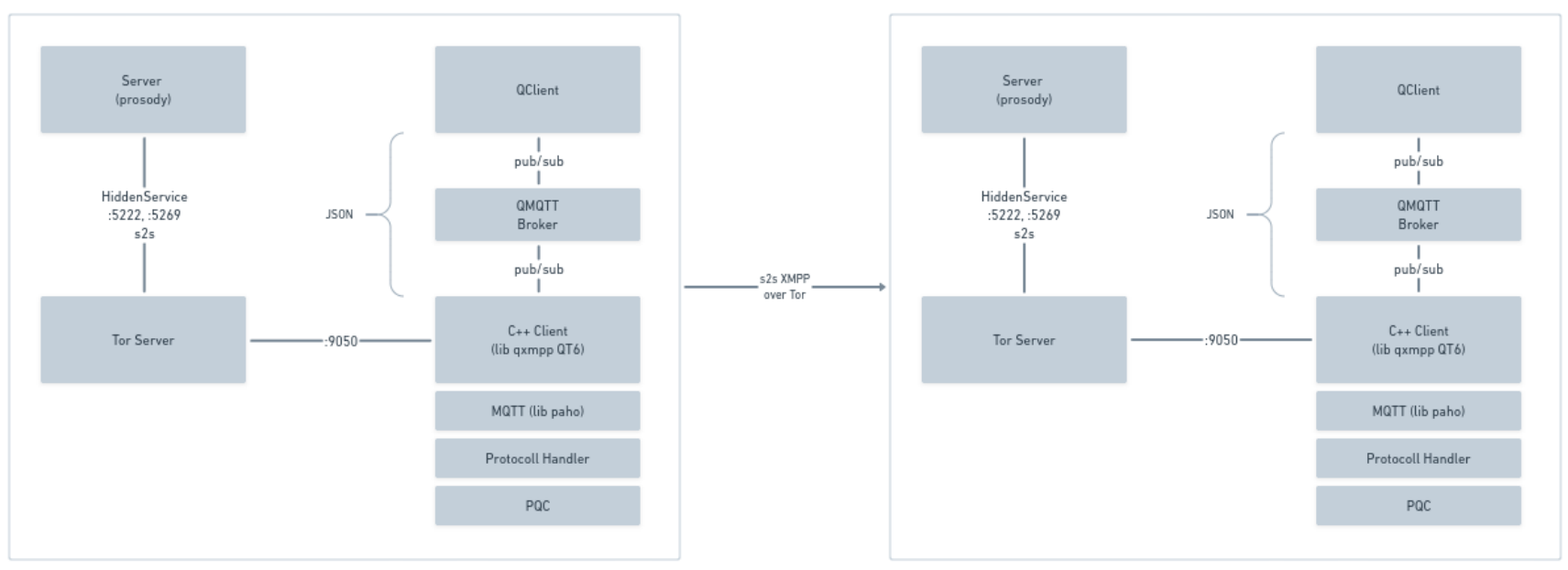
OST
Ostschweizer
Fachhochschule

CRYSTALS-KYBER



OST
Ostschweizer Fachhochschule

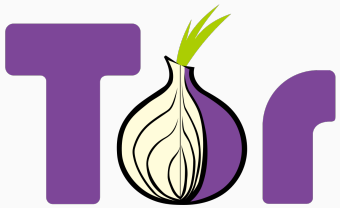
Architecture



OST
Ostschweizer
Fachhochschule

Design Decisions

Why Tor?



- *Circumvent NAT*
- *Anonymity*
- *Security (E2E in Tor v3)*

OST
Ostschweizer
Fachhochschule

Why XMPP?

