



QKD4GOV

Sicherung von Behördendaten mittels quanten-sicherer
Kryptographie

Hannes Hübel

AIT Austrian Institute of Technology GmbH

Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

Projekt- und Kooperationspartner:innen



≡ Bundesministerium
Europäische und internationale
Angelegenheiten



≡ Bundesministerium
Landesverteidigung

≡ Bundeskanzleramt



≡ Bundesministerium
Inneres

Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

Motivation



Nature, Oct. 2019:
"Quantum supremacy
using a programmable
superconducting
processor"

Google 
54-qubit Sycamore processor







**Dec. 2020: New Record in Chinese lab:
10 billion times faster than Google**

Chinese photonic Quantum
computer "Jiuzhang"

20-qubit processor in rack



Gefördert/finanziert durch die Sicherheitsforschungs-Förderprog



RNET PASS des Bundesministeriums für Finanzen

Kryptographie und Algorithmus von Shor

- Asymmetrische Kryptographie (**Schlüsselverteilung**) basiert auf der mathematischen Vermutung, dass es sehr aufwändig ist, **große Zahlen zu faktorisieren**
- **Der Shor-Algorithmus macht diese Faktorisierung auf einem Quantencomputer effizient möglich!**

Rechenaufwand für die Zerlegung einer Zahl N :

- *Klassischer Computer:*
 $\sim e^{1.9} (\log N)^{1/3} (\log \log N)^{2/3}$
Rechenschritte

