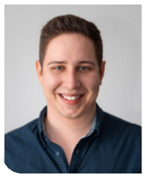
qChat

post-quantum peer-to-peer chat for privacy

Students



Miles Strässle

Svenja Sutter

Introduction:

Our application, qChat, is a decentralized, peer-to-peer chat application meant for future-proof privacy. It uses the latest encryption algorithms to ensure secret message exchange in the post-quantum era.

Quantum computing poses a significant threat to current encryption methods, particularly due to advancements like Shor's Algorithm. This algorithm, in theory, allows quantum computers to break widely-used encryption schemes such as RSA and ECC much faster than conventional computers.

Result:

The solution involves developing a peer-to-peer chat application using post-quantum cryptography, eliminating reliance on external servers for data storage.

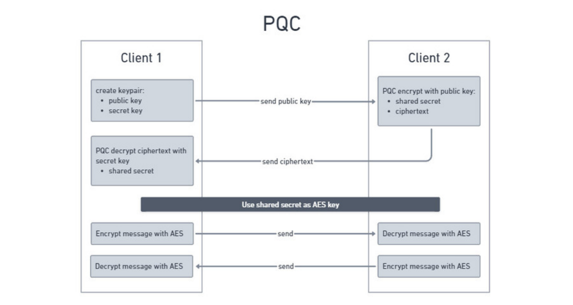
The project has successfully created a prototype demonstrating peer-to-peer functionality with integrated post-quantum cryptography.

Conclusion:

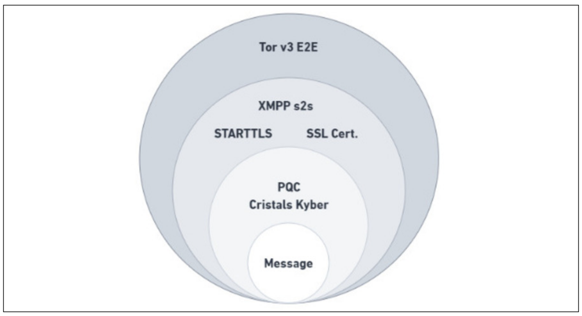
These developments are significant as they provide a practical approach to secure communication, setting a precedent in the field of quantum-resistant digital communication.

The insights and technologies developed in qChat lay the groundwork for future advancements in secure communications. This also marks a significant advancement in protecting the private sphere in an increasingly interconnected post-quantum world.

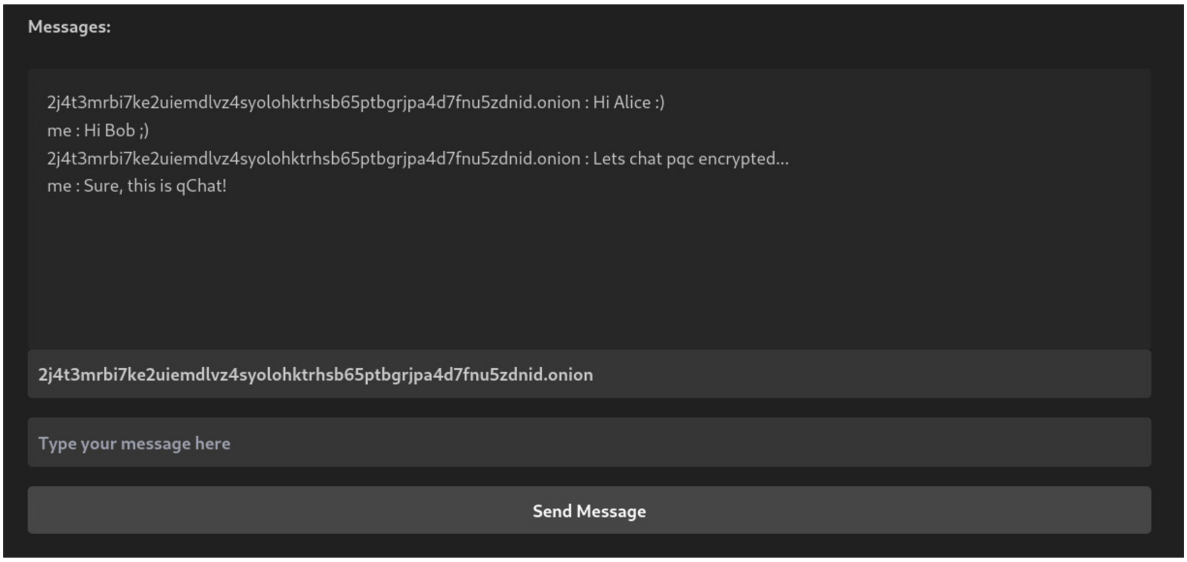
Client 1 and Client 2 negotiate the shared secret for symmetric encryption.
Own presentment



All security layers which protect the message along the way from peer-to-peer over tor network.
Own presentment



qChat chat window which demonstrates post-quantum encrypted messaging.
Own presentment



Messages:

2j4t3mrbi7ke2uiemdlvz4syolohktrhsb65ptbgrjpa4d7fnu5zdnid.onion : Hi Alice :)
me : Hi Bob ;)
2j4t3mrbi7ke2uiemdlvz4syolohktrhsb65ptbgrjpa4d7fnu5zdnid.onion : Lets chat pqc encrypted...
me : Sure, this is qChat!

2j4t3mrbi7ke2uiemdlvz4syolohktrhsb65ptbgrjpa4d7fnu5zdnid.onion

Advisor

Dr. Alexandru Caracas

Subject Area

Software, Security, Communication systems, Internet Technologies and Applications