Nino Walenta
Principal Research Scientist for Quantum Technologies
Battelle Memorial Institute
May 18, 2016

Certification of Quantum Cryptographic Network Security Devices

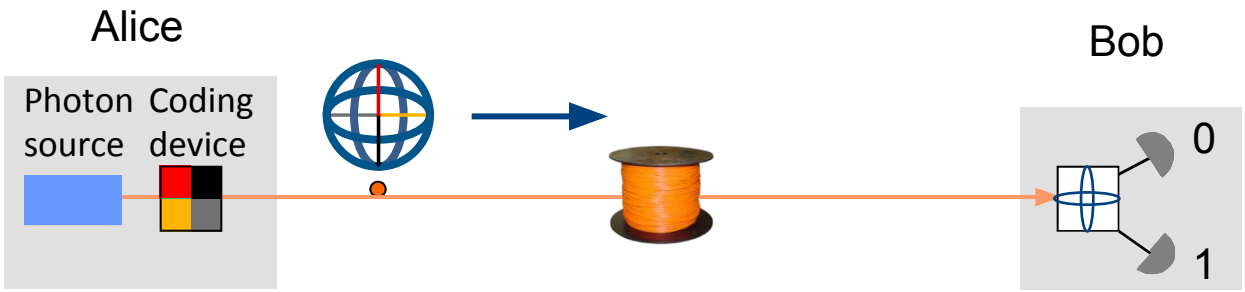
IDQ

Battelle
The Business of Innovation

Basics of Quantum Key Distribution

Quantum key distribution allows

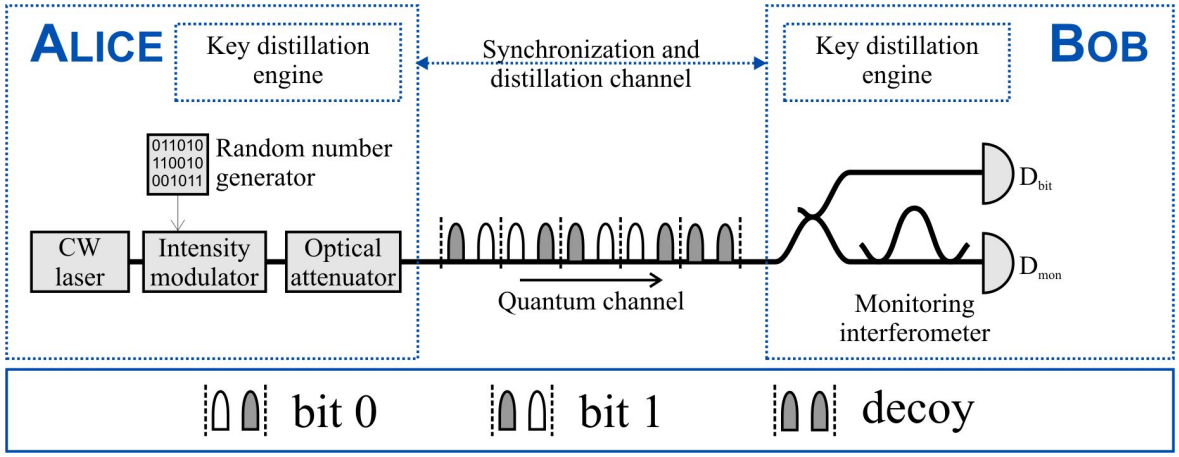
- continously expanding a **secret key shared** between Alice and Bob
- while measuring the information an **arbitrary powerful eavesdropper** could gain.



Quantum key distribution (Bennett and Brassard, 1984)

- **Idea:** - Encoding information in quantum states (Qubits)
- **Basis:** - No-cloning theorem for quantum states
  - Unavoidable perturbation through a measurement on an unknown quantum system
- **Aim:** - Distribution of a shared secret key and measurement of the information accessible to a potential eavesdropper about the key

