MUCKLE+: END-TO-END HYBRID AUTHENTICATED KEY EXCHANGES

Christoph Striecks

AIT Austrian Institute of Technology

Joint work with Sonja Bruckner* (FHOÖ) and Sebastian Ramacher (AIT)

17/08/2023

*work done while at AIT

AUSTRIAN INSTITUTE OF TECHNOLOGY

NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

PROJECTS

Post-Quantum Cryptography PQC

Overview

The Candidates to
Third Round of the

Federal Office for Information Security

CONTACT DEUTSCH PLAIN ENGLISH TERMS AND CONDITIONS

Deutschland
Digital·Sicher·BSI·

ANSSI Agence nat systèmes d

MISSIONS

SCIENTIFIC STANDING > TECHNICAL POSITION

Call fo

ANSSI VIE

PDF

January 4, 2022

In this position pap
quantum threat and
without introducing
products and outlini

European Commission

EN English

Search

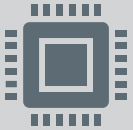
The European Quantum Communication Infrastructure (EuroQCI) Initiative

The EuroQCI will be a secure quantum communication infrastructure spanning the whole EU, including its overseas territories.

The European Commission is working with all 27 EU Member States, and the European Space Agency (ESA), to design, develop and deploy the EuroQCI, which will be composed of a terrestrial segment relying on fibre communications networks linking strategic sites at national and cross-border level, and a space segment based on satellites. It will be an integral part of IRIS², the new EU space-based secure communication system.

CENTRAL TOPICS TO BE COVERED

Distributing trust in quantum-safe networks (“Do not pull all your eggs in one basket”)



Hybridization approach (combining PQC/QKD)

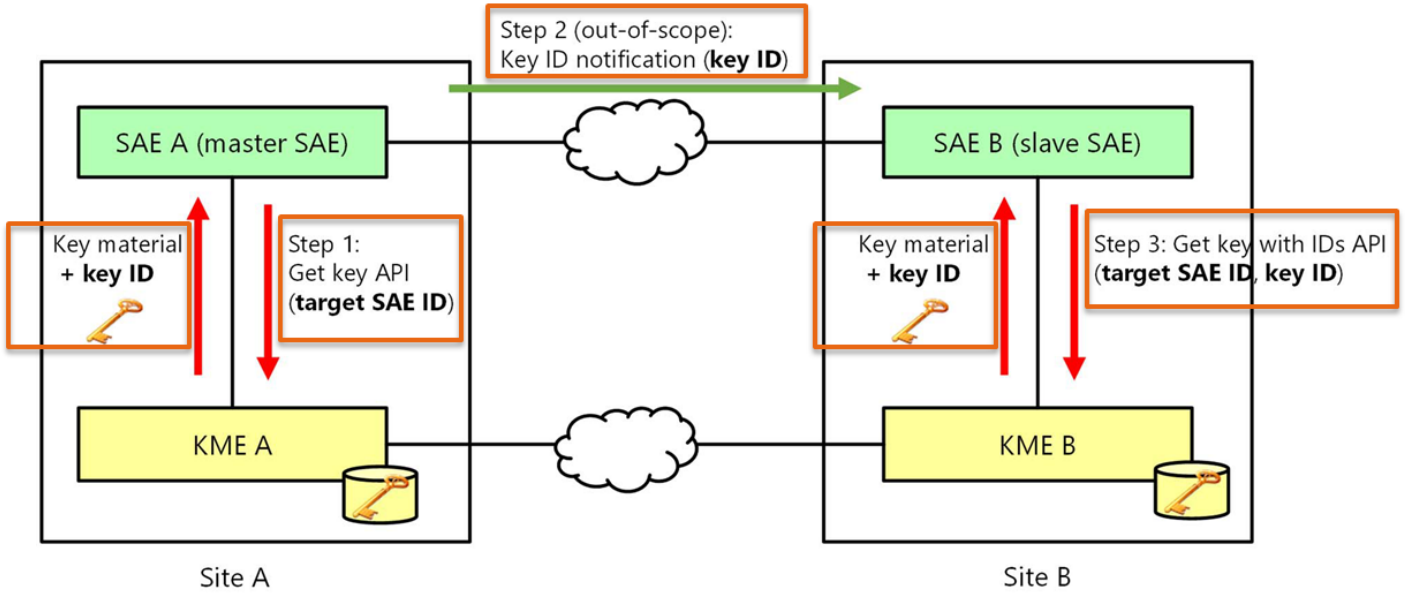
AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

