Introduction of FG QIT4N D2.3-part 1: Quantum key distribution network protocols: Quantum layer

ITU Workshop on "Quantum key distribution protocols, security and certification"

8 November 2022

*Hao QIN**

Quantum Communication Technologist

ITU/ETSI NUS Focal Point

IMDA TSAC FA7 QCNTF Co-Chair

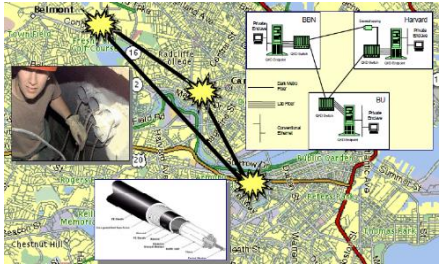
*hao.qin@nus.edu.sg

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

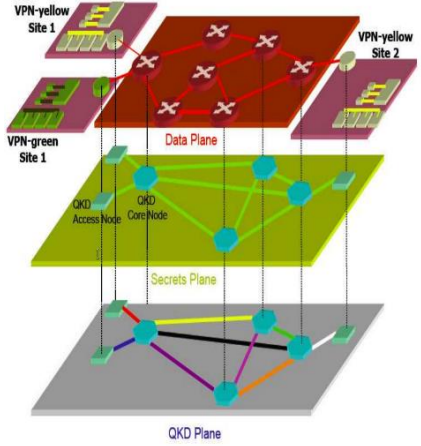
Centre for Quantum Technologies

NUS National University of Singapore

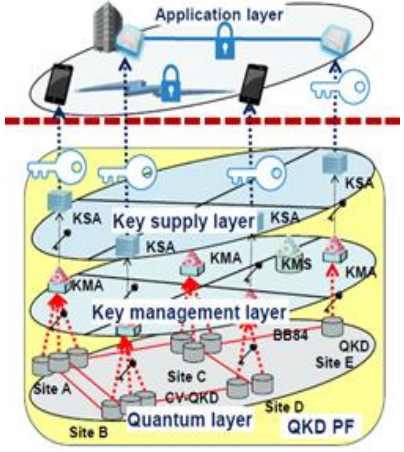
Quantum Key Distribution Networks (QKDN) Globally



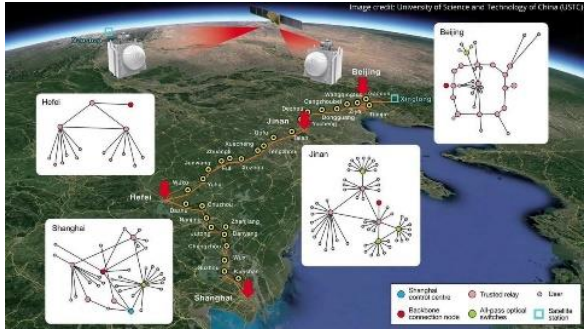
US DAPRA 2002-2007



EU SECOQC 2004-2008



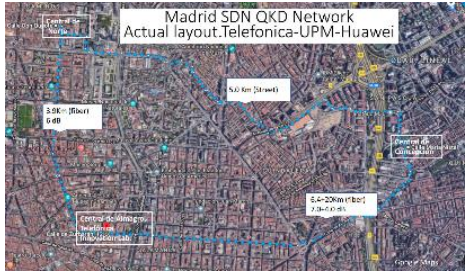
Tokyo Network 2011



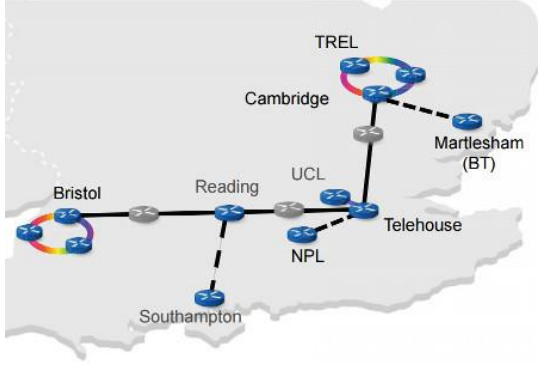
China satellite backbone metropolitan 2013~2021

