Talk at Norsk kryptoseminar, Trondheim, 8 September 2015 (now), by Vadim Makarov

Norsk kryptoseminar, 17-18. oktober 2002. NTNU, Trondheim

NTNU

Quantum Cryptography

Vadim Makarov and Dag R. Hjelme

Institutt for fysikalsk elektronikk   NTNU

www.vad1.com/qcr/

NTNU   SINTEF Electronics and Cybernetics   Telenor FoU

Trondheim 2002

Has anything changed since 2002?

QKD is commercial Market: tiny

Deployed in networks

Implementation security is taken seriously

Quantum computer *not* built Market: 2 sold*

Factorization records: 15 (2001)

21 (2012)

56153 (2014)**

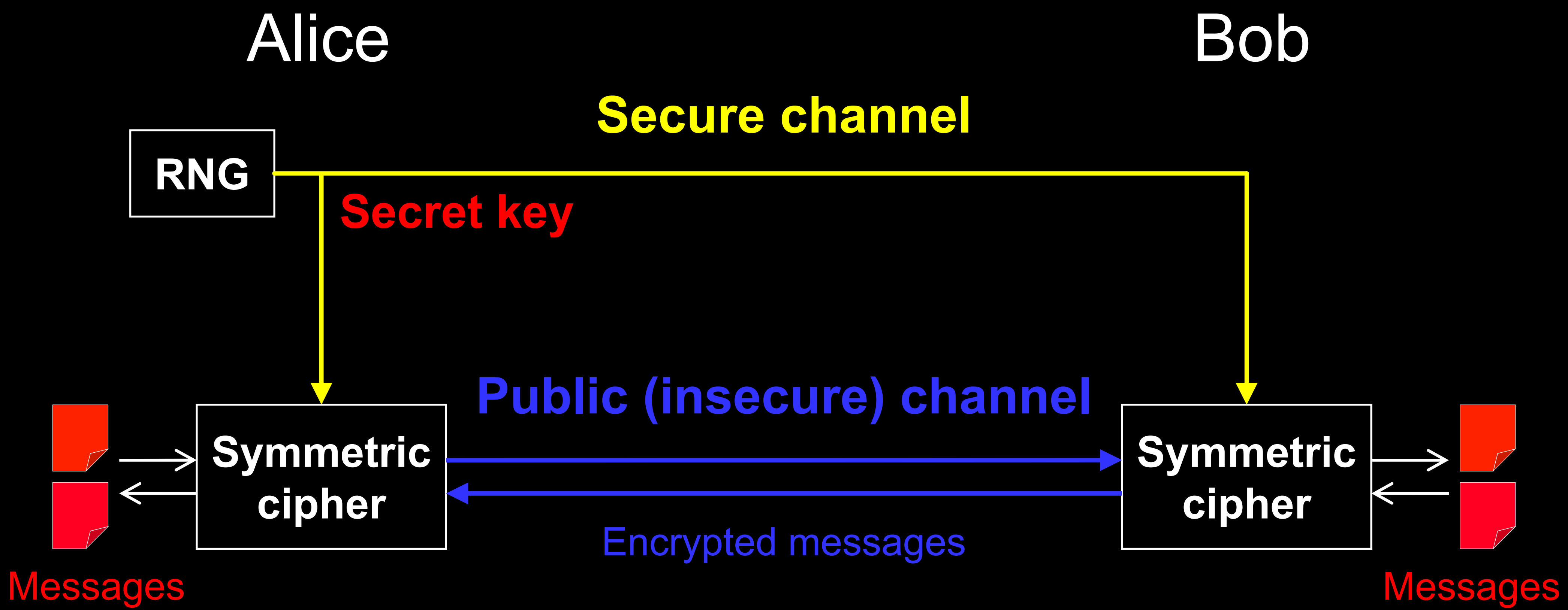
Steady improvement in experiment and theory

Several communication primitives with decisive quantum advantages

* D-Wave, not really a quantum computer?