QUANTUM KEY DISTRIBUTION

Establishing Shared Keys with Perfect Secrecy (ideally)

QUANTUM KEY DISTRIBUTION (QKD)

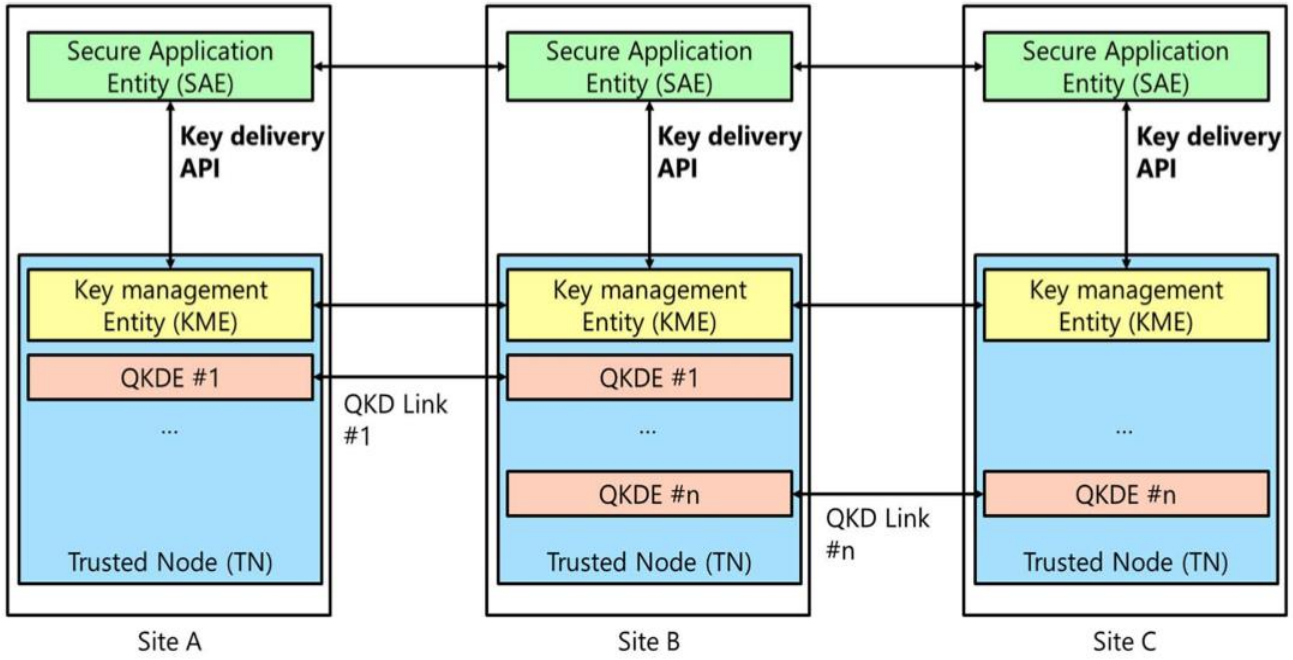
- Main features:
  - **Perfectly** secret key distribution
  - Between any **two end-points**
  - **Terrestrially** or via **space**



Key Establishment Scheme. Source: ETSI QKD GS 014 v1.1.1

QKD NETWORKS

- Gaps to solve:
  - QKD links have a **limited range** (depending on technology and desired key bit-rates)
- Needs:
  - **Trusted nodes** to bridge longer distances
  - **Pre-shared keys** to authen-ticate link-to-link nodes

