ETSI/IQC Quantum Safe Cryptography Conference

Building a fully interoperable quantum-safe network testbed with versatile reference applications

Dr. Jing Yan (Joshua) Haw

15/05/2024

SINGAPORE'S QUANTUM-SAFE COMMUNICATIONS INITIATIVES

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

2006 — Free space QKD across 1.5 km with entangled photon pairs

2007 — NUS-SingTel Cyber Security R&D to support QKD trials

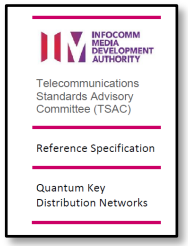
2016 — Quantum nanosatellite SpooQy-1 deployed from ISS

2017 — Entanglement over Metro-Fibre Network

2019 — Entanglement demo on nano-satellite

2020 — ITU QKD Protocol Standard

2022 — SG's 1st local RS on QKD Networks



2023 — NQSN+

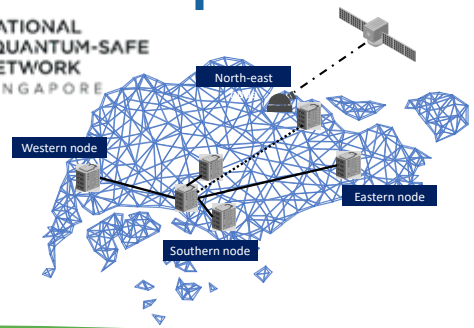
Centre for Quantum Technologies

SPEQTRAL

S FIFTEEN INSTRUMENTS

Entanglement-based QKD System

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE



Singapore launches Southeast Asia's first quantum-safe network infrastructure to help businesses tap on quantum-safe technologies

*Quantum Key Distribution (QKD)

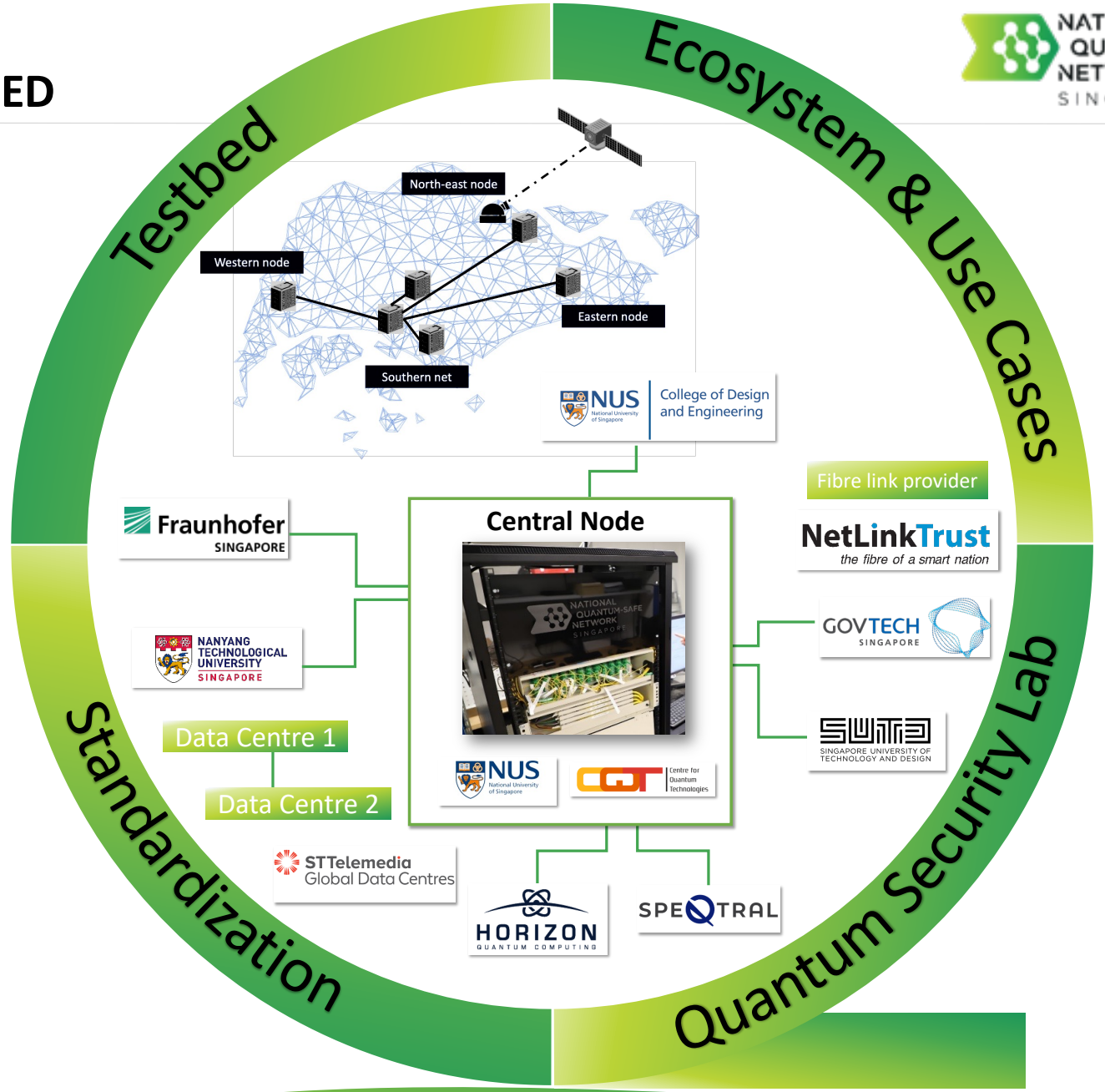
QUANTUM-SAFE NETWORK TESTBED

PILOT INFRASTRUCTURE

- Star-type Quantum Key Distribution (QKD) network topology
- Public-private collaborations with >20 companies & govt agencies
- **Vendor neutral** and **multiprotocol**
- Hybrid QKD/PQC (Post-quantum cryptography) approach