Korea network 2015~

Germany QuNET 2018 -

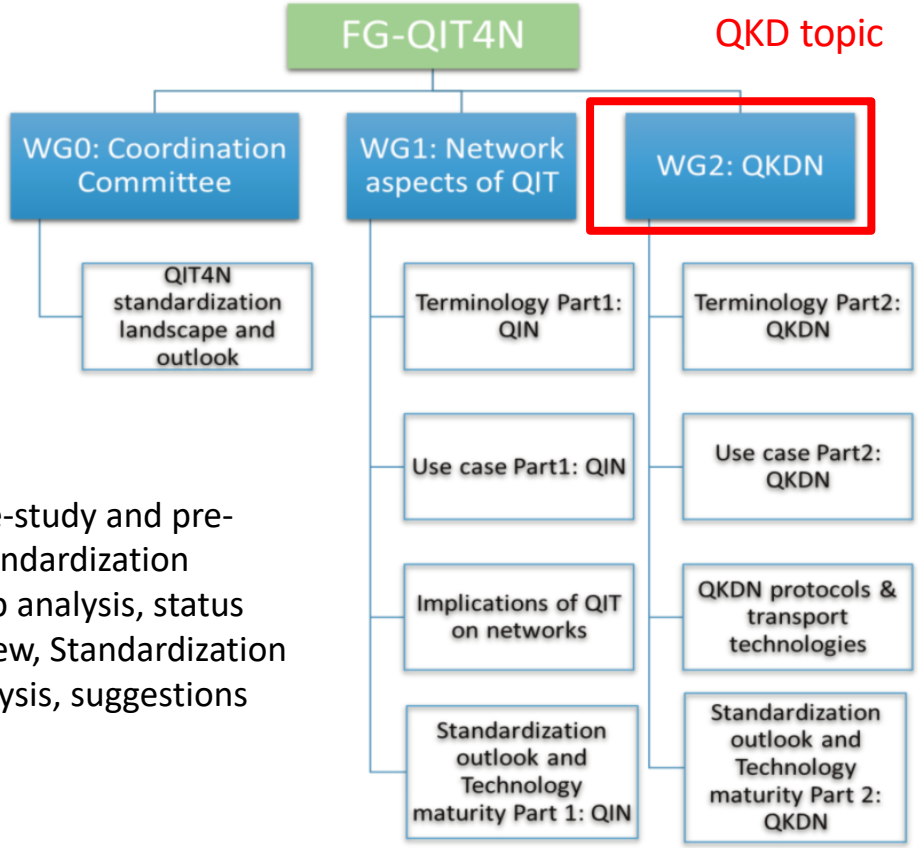


Madrid SDN 2018



UK BT 2020

ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N)



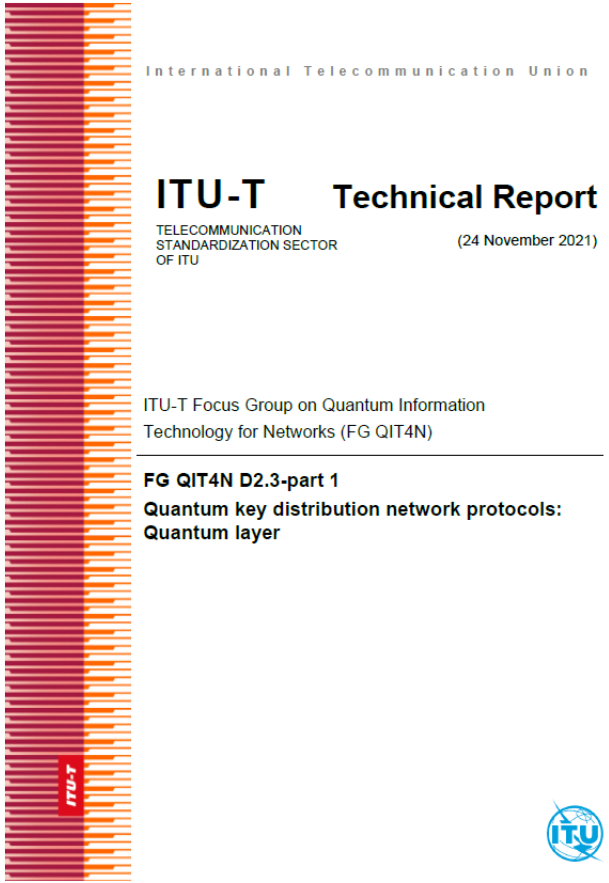
- Pre-study and pre-Standardization
- Gap analysis, status review, Standardization analysis, suggestions