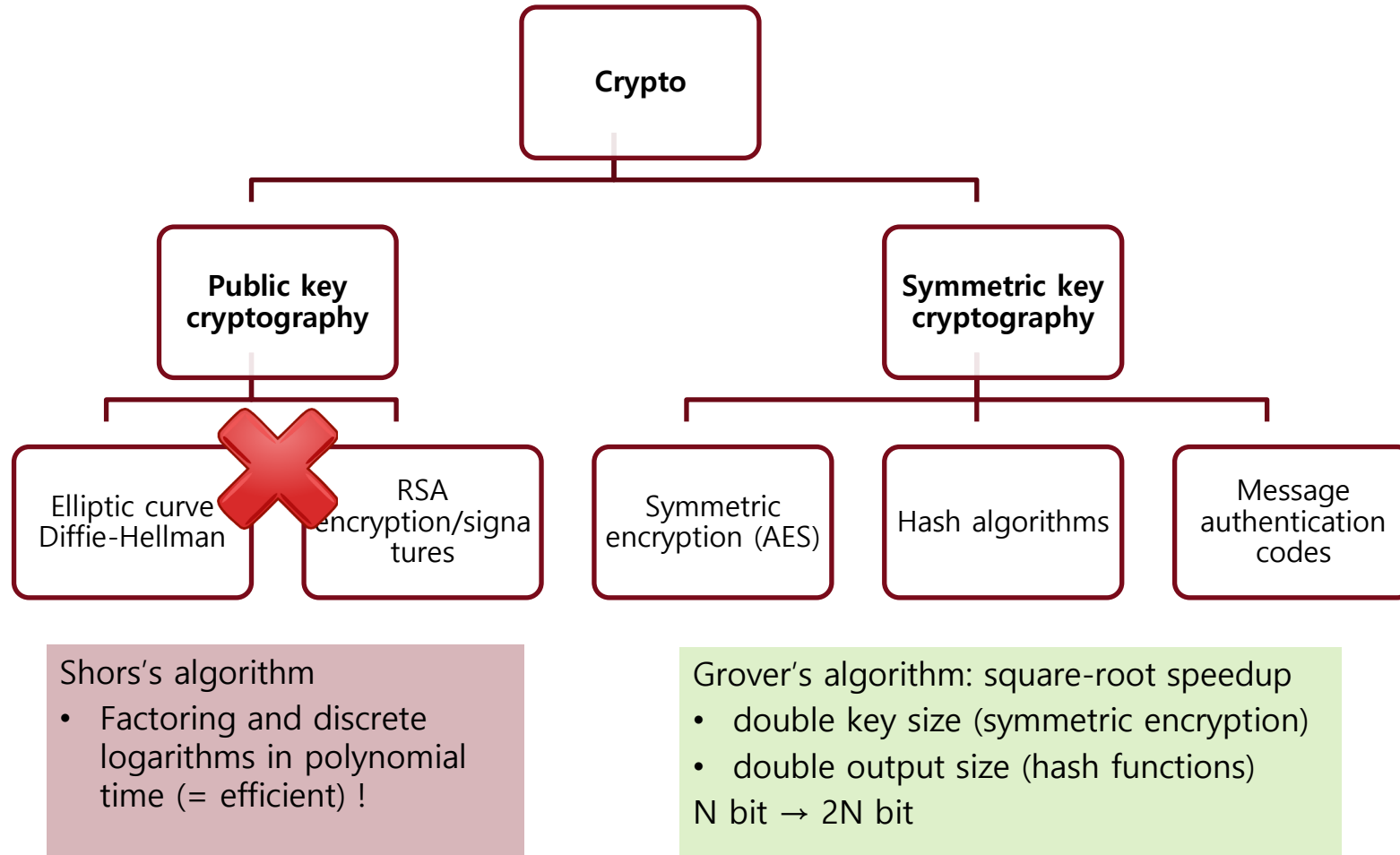


*Shor-
Algorithmus*

- ***Quantencomputer:***
 $\sim (\log N)^2 (\log \log N) (\log \log \log N)$ Rechenschritte

Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

Auswirkung auf klassische Kryptographie



Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

Müssen wir handeln?

Mosca's Theorem*:

$$\text{Lifetime of secret} + \text{Migration time} > \text{Development of Quantum Computer}$$

... you are in trouble

NIST Competition für quanten-resistente Kryptographie: Post-Quantum Cryptography (PQC)

*Michele Mosca, Co-Founder of Institute of Quantum Computing in Waterloo (Canada)

Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

Quantenschlüsselverteilung

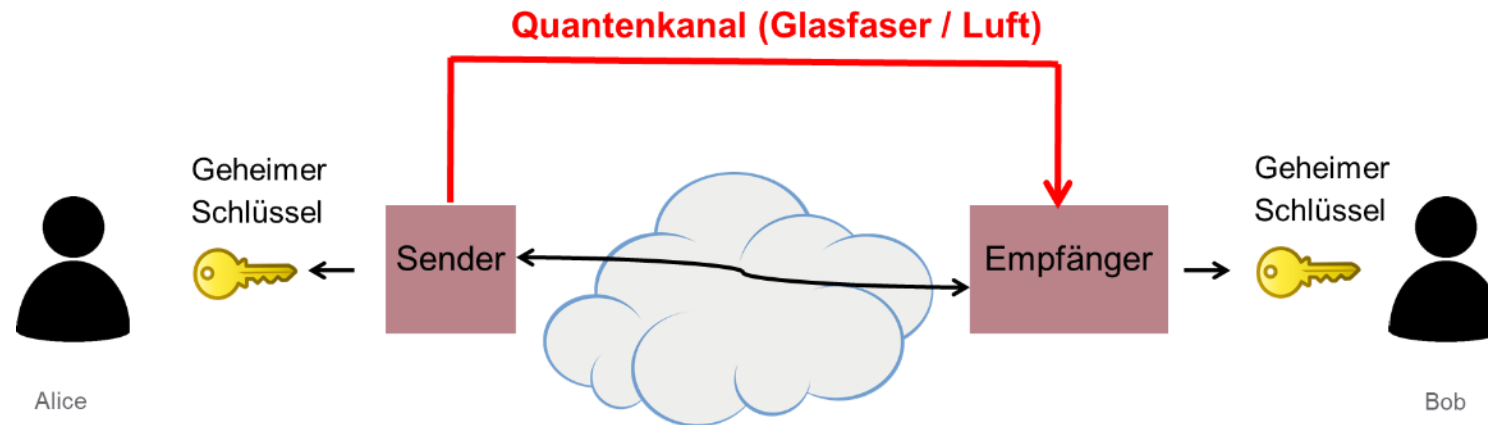
Quantenschlüsselverteilung QKD: **Informations-theoretisch sichere** Methode um einen **Schlüssel** zwischen 2 Partner auszutauschen