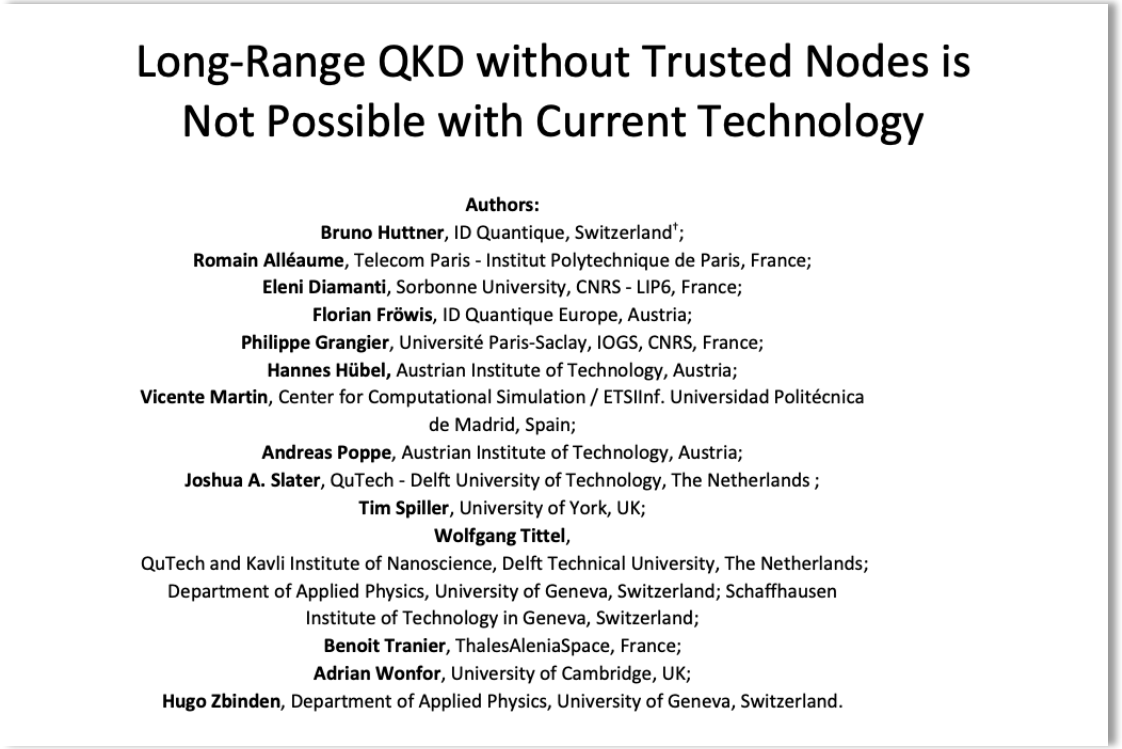


QKD Network connecting different sites. Source: ETSI GS QKD 014 V1.1.1

LIMITATIONS FOR LONG-RANGE QKD NETWORKS

1. "QKD is [...] a solution for transforming a non-confidential **authenticated** channel into a confidential **authenticated** one." (Huttner et al.)