FG QIT4N WG2:QKDN

Sub-group	Name	Status
D2.1	QIT4N terminology part 2: quantum key distribution network	Published
D2.2	Technical report on the QIT4N use case part 2: quantum key distribution network	Published
D2.3	Technical report on QKDN protocols Part1:Quantum layer Part2: Classical layers	Published
D2.4	Technical report on QKDN transport technologies	Published
D2.5	Technical report on QIT4N standardization outlook and technology maturity part 2: quantum key distribution network	Published

https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx

Technical report on QKDN protocols Part1:Quantum layer



❑ **Time line**

- Draft initiated, Feb 2020
- Drafting with 9 FGQIT4N E-meetings, 2020-2021
- Stable draft Nov 2021; Final publication Feb 2022

❑ **Joint session with other SDOs**

- Joint ITU-T FG-QIT4N/ETSI ISG QKD meeting, E-meeting, June 2020
- Joint meeting with ISO/IEC JTC 1 SC27/WG3, E-meeting 21 April 2020

❑ **Briefing session**

- ITU-T SG 11 & SG 13 Joint session, Dec 2021
- ITU-T SG 17 Plenary meeting, May 2022

❑ **Editing team:**

Chief editor:

- **Hao Qin**, National Quantum-Safe Network|National University of Singapore, Email: hao.qin@nus.edu.sg

Co-editors:

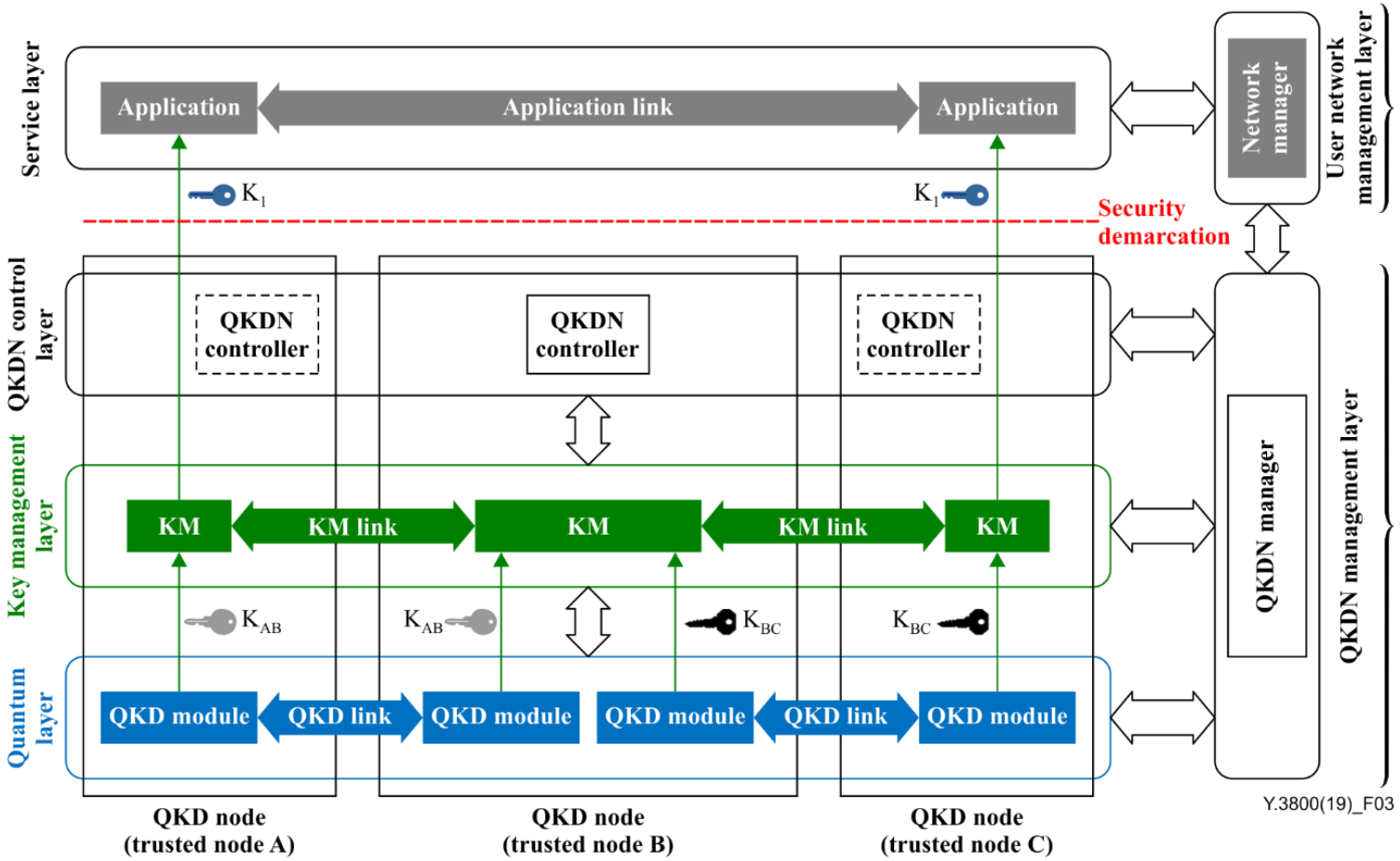
- **Peng Huang**, Shanghai Jiao Tong University, XT Quantech, Email: huang.peng@sjtu.edu.cn
- **Hongyu Wu**, QuantumCTek, Email: hongyu.wu@quantum-info.com

