Quantum-Secure Hybrid Key Exchanges

"Do not put all your eggs in one basket"

Christoph Striecks and Ludovic Perret

AIT Austrian Institute of Technology and Sorbonne University

Webinar, 2nd October 2024

This project has received funding from the European Union's Horizon Europe research and innovation programme under the project "Quantum Security Networks Partnership" (QSNP, grant agreement No 101114043).

REGULATION (EU) 2023/588 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 15 March 2023

establishing the Union Secure Connectivity Programme for the period 2023-2027

(16) In order to protect EUCI in a satisfactory secured manner, primary solutions to counter threats posed by quantum computing should be the combination of conventional solutions, post-quantum cryptography and possibly QKD in hybrid approaches. The Programme should therefore use such approaches, for the purpose of ensuring both state-of the-art cryptography and key distribution.

https://e

Official Journal
of the European Union

EN
L series

2024/1101

12.4.2024

COMMISSION RECOMMENDATION (EU) 2024/1101

of 11 April 2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

.4.2024

across the Union of Post-Quantum Cryptography technologies into existing public administration systems and critical infrastructures via hybrid schemes that may combine Post-Quantum Cryptography with existing cryptographic approaches or with Quantum Key Distribution.

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401101

*Assuming that conventional/existing approaches mean: classical asymmetric and symmetric cryptography, but also pre-shared keys (PSKs)

Central Topics

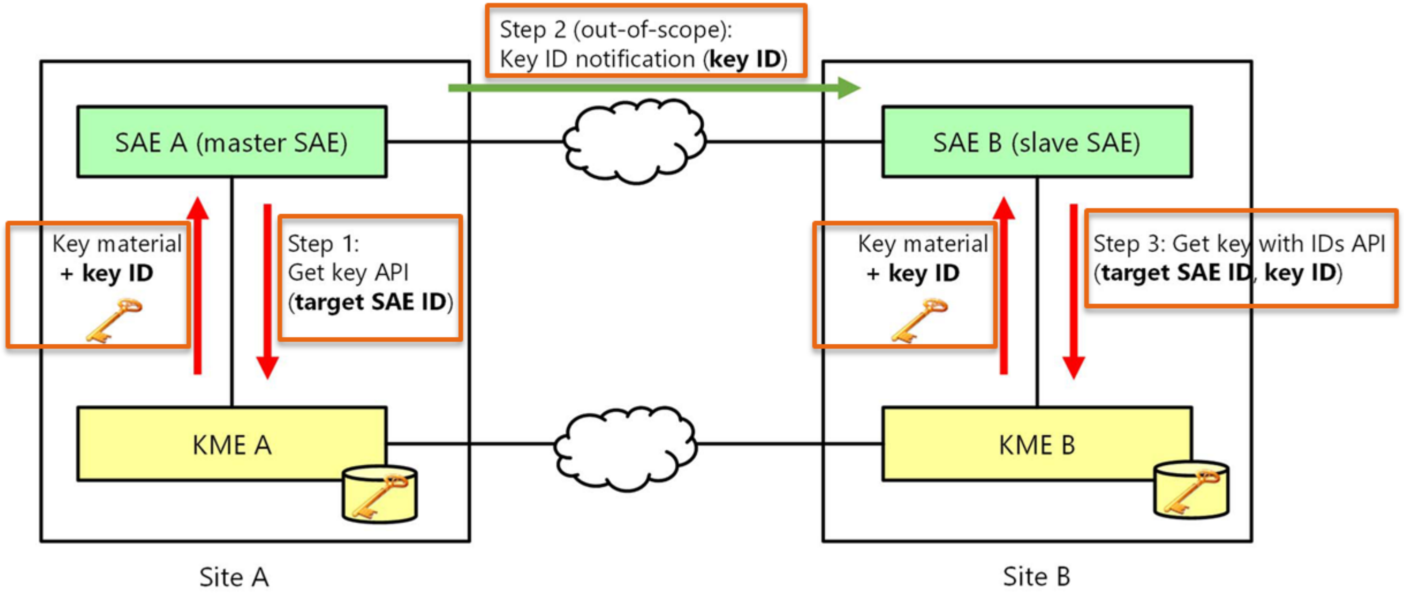
Hybrid PQC/QKD/Conventional cryptographic framework ("Muckle approach")

International point of view, standardization efforts, recommendations for EuroQCI and beyond

Quantum Key Distribution (QKD)

Main features:

- **Information-theoretically secure (ITS)** key expansion
- Between **two end-points**
- **Terrestrially** or via **space**



Key establishment scheme. Source: ETSI QKD GS 014 v1.1.1

From Small to Large QKD Networks

1. "QKD is [...] a solution for transforming a non-confidential **authenticated** channel into a confidential **authenticated** one."