The Coherent One-Way QKD Protocol

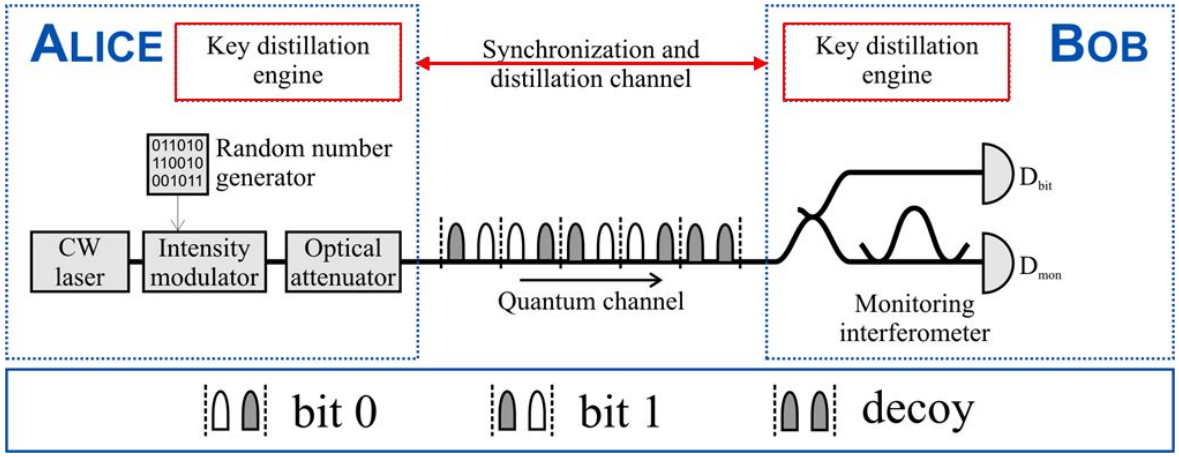


1. **Preparation**: Alice encodes information in sequence of pairs of weak coherent states
2. **Measurement**: Bob randomly chooses to measure either pulse arrival time (bit value) or coherence between successive pulses (eavesdropper's potential information about key)
3. **Sifting**: Bob tells Alice publicly, in which basis he measured (bit or coherence measurement), incompatible measurements are discarded

Eavesdropper who tries to measure bit value inevitably perturbs the sequence of quantum state and introduces errors in the coherence between successive time bins!

Appl. Phys. Lett. ***87****, 194108 (2005)*

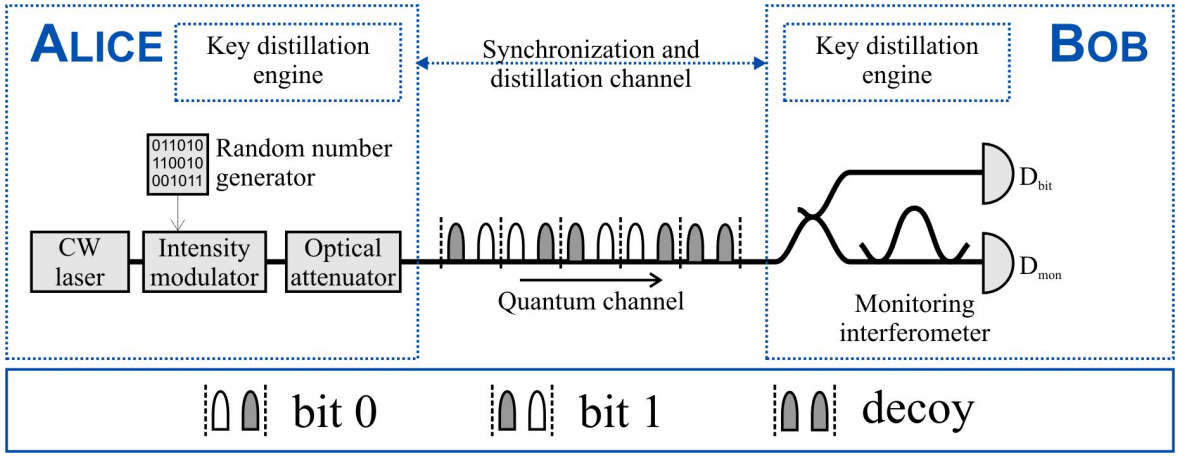
The Coherent One-Way QKD Protocol



1. **Preparation**: Alice encodes information in sequence of pairs of weak coherent states
2. **Measurement**: Bob randomly chooses to measure either pulse arrival time (bit value) or coherence between successive pulses (eavesdropper's potential information about key)
3. **Sifting**: Bob tells Alice publicly, in which basis he measured (bit or coherence measurement), incompatible measurements are discarded
4. **Error correction, parameter estimation and privacy amplification**: Alice and Bob eliminate quantum bit errors, measure and reduce eavesdropper's potential information about the key
5. **Authentication**: Alice and Bob verify integrity of public communication

Appl. Phys. Lett. ***87****, 194108 (2005)*

The Coherent One-Way QKD Protocol



Security parameter

$$\varepsilon = 4 \cdot 10^{-9}$$

- Specifies the probability that a QKD run failed.