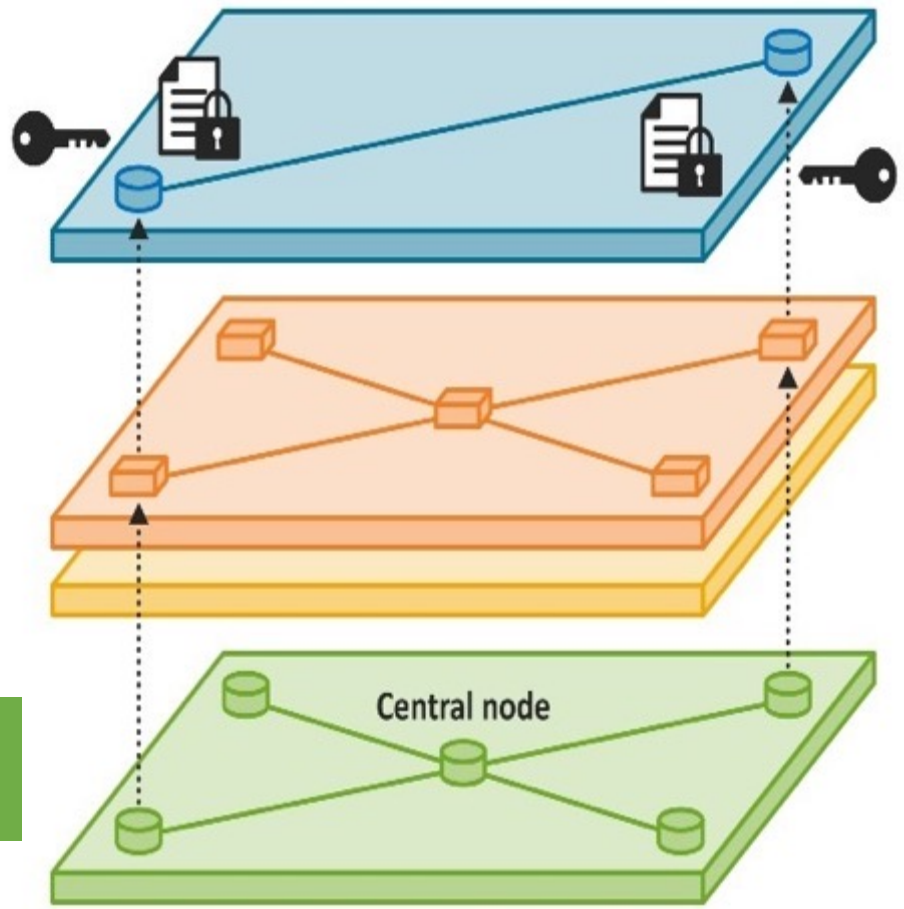
SECURITY FRAMEWORK & GUIDELINES

- In-depth **functional & security evaluation** of Quantum-safe technologies to seed certification
- Build readiness by developing **national reference specifications**



TESTBED – DIFFERENT LAYERS IN NQSN

- Encryptors & Quantum-Safe Applications
- Interoperability
- Scalability
- Multi QKD protocol
- Production-grade link



Application layer

Network management layer

Key management layer

Quantum layer

Open Systems Interconnection (OSI) Layers

Layer 5-7 Session Presentation Application

Layer 3 Network

Layer 2.5 MPLS

Layer 2 Data Link

Layer 1 Physical

TESTBED – QUANTUM LAYER

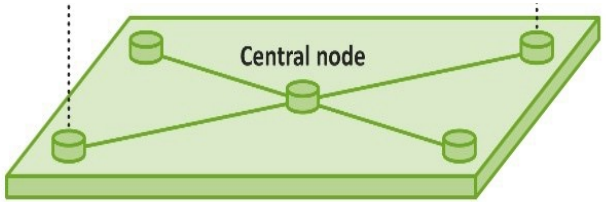
Prepare-&-Measure Discrete-Variable (DV) QKD

Prepare-&-Measure Continuous-Variable (CV) QKD

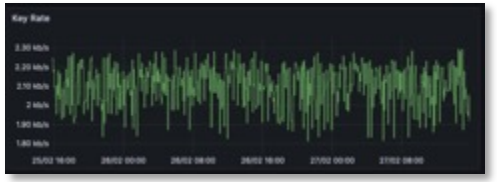
Entanglement-based (EB) QKD

*From respective public websites. Non-exhaustive list

- **Multi-protocol, vendor-neutral QKD network testbed**
- **Evaluation of DV & CV QKD protocols: BB84, COW, GMCS, BBM92 etc**



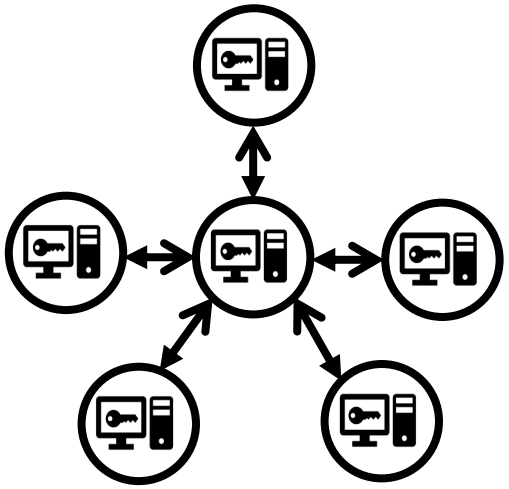
Quantum layer



TESTBED – KEY MANAGEMENT & NETWORK MANAGEMENT LAYER

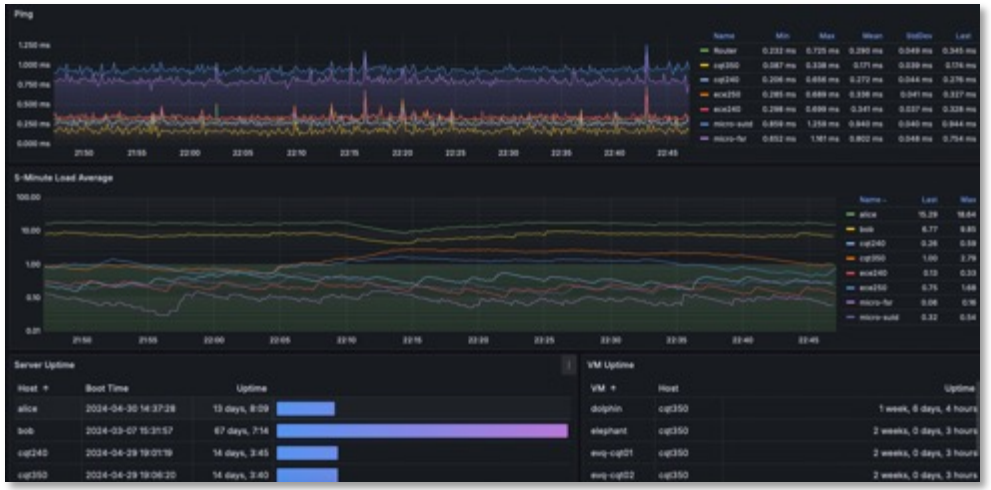
Key Management Layer

- ITU-T and ETSI compliance
- **Interoperable** with different QKD providers
- Multi-input &-output key interface with high **scalability**
- Enable & integrated with PQC technology