Standardization on quantum key distribution network (QKDN) in ITU-T

FG QIT4N: use cases

FG QIT4N: Classical protocols

FG QIT4N: QKD protocols, transport tech.



ITU-T SG 11: Protocol aspects

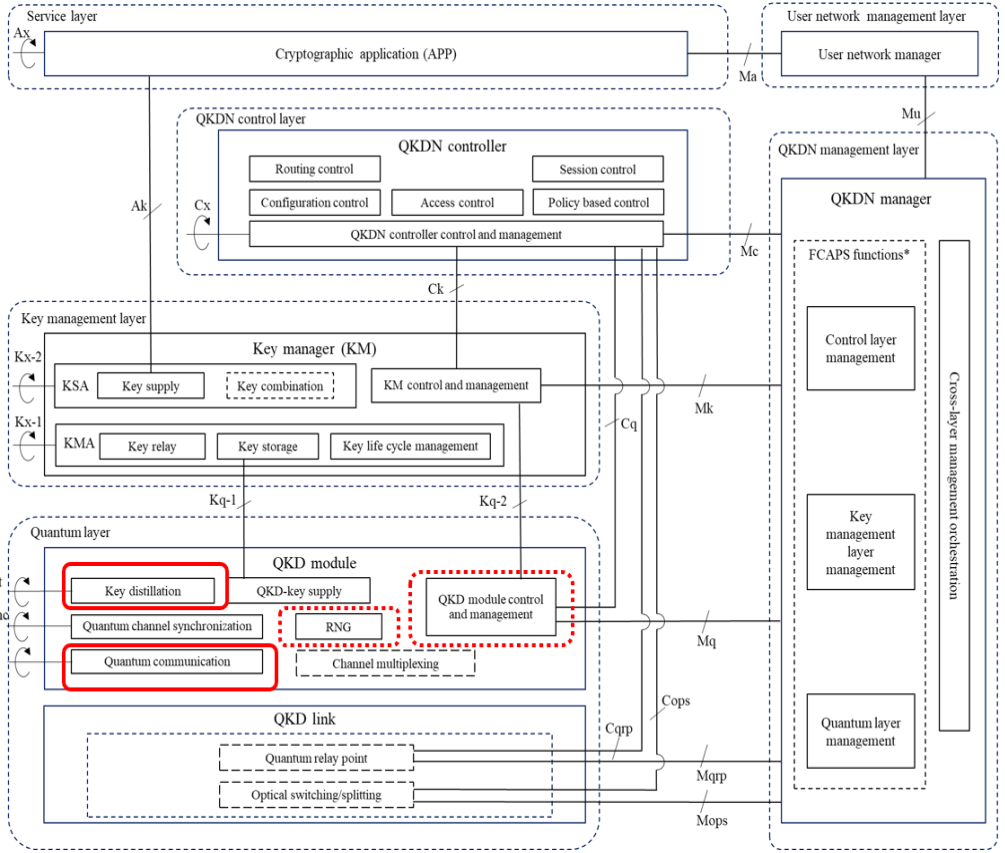
ITU-T SG 13: Network arch. Functions; QoS