2. **Trusted nodes** are needed for long-range QKD



Long-Range QKD without Trusted Nodes is Not Possible with Current Technology

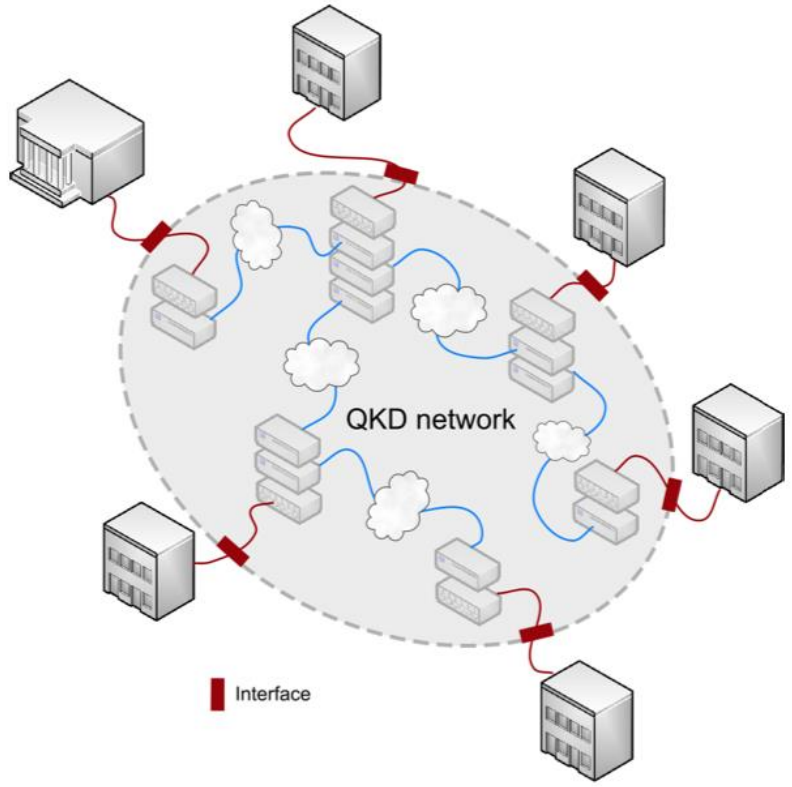
Authors:
Bruno Huttner, ID Quantique, Switzerland[†];
Romain Alléaume, Telecom Paris - Institut Polytechnique de Paris, France;
Eleni Diamanti, Sorbonne University, CNRS - LIP6, France;
Florian Fröwis, ID Quantique Europe, Austria;
Philippe Grangier, Université Paris-Saclay, IOGS, CNRS, France;
Hannes Hübel, Austrian Institute of Technology, Austria;
Vicente Martin, Center for Computational Simulation / ETSIInf. Universidad Politécnica de Madrid, Spain;
Andreas Poppe, Austrian Institute of Technology, Austria;
Joshua A. Slater, QuTech - Delft University of Technology, The Netherlands ;
Tim Spiller, University of York, UK;
Wolfgang Tittel,
QuTech and Kavli Institute of Nanoscience, Delft Technical University, The Netherlands;
Department of Applied Physics, University of Geneva, Switzerland; Schaffhausen Institute of Technology in Geneva, Switzerland;
Benoit Tranier, ThalesAleniaSpace, France;
Adrian Wonfor, University of Cambridge, UK;
Hugo Zbinden, Department of Applied Physics, University of Geneva, Switzerland.

Source: https://arxiv.org/pdf/2210.01636.pdf

LIMIT 1: END-TO-END AUTHENTICITY

- Problem:
  - Authentication via pre-shared keys (PSKs) is **only link-to-link**, but **not end-to-end**
  - Reason: authentication is **not transitive**

- One solution:
  - **Unique PSKs** for each entity (results in O(N^2) PSKs for N entities)
  - Requires **offline key exchanges** (e.g., via a “trusted courier”)
  - **Manageable** on a QKD device basis (but **inefficient** when the network gets larger)