2. **Trusted nodes** are currently required 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.

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

Hurdle 1: Entity Authentication

- "Authentication provides **guarantees** on the **identities** of the parties involved in the protocol execution." [GFW19]
- Problem: QKD does not solve **source authenticity**
- Solutions:
  - **Pre-placed keys:** need trusted couriers or key-distribution centers, ITS
  - **Asymmetric Cryptography:** using PQC via public key infrastructures (PKIs) in *hybrid* approaches, non-ITS

Technical limitations

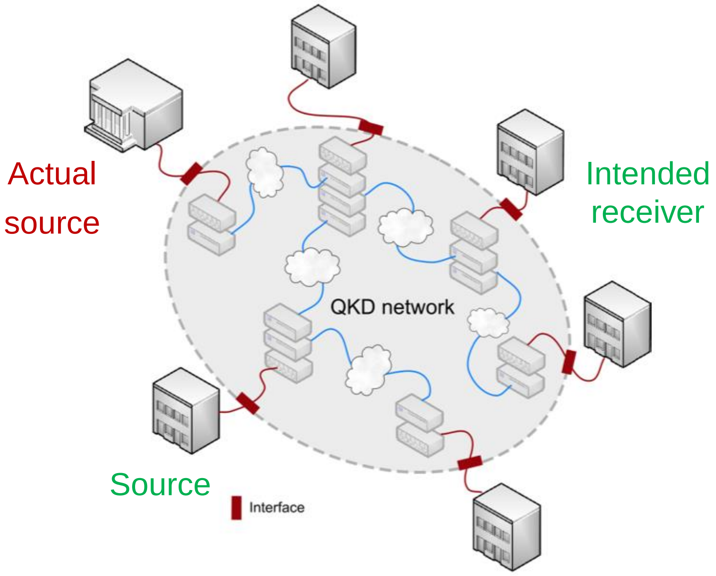
1. **Quantum key distribution is only a partial solution.** QKD generates keying material

Reliance on classical cryptography for peer authentication

As explained before, QKD requires a classical authenticated channel between the communicating parties. There are several options for how to implement an authentication mechanism. One option is the use of pre-shared keys with *symmetric* message authentication. To this end, a secret shared key must already be present at both ends wishing to communicate with each other before running a QKD protocol. Consequently, secret keys must be distributed and then periodically renewed in a secure manner before being able to perform QKD. Another option is to use post-quantum *signature schemes* with an associated *public-key infrastructure*. However, in this case, the authentication relies on the security of the post-quantum scheme.

