QKD Network approaches – beyond the “classical” – SECOQC et al. approach

Momtchil Peev
Optical and Quantum Laboratory, Munich Research Center MRC
Huawei Technologies Duesseldorf GmbH

June 06, 2019

Contents

- QKD Network Definitions & Basic Consequences
- QKD Networks towards a systematic approach?
- QKD Networks fundamental constituents – static and dynamic
- Outlook

What is a QKD Network?

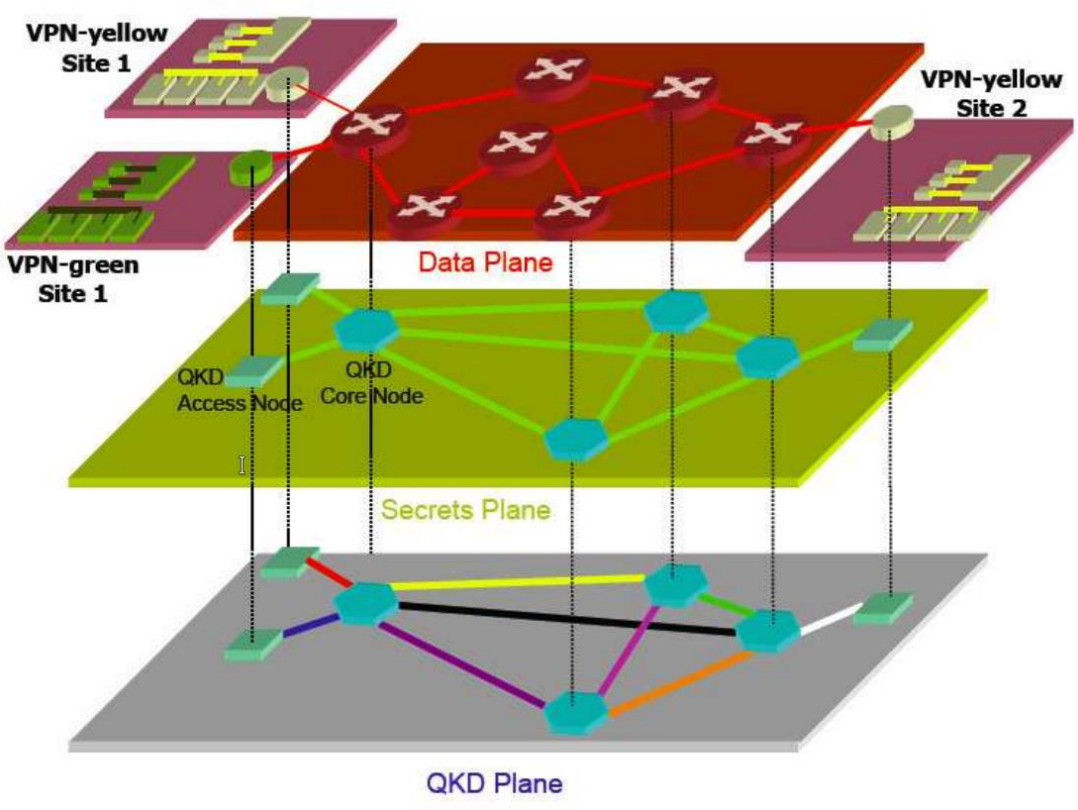
- **New Journal of Physics, M Peev et al 2009 New J. Phys. 11 075001**

" …. a QKD network … an infrastructure, based on point-to-point QKD capabilities, that aims at information theoretically secure (ITS) key agreement and NOT at secure communication"

- **Current discussion in ITU-T, ETSI. Toshiba, IdQuatique, Huawei, Telefonica, UPM:**

"a Communication network that supports secure communication and security applications at large by utilizing different security primitives, including but not restricted to QKD"

Original approach: SECOQC – key generation separation



HUAWEI

Consequences of Definitions

- **A network design according to the traditional approach implies**

An (at least logically) standalone infrastructure that is dedicated to (ITS) key generation alone

- **The recent “industry promoted” attempts imply**

A general communication infrastructure that by virtue of QKD has additional security features, in which key generation is not restricted to a specific domain of its own

Consequences of Definitions

- **A network design according to the traditional approach implies**

An (at least logically) standalone infrastructure that is dedicated to (ITS) key generation alone

- **The recent "industry promoted" attempts imply**

A general communication infrastructure that by virtue of QKD has additional security features in which key generation is not restricted to a specific domain of its own

Why, What about security?

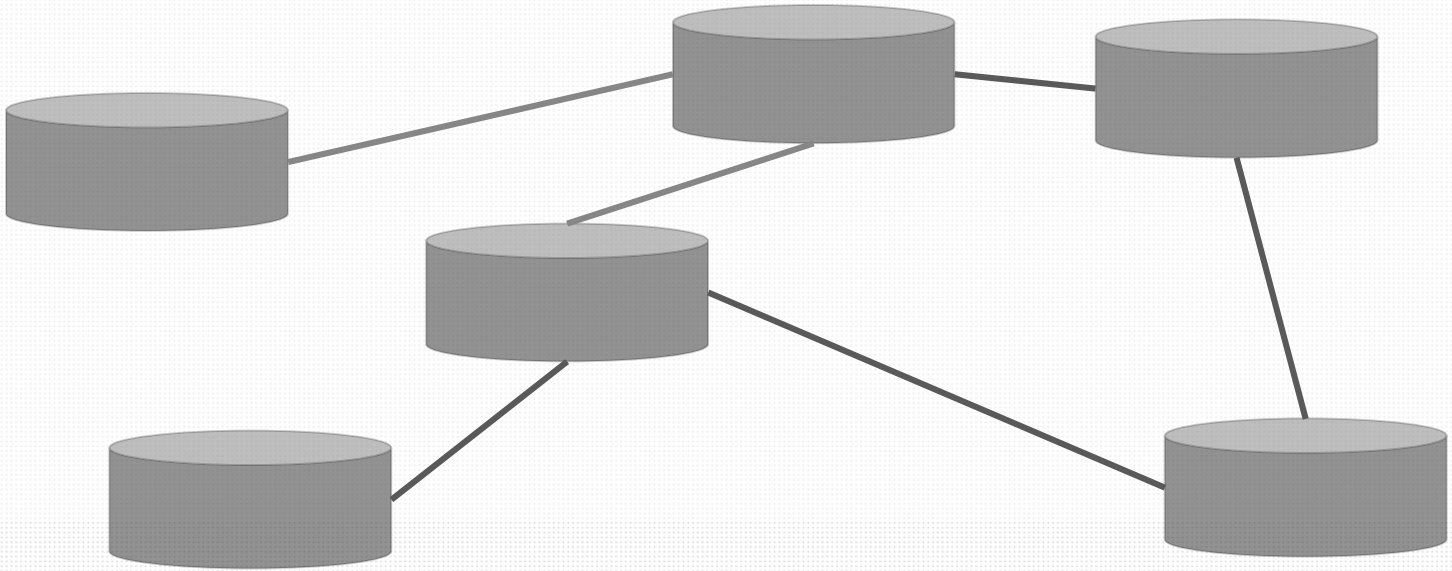
What about security?

