Work Progress on QKDN Use Cases in ITU-T FG-QIT4N

Zhangchao Ma
FG-QIT4N WG2 Chair

26 May 2021

FG-QIT4N activities on QKDN use cases

FG-QIT4N WG2 deliverables

D2.1 Technical report on QIT4N terminology part 2: quantum key distribution network

D2.2 Technical report on the QIT4N use case part 2: quantum key distribution network

D2.3 Technical report on QKDN protocols

D2.4 Technical report on QKDN transport technologies

D2.5 Technical report on QIT4N standardization outlook and technology maturity part 2: quantum key distribution network

D2.2 status

Co-editors:

- Mr. Andreas Poppe (AIT, Austria)
- Mr. Thomas Laenger (AIT, Austria)
- Mr. Dong-Hi Sim (SKT, Korea, (Rep. of))
- Mr. Zhangchao Ma (CAS Quantum Network Co., Ltd., China)

FG-QIT4N has held 8 meetings (7 e-meetings) since its Dec. 2019.

21 QKDN use cases have been captured.

- Expected stable draft deliverable for comments: August 2021
- Expected final draft for review: October 2021
- Expected approval: Final FG-QIT4N meeting, November 2021s

D2.2 Technical report on the QIT4N use case part 2: quantum key distribution network

Summary

This document consolidates the real-world QKDN use cases gathered during the lifetime of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N).

The QKDN uses cases are classified into vertical and horizontal domains. And it also highlights the competitive advantage of use cases brought by QKDN, the main barriers to QKDN adoption, and the benefits and needs for future standardization efforts.

Scope

- Competitive advantage brought by QKDN
- QKDN use cases in vertical and horizontal domains
- Barriers for QKDN adoption
- Suggestions for future works

Table of Contents

Latest version: QIT4N-O-024

QKDN Use Cases Class 1:
QKD combined with other cryptographic primitives

- **QKD + Encryption:** QKD can be combined with either OTP or AES to perform symmetric encryption.

- **QKD + Message authentication:** QKD can be combined with other authentication primitives to perform message authentication function, e.g., universal-II hash functions, symmetric key based message authentication code (MAC).