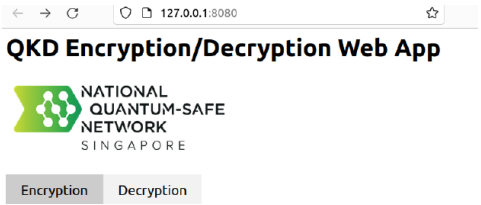
Network Management Layer

- A **centralized** network management on QKD Network (QKDN)
- Control Function:
  - Instructs the key delivery path across QKDN
  - Configure network components
- Management functions
  - **QKDN Telemetry**
  - **Fault detection & reporting**



TESTBED – APPLICATIONS LAYER

- ✓ NQSN **Quantum-safe software**
  - One-Time Pad (OTP) & PQC secured data transfer
- ✓ Quantum-secured **VPN**
  - Fortinet Firewall L3 Appliances
- ✓ Quantum-secured **video surveillance**
  - Hitachi Energy L2.5 Hardware Encryptor
- ❑ GovTech **data link** quantum Encryption
  - ST Engineering L2 encryptor
- ❑ Quantum-encrypted **5G infrastructure**
  - Thales SENETAS L2 encryptor on SUTD 5G Testbed
- ❑ **OTN Layer** quantum encryption
  - Ciena L1 hardware encryptor



NQSN OTP-PQC Software

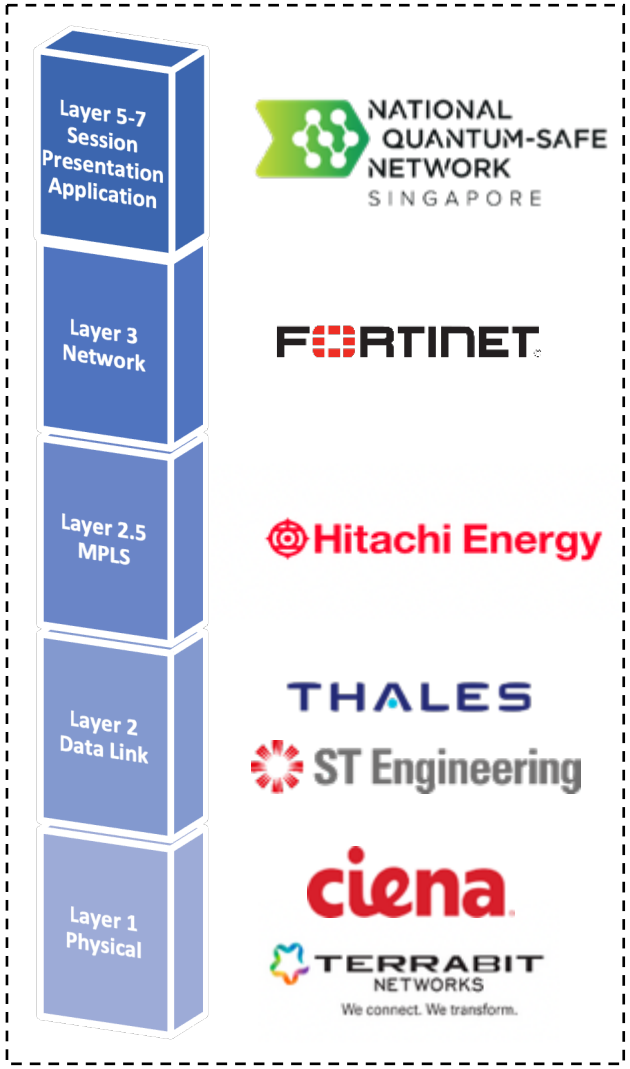
Fortinet FGT-100F

Hitachi FOX615 Encryptor

Thales SENETAS

Ciena Waveserver 5

OSI Layers



USE CASES – QKD LINK IN NQSN TESTBED

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

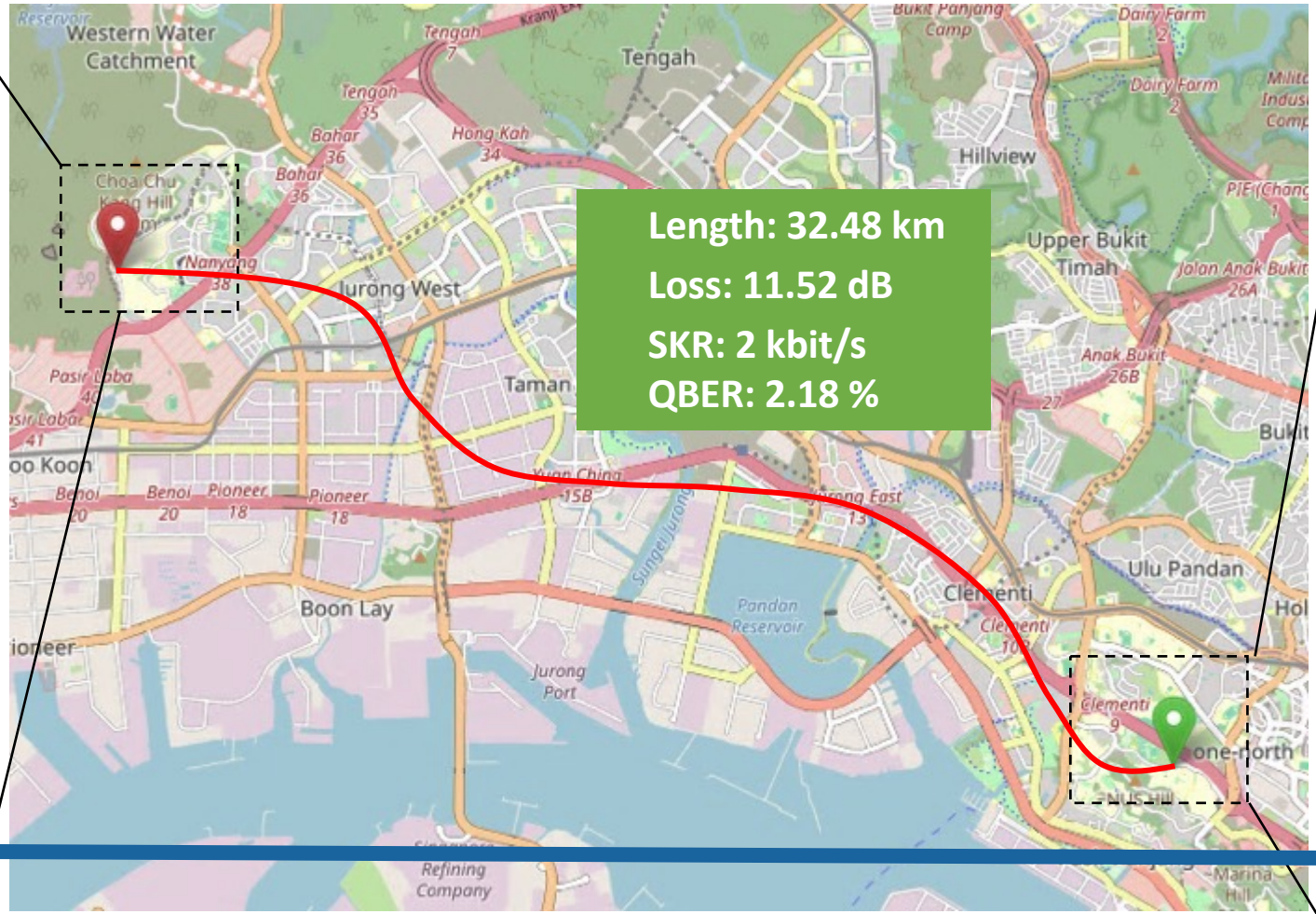
NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Fraunhofer SINGAPORE