ITU-T SG 17: Security aspects

- **Standards**
- **Pre-study**

*** Conceptual structures of a QKDN and a user network in Rec. ITU-T Y.3800 (10/2019)**

Scope & Summary



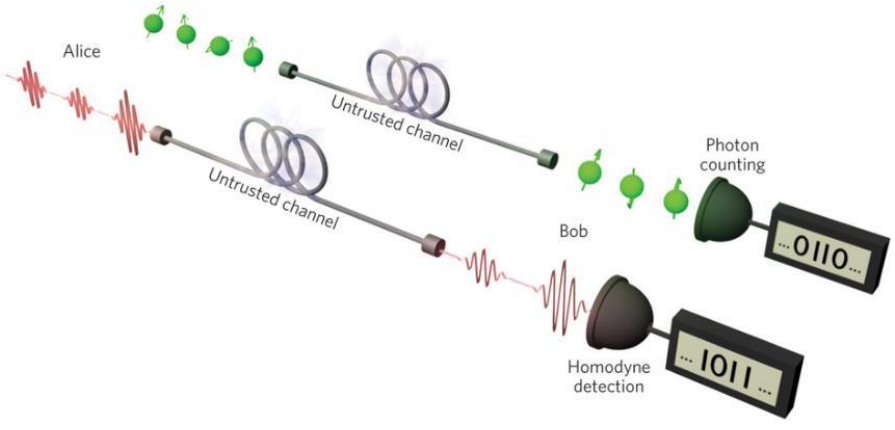
FGQIT4N D2.3 part1 relevance in the functional architecture model of QKDN [ITU-T Y.3802]

❑Study and review protocols in the quantum layer of QKDN

❑Focuses on QKD protocols that implemented on QKD modules in the quantum layer:

- General aspects: Workflow; Categories
- Security: Security notions, Epsilon security, Implementation security
- Introduction of discrete variable (DV) QKD protocols
- Introduction of continuous variable (CV) QKD protocols
- Standardization analysis and suggestions

General aspects



DV & CV QKD protocols [Nature Photonics 7,350–352 (2013)]

❑Quantum layer standardization

- QKD protocols implement on QKD modules: core part of quantum layer and QKDN
- Own features of both cryptographic protocols and communication protocols

❑QKD Protocol workflow & pattern

- Quantum communication stage
  Raw key exchange
- Post processing stage
  Sifting, parameter estimation, error correction, privacy amplification

❑QKD protocol classification

- Prepare-and-measure (**P&M**), measurement device independent (**MDI**) and entanglement based (**EB**)
- device dependent QKD protocols, device independent (DI) QKD, and one-sided DI QKD
- two-way or one way QKD
- discrete-variable (**DV**)-QKD and continuous-variable (**CV**)-QKD

Security aspects in QKD protocols

❑The notions of security

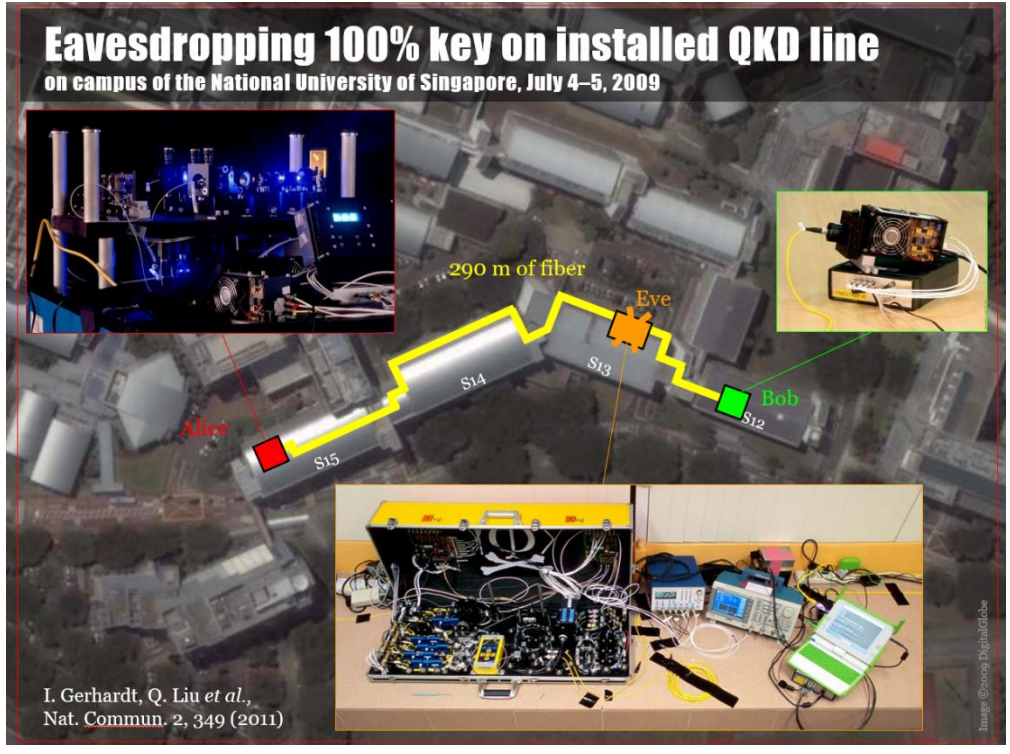
- Epsilon security ε ≤ ε'+ε''
- Security proof
- Information theoretic security
- Finite size