** Not by Shor's algorithm

Encryption and key distribution



Public key cryptography

E.g., RSA (Rivest-Shamir-Adleman)

Elliptic-curve

Based on *hypothesized* one-way functions

- Unexpected advances in classical cryptanalysis
- Shor's factorization algorithm for quantum computer

P. W. Shor, SIAM J. Comput. **26**, 1484 (1997)

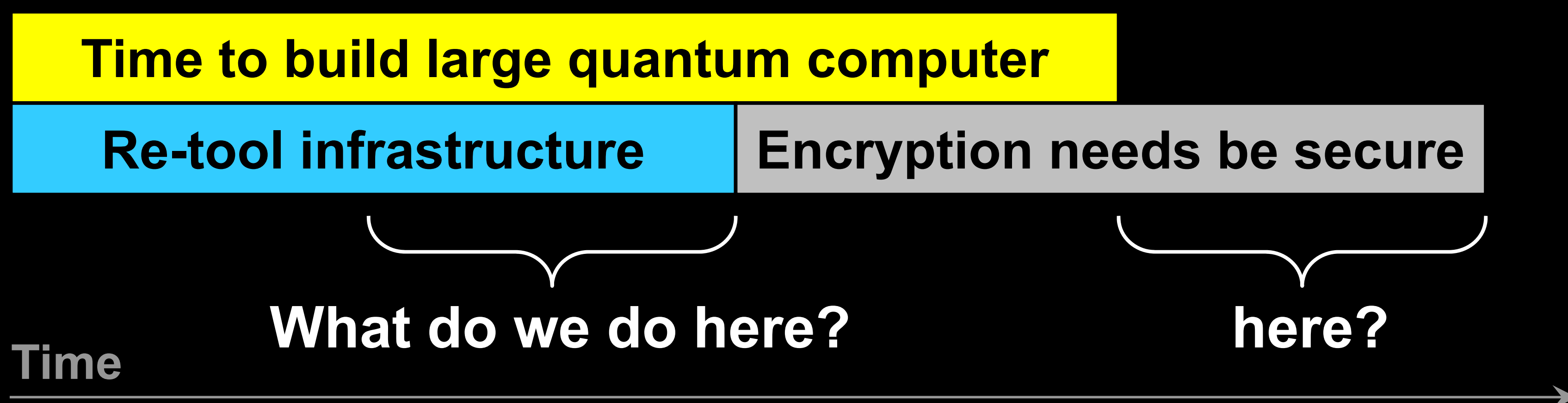


Diagram courtesy M. Mosca

How close is quantum computer?

