Sichere Zukunft:

Quantensicheres Verschlüsselungssystem für den praktischen Einsatz in Firmennetzwerken und Internet

03-02-2021

Christoph Wildfeuer,
Institut für Sensorik und Elektronik
FHNW, Brugg-Windisch
Team: Nico Schwab, Willi Meier, Christoph Wildfeuer

Motivation:

- Stellen Sie sich vor: In 10 Jahren sagt jemand an, dass er einen *Large Scale Quantum Computer* entwickelt hat!

  „NIST estimates that the first cryptographically relevant quantum computer could be built by **2031** for a cost of about **one billion US dollars**“

- Was wären die Folgen?

The New York Times

„INTERNET CRYPTOGRAPHY KILLED BY PHYSICISTS“

Users panic: What happens to Cryptography?

The New York Times

„INTERNET CRYPTOGRAPHY KILLED BY PHYSICISTS“

• Public-Key Cryptography	RSA	Dead!
• Elliptic-Curve Diffie-Hellman	ECDH	Dead!
• Elliptic-Curve Cryptography in general	ECC	Dead!

- Die Sicherheit von nahezu der gesamten Internetkommunikation basiert auf Public-Key Cryptography (PKC).

- Die Sicherheit der Algorithmen beruht auf dem für klassische Computer schwierigen mathematischen Problemen der Faktorisierung von grossen Zahlen und der Berechnung des diskreten Logarithmus.

Post-Quantum Cryptography PQC

Round 3 Submissions

Official comments on the Third Round Candidate Algorithms should be submitted using the "Submit Comment" link for the appropriate algorithm. Comments from the pqc-forum Google group subscribers will also be forwarded to the pqc-forum Google group list. We will periodically post and update the comments received to the appropriate algorithm.

All relevant comments will be posted in their entirety and should not include PII information in the body of the email message.

Please refrain from using OFFICIAL COMMENT to ask administrative questions, which should be sent to pqc-comments@nist.gov

Guidelines for Submitting Tweaks for Third Round Finalists and Candidates (pdf)

By selecting the "Website" links, you will be leaving NIST.gov. We have provided links to submitter web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites.

History of Round 3 Updates

PROJECT LINKS
Overview
FAQs
News & Updates
Events
Publications
Presentations

ADDITIONAL PAGES
Post-Quantum Cryptography Standardization
Call for Proposals
Example Files
Round 1 Submissions
Round 2 Submissions
Round 3 Submissions
Workshops and Timeline
Round 3 Seminars
External Workshops

Ersetzen der kryptographischen Algorithmen in entsprechenden Anwendungs-Protokollen:

- Transport Layer Security Protocol (**TLS**), auch bekannt unter der Vorgängerbezeichnung Secure Sockets Layer, ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet (Wird von HTTPS eingesetzt).
- Secure Shell Protokoll **SSH**, bezeichnet ein kryptographisches Netzwerkprotokoll für den sicheren Betrieb von Netzwerkdiensten über ungesicherte Netzwerke.
- **X.509** ein ITU Standard für eine Public-Key Infrastruktur zum erstellen digitaler Zertifikate.
- **CMS** and S/MIME, Cryptographic Message Syntax ist ein Standard vom IETF für gesicherte kryptographische Mitteilungen.

Das Open Quantum Safe Projekt hat zum Ziel die Unterstützung, Entwicklung und Prototypen-Entwicklung von quantensicherer Kryptographie.