Systematic Approach towards a QKD Network

- Elementary Functions
- Functionality Layers
- Architectures
- Implementations

(QKD) Networks – what are these in fact?

- **Connected locations (Nodes)**

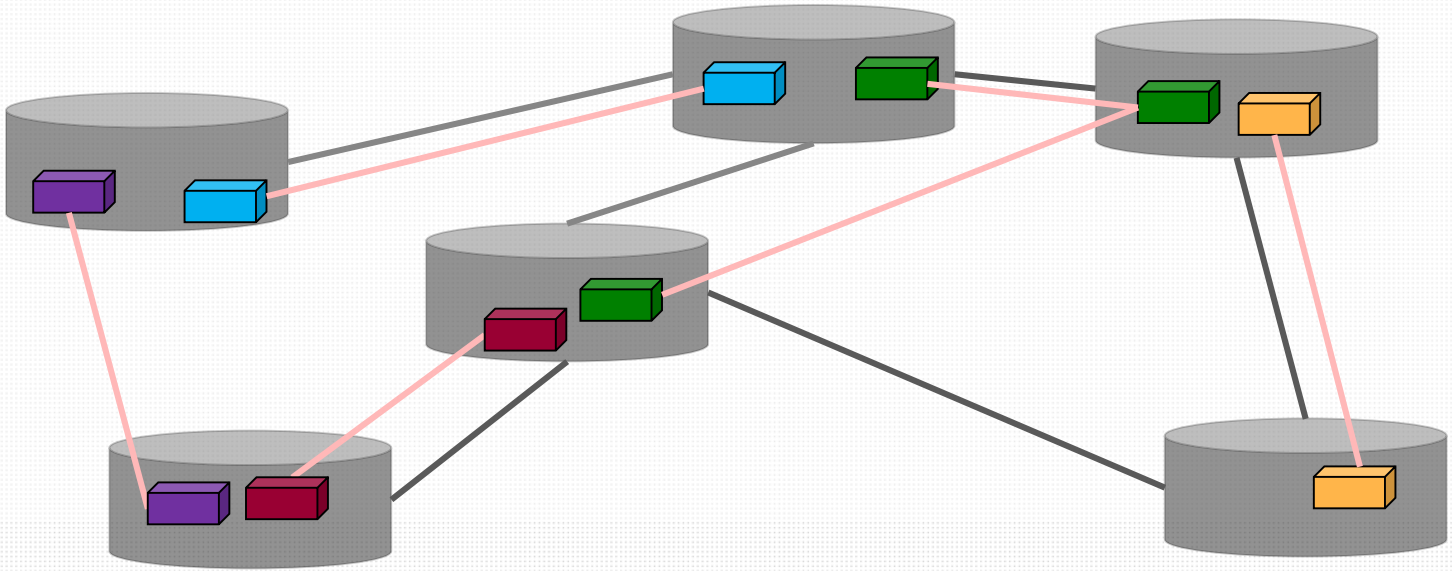


Systematic Approach towards a QKD Network II

- **The fundamental constituents**
  - ✓ A Crypto Subsystem (Note: A QKD Network is only an ephemeral Quantum Network)
  - ✓ A Communication/Computation Subsystem
- **Potential Dynamics of the Network and its Subsystems**