Authentication must go together with confidentiality.*

*PETRUS had a recent webinar series on network authentication methods



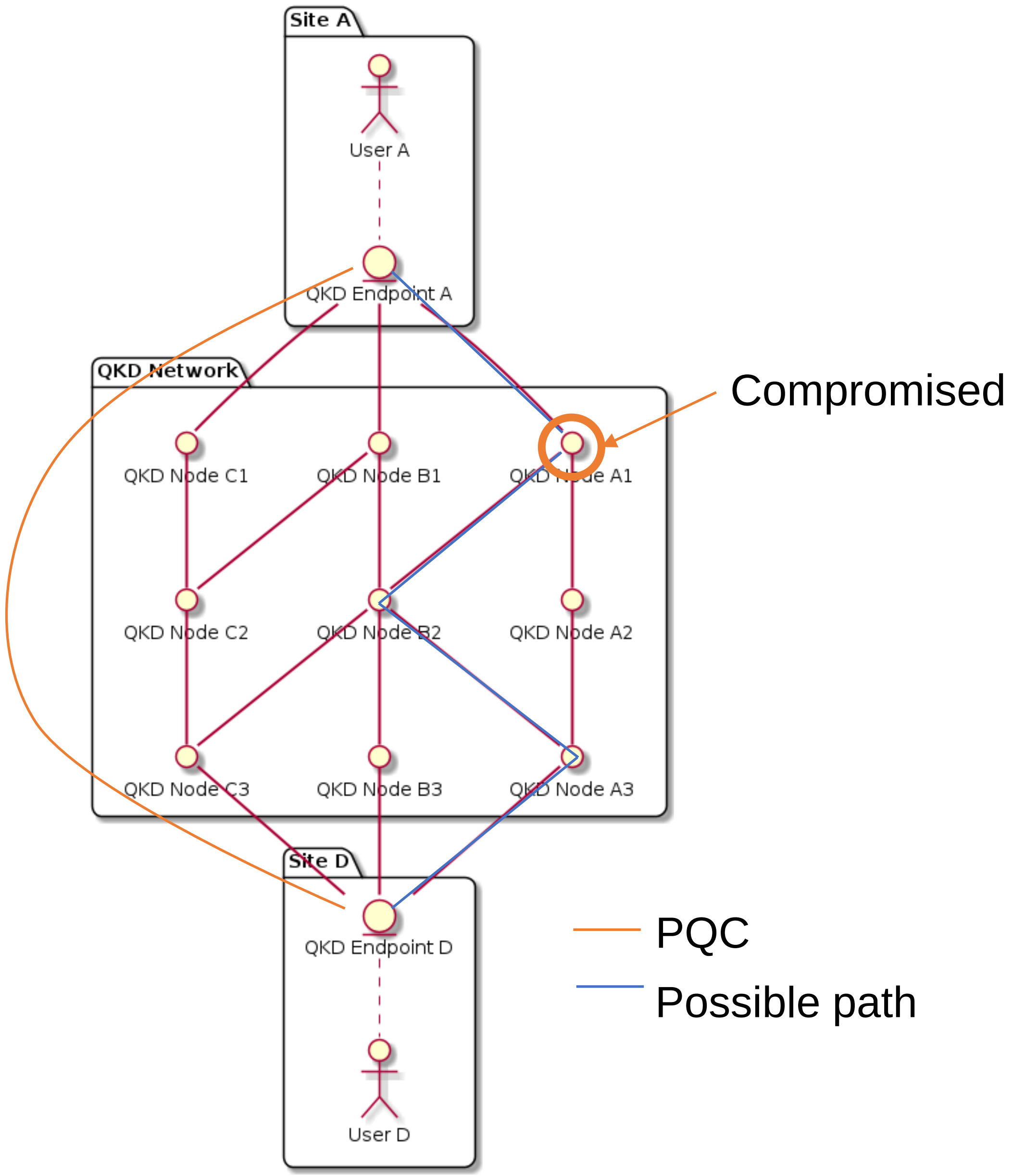
QKD network. Source: ETSI GS QKD 002 V1.1.1

Hurdle 2: Trusted Nodes

- Problem:
  - Nodes on the QKD path **learn secret key** given also **access to public traffic**
  - End nodes **might not fully trust** intermediate nodes not in their trust domain

- One mitigation:
  - **Hybridization**, i.e., combine with PQC confidentiality mechanisms (via suitable protocols)