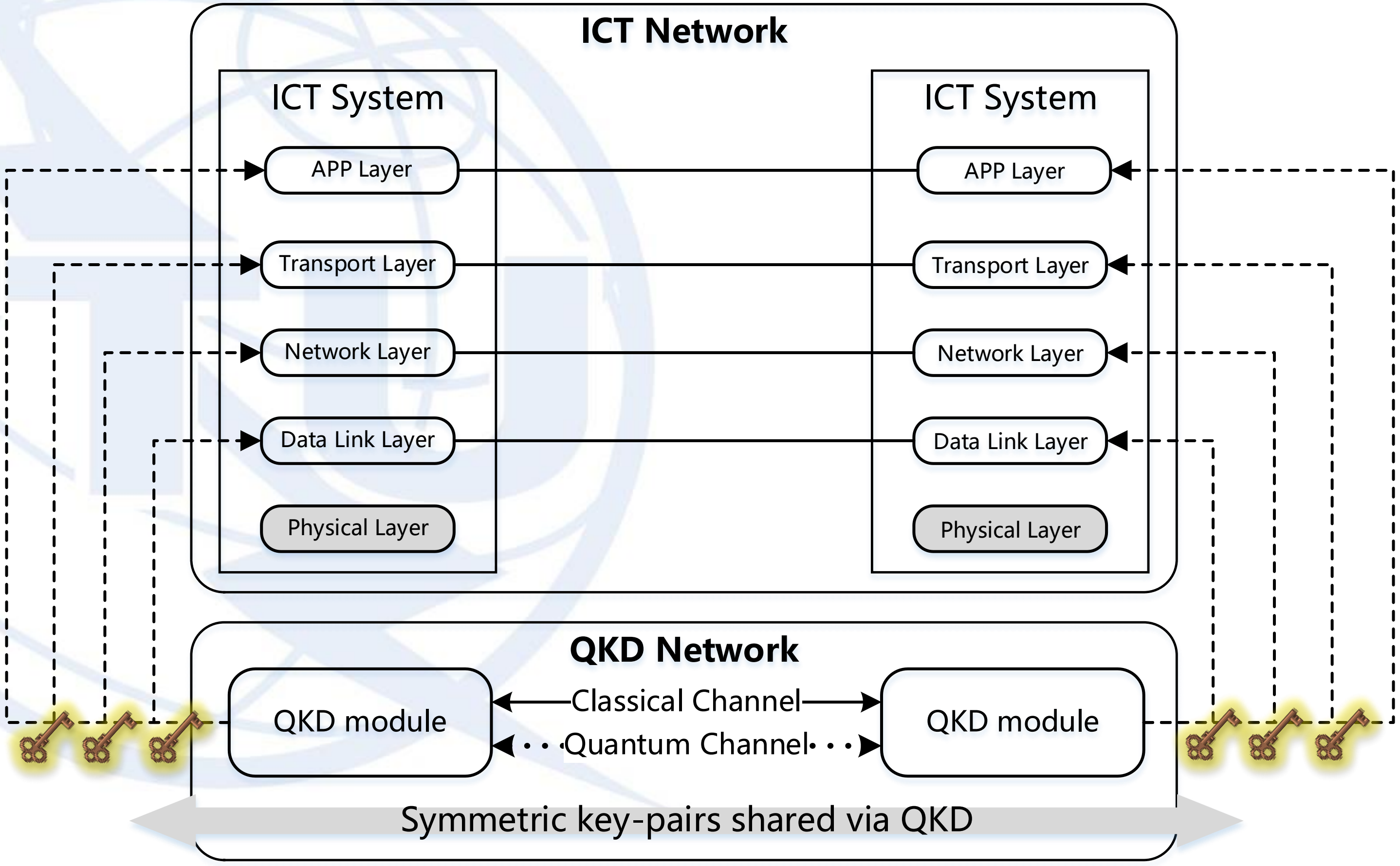
- **QKD + Secret sharing:** QKD can be combined with Shamir's secret sharing algorithm to perform secure storage function, as detailed in UC-V-020.

- **QKD + Secure multi-party computation (SMC):** QKD raw key can be used to implement oblivious key transfer to perform SMC, as detailed in UC-V-040.

- **QKD +Public key cryptography(PKC):** QKD can be combined with PKC including post-quantum cryptography (PQC) to provide hybrid security guarantee, as detailed in QKDN-PQC-002.

QKDN Use Cases Class 2:
QKD integrated with various TCP/IP protocols

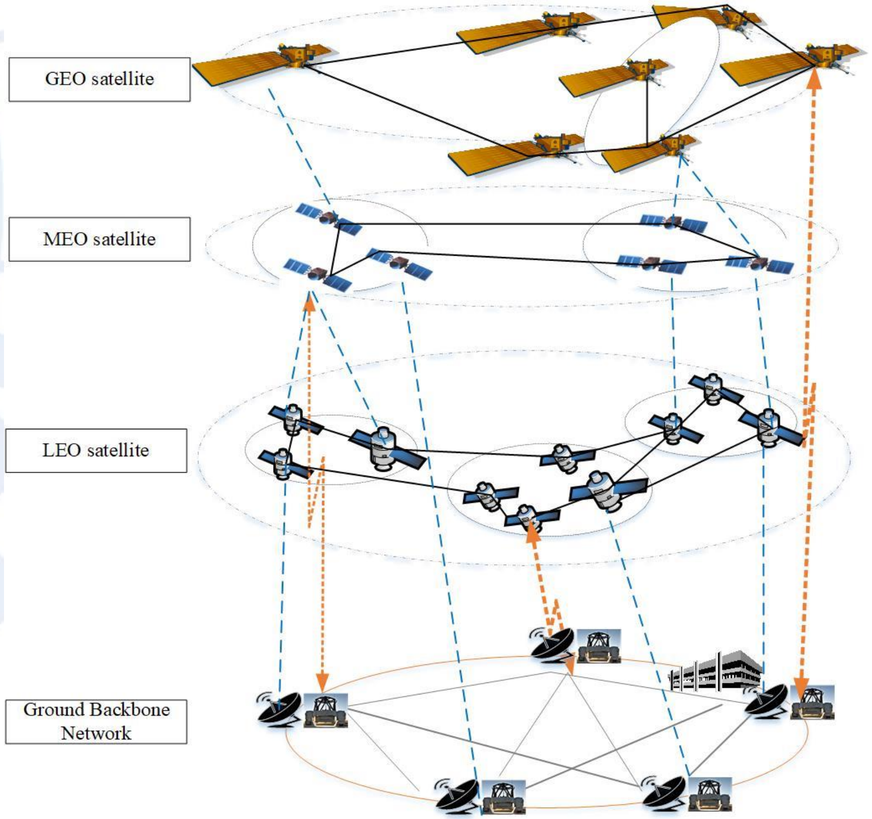
- **QKD can be integrated with TCP/IP protocols at various layers, e.g.,**
  - PPP and MACSec protocol at MAC layer,
  - IPSec protocol at network layer,
  - TLS protocol at transport layer.
  - User defined protocols at application layer.