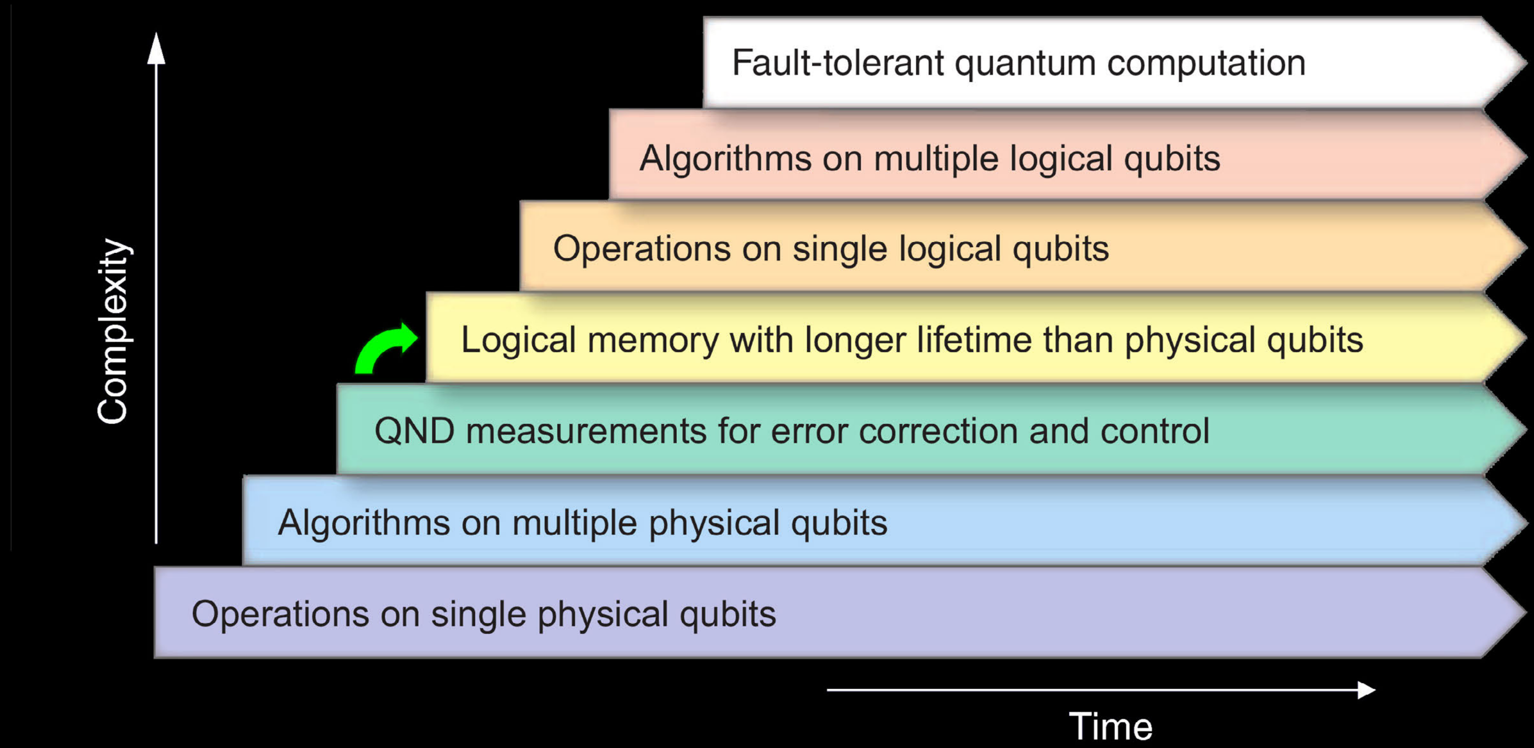


Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they now aim at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit components.

M. H. Devoret, R. J. Schoelkopf, Science **339**, 1169 (2013)

How close is quantum computer?

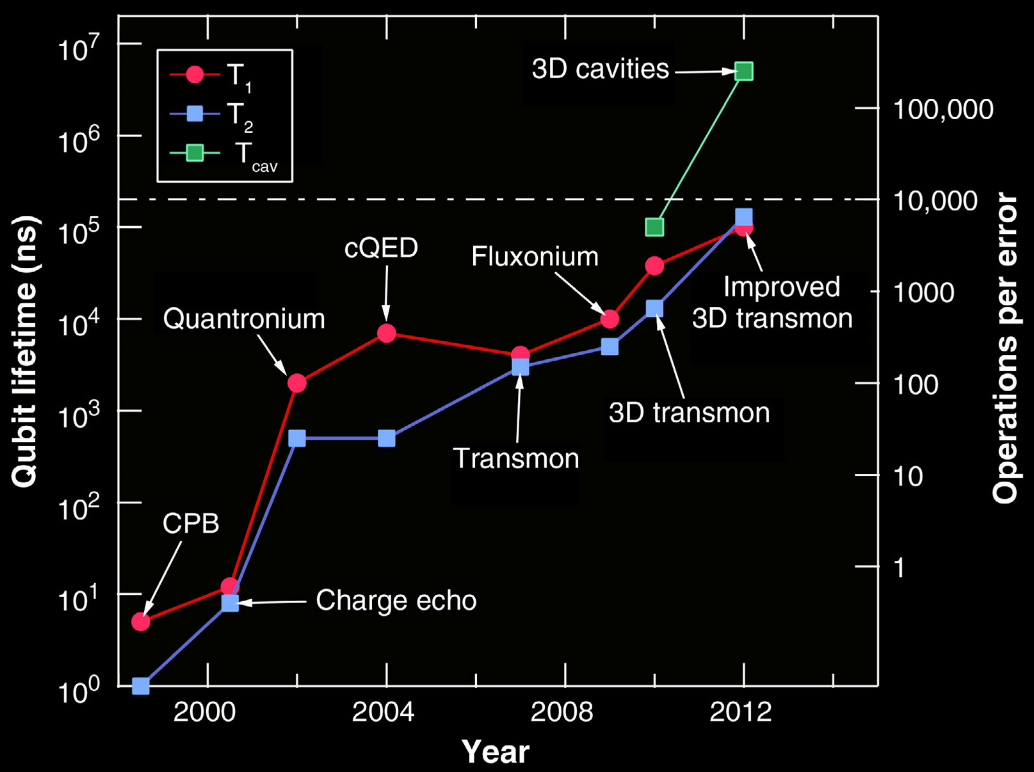


Fig. 3. Examples of the "Moore's law" type of exponential scaling in performance of superconducting qubits during recent years.