Symmetrischer Schlüssel:

- QKD verschlüsselt keine Nachrichten.
- QKD produziert einen Schlüssel: **sicher, identisch, zufällig**
- QKD Schlüssel wird in **klassischen** symmetrischen **Verschlüsselungsverfahren** eingesetzt (z.B. One time pad, AES)

Sicherheit:

- die Sicherheit des Schlüssels basiert auf **quantenphysikalischen Grundsätzen**.
- ein Abhörer baut unweigerlich Fehler ein (Heisenbergsche Unschärfe).
- sicher gegen **klassische Attacken** und alle Quantenattacken



Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

Zielsetzung

Innerstädtisches QKD Netz

Ziel: Demonstration von QKD gesicherter Kommunikation zwischen staatlichen Einrichtungen

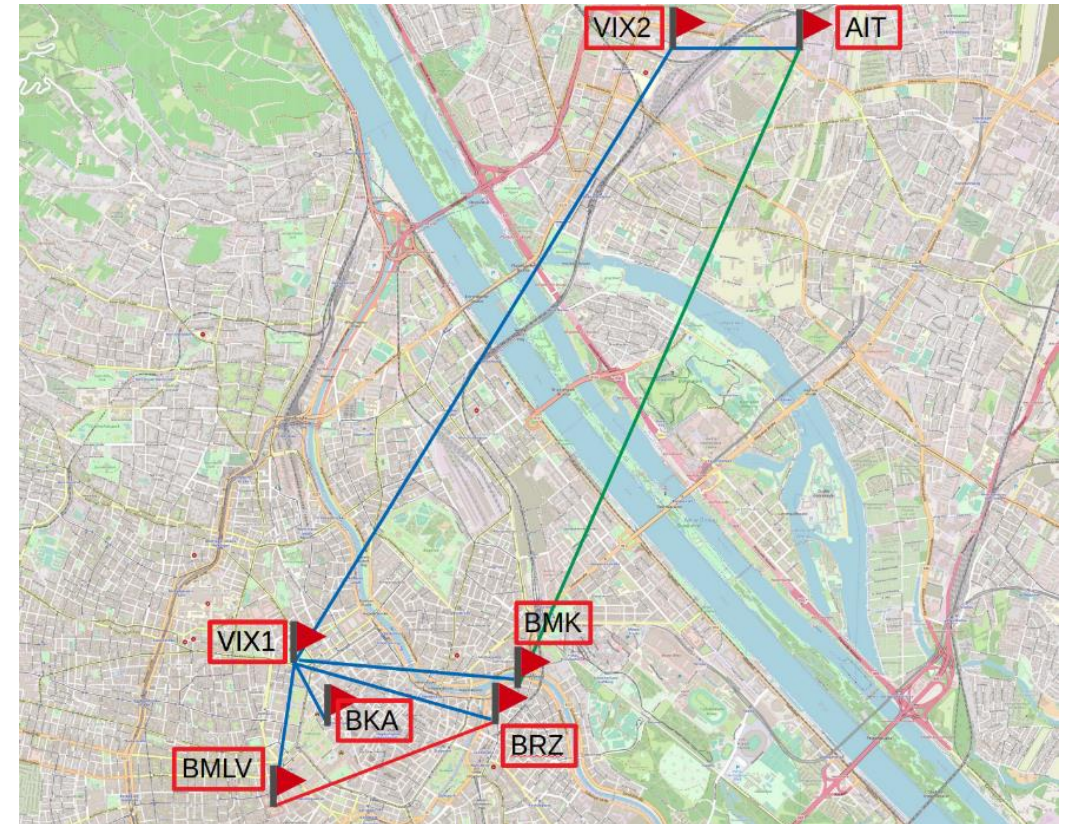
7 Knoten: BKA, BMLV, BMK, BRZ, AIT, VIX1 und VIX2