Appl. Phys. Lett. ***87****, 194108 (2005)*

IDQ

Battelle
The Business of Innovation

Advantages and Limitations of QKD

Advantages of QKD

- Security based on fundamental physical principles instead of computational hardness
- Information-theoretically provable against most powerful adversaries:
  - Not weakened by quantum computing, mathematical discoveries, massively parallel computing networks
- Forward security:
  - Secret now – secret forever
- High key rates

Limitations of QKD

- Intrinsically point-to-point
  - Suitable for operations like secure data storage, disaster recovery
  - Less suitable for sharing keys between large number of users
- Distance limitations
  - Few hundred kilometer
  - Incremental increase expected through detector improvements (<400 km)
- No security certification standards yet

Quantum Hacking

Security fundamentals

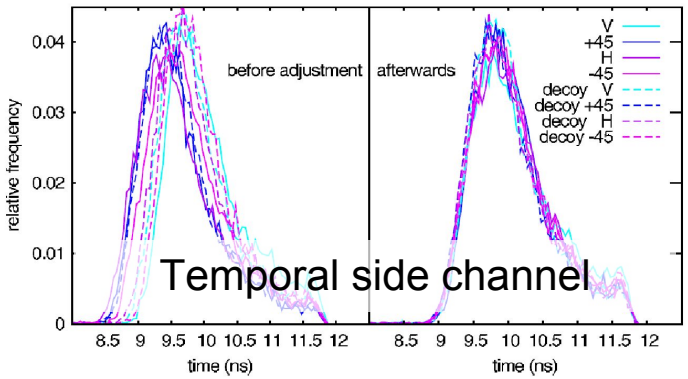
1. Eavesdropper mustn't have access to the QKD devices.
2. The random number generators must be (truly) random.
3. The service communication channel must be securely authenticated (Wegman-Carter).
4. Quantum hacking attacks the device implementation, not the underlying principle.
5. Quantum hacking is an active research area.

Attacks that are ineffective due to fundamental principles

- Fiber tapping ineffective due to single photons
- Man in the middle attack prevented by secure authentication
- Intercept-resend attack considered in security proofs

Practical attacks that require device characterization

- Side channel attacks
- Detector control attacks
- Trojan horse attacks
- Fake-state attacks (on certain implementations)



IDQ

Battelle
The Business of Innovation

QKD Standardization Efforts

Quantum-Safe Security Working Group at Cloud Security Alliance

- "Influence, set and promote standards and certification procedures for adoption and implementation of quantum-safe technologies"
- Bring quantum cryptography solutions into a traditional security framework
- 94 members from over 40 organizations and enterprises