Improvement of coherence times for the "typical best" results associated with the first versions of major design changes. The blue, red, and green symbols refer to qubit relaxation, qubit decoherence, and cavity lifetimes, respectively. Innovations were introduced to avoid the dominant decoherence channel found in earlier generations. So far an ultimate limit on coherence seems not to have been encountered.

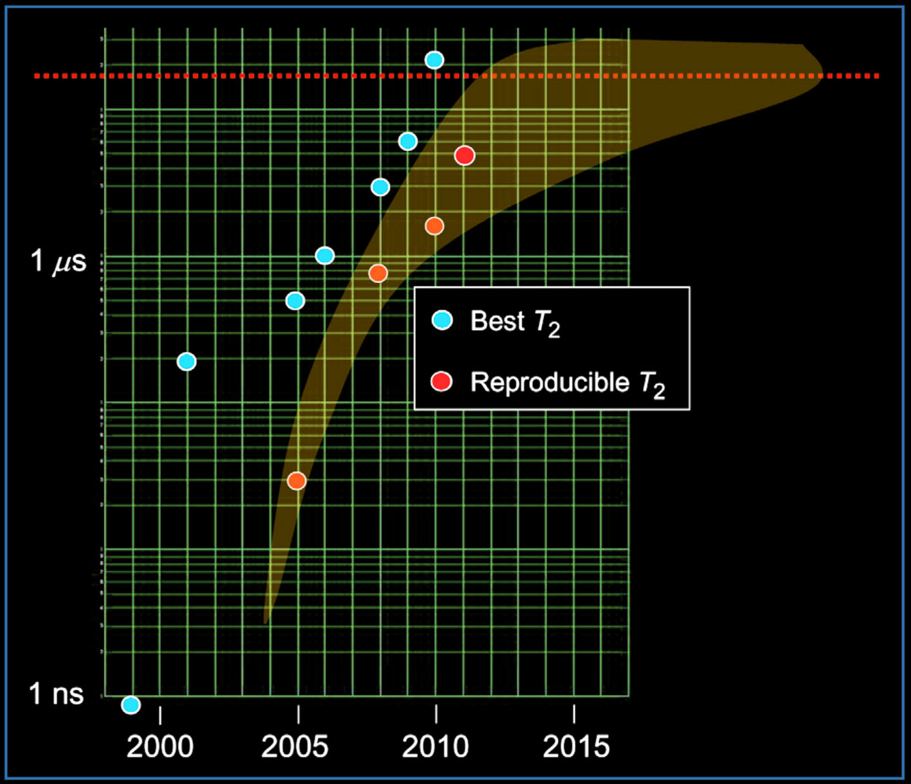


Figure 5

Progress toward reaching long dephasing (T_2) times for superconducting qubits. (Red dashed line) Minimum necessary for fault-tolerant quantum computer, based on a 30-ns two-gate time. (Yellow field) Predicted improvements in T_2.

M. H. Devoret, R. J. Schoelkopf, Science **339**, 1169 (2013)

M. Steffen *et al.*, "Quantum computing: An IBM perspective," IBM J. Res. Dev. **55**, 13 (2011)

Quantum computers capable of catastrophically breaking our public-key cryptography infrastructure are a medium-term threat.

Quantum-safe cryptographic infrastructure

"post-quantum" cryptography + quantum cryptography

"post-quantum" cryptography

- Classical tools deployable without quantum technologies
- Believed/hoped to be secure against quantum computer attacks of the future