Hybrid (or, defense-in-depth) approaches mitigate both hurdles



Ad-Hoc Approaches

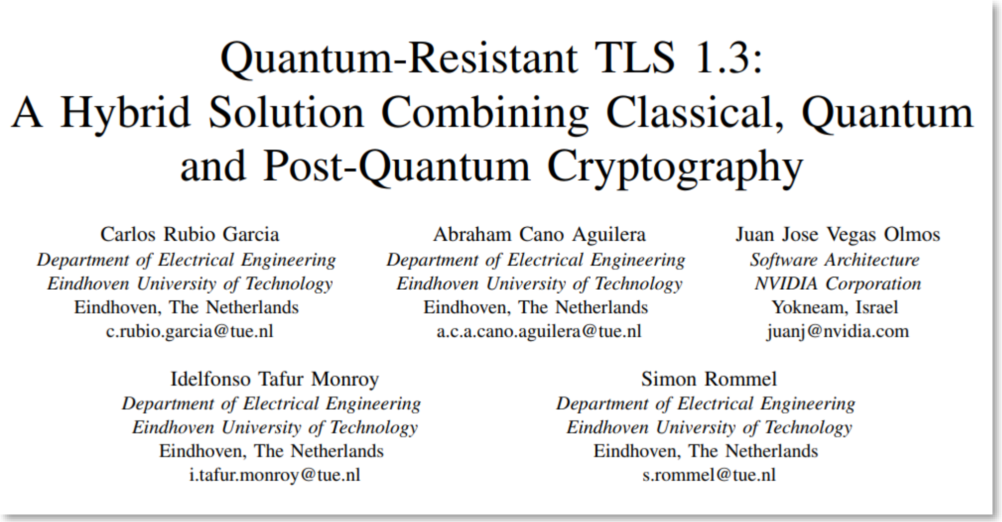
- **Some works** available to hybridize QKD & PQC
- Brauer et al.:
  - PQC+QKD in some variants via key derivation functions (KDFs)
- Garcia et al.:
  - PQC+QKD+Coventional in Transport Layer Security (TLS) 1.3, integrated in key schedule
- Some more related works available
- However: mostly **ad-hoc constructions**, i.e., **without a proof of security** (assessing formal security of hybridization hard to verify)

- Additionally: **KDFs must be carefully designed** (e.g., depending on the use cases):
  - Simple XOR *might not* guarantee active security [GKP18]
- For **KEM combiners**: start at BSI recommendations [BSI], ETSI TR 103 744 [ETS]

Article

Linking QKD testbeds across Europe

Max Brauer[1], Rafael J. Vicente[2], Jaime S. Buruaga[2], Rubén B. Méndez[2], Ralf-Peter Braun[1], Marc Geitz[1], Piotr Rydlichkowsk[3], Hans H. Brunner[4], Fred Fung[4], Momtchil Peev[4], Antonio Pastor[5], Diego Lopez[5], Vicente Martin[2], and Juan P. Brito[2]



Quantum-Resistant TLS 1.3:
A Hybrid Solution Combining Classical, Quantum and Post-Quantum Cryptography

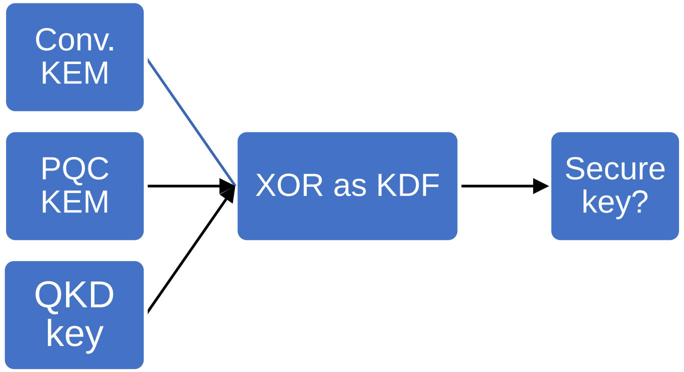
Carlos Rubio Garcia
Department of Electrical Engineering
Eindhoven University of Technology
Eindhoven, The Netherlands
c.rubio.garcia@tue.nl

Abraham Cano Aguilera
Department of Electrical Engineering
Eindhoven University of Technology
Eindhoven, The Netherlands
a.c.a.cano.aguilera@tue.nl

Juan Jose Vegas Olmos
Software Architecture
NVIDIA Corporation
Yokneam, Israel
juanj@nvidia.com

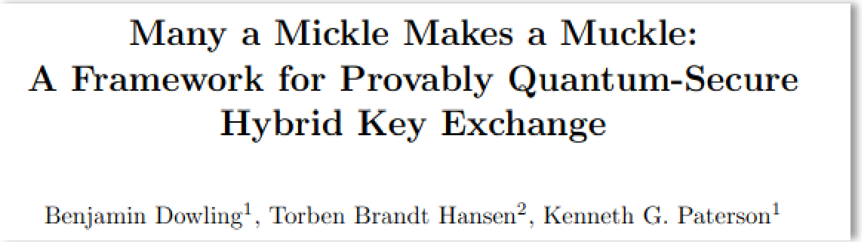
Idelfonso Tafur Monroy
Department of Electrical Engineering
Eindhoven University of Technology
Eindhoven, The Netherlands
i.tafur.monroy@tue.nl