Durchgeführte Demos

1. Secret Sharing für sichere Datenspeicherung
2. Gesicherte Chat Applikation

Techdemos

1. Mehrweg-Routing QKD
2. QKD / PQC hybride Verschlüsselung



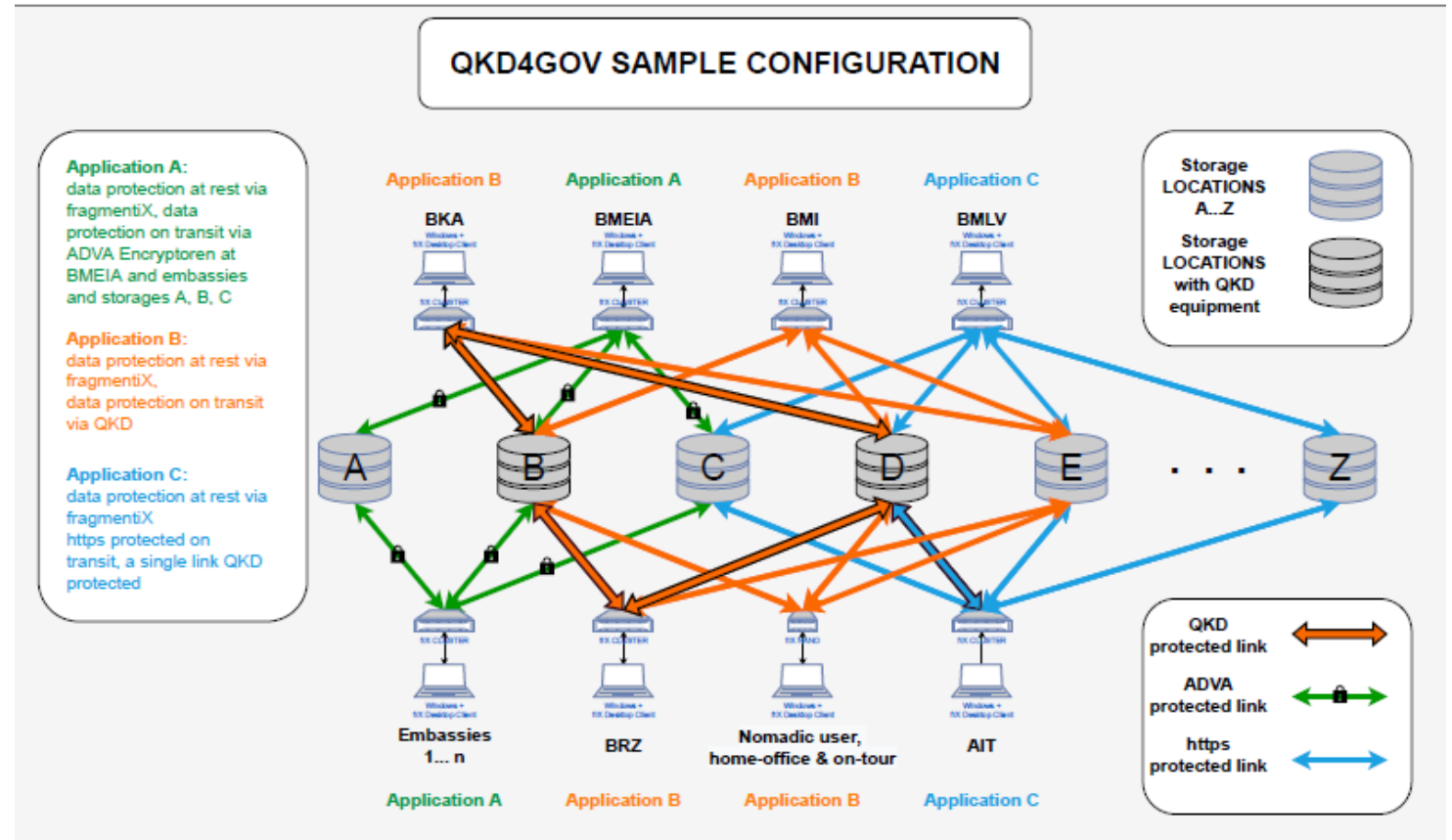
Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