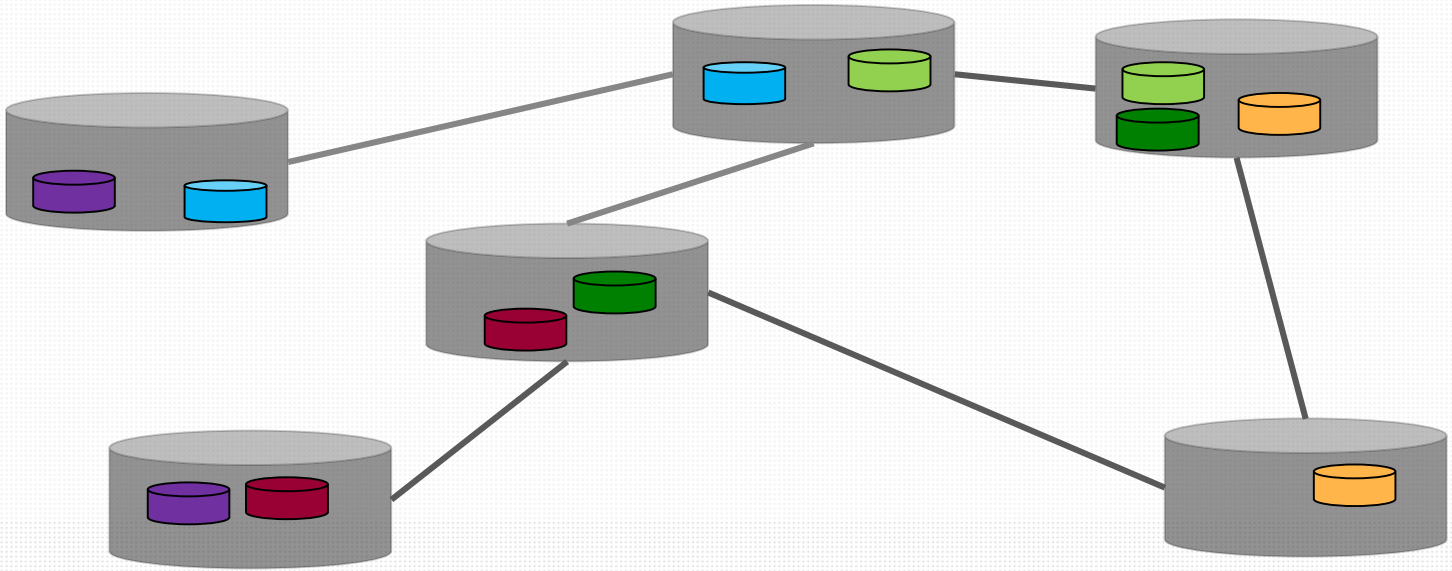
(QKD) Networks – the crypto segment

- **Crypto Subsystem from QKD 1**



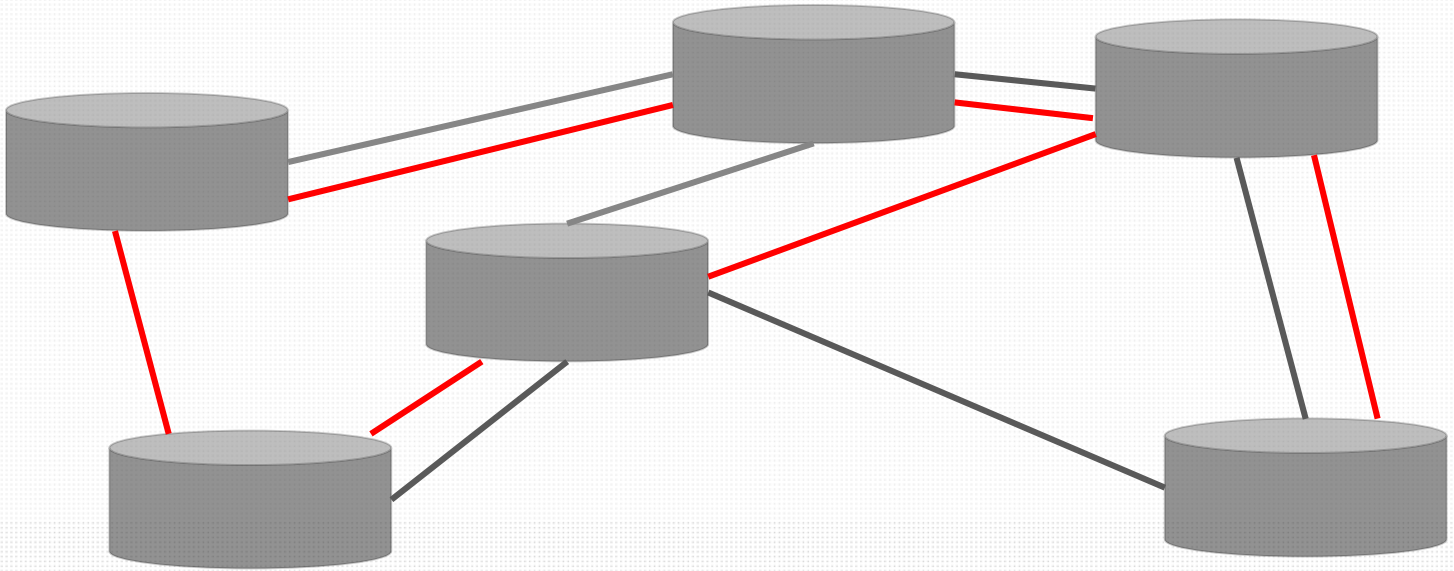
(QKD) Networks – the crypto segment

- **Crypto Subsystem from QKD 2**