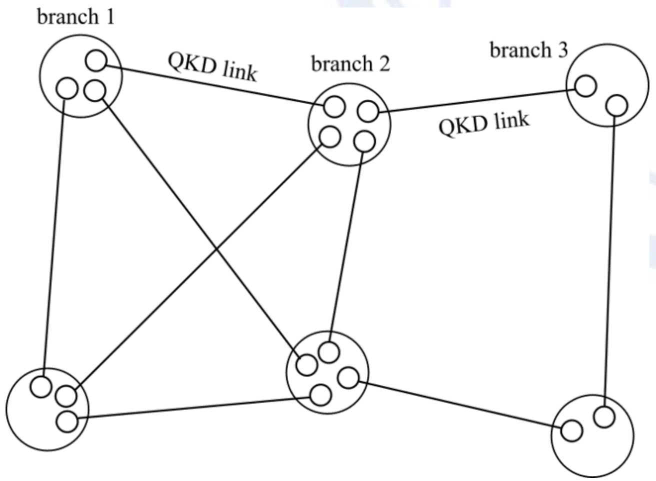


Setting the standard

QKDN Use Cases Class 3:
QKD implemented in various network topologies

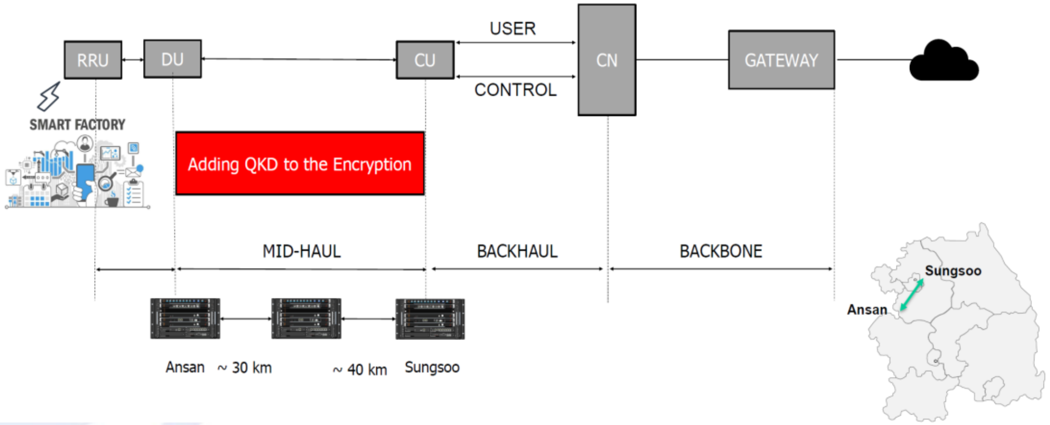
- **QKD can be implemented in various network topologies with either fibre or free-space channels, e.g.,**
  - metropolitan access network (as detailed in UC-V-010)
  - inter-city backbone network(QKDN-INF-001)
  - free-space satellite-ground or inter-satellite network (as detailed in UC-V-030)