Simon Rommel
Department of Electrical Engineering
Eindhoven University of Technology
Eindhoven, The Netherlands
s.rommel@tue.nl



[BSI] https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_stephan-ehlen_bsi_post-quantum-policy-and-roadmap-of-the-bsi.pdf, slide 13
[ETS] https://www.etsi.org/deliver/etsi_tr/103500_103599/103570/01.01.01_60/tr_103570v010101p.pdf
[GKP18] https://eprint.iacr.org/2018/024.pdf

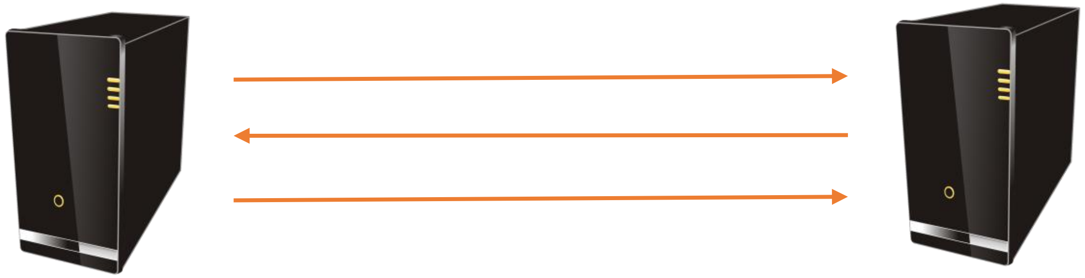
Hybrid Key Exchange


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]

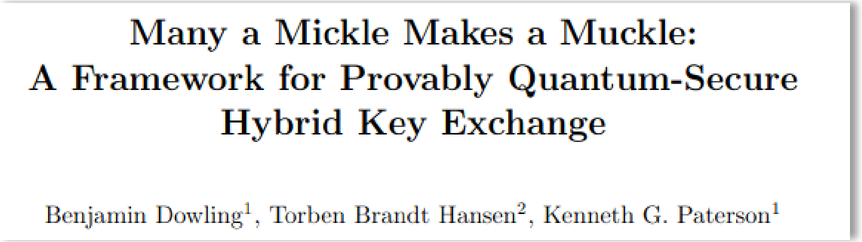
- Main features:
  - Security by design (with **security proof**)
  - Overall goal: derive an **authenticated shared key** from **several cryptographic primitives** such as PQC, QKD, and conventional crypto ("from primitives to protocols")

- Security goals:
  - **Authenticity/integrity** for both entities
  - **Confidentiality** of exchanged messages
  - **Forward** and **post-compromise** security (de-facto standard in, e.g., TLS 1.3 today)
  - Rigorous **proof of security**



- Efficiency goals:
  - **Authentication** via PSKs and/or certificates (may be even passwords)
  - **Modularity**: allows any combination of primitives (if at least one component is secure)
    - Interesting choices: PQC authentication with QKD confidentiality or PQC/conv. for mobile use-cases
  - **Crypto agility**, i.e., being agnostic to instantiations of underlying primitives