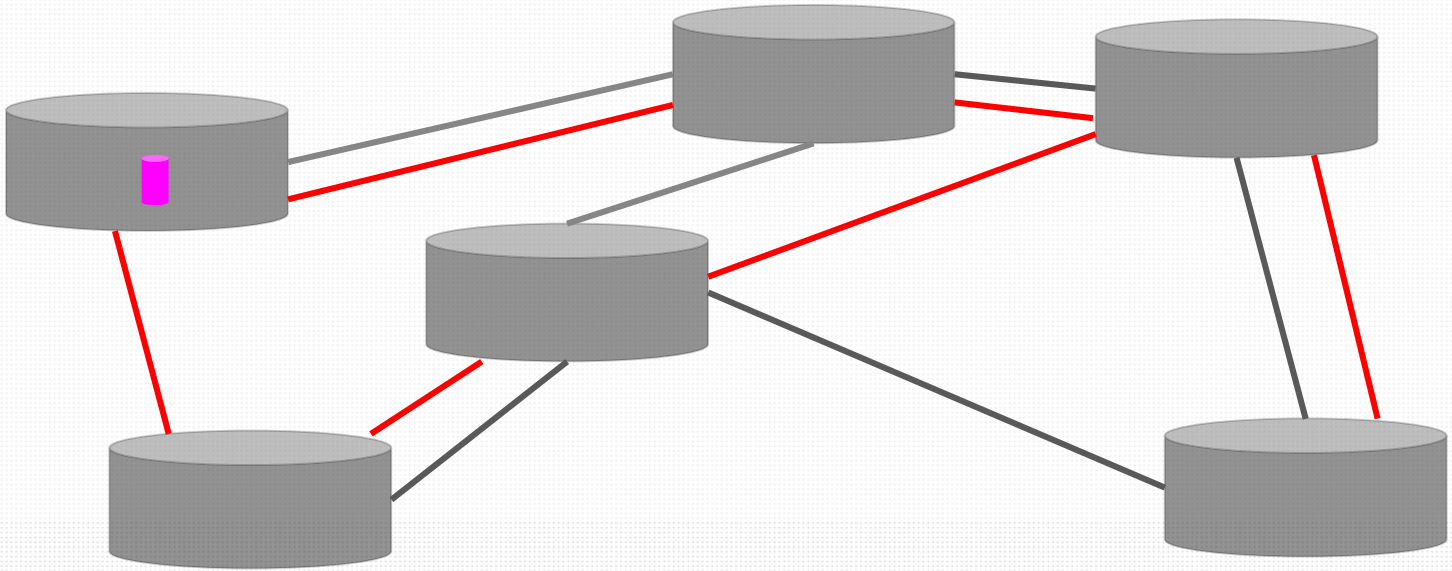
(QKD) Networks – the crypto segment

- **Crypto Subsystem 3**



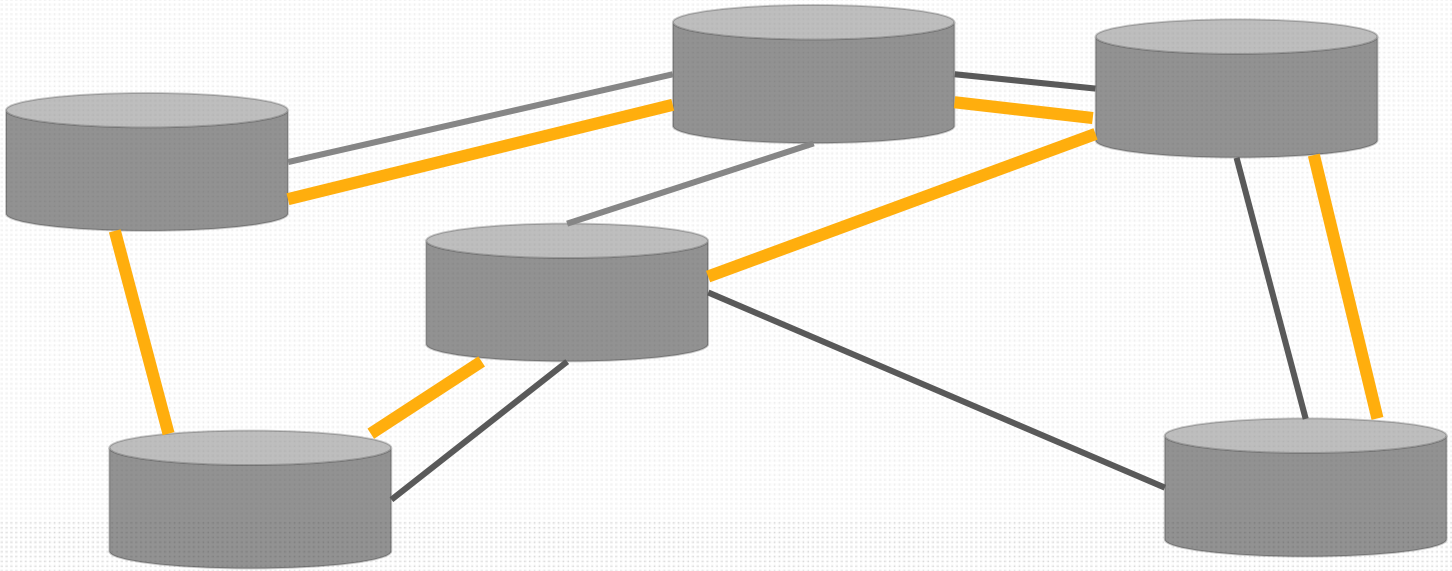
(QKD) Networks – the crypto segment

- **Crypto Subsystem 4**



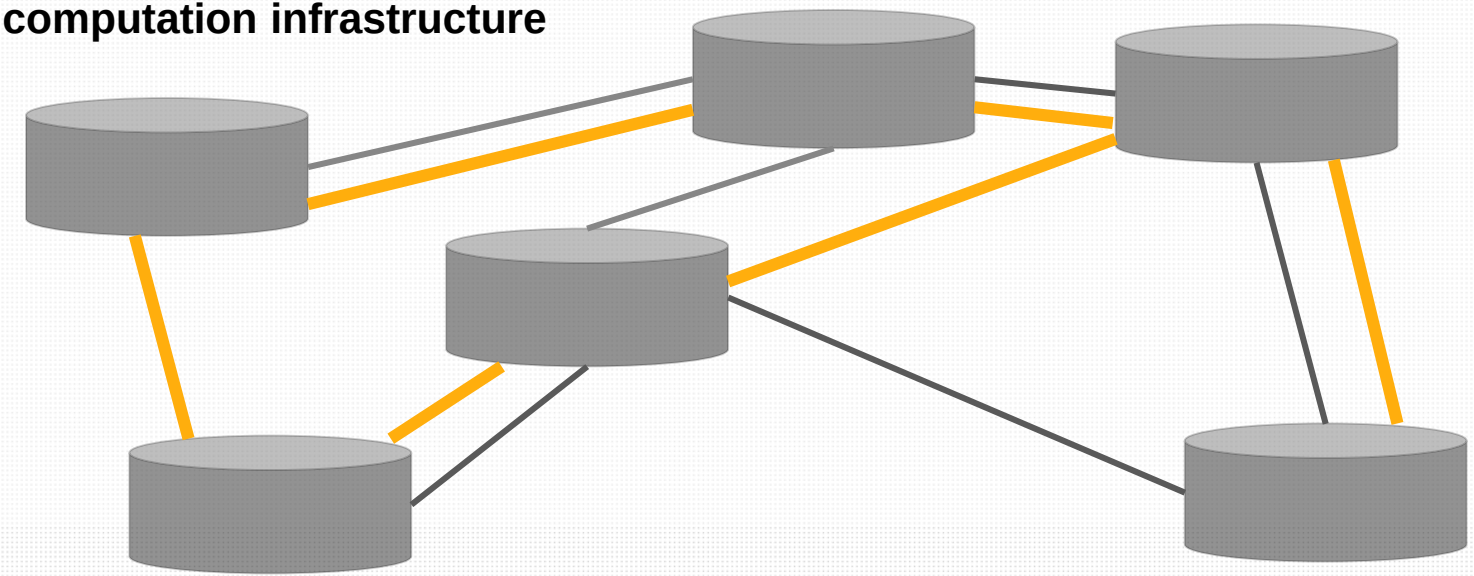