- *Well established P2P Protocol*
- *Customizable Server Settings (prosody)*
- *Lightweight*
- *Maintained Libraries for our client (qxmpp)*
- *Suited for our client/server design*

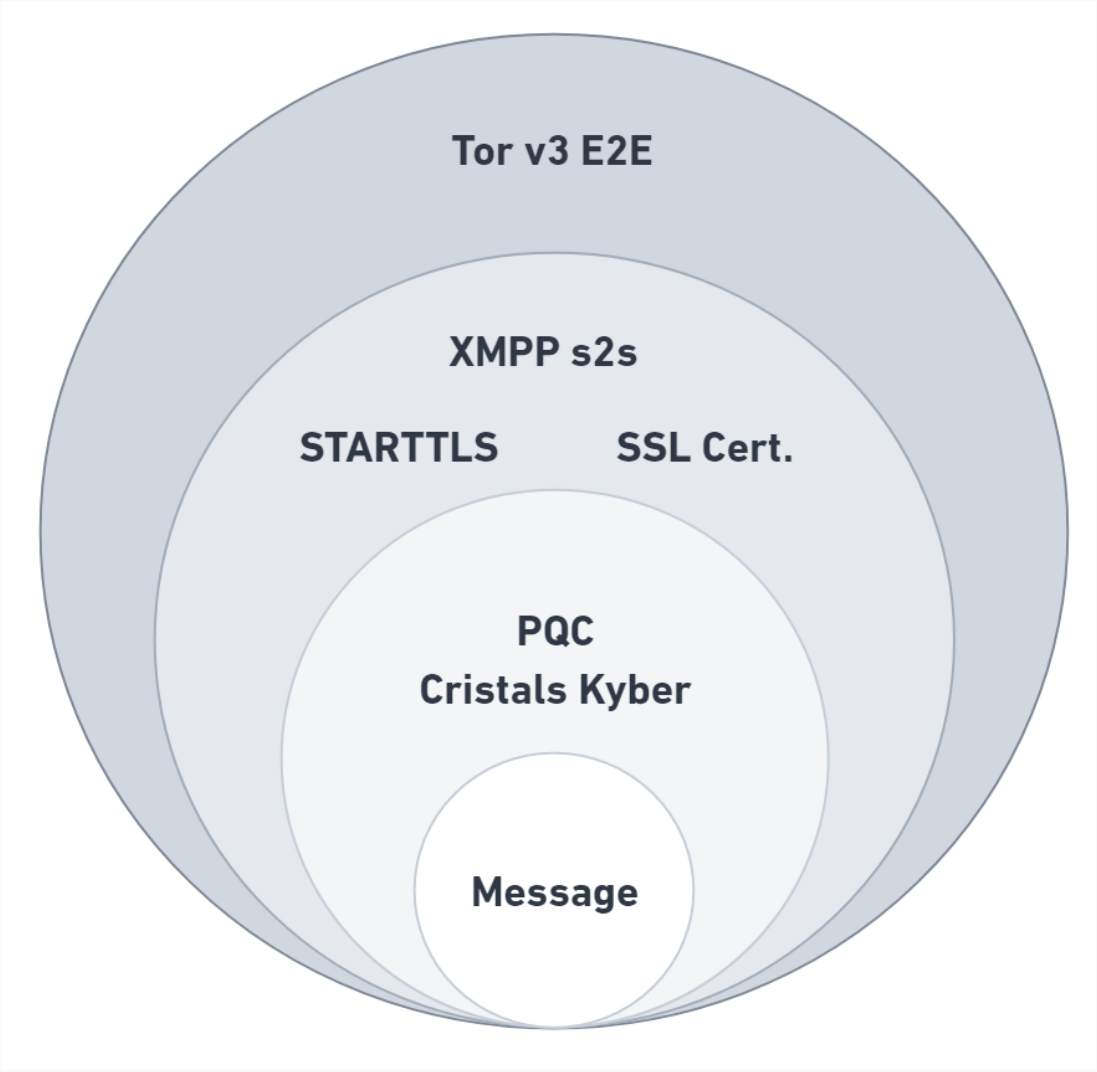
OST
Ostschweizer
Fachhochschule

Why MQTT?

- *Simple communication between back- and frontend*
- *Efficient*

OST
Ostschweizer
Fachhochschule

Security Layers



OST
Ostschweizer
Fachhochschule

Demo

Questions