QKD Key

Hitachi Energy

FORTINET



- QKD-secured Video app demo (Hitachi & Fortinet)
- Fully commercial-off-the-shelves equipment

NUS National University of Singapore

CQT Centre for Quantum Technologies

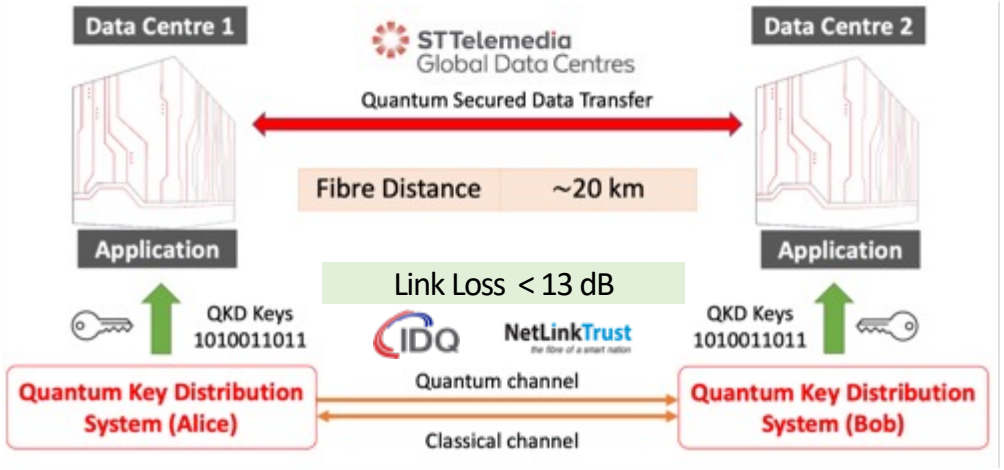
QKD Key

Hitachi Energy

FORTINET

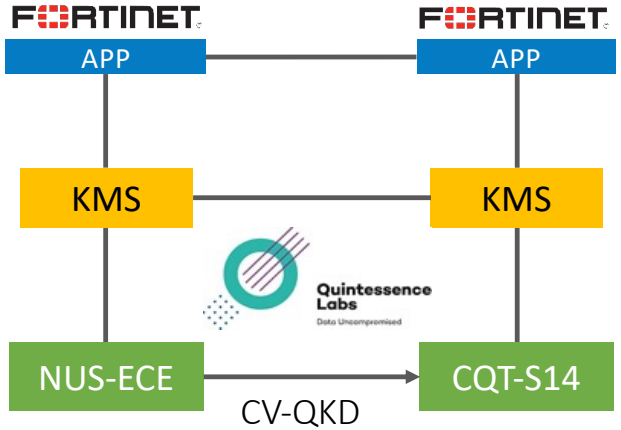
USE CASES – REFERENCE APPLICATIONS

QKD-secured Data Centre Interconnect (STT-GDC)



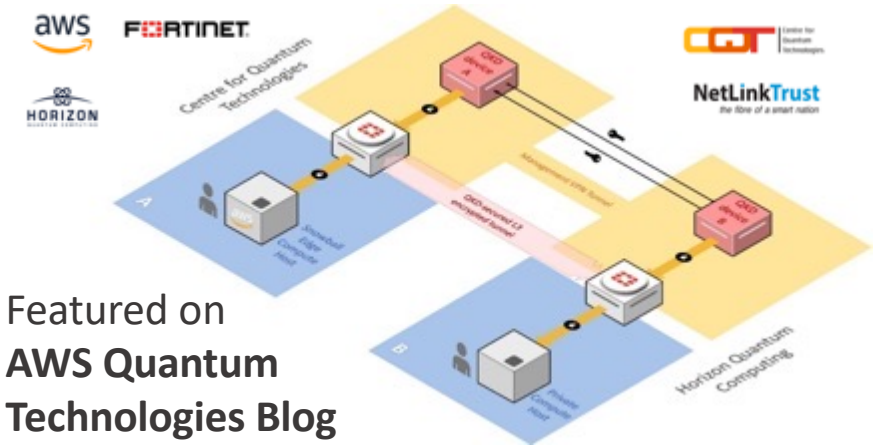
Continuous-Variable QKD with Application (QLabs & Fortinet)

Secret Key Rate
40 kb/s



CV-QKD
(qOptica)

Quantum-Secured VPN (AWS-Fortinet-Horizon QC)



Featured on
AWS Quantum Technologies Blog

Presentation at **Q2B 22**

QKD over Diverse Fibre Network (SpeQtral-ST Eng-SpTel)