(QKD) Networks – the crypto segment

- **Crypto Subsystem 5**



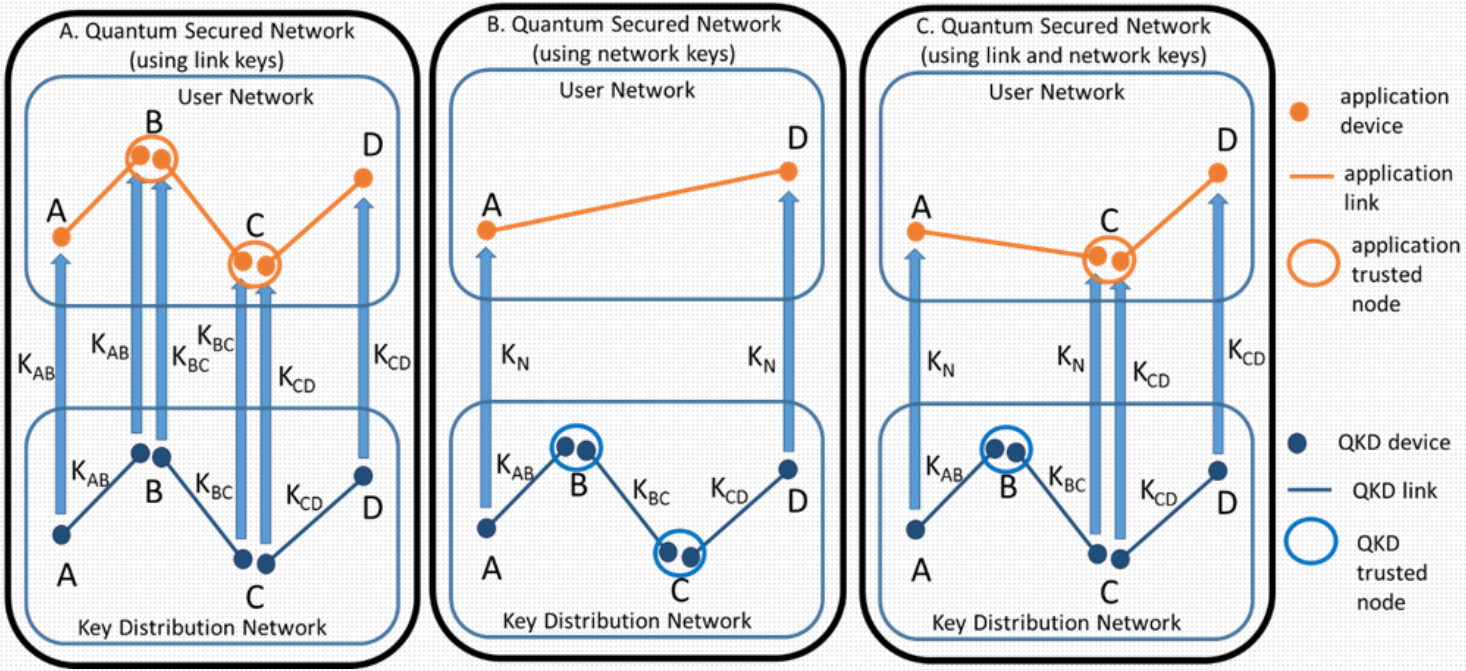
(QKD) Networks

- **Crypto Subsystem as a feature and subsystem of a general communication/ computation infrastructure**