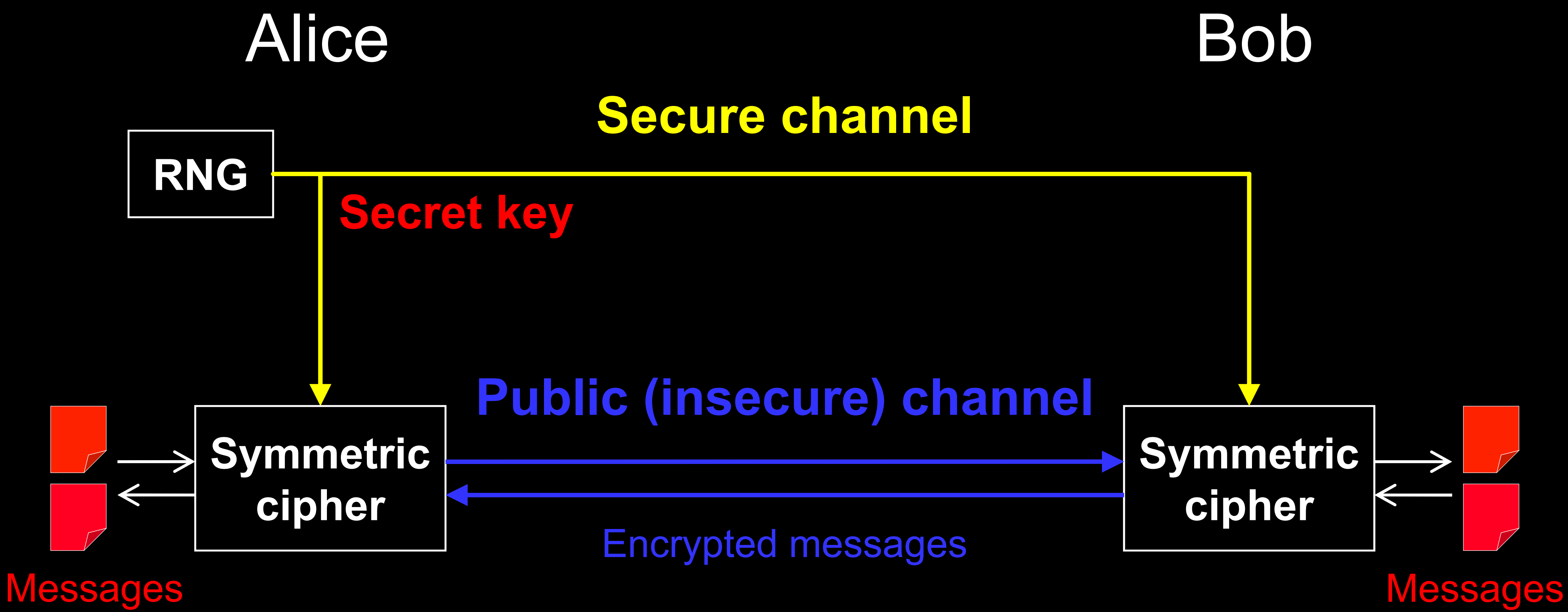
quantum cryptography

- Quantum tools requiring some quantum technologies (typically less than a large-scale quantum computer)
- Typically no computational assumptions and thus known to be secure against quantum attacks

Both sets of cryptographic tools can work very well together in quantum-safe cryptographic ecosystem.