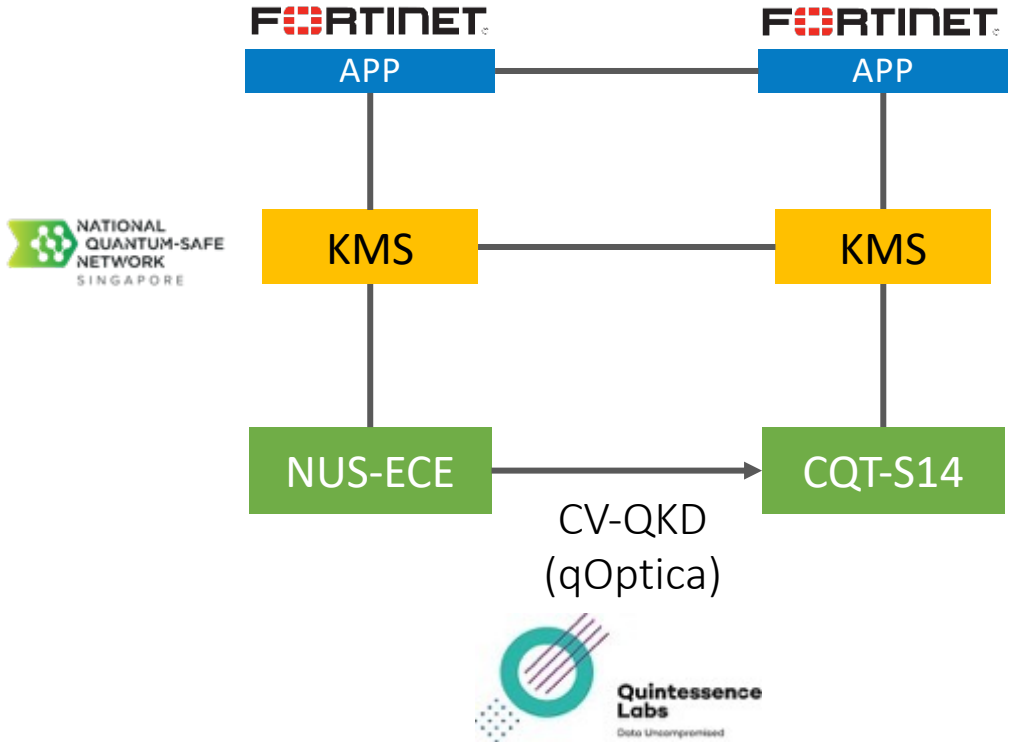
SPTel, SpeQtral and ST Engineering Held Successful Trial for Quantum-Secure Networks to Enable Robustly Secure Digital Communications

SINGAPORE – 10 November 2022 – SPTel and SpeQtral announced today their success on initial trials toward setting up Quantum-Secure Networks on SPTel's diverse fibre network, in the first among such trials in Singapore. SpeQtral conducted the trial using ST Engineering's quantum-enabled encryptors and Toshiba Digital Solutions' ("Toshiba") Quantum Key Distribution ("QKD") system over SPTel's diverse fibre network. The successful trial paves the way for robustly secure digital communications.

NQSN Advisory

USE CASES – KEY MANAGEMENT SYSTEM & SOLUTIONS

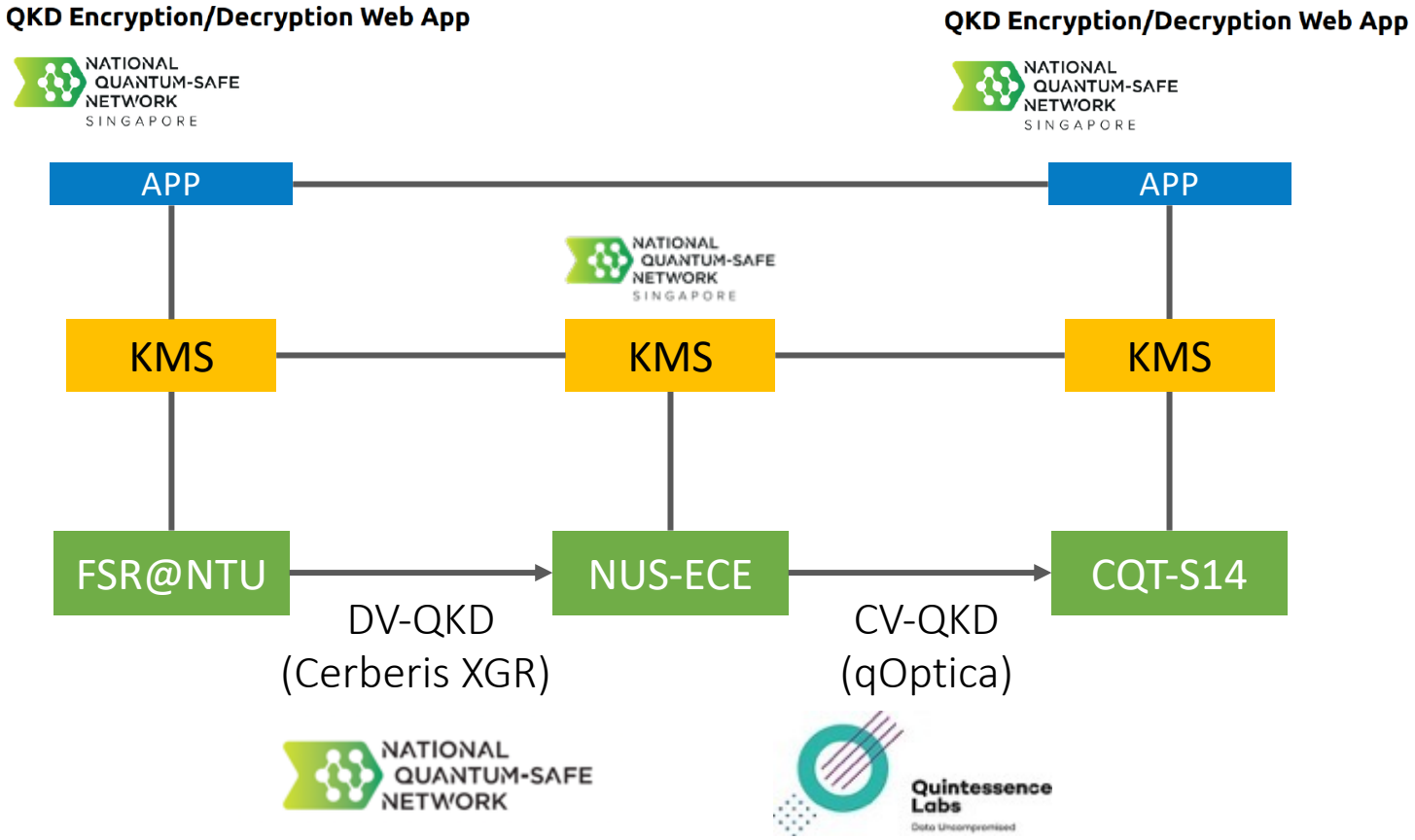
NQSN Key Management System



- ✓ KMS over 2 nodes with Fortinet L3 IPSec VPN

USE CASES – KEY MANAGEMENT SYSTEM & TECHNOLOGIES

NQSN Key Management System



- KMS over 2 nodes with Fortinet L3 IPSec VPN
- Key relay over 3 nodes with NQSN QKD-PQC Web Application