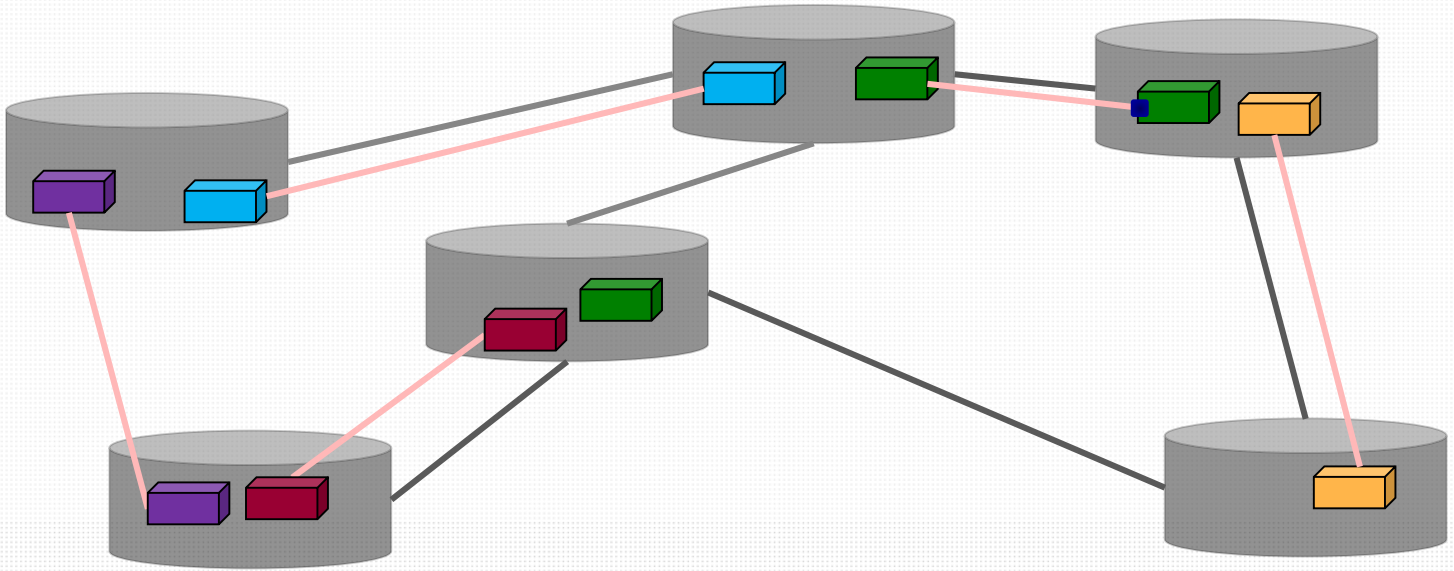
QKD Network types: a Static Version

Contribution to ITU-T Standardization Document: Toshiba, IdQuantique, Huawei…



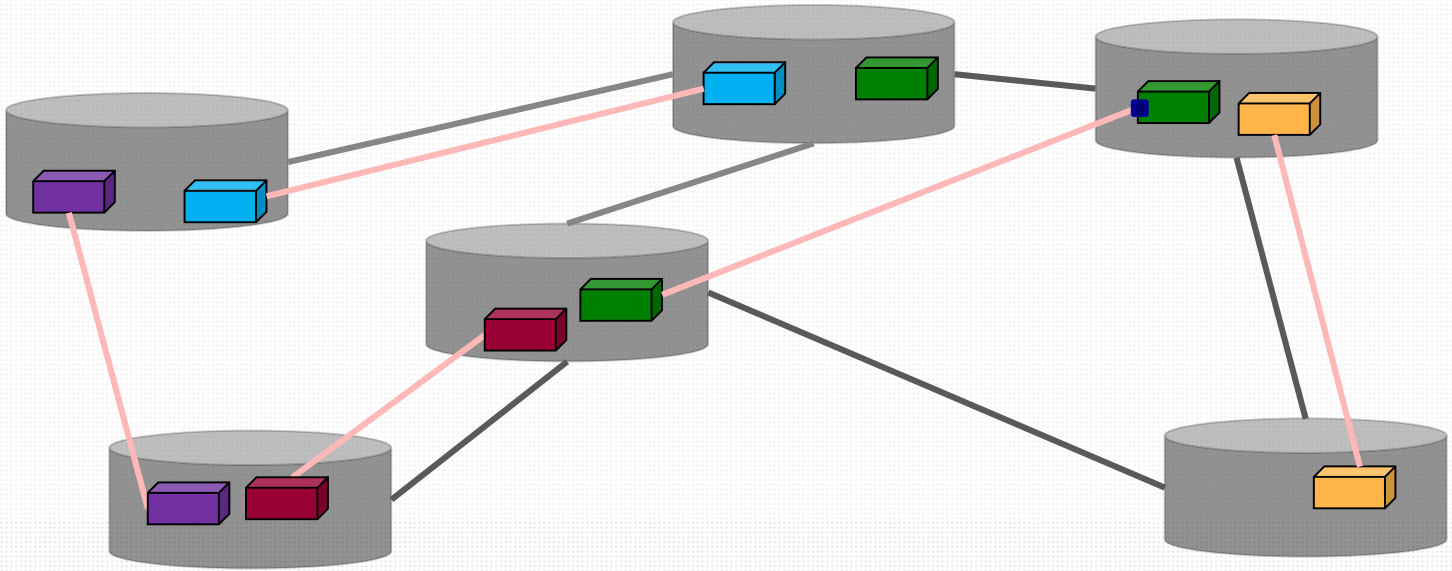
Dynamic (QKD) Networks – the crypto segment

- **Crypto Subsystem from QKD 1**



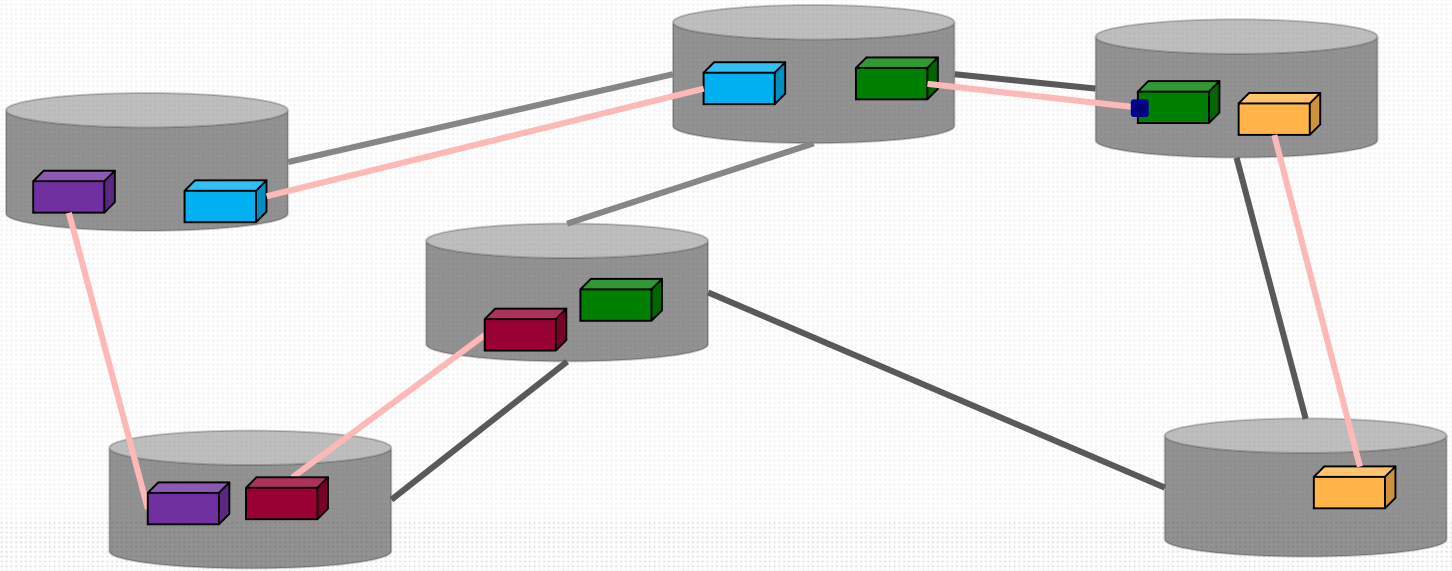
Dynamic (QKD) Networks – the crypto segment