QKDN Use Cases Class 4:
QKD integrated in various network forms

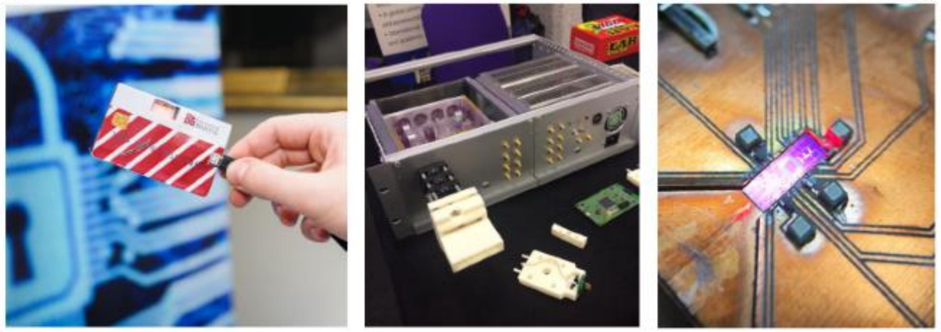
- **QKD can be integrated in various ICT network forms which require high security guarantee, e.g.**
  - 4G/5G network (as detailed in QKDN-Telecom-001~004),
  - SDN/NFV based network (as detailed in UC-H-040),
  - Cloud computing network (as detailed in UC-H-040/050),
  - Block chain network (as detailed in QKDN-BLC-001/002)
  - TSN network (as detailed in QKDN-TSN-001)
  - Service chain network (as detailed in UC-H-060),
  - and other future network evolutions, e.g., SCION (as detailed in UC-H-010), quantum internet



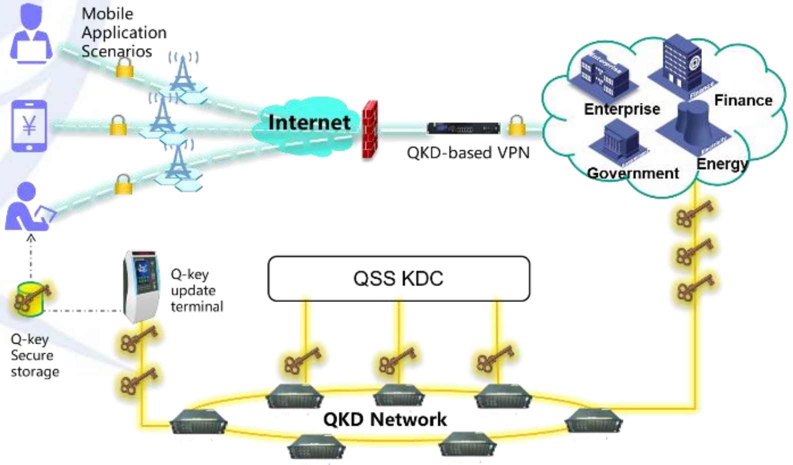
5G mid-haul QKD deployment for Smart factory

QKDN Use Cases Class 5:
QKD with different terminal types

- **QKD can be applied in different terminal types with different integration level, e.g.,**
  - fixed terminals which utilize QKD from separate devices;
  - fixed terminals which integrate QKD as internal component;
  - mobile terminals which simply embedded keys provided by QKD devices, as detailed in UC-H-020;
  - mobile terminals which integrate QKD functions.



Sibson, P., et al. (2017). "Networked Quantum-Secured Communications with Hand-held and Integrated Devices: Bristol’s Activities in the UK Quantum Communications Hub. " QCrypt 2017.



QKDN Use Cases Class 6:
QKD applied in different vertical sectors

- **QKD can be applied in various vertical sectors which require high level and long-term security, e.g.,**
  - Finance, Government (as indicated in UC-V-010),
  - Health care (as indicated in UC-V-040),
  - Telecom industry (as indicated in QKDN-Telecom-00x)
  - Critical infrastructure, e.g., energy, transportation

Any further comments or contributions on FG-QIT4N D2.2 QKDN use cases will be helpful and appreciated!

ITU-T FG-QIT4N:

- ✓ **Open to all**
- ✓ **Free participation:**
  - ➢ **no membership requirement**
  - ➢ **no cost**
- ✓ **Documents publicly available at no cost**

https://extranet.itu.int/sites/itu-t/focusgroups/qit4n/wg/SitePages/WG2.aspx