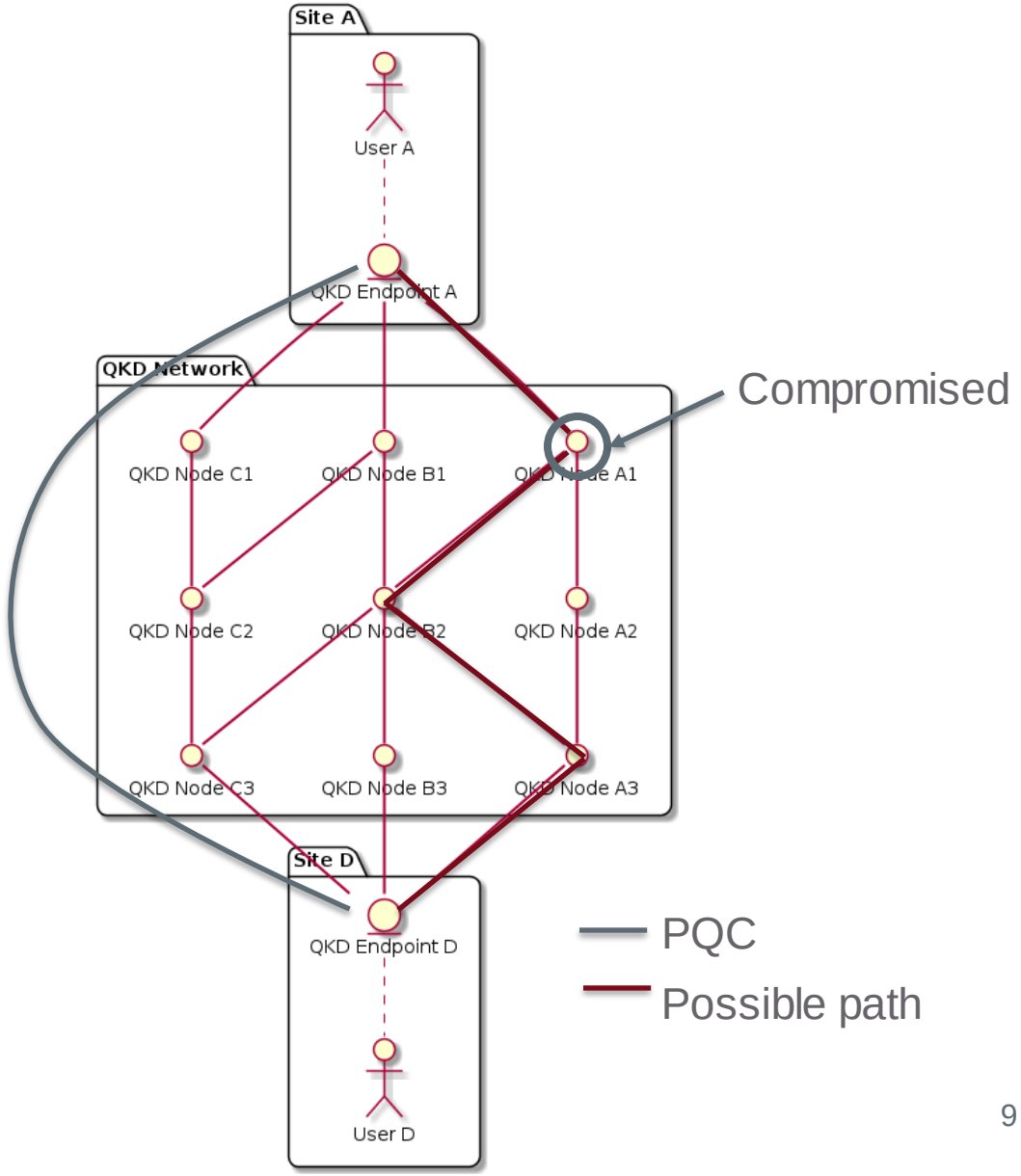


QKD network. Source: ETSI GS QKD 002 V1.1.1

LIMIT 2: TRUSTED NODES

- Problem:
  - Nodes on the QKD path **learn secret keys** (need to be trusted)
  - What happens if one node is **compromised**?

- One solution:
  - **Hybridization**, i.e., combine with post-quantum secure (PQC) mechanisms
  - Establishes **end-to-end security** (albeit under computational assumptions)



AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

HYBRID AUTHENTICATED KEY EXCHANGES

Authenticated Key Exchanges with End-to-End Confidentiality

PRIMITIVE: HYBRID AUTHENTICATED KEY EXCHANGE (HAKE)

- Main features:
  - (Session-based) protocol between **two entities**
  - Establishes **authenticated shared key**

- Goals:
  - **Authenticity** of both entities
  - **Confidentiality** of exchanged messages
  - Desired features: **forward** and **post-compromise** security

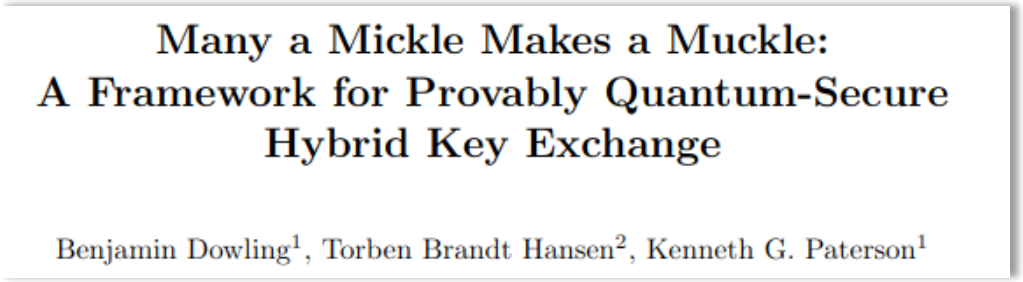
- Authentication via:
  - PSKs, certificates, or passwords