- **Crypto Subsystem from QKD 1**



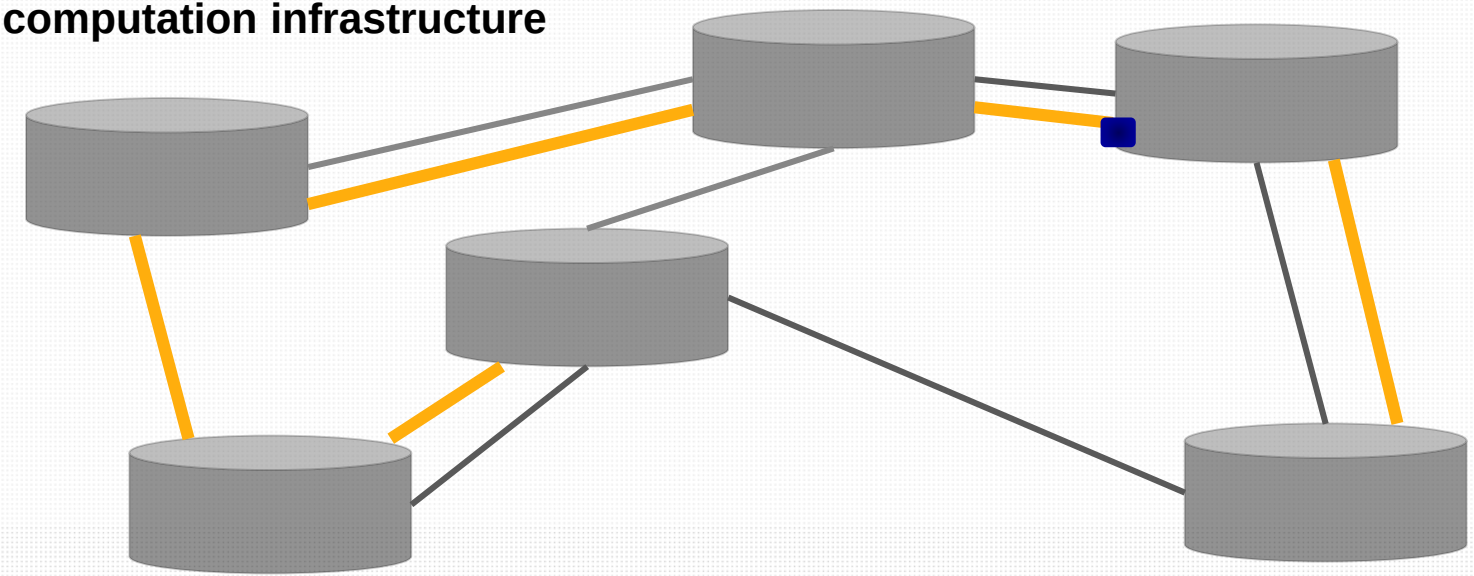
Dynamic (QKD) Networks – the crypto segment

- **Crypto Subsystem from QKD 1**



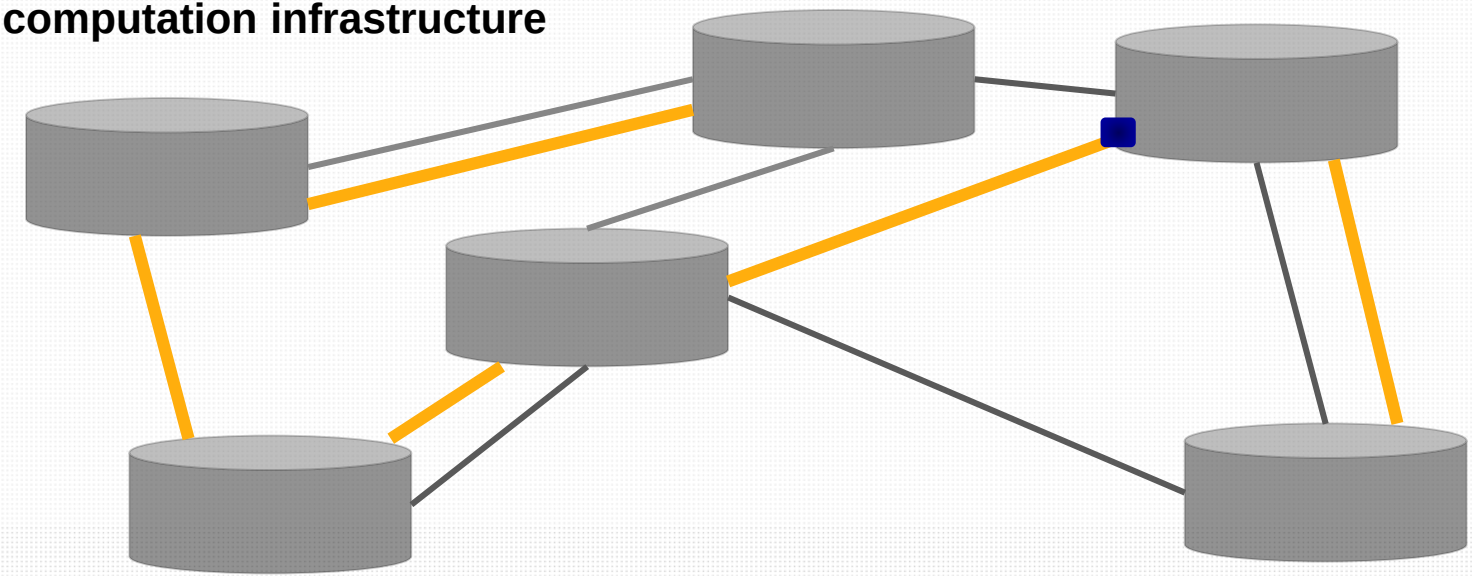
Dynamic (QKD) Networks

- **Crypto Subsystem as a feature and subsystem of a general communication/ computation infrastructure**