Multi-hops, Multi Vendor KMS

evolution

Key Management layer

- ❑ Quantum Key Management for multi-hops (5 nodes), multi-vendor QKDs (DV, CV, EB, QKD Sim) with evolutionQ Basejump software

Symmetric Key Distribution

Quantum Bridge

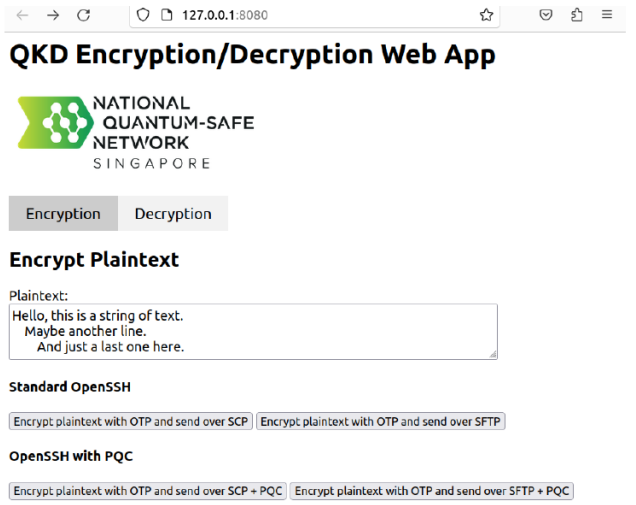
DSKE Protocol

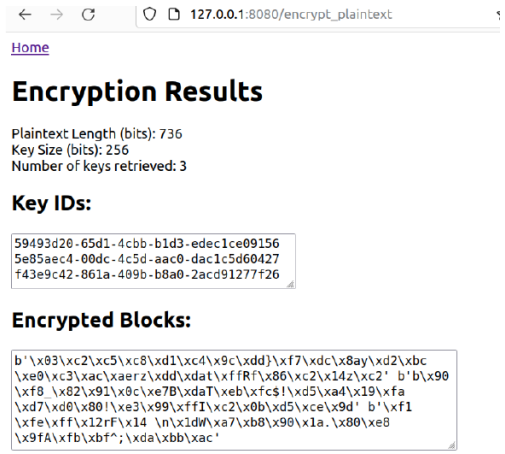
- ❑ Distributed Symmetric Key Exchange (DSKE) Protocol on NQSN Testbed with Quantum Bridge software

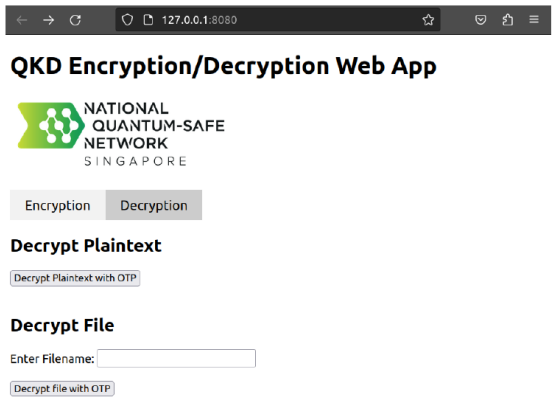
USE CASES – NQSN HYBRID QKD-PQC APPLICATION

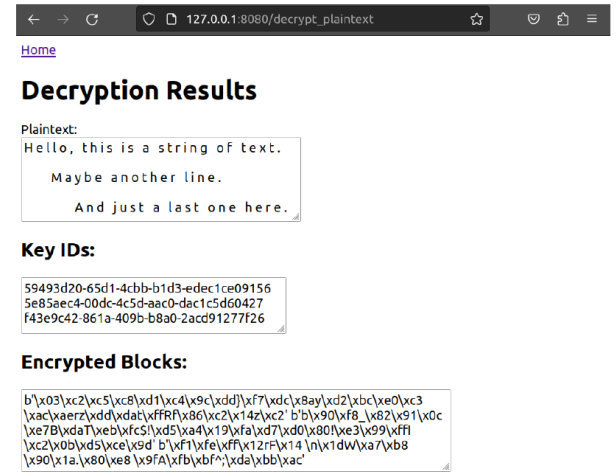
Hybrid Quantum Safe application

- **Two-layer quantum safe encryption**
- One Time Pad (OTP) encryption with QKD keys plus Quantum-safe OPEN-SSH*
- Kyber for key exchange (NIST Post quantum cryptography standard selection) + AES encryption
- **For short messages & high confidentiality use cases**



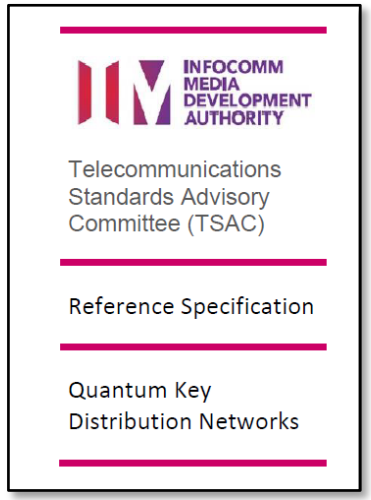


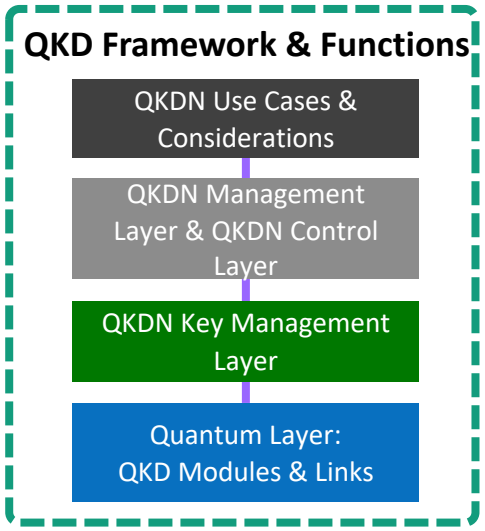




*SSH | Open Quantum Safe (openquantumsafe.org)

STANDARDISATION – INTERNATIONAL & LOCAL???