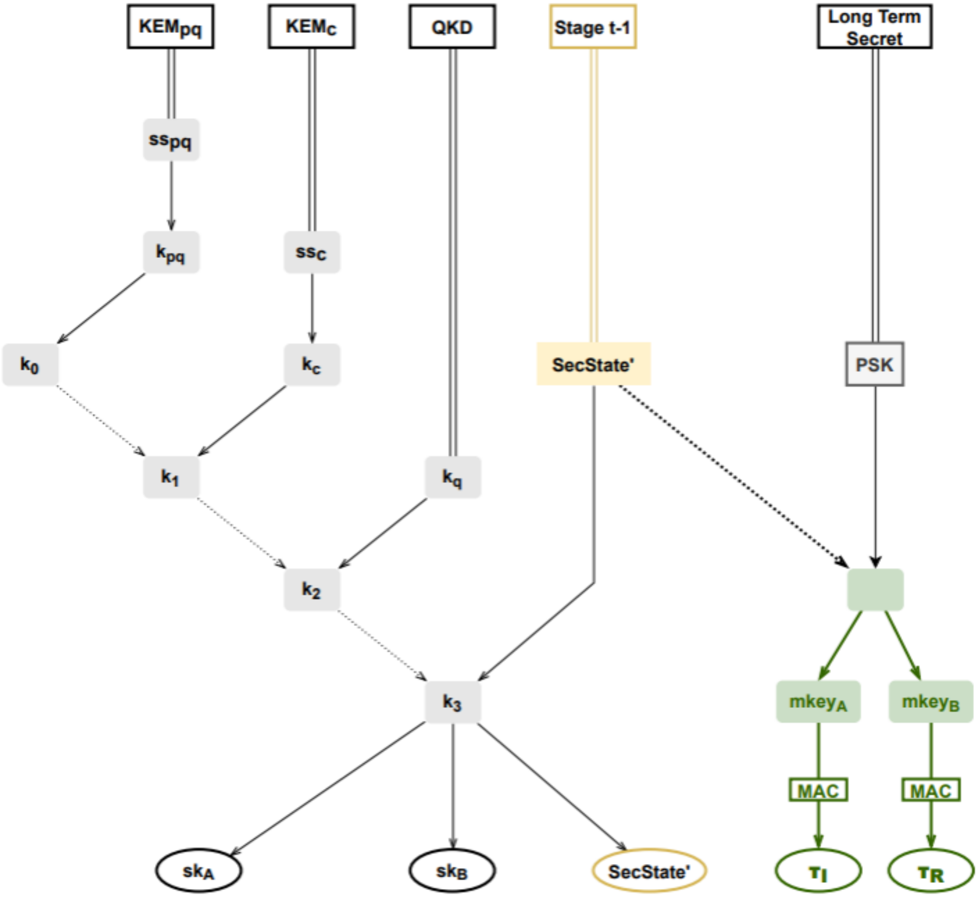
Instantiation: Muckle


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]

- Modularly combining:
  - Keys from **QKD** layer, **PQC** key encapsulation mechanism (KEM), and *optionally* from **conventional** KEM
  - **PSK** for authentication

- Special benefits:
  - **Proof of security** for **confidentiality, authentication, integrity, FS/PCS** with potentially failing components
  - Meets **EC** and **BSI* recommendations**