Anwendungen und Demonstrationen

Sichere Datenspeicherung

Datenspeicherung mittels Secret Sharing

- Höchste Sicherheitseigenschaften
- Verknüpfung mit QKD-Netzwerken zur Übertragung der Daten zwischen Storage Locations / Rechenzentren



Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

Anwendungen und Demonstrationen

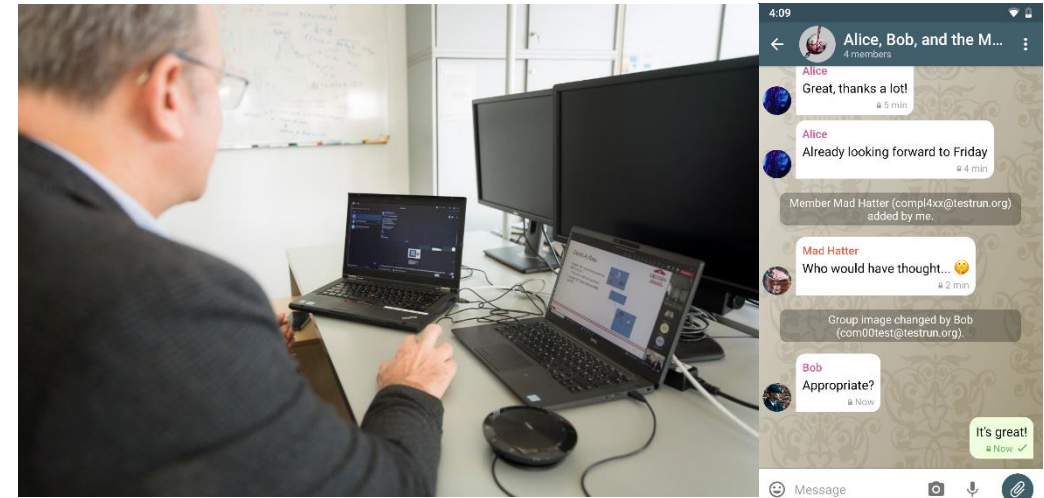
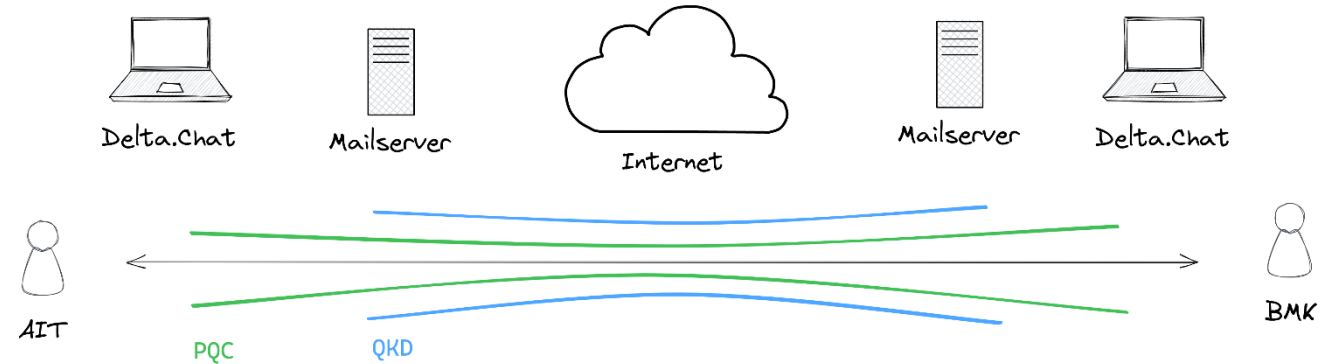
Sichere Kommunikation