❑ International standards

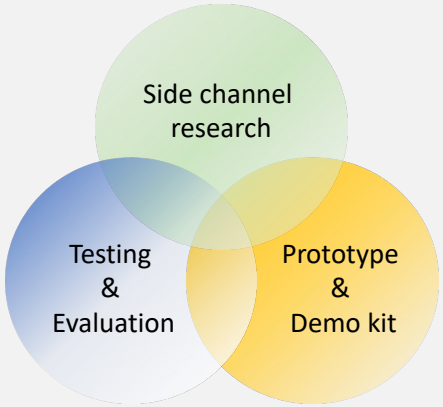
1. Led and established the work item for **1st standard on QKD protocol framework** in ITU-T
2. Hosted ITU-T Q15/17 interim meetings in 2022/2023
3. Contributed to ETSI ISG QKD, e.g. GR QKD 017
4. Co-hosting* **10th ETSI/IQC Quantum-Safe Workshop in May 2024 in Singapore, GSMA PQTN & ITU-T Joint Coordination Activity on QKD Network Meeting**

* In partnership with IMDA & CSA

❑ Local standards

1. IMDA TSAC **Quantum Communications Network Task Force**, with chairs & editors from NQSN, consolidated the contributions from 20 partners
2. Singapore's **1st standard (Reference Specification)** on **QKD Networks** published, with high level descriptions of QKDN & aligned with SDOs on QKDN, e.g. ITU-T, ETSI
3. QCNTF 2nd phase study on QKD modules & networks **evaluation & certification**

QUANTUM SECURITY LAB



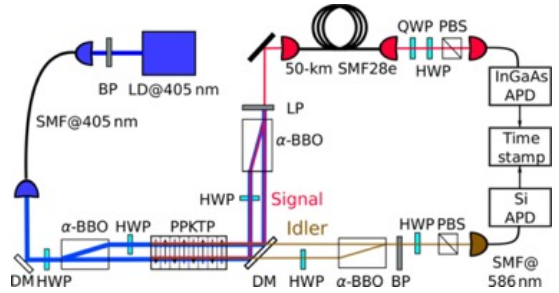
Functionality & Security Evaluation on QKD Module & QKD Networks

Bundesamt für Sicherheit in der Informationstechnik

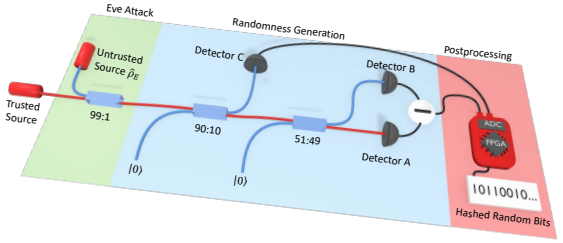
Deutschland Digital•Sicher•BSI•

Implementation Attacks against QKD Systems

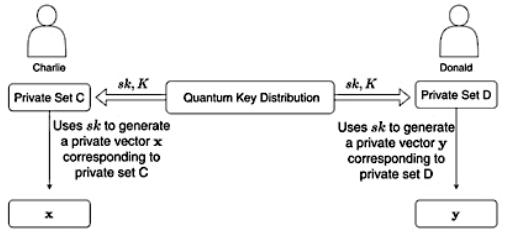
NQSN reviewed Germany BSI's "Implementation Attacks against QKD Systems"



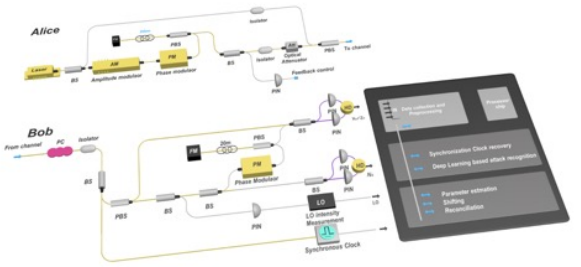
Physical Review Applied, *18*(4), 044075 (2022)



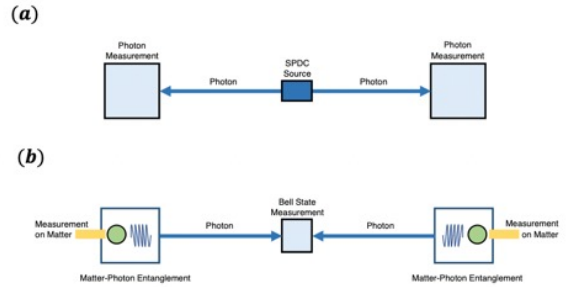
AQIS 2023 & *IPS* 2023



IEEE Internet of Things Journal (2023)



Physical Review A 105, 042411 (2022)



Quantum, *7*, 932 (2023)

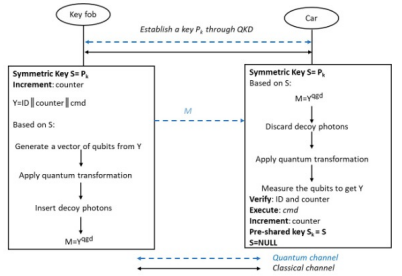
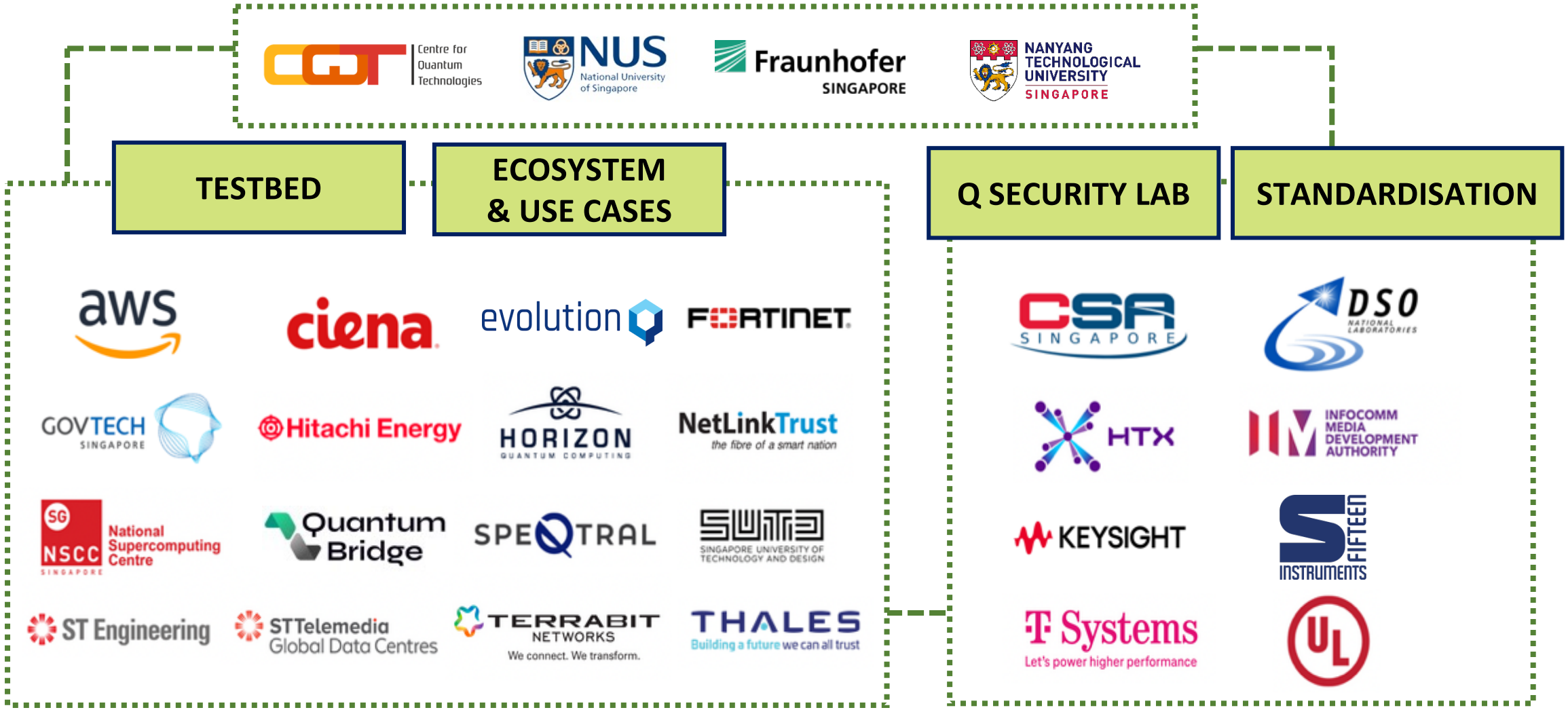