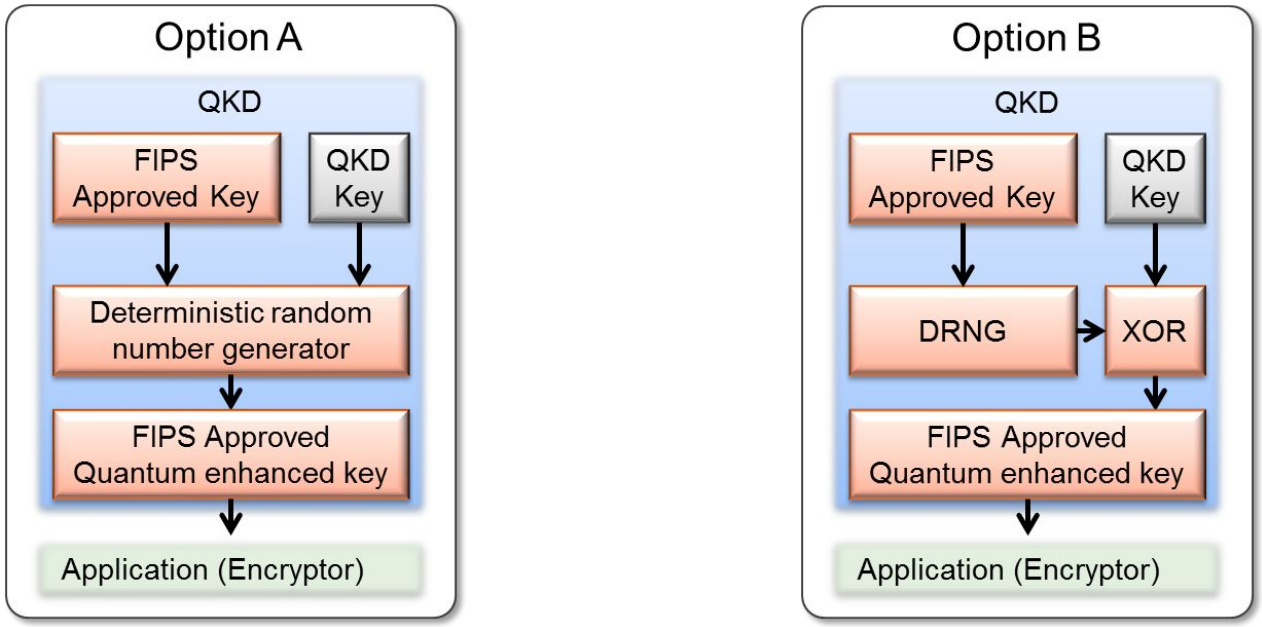
ETSI's „pragmatic approach"

- Develop implementation standards for quantum technology, based on FIPS 140
- Defines a process based on current QKD security proof techniques to quantitatively assesses the discrepancy between a real system and an ideal model systems
- Derivation of a detailed generic catalogue of security relevant properties for QKD systems
- 24 members from academia and industry

FIPS 140-2: Scopes of Requirements & QKD

FIPS 140-2 defines eleven areas that are evaluated in order to receive a validation certificate	
Cryptographic module specification	*What must be documented*
Cryptographic key management	*Generation, entry, output, storage and destruction of keys*
Ports and interfaces	*What information flows in and out, and how it's segregated*
Physical security	*Tamper evidence and resistance, robustness against extreme environmental conditions*
Roles, services and authentication	*Who can do what with the module, and how this is checked*
Self-tests	*What must be tested and when, and what must be done if a test fails*
Finite state model	*Documentation of the high-level states the module can be in, and how transitions occur*
EMI/EMC	*Electromagnetic interference and compatibility*
Operational environment	*What sort of operating system the module uses and is used by*
Design assurance	*Documentation that module is well designed and implemented*
Mitigation of other attacks	*If module mitigates other attacks, documentation must say how*

Certification Strategies for QKD



Option A: QKD seeds DRBG as approved key generation method

- QKD key is used as seed/reseed, resulting in an approved quantum enhanced key
- FIPS approved key needs to be secretly shared by both QKD stations
- **Information-theoretical security lost due to DRBG assumptions**

Proc. of SPIE **9648**, 96480U (2015)

QKD Device Security

Front panel

- QKD quantum and service channels
- Initial key data input
- Key output to consumer device
- Configuration, monitoring and operator ports
- FIPS mode status LEDs

ATCA ports

- ATCA fan speed and temperature control
- Enc… KCs
- Phy…

Detectors

- Physically encapsulated
- Require cooling to -40°C
- Enclosure supports cooling