Viele verschiedene etablierte Kommunikations-Systeme

- Chat: WhatsApp, Signal, etc.
- Video: Teams, Zoom, Jitsi, BBB, etc.

Absicherung mit QKD und PQC für Systeme in eigener Infrastruktur

- ITS-Sicherheit durch QKD
- Ende-zu-ende sichere Kommunikation mittels PQC
- Demonstriert mit open source Chat Software delta.chat



Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

Anwendungen und Demonstrationen

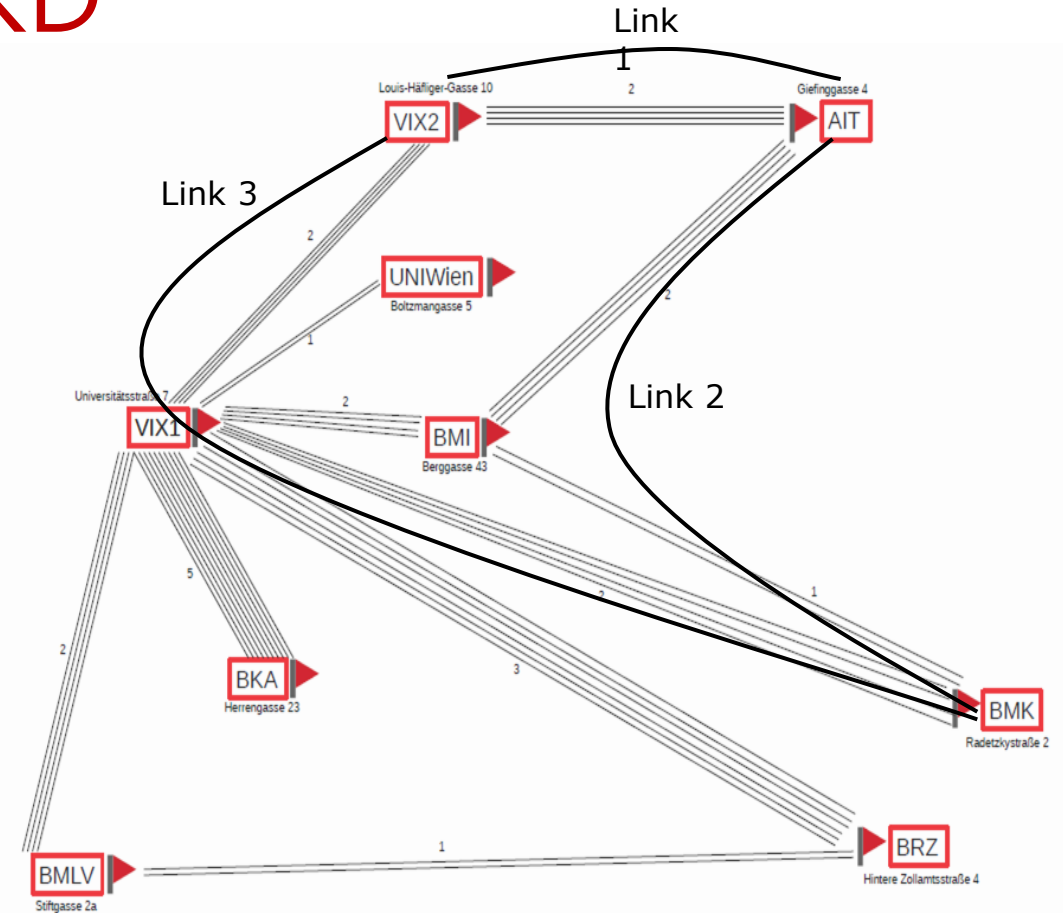
Tech Demo: Mehrweg-QKD

Trusted Nodes bekommen vollständiges Schlüsselmaterial übermittelt

- Hoher Schutzbedarf für Trusted Nodes

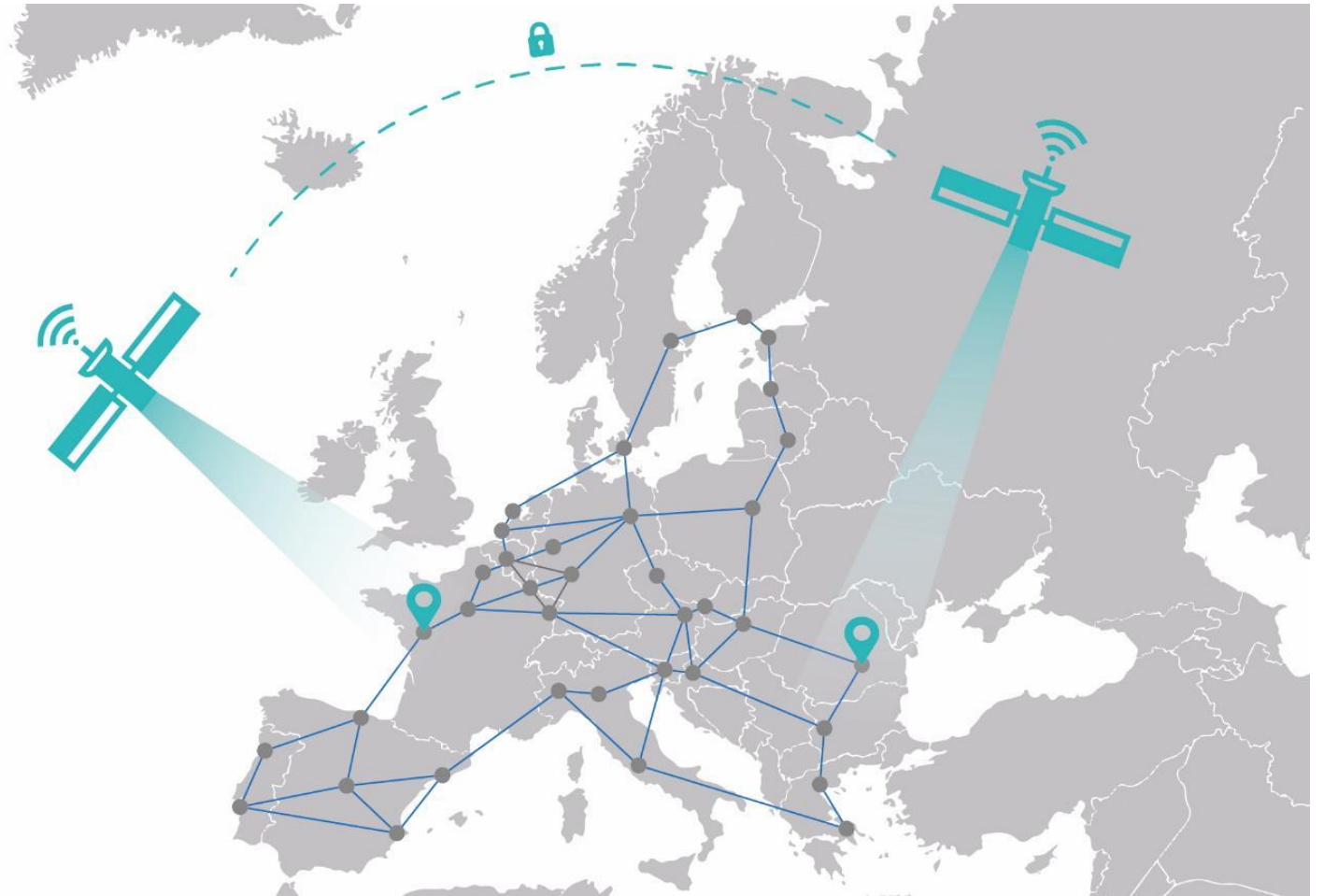
In großen Netzwerken Möglichkeiten Schlüssel auf mehreren Pfaden zu verteilen