❑ Assumptions in the security proofs

- Classical channel, integrity protection
- Random number generator
- Model = Realization

❑ Implementation security

- Violation of assumptions
- Kerckhoffs' principle -> White box
- Quantum hacking attacks
- On the QKD modules, Not on the QKD protocols
- Practical security breach
- Mitigated by countermeasures



Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. 2, 349 (2011)

Overview of QKD protocols

- ❑ Discrete-variable (DV)-QKD Vs Continuous-variable (CV)-QKD

- ❑ Protocol features

- ❑ Detailed protocol procedure
  - Quantum communication stage: Preparation, Transmission ,Measurement
  - Post processing stage: Sifting, parameter estimation, error correction, privacy amplification

- ❑ Parameters report to other QKDN layers

- ❑ Commercialization status

Introduction of DV QKD protocols

❑ **DV QKD**

- Encoding: QKD-Tx uses discrete variables of finite dimension such as phase, polarization or time bin of single photons
- Decoding: QKD-Rx uses single photon detectors (SPDs)

❑ **Protocol features**

- BB84, E91, B92, Six-state, BBM92, SARG04, coherent-one-way, differential-phase-shift, round-robin-DPS, MDI-QKD protocol, Twin-field, DI-QKD

❑ **Details** on decoy state BB84, BBM92

- Protocol procedure in quantum communication stage and post processing stage

❑ **Main parameters**

- Quantum Bit error rate (QBER), channel loss, secret key rate

❑ **Commercialization status**

- Several companies work on commercial QKD products using different DV QKD protocols

Introduction of CV QKD protocols

❑ **CV QKD**

- Encoding: QKD-Tx encodes information using the position and momentum quadrature of a quantized electromagnetic field in an infinite dimensional Hilbert space
- Decoding: QKD-Rx uses the coherent detection such as homodyne or heterodyne detection

❑ **Detail introduction & Protocol features**

- Gaussian modulation coherent state (GG02, No-Switching), Unidimensional CV-QKD, CV MDI QKD, Discrete modulation CV-QKD, Data interaction protocol for classical post processing

❑ **Main parameters**

- Excess noise, channel transmission, modulation variance, secret key rate

❑ **Commercialization status**

- Several companies work on commercial QKD products using Gaussian modulation CV QKD protocols

Pros & Cons for QKD protocol standardization

✓ Pros

❑ Definition

- *What is a QKD protocol and what does this protocol do?*

❑ Certification

- Complicated and challenging task
- QKD protocol standardization is not enough
- Protocol standardization can make it easier
- The first step and starting point

❑ Interoperability

- QKD software
- QKD software <> hardware
- Components in QKD-Tx, Rx
- Challenging and not likely QKD-Tx <> RX

❑ Confidence

- QKD users
- Wider adoptions

❖ Cons

❑ Innovation and research

- Still evolving fast
- New QKD protocols, techs, security proofs

❑ However,

- Standardization procedure is complex, also comprehensive
- Step by step approach

❑ Research and standardization are **NOT in conflicts**:

- Optical communication protocols, SG15
- **Cryptographic protocols, AES, X.509, PKI….**
- Post quantum cryptography NIST, ETSI Cyber QSC

Finding & suggestions

❑ **Quantum layer standardization is missing**

- QKD is the core part of quantum layer and QKDN
- QKD protocol is relatively a **new** concept to SDOs
- owns the features of cryptographic protocols and communication protocols

❑ **QKD protocol standardization**

- Many QKD protocols in academic and industry
- Protocol **workflow & pattern** serves as basis of the framework
- Each step in a QKD protocol is **security concerned**
- Further study on specific QKD protocols

❑ **Various security topics on QKD protocol**

- **Security** is the core of QKD protocol
- **Unique security** features of QKD protocol
- Information-theoretic security (**ITS**) and beyond
- **Security** notions, epsilon security, finite size
- Theoretical **security** and implementation **security**
- Security requirements and measures

ITU

ISO IEC

ETSI World Class Standards

THANK YOU
QUESTIONS?