WORLD QUANTUM DAY
APRIL 14

Post-Quantum Cryptography


Esther Hänggi


Iyán Méndez Veiga

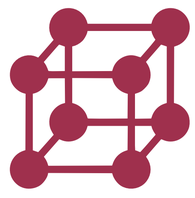
HSLU Lucerne University of Applied Sciences and Arts

n|w University of Applied Sciences and Arts Northwestern Switzerland

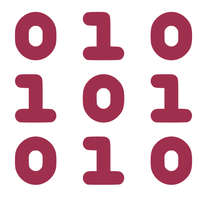

Christoph Wildfeuer


Timeo Jauslin

New mathematical problems that are also hard for quantum computers


Lattice-based

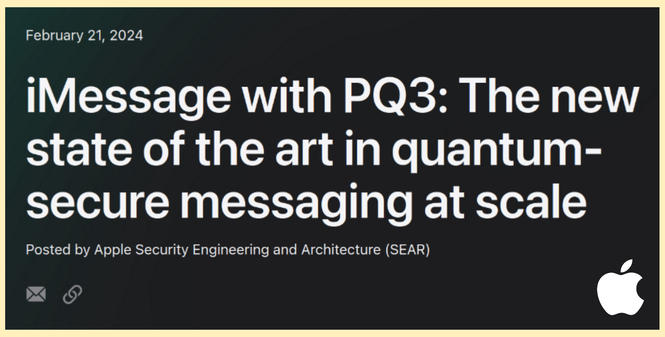

Hash-based


Code-based

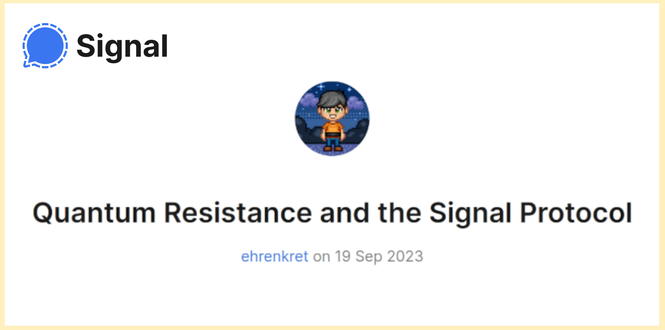
...

PQC Migration 1: Quantum-Safe Key Exchanges

When? 2024...



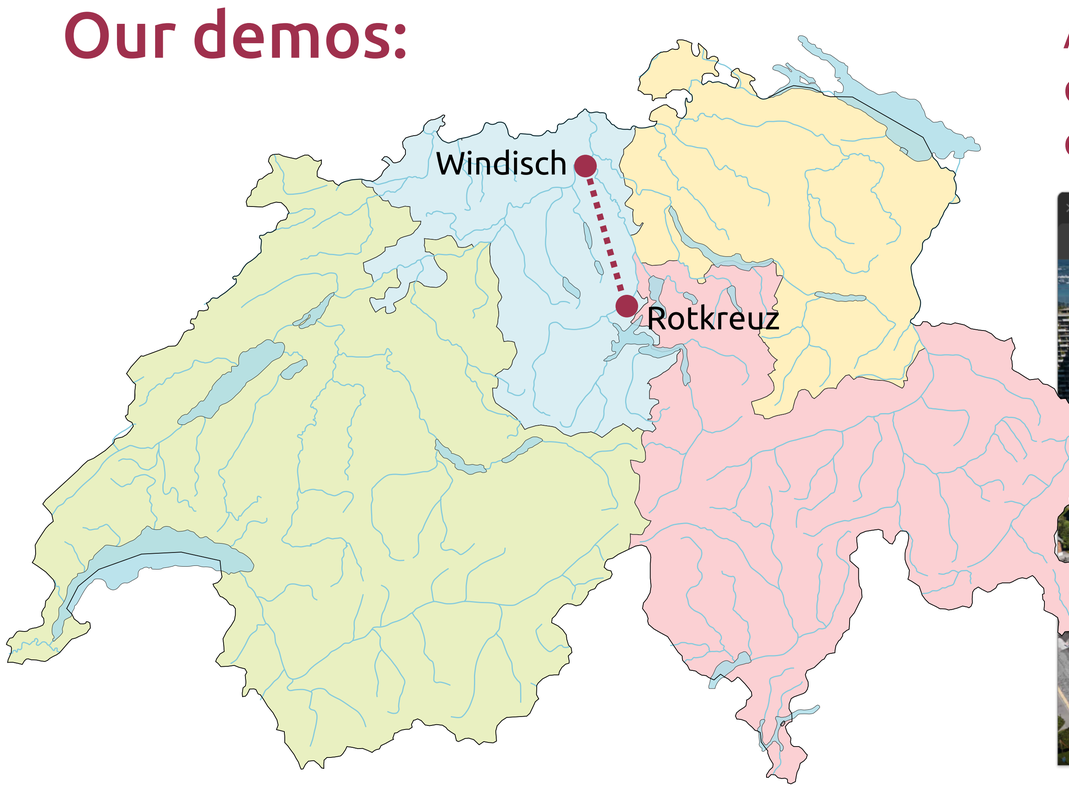
Apple will start using post-quantum cryptography for iMessage in 2024.