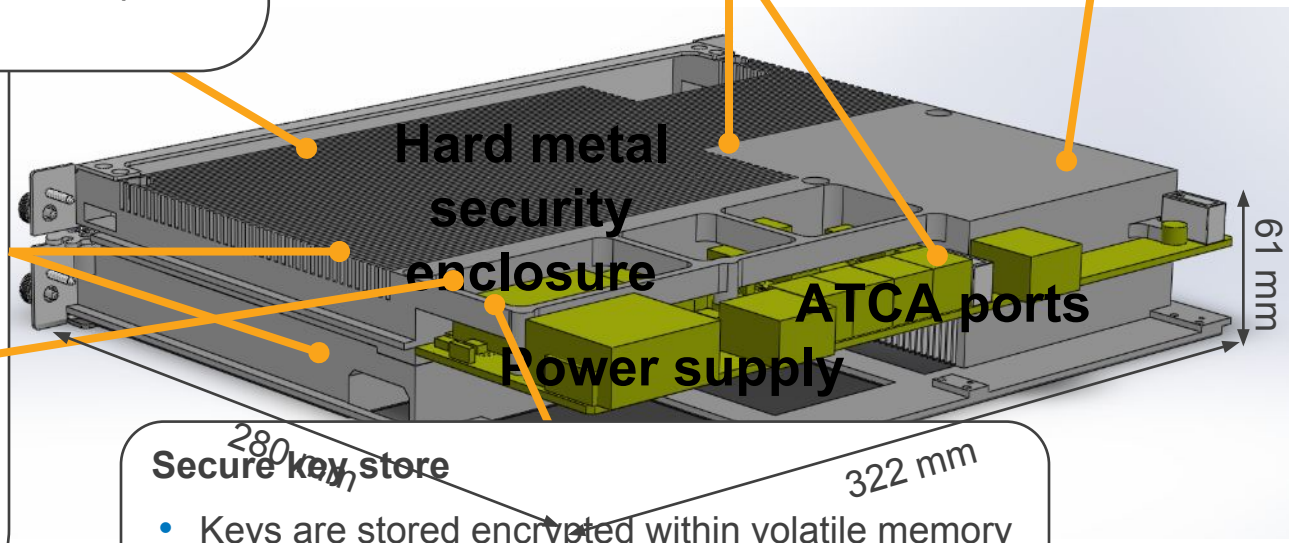
QRNG

- Certified random number generator based on quantum randomness

- Hard, opaque material
- Tamper evident and

Secure Memory and Tamper Detection

- Securely stores critical security parameters
- Tamper processing and zeroization
- On tamper detect all CSPs are overwritten multiple times



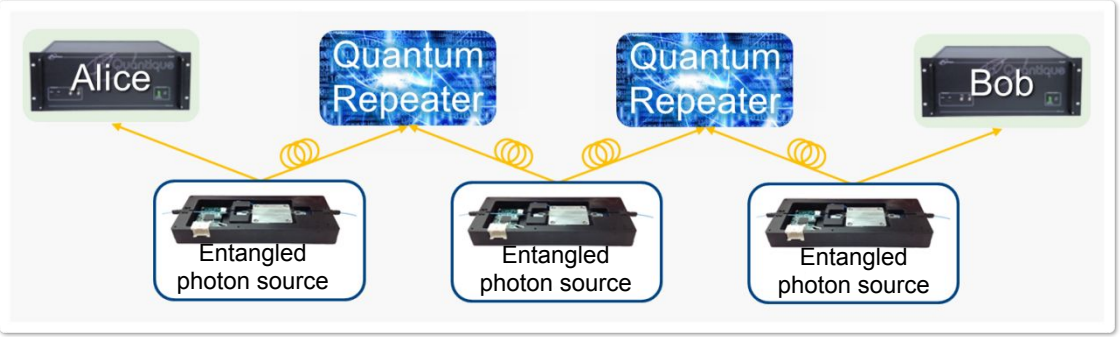
Secure key store

- Keys are stored encrypted within volatile memory
- Zeroization of key encryption key render key store unusable