- (Ephemeral) keys via:
  - Key encapsulation mechanisms and QKD keys

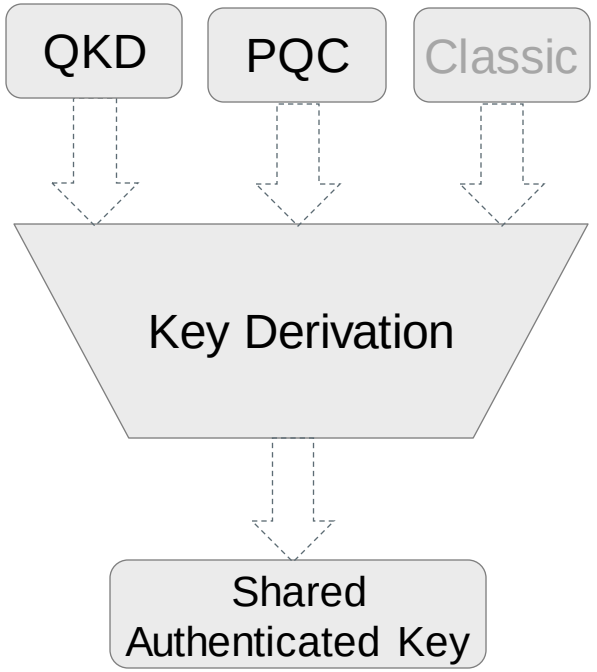
HAKE INSTANTIATION: MUCKLE

- Combining:
  - Keys from **QKD** layer
  - **PQC** key encapsulation mechanism
  - *Optional*: keys from **classical** cryptography
  - **PSK** for authentication

- Benefits:
  - **End-to-end authentication** and **confidentiality** (relying on PSKs)
  - **Forward/PC security** (e.g., if PQC fails, guarantees for QKD still hold for older/newer sessions)
  - **"Backwards-compatibility"** (i.e., add a PQC/QKD layer to existing classical one)


Many a Mickle Makes a Muckle:
A Framework for Provably Quantum-Secure
Hybrid Key Exchange

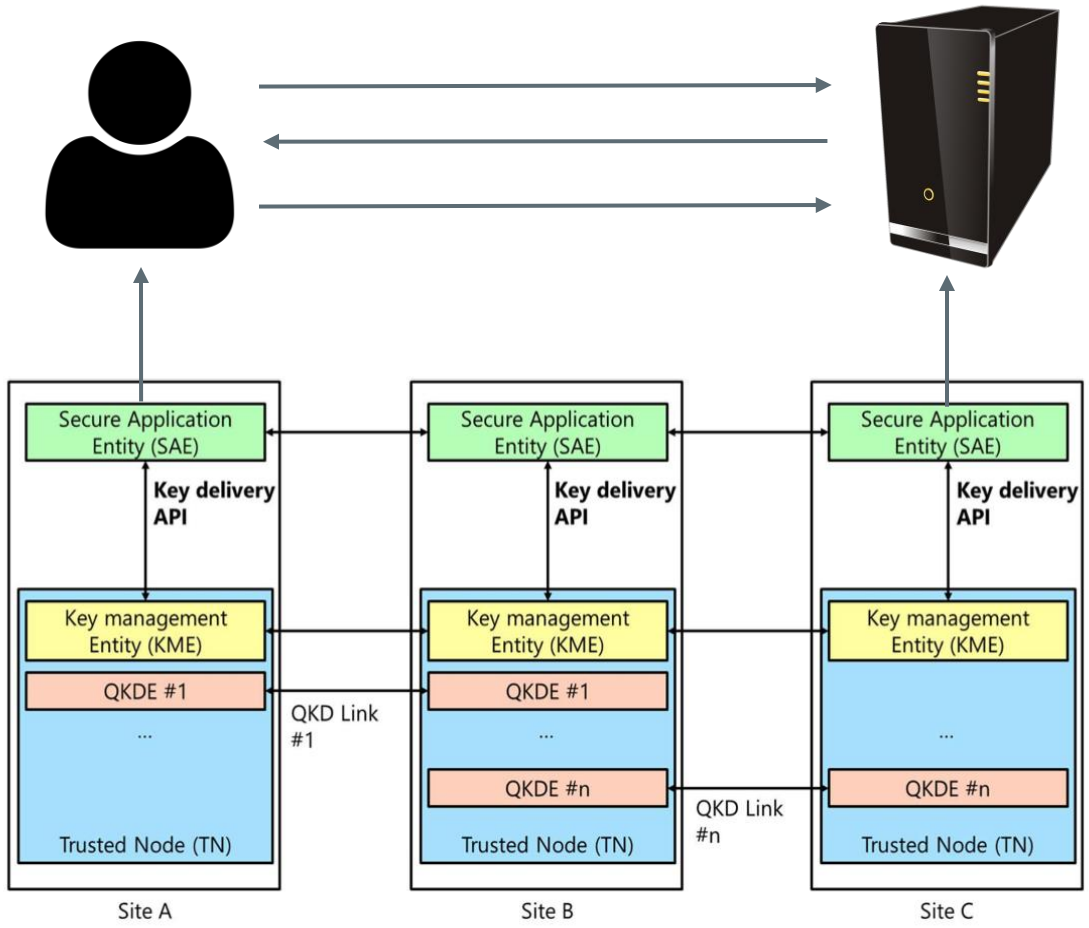
Benjamin Dowling[1], Torben Brandt Hansen[2], Kenneth G. Paterson[1]