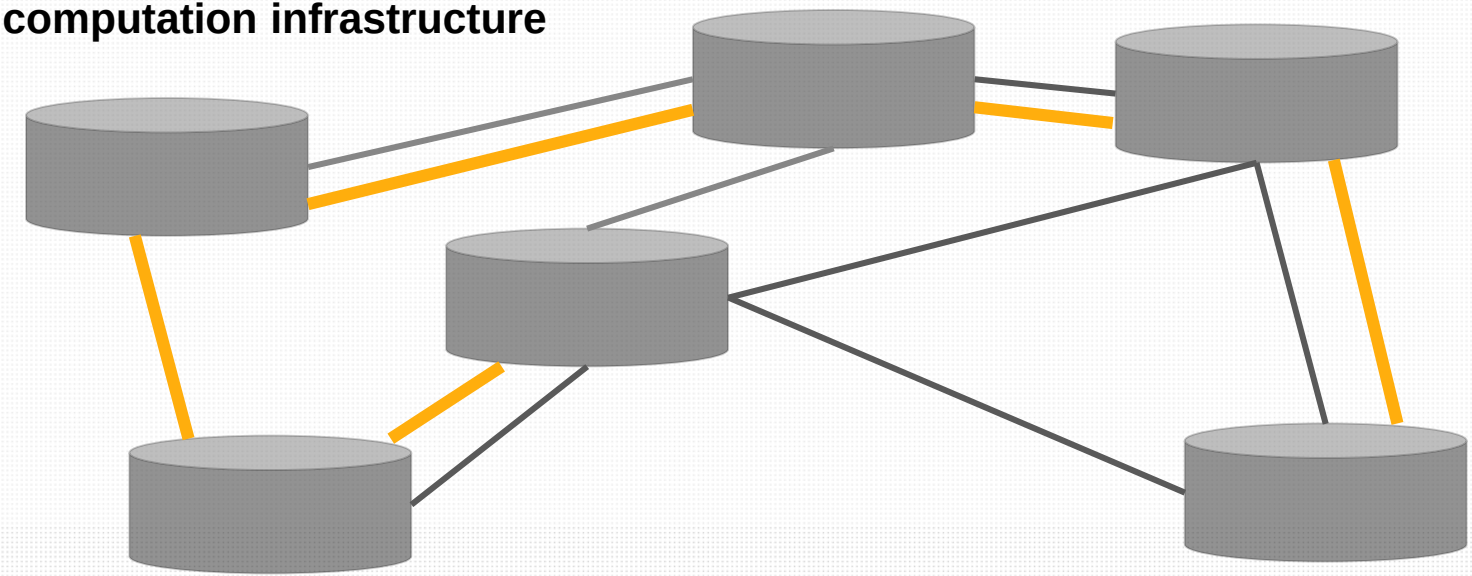
Dynamic (QKD) Networks

- **Crypto Subsystem as a feature and subsystem of a general communication/ computation infrastructure**



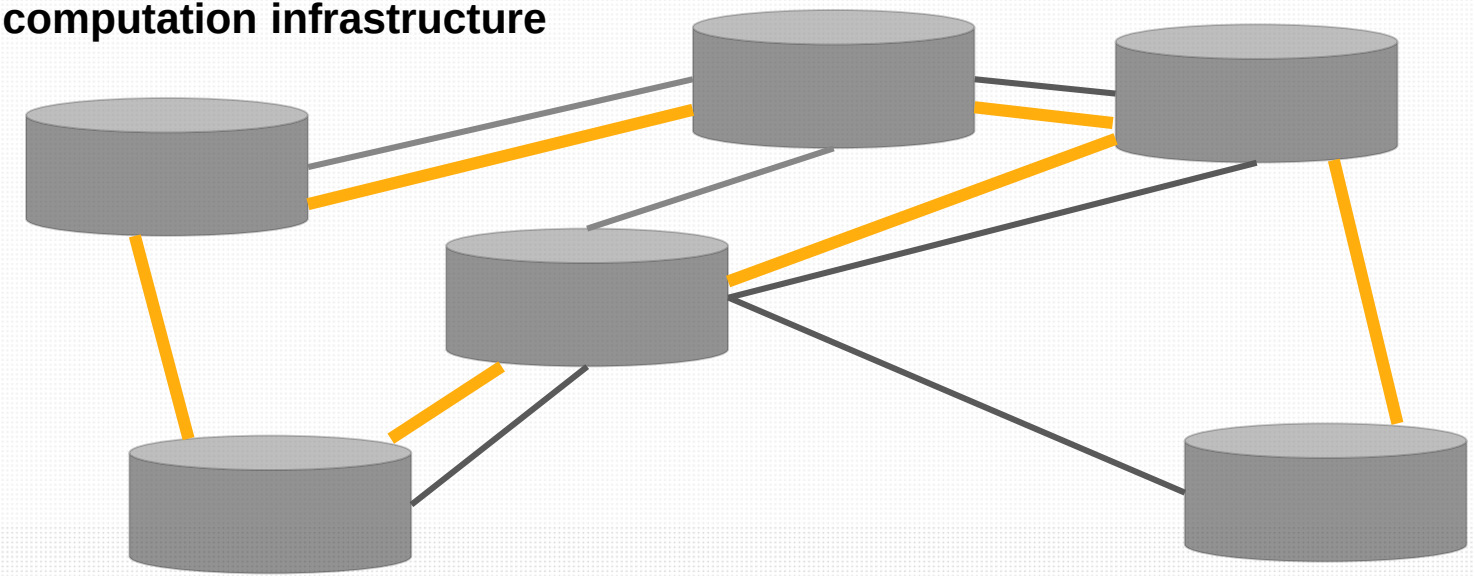
Dynamic (QKD) Networks

- **Crypto Subsystem as a feature and subsystem of a general communication/ computation infrastructure**



Dynamic (QKD) Networks

- **Crypto Subsystem as a feature and subsystem of a general communication/ computation infrastructure**



Outlook

- Most general QKD Networks should include QKD as a crypto enabling segment, not necessarily focus on network-wide key distribution alone
- Dynamic solutions would most probably be better served by a unified control & management
- Moreover, for such solutions QKD devices must be more general purpose, controllable and must fit in general network designs, not vice versa
- The security levels should follow a network-wide design rather than create ITS, super secure islands, awash in lower level security approaches
- Translate the fundamental constituents insight to a logical hierarchy: basic functions, functional layers, architectures, implementations
- New QKD Network Designs are necessary!

Thank you

www.huawei.com