- Danach Kombination der Schlüssel mittels Secret Sharing
- Nur Start- und Endknoten kennen Schlüsselmaterial



Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

EuroQCI



EUROQCI – Quantum Communication Infrastructure Europe, 2019-2029 – Sicherheit+Infrastruktur+Industrie



Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

QCI-CAT

QCI: Proof of Concept – Secure Connectivity Austria

Aufbau QKD Netzwerk in Österreich

- Datenaustausch zwischen Ministerien in Wien
- Austausch medizinischer Daten zwischen Wien und Graz
- Entwicklung von Trusted Nodes "made in Austria"



Kombination von QKD und PQC

Benutzer-orientierte Trainingsprogramme

Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

CEF CALL

Connecting Europe Facility

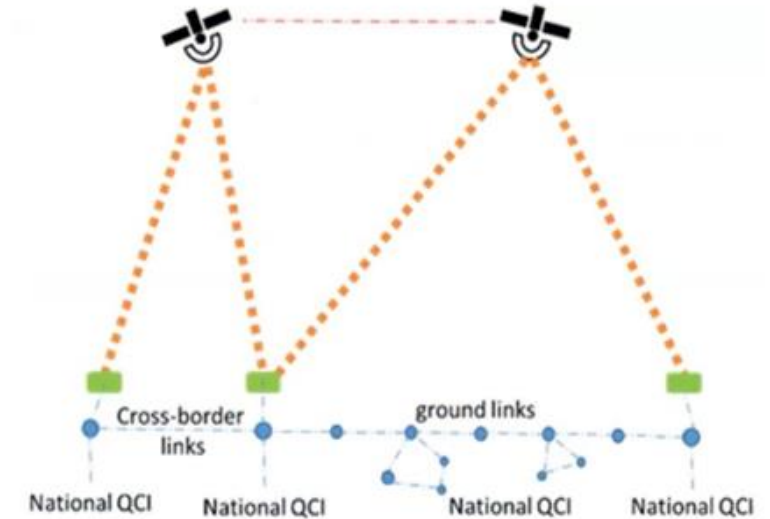
Call ist seit 22.10.2024 geöffnet

Submission Deadline ist 13.02.2025

[Link der Ausschreibung](#)

Die Ausschreibung zielt darauf ab:

- Ermöglichung einer zuverlässigen und stabilen Übertragung sensibler Kommunikation und Daten zwischen Behörden, Forschungseinrichtungen und kritischen Infrastrukturen in den Mitgliedstaaten
- Stärkung der europäischen Fähigkeiten zur Entwicklung quantengestützter sicherer optischer Kommunikationsnetze und der Fähigkeit, kritische öffentliche Infrastrukturen zu schützen, indem ihre Kommunikation und Daten gesichert werden, insbesondere solche, die grenzüberschreitend sind und mehr als einen Mitgliedstaat bedienen
- Förderung quantengestützter sicherer Netze und Aufbaus eines Ökosystems, das eine breite Marktakzeptanz ermöglicht



Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen

Einladung zur Live Demo

Demonetzwerk bei KIRAS Fachtagung:

- 2 QKD Links mit ThinkQuantum QKD Devices
- Key Management System von AIT
- QKD4Gov Chat Demo mit QKD und PQC von X-Net



Besuchen Sie uns
beim dem AIT-
Stand!



Gefördert/finanziert durch die Sicherheitsforschungs-Förderprogramme KIRAS und KYBERNET PASS des Bundesministeriums für Finanzen