Fig. 1: The key fob authentication phase.

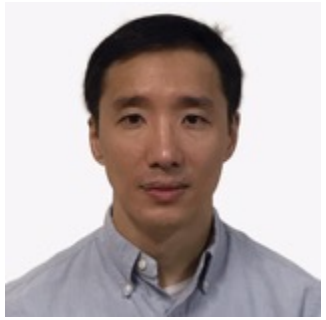
IEEE 98th Vehicular Technology Conference (2023)

ECOSYSTEM – NQSN PARTNERS & COLLABORATORS (2024)

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE



NQSN TEAM

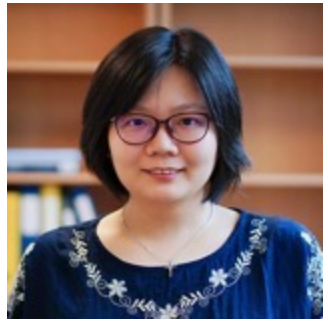


Lead PI
Alexander Ling
CQT & NUS

Co-Coordinator
Michael Kasper
Fraunhofer SG@NTU

Co-PI
Christian Kurtsiefer
CQT & NUS

Co-PI
Biplab Sikdar
ECE, NUS



Co-PI
Nelly Ng
SPMS, NTU

Snr Research Fellow
Hao Qin*
CQT

Snr Research Fellow
Jing Yan Haw*
CQT

*Contributed Equally

Project Manager
Ramana Murthy
CQT

Research Fellow
Gordon Duan
FraunhoferSG@NTU

Snr Research Scientist
Sanat Sarda
FraunhoferSG@NTU

Research Fellow
Yu Cai
SPMS, NTU

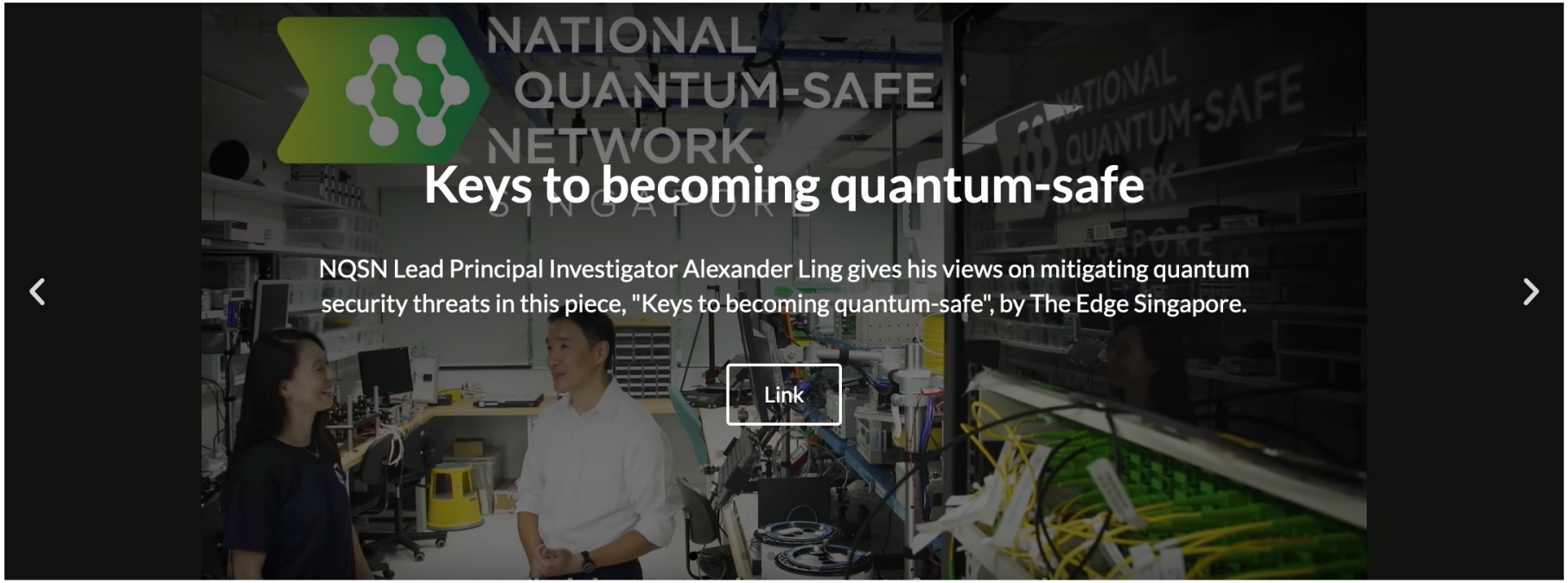
- NUS CQT:
Cassey Liang
Matthew Wee

- NTU:
Qiu KaiWei
Joseph Goo

+ Interns /Students

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

ABOUT NQSN TEAM COLLABORATION JOIN US Contact Us



NQSN

nqsn.sg

IMDA RS

IMDA RS QKDN

https:// → httpqs://