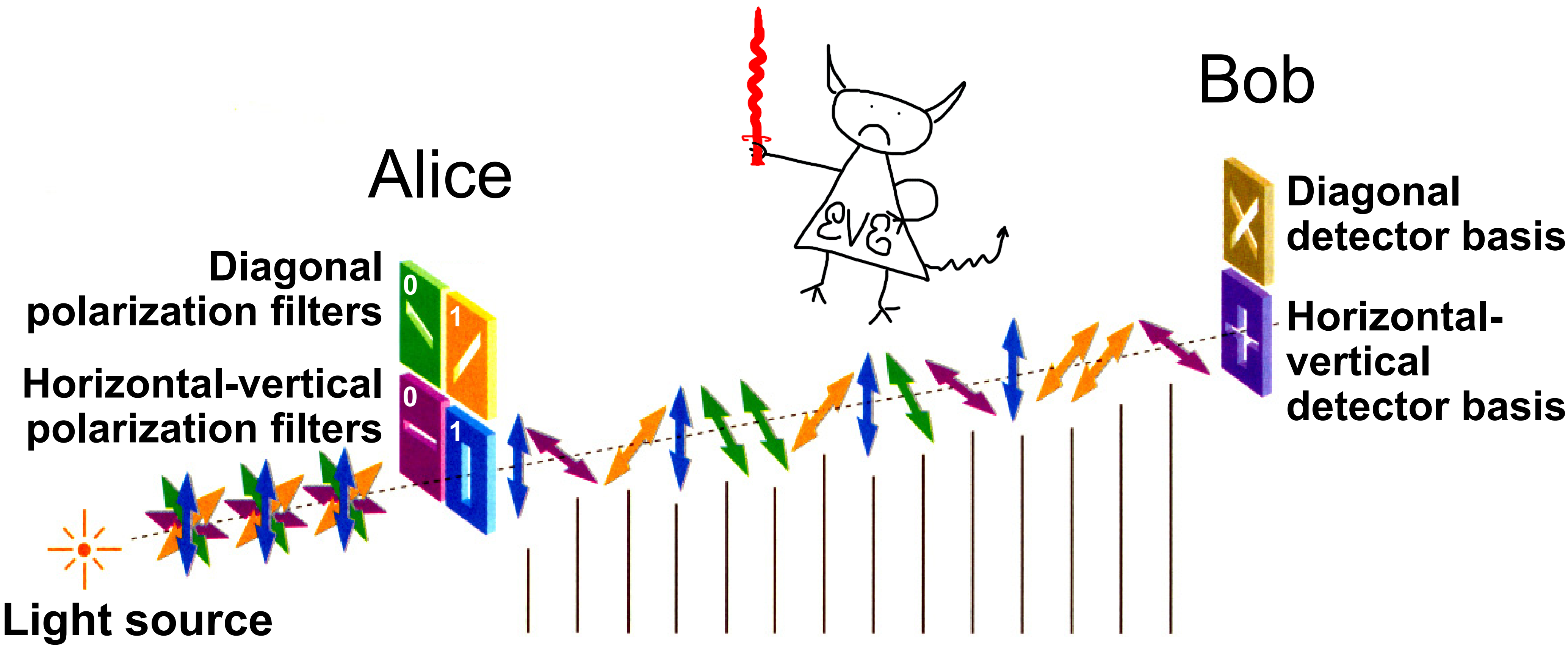
Slide courtesy M. Mosca

Encryption and key distribution



Quantum key distribution transmits secret key by sending quantum states over *open channel.*

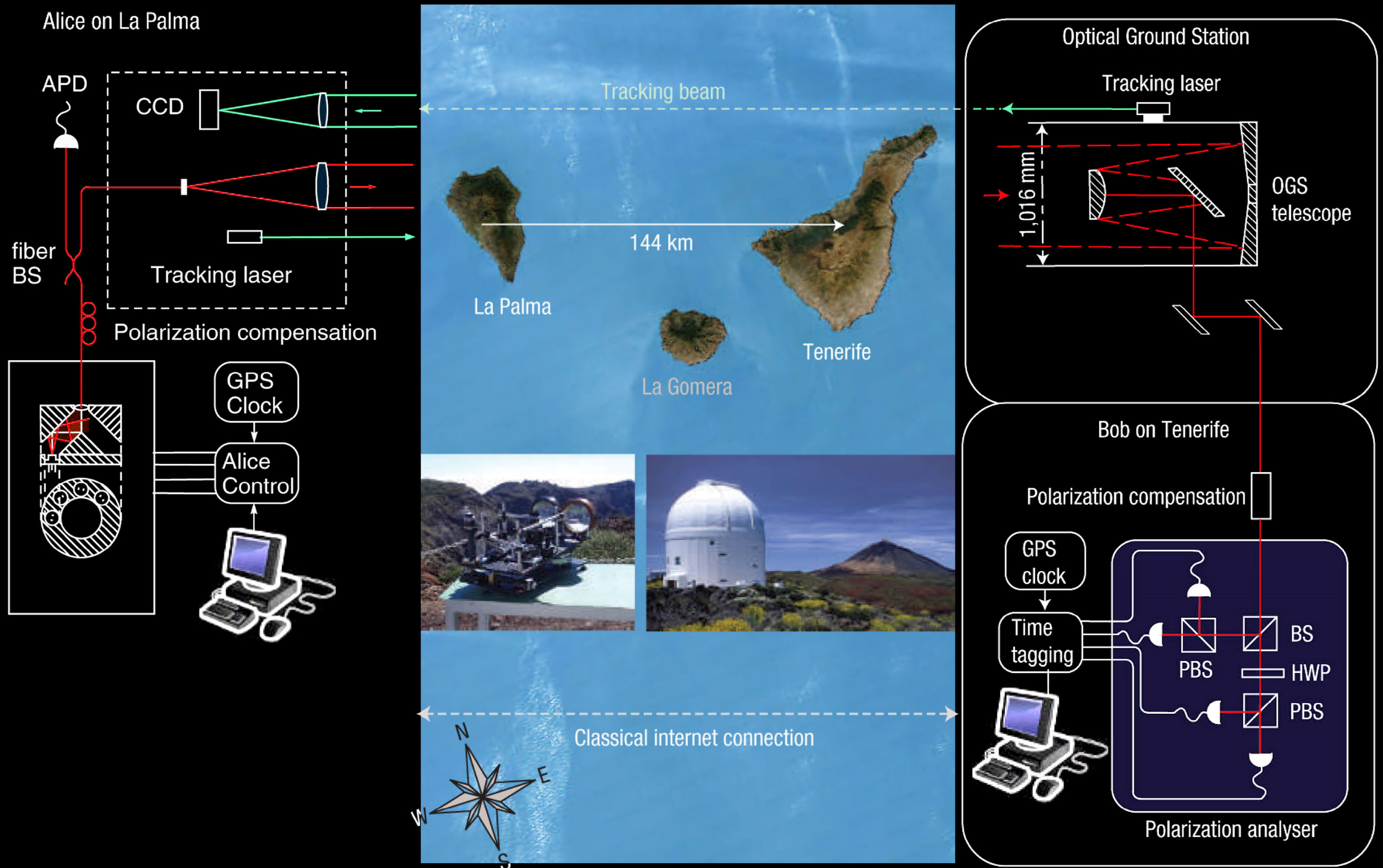
Quantum key distribution (QKD)



Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Bob's detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+
Bob's measurement	1	0	0	1	0	0	1	1	0	0	0	1	0	0
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0

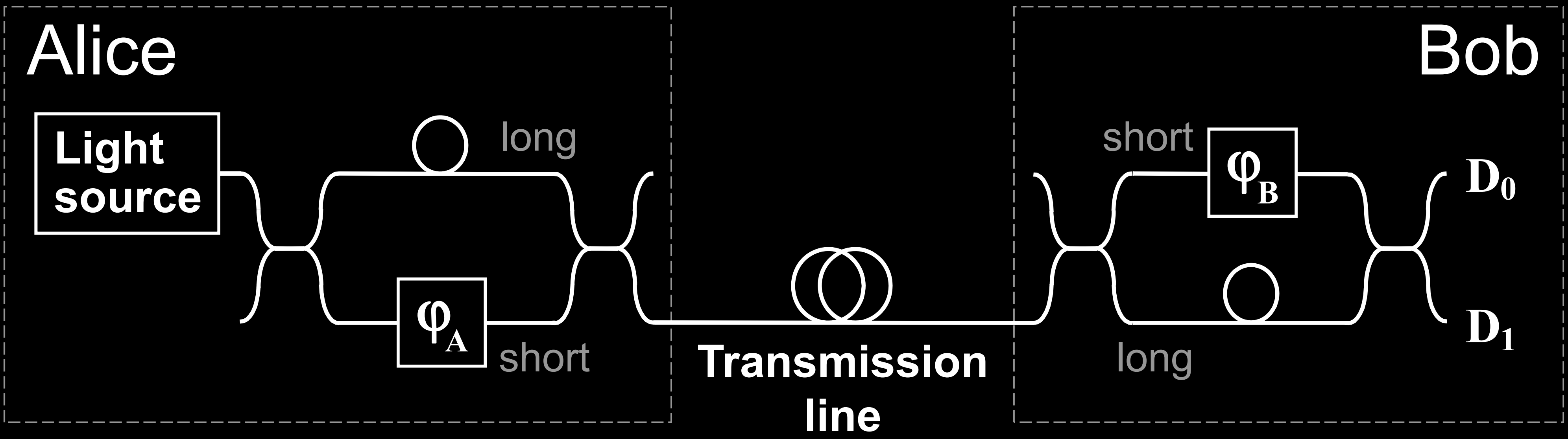
Image reprinted from article: W. Tittel, G. Ribordy & N. Gisin, "Quantum cryptography," Physics World, March 1998