OUR PROPOSAL: MUCKLE+

- Result:
  - "**Muckle with PQC signatures for end-to-end authentication**" via a PKI instead of PSKs at end-user site (surprisingly non-trivial)

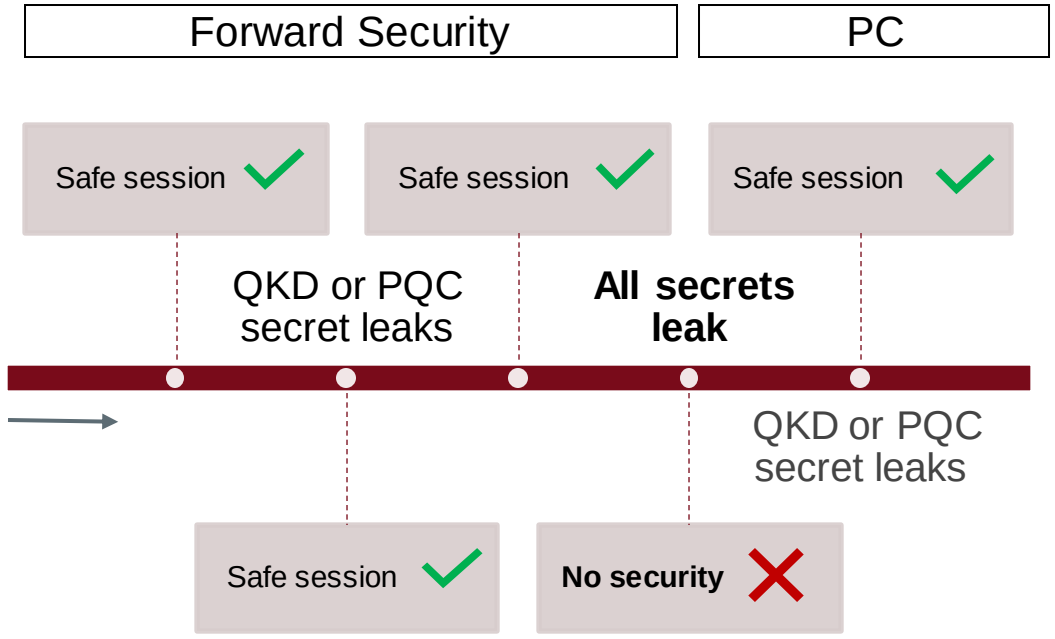
- **Distinguishing feature:**
  - We opted for **SIGMA**-style protocol
  - To establish end-to-end authentication with signatures, PQC KEMs are **required** due to the (single-path) QKD trusted-node issue
  - Fallback: if we want to allow the PQC KEM to fail, **multi-path QKD** is needed



