qChat - Post Quantum P2P Chat

Miles Strässle, Svenja Sutter December 20, 2023

OST - Ostschweizer Fachhochschule

Table of Content

- Motivation
- State of the Art
- Application
- PQC: Post Quantum Cryptography
- Architecture and Design Decisions
- Security Layers
- Demo



Motivation

Ensure secure messaging in post-quantum era \dots



State of the Art



Pros:

- P2P
- Tor
- Offline communication

Cons:

• No PQC



Pros:

- P2P
- PQC

Cons:

 Phone number for registration



Application - User Information

qChat			
	My Hostname:		
		Fetch My Hostname	
	My Certificate:		
		Fetch My Certificate	
	My Public Key:		
			•
		Fetch My Public Key	
	Enable PQC:	•	



Application - Registration Friend

Friends Hostname	
	Save Certificate
PQC Public Key	
	Save PQC Public Key
	Saveracrabilities



Application - Send Messages

Messages:
2j/43mrbi7ke2uiemdlvzdsyolohktrhsb65ptbgrjpa4d7fnu5zdriid onton : Hi Alice :) ms : Hi Bob ;) 2j/413mrbi7ke2uiemdlvz4syolohktrhsb65ptbgrjpa4d7fnu5zdriid onton : Lets chat pqc encrypted ms : Sure, this is qChatt
2j4t3mrbi7ke2uiemdlvz4syolohktrhsb65ptbgrjpa4d7fnu5zdnid.onion
Send Message



PQC: Post Quantum Cryptography



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

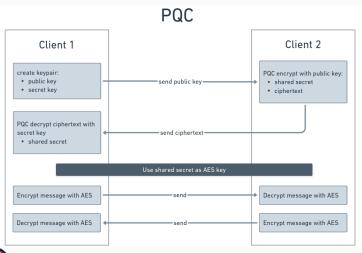


Lattice-based Cryptography

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

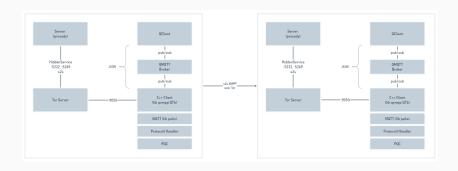


CRYSTALS-KYBER





Architecture





Design Decisions

Why Tor?



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



Why XMPP?



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



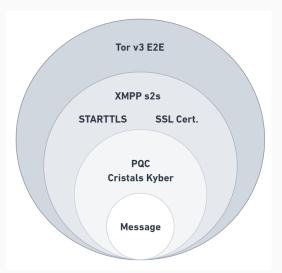
Why MQTT?



- Simple communication between back- and frontend
- Efficient



Security Layers





Demo

Questions