But: Muckle uses PSKs for authentication which is inefficient for large networks

*https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf, Sec. 6.11

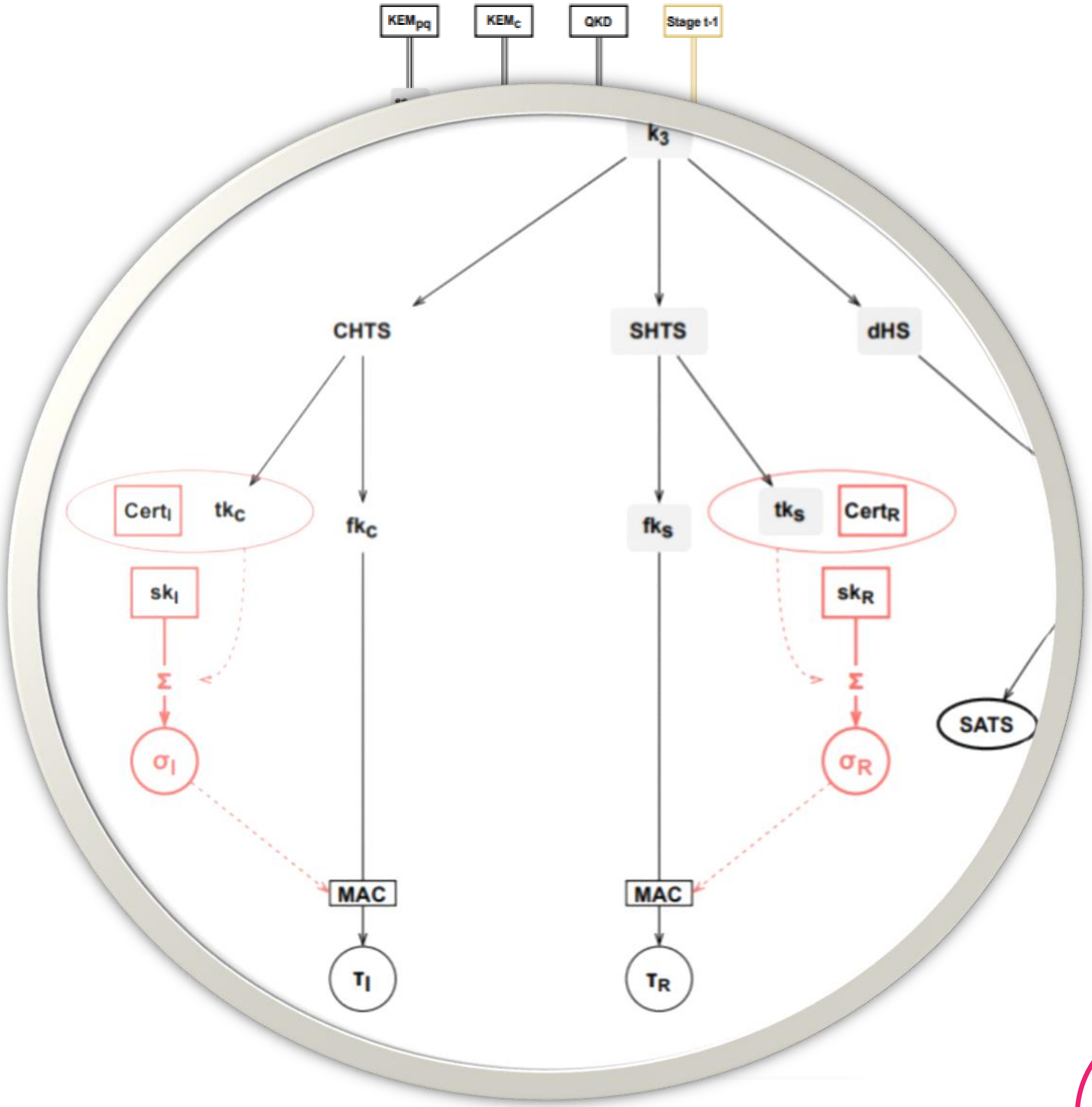
For Networks: Muckle+


Muckle+: End-to-End Hybrid Authenticated Key Exchanges*

Sonja Bruckner[1]**, Sebastian Ramacher[2], and Christoph Striecks[2]

- Special features:
  - Motivation: "**Muckle without PSKs but with PQC certificates for authentication**“
  - Allows **efficient end-to-end authentication** in large-scale quantum-safe networks

- Benefits:
  - **Proof of security** for **confidentiality, authentication, integrity, FS/PCS** with potentially failing components
  - Meets **EC** and **BSI recommendations** as Muckle
  - **First proof of concept** in a real QKD network



More Efficient: Muckle#

- AIT and Sorbonne **joint work***, in preparation
- Special features:
  - "**Practical optimization of Muckle+**": swaps the use of **PQ signatures** with **PQ KEMs** for **authentication**
  - Inspired by **recent work** improving the TLS 1.3 protocol ("KEMTLS")