R. Anderson, "Security Engineering". Wiley, ISBN 978- 0470068526 (2008).

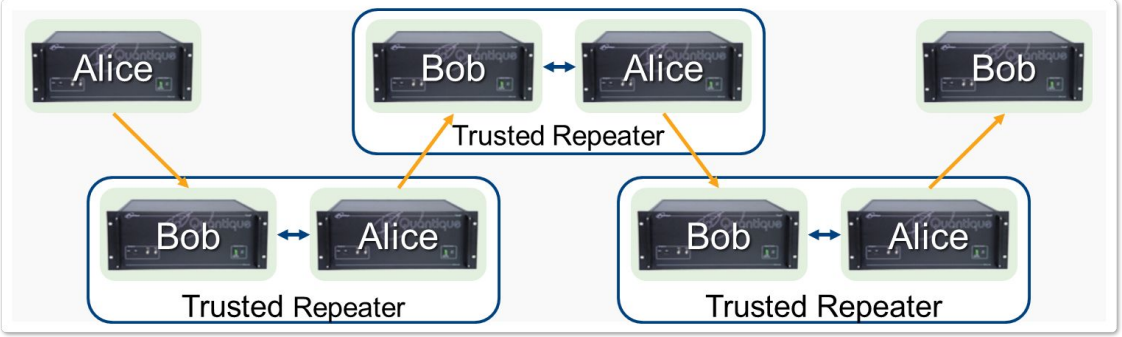
Overcoming the Distance Limit of QKD

Quantum repeater networks



- Based on quantum teleportation and Bell state measurements
- Require entangled photons and quantum memories

Trusted repeater networks



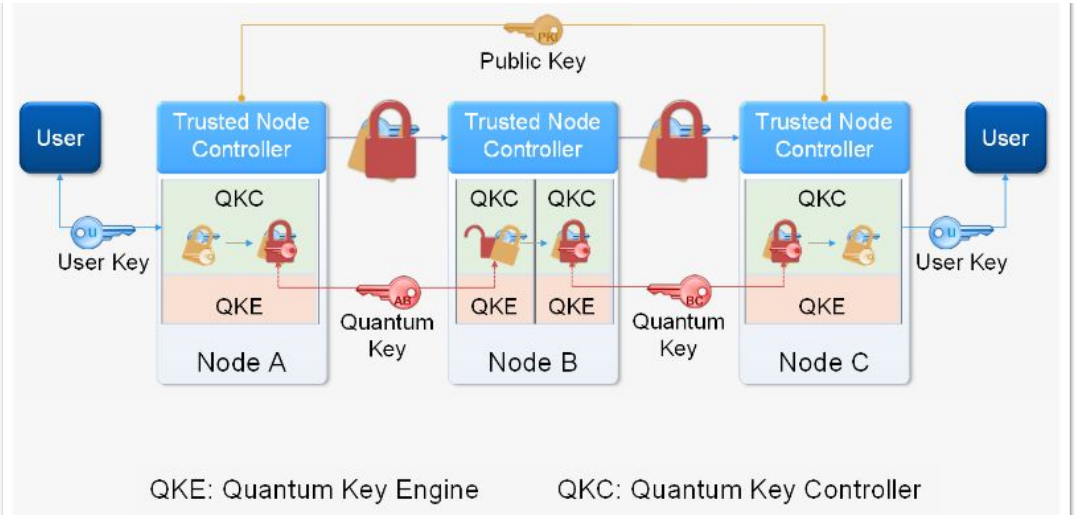
- Relay of QKD keys in intermediate nodes
- Nodes have to be trusted
- Any network topology possible

Battelle's Trusted Node QKD System

Overview

- Can realize any network topology with arbitrary number of nodes and user devices, separated by up to 100 km
- Current Quantum Key Engine based on the COW-QKD protocol, but in general independent of QKD protocol
- Builds on the ATCA telecommunication architecture
- For the first time, targets compliance of QKD with the FIPS 140-2 security certification standards