QKD Network connecting different sites. Source: ETSI GS QKD 014 V1.1.1

QUANTUM-SAFE SECURITY OF MUCKLE/+

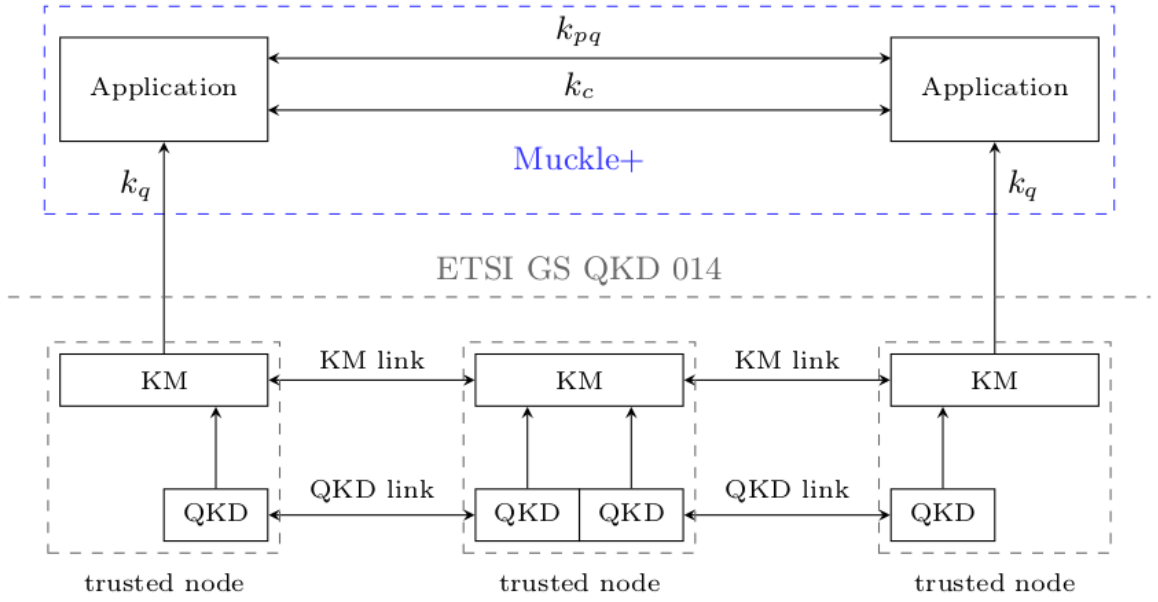
- **Forward security** is an **important security feature** which is well-researched for key exchange and has gained massive interest in other domains (e.g., FS-PKE, FS 0-RTT KE, ...)
- **Post-compromise (PC) security** allows channels to "heal"
- Implies important **threat mitigation**: **"store-now decrypt-later"** attacks are mitigated via forward security



IMPLEMENTATION RESULTS

- **Real** QKD systems:
  - **1-2 kbit/s key rate**
  - up to **1 second delay** to fetch 256-bit keys from QKD devices

- Choice of PQC (signatures) schemes does **not impact performance**
  - Delay from QKD systems dominate over overhead from signature and public key sizes



TAKEAWAYS

- Massive interest in **PQC** (NIST, BSI, ANSSI, ...) and **QKD** (EuroQCI, IRIS2, ...) with huge number of currently ongoing projects

- Building large-scale quantum-safe networks with **end-to-end authenticity**, **integrity**, and **confidentiality** is non-trivial

- **Hybrid AKEs** hedge against various forms of future threats with **strong forward and post-compromise security** for the to-be-anticipated quantum-safe networks

- **ePrint version:** https://eprint.iacr.org/2023/653

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Supported by DIGITAL Europe Program project QCI-CAT (101091642), Austrian Research Promotion Agency project QKD4GOV (FO999886370), and European Defence Industrial Development Programme DISCRETION (SI2858093).

Christoph.Striecks@ait.ac.at