Openquantumsafe.org

UNIVERSITY OF WATERLOO

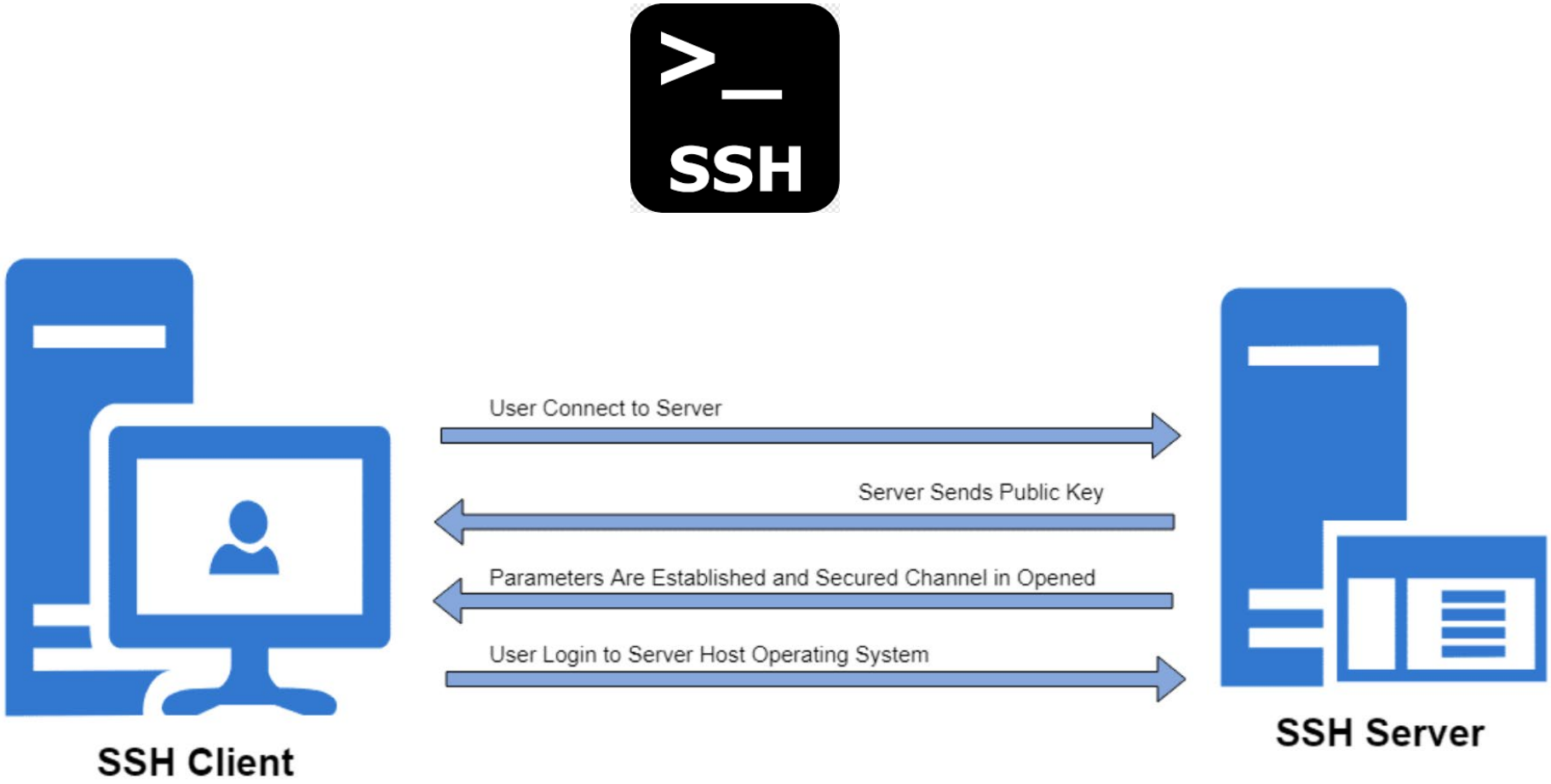
Financial and in-kind support:

aws NSERC CRSNG

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

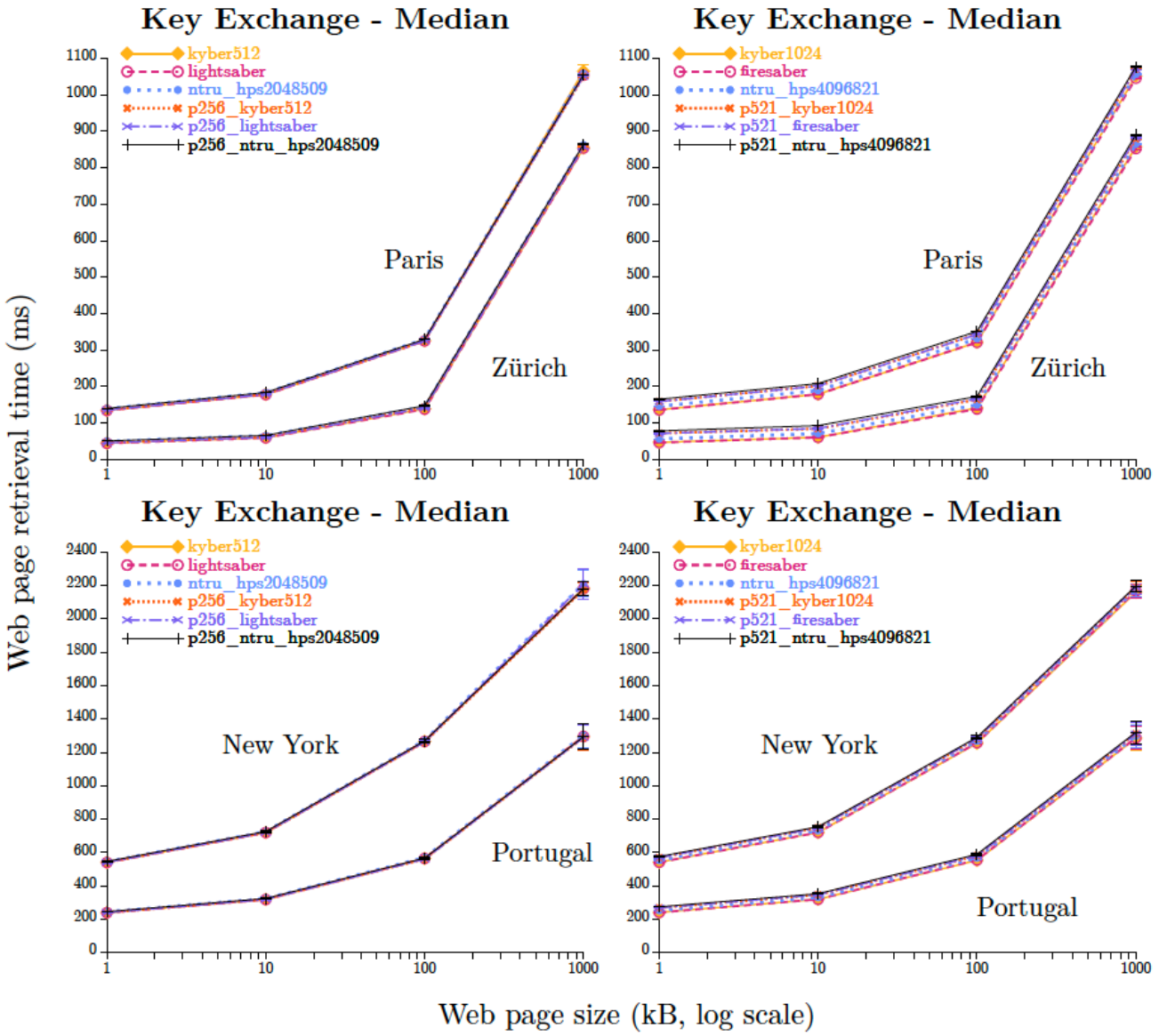
evolution Microsoft

IBM Research



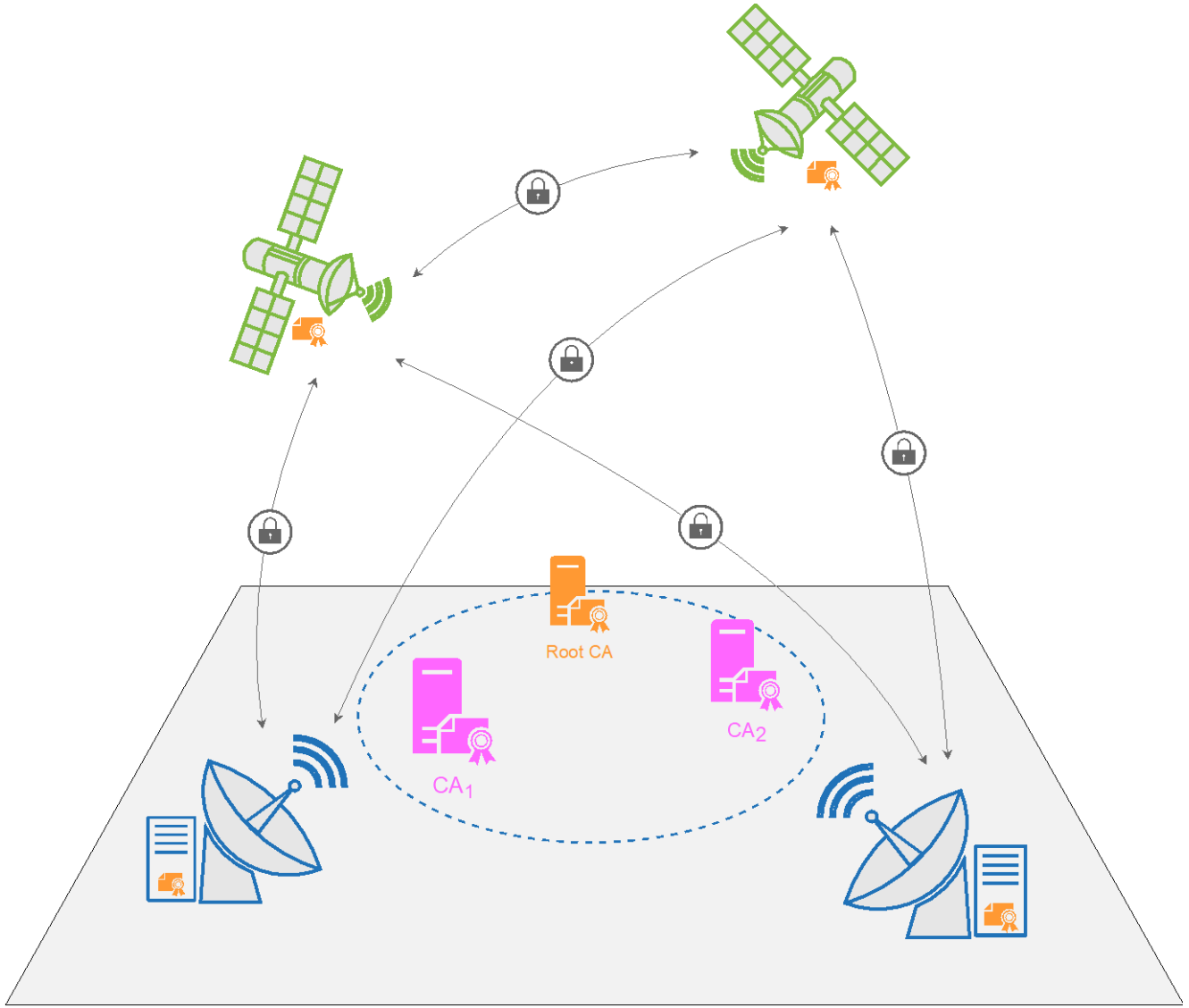
Docker-Image für quantensicheren SSH Server und Client:
https://github.com/open-quantum-safe/oqs-demos/tree/main/openssh

Benchmarking von TLS 1.3 mit quantensicherem key exchange



@Frank Imhof

Quantensichere Satelliten-Funkverbindung, ESA Gesuch in Vorbereitung



Die Transformation zur Post-Quantum Cryptography (PQC) ist notwendig und ist ein längerer Prozess!

Die Industrie sollte sich Gedanken machen:

- Über die ganze Tragweite und die Folgen der Transformation zur PQC.
- Welche Bereiche in den sicherheitsrelevanten Anwendungen betroffen sind?
- Der Transformationsprozess wird einige Jahre dauern, mit einer (möglicherweise hybriden) Übergangsphase.
- Welche Konsequenzen hat dies für die bestehenden Implementierungen und Infrastruktur?

Contact:

Github Quellen vom ISE @ FHNW
https://github.com/fhnw-ise-qcrypt

Docker-Image für quantensicheren SSH Server und Client:
https://github.com/open-quantum-safe/oqs-demos/tree/main/openssh

Weitere Informationen:
www.openquantumsafe.org

- Prof. Dr. Christoph Wildfeuer
- christoph.wildfeuer@fhnw.ch