Signal already migrated to a quantum-safe key exchange for its end-to-end encrypted messaging service.

Google's Chrome web browser already supports a quantum-safe key exchange. It is enabled in ~10% of users.

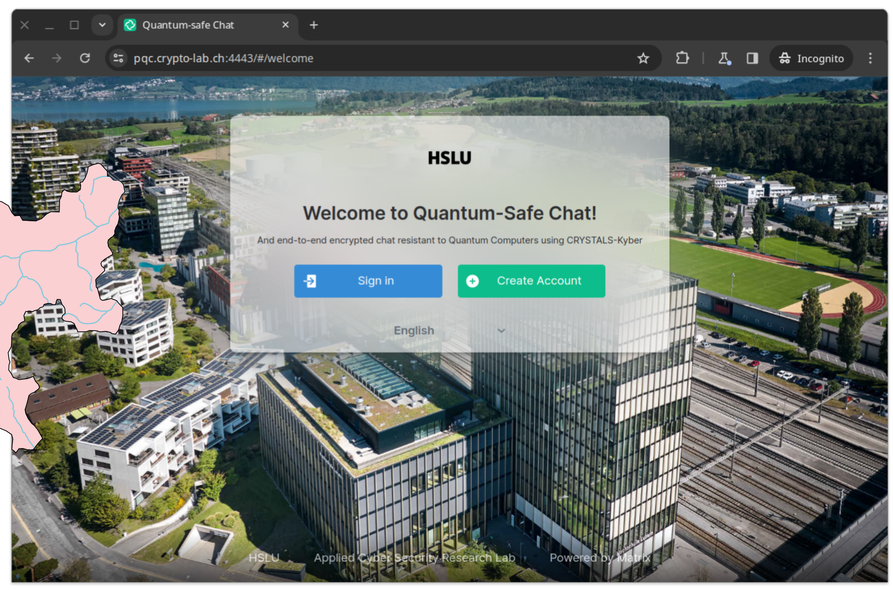
Our demos:



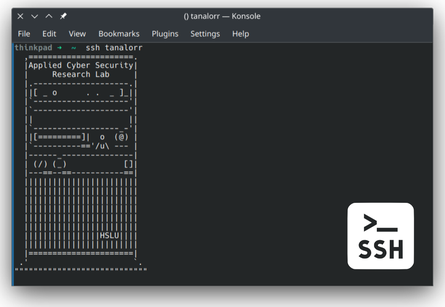
An end-to-end encrypted chat and quantum-safe videoconference with our own Matrix server

matrix

https://pqc.crypto-lab.ch/



A Quantum-safe tunnel over SSH between HSLU and FHNW



PQC Migration 2: Quantum-Safe Digital Signatures

When? ~2026...

Migrating to quantum-safe authentication and digital signatures will involve many more changes. We expect to see the first PQC Internet certificates around 2026. A second PQC migration will begin then. We are working with essendi it and securosys to better understand the challenges of this migration.

HSLU securosys essendi it