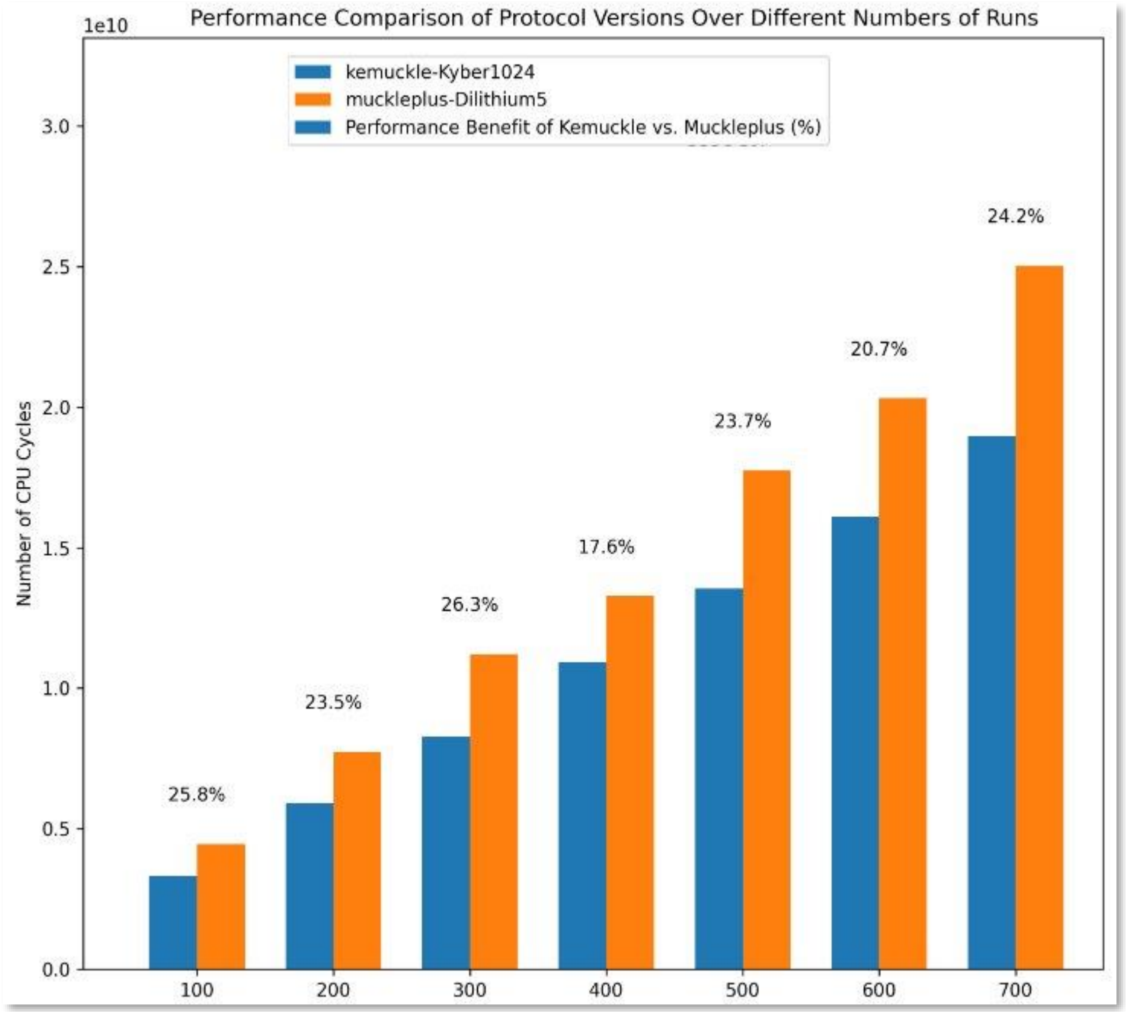
$(c_I, ss_I) \leftarrow \mathsf{KEM}_s.\mathsf{Enc}(\mathsf{pk}_R)$

$\xrightarrow{m_4 : \{c_I\}_{\mathsf{IHTS}}}$

$ss_I \leftarrow \mathsf{KEM}_s.\mathsf{Dec}(\mathsf{sk}_R, c_I)$

$\mathsf{AHS} \leftarrow \mathcal{F}(\mathsf{dHS}, \ell_9 \| ss_I)$

- Benefits:
  - **Faster protocol** runs due to efficiency deficiencies in PQ signatures currently available (e.g., via the NIST standards)
  - **Up to ~26% runtime benefit** on Python prototype compared to Muckle+



*additionally involved: C. Batarbee (Sorbonne), K. Verhaeghe (ETH, while at AIT), S. Ramacher (AIT)

Conclusion and Recommendations (of Part 1)

- **Hybrid Authenticated Key Exchange (HAKE)** protocols combine PQC, QKD, and conventional cryptographic primitives
- Technical recommendations:
  - Cryptographic hybrid protocols should have a **rigorous proof of security** (with state-of-the-art security guarantees such as forward & post-compromise security)
  - Hybrid protocols should be **crypto-agile** (agnostic to actual primitive implementation; secure combination of used primitives should be allowed)