QKD-secured transport of user keys

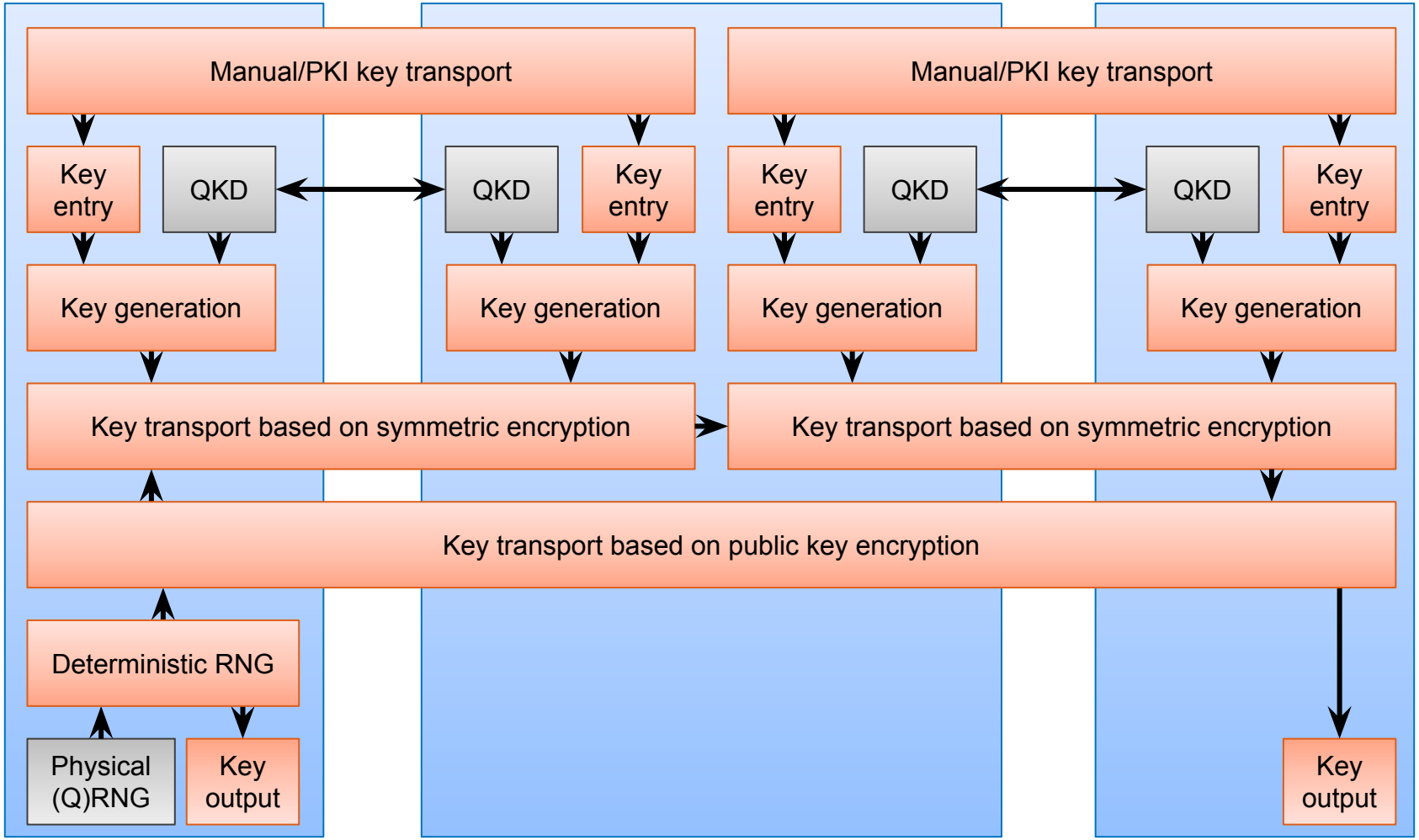


User keys move securely across the network in a piece-wise fashion:

- User keys *U* are first encrypted by public key cryptography *PK*
- Then hop from node to node while they are additionally encrypted using quantum keys *QK* with symmetric encryption
- Fault tolerant dynamic routing algorithm finds least cost path across the network and uses alternate routes when available

Proc. of SPIE **9648**, 96480U (2015)

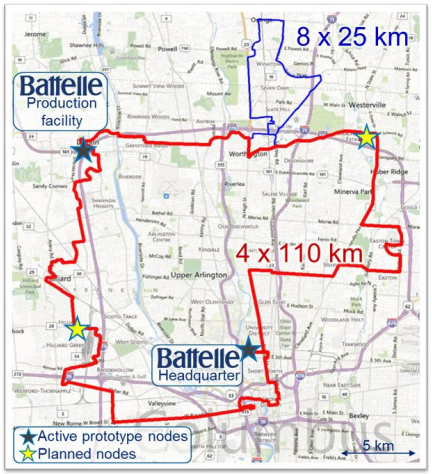
FIPS 140-2 compliant quantum-secured key transfer



Proc. of SPIE **9648**, 96480U (2015)

Summary

1. QKD provides highly secure symmetric keys with strong forward security that is resilient against future attacks, improved attack algorithms, and the emergence of quantum computers.
2. QKD can be rendered compliant with FIPS 140-2.
3. QKD networks circumvent the distance and point-to-point limitations of QKD and are emerging all around the world.



IDQ

Battelle
The Business of Innovation