Free-space QKD



T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007)

Phase encoding, interferometric QKD channel



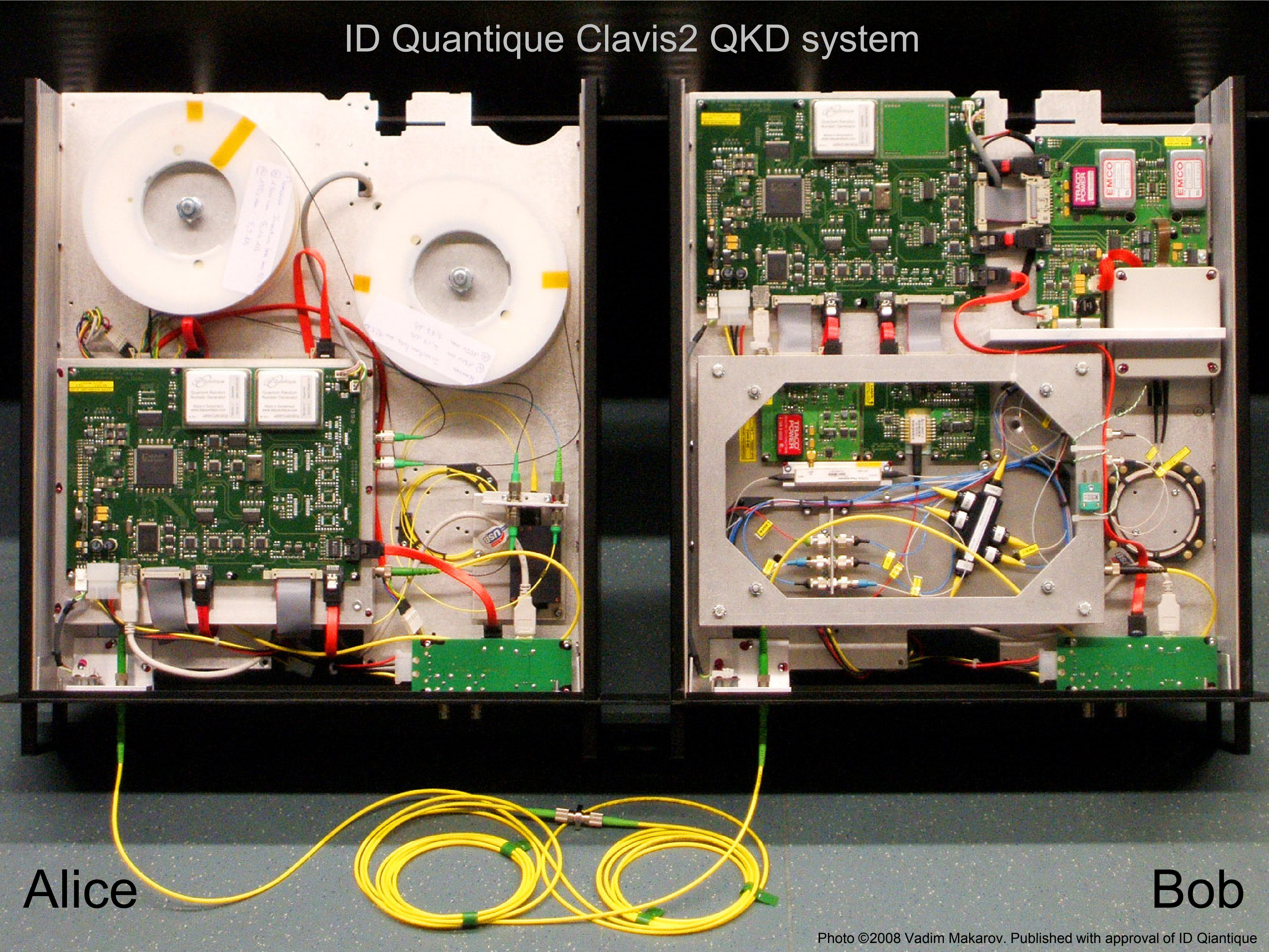
Detection basis:

$\varphi_A =$ 0 or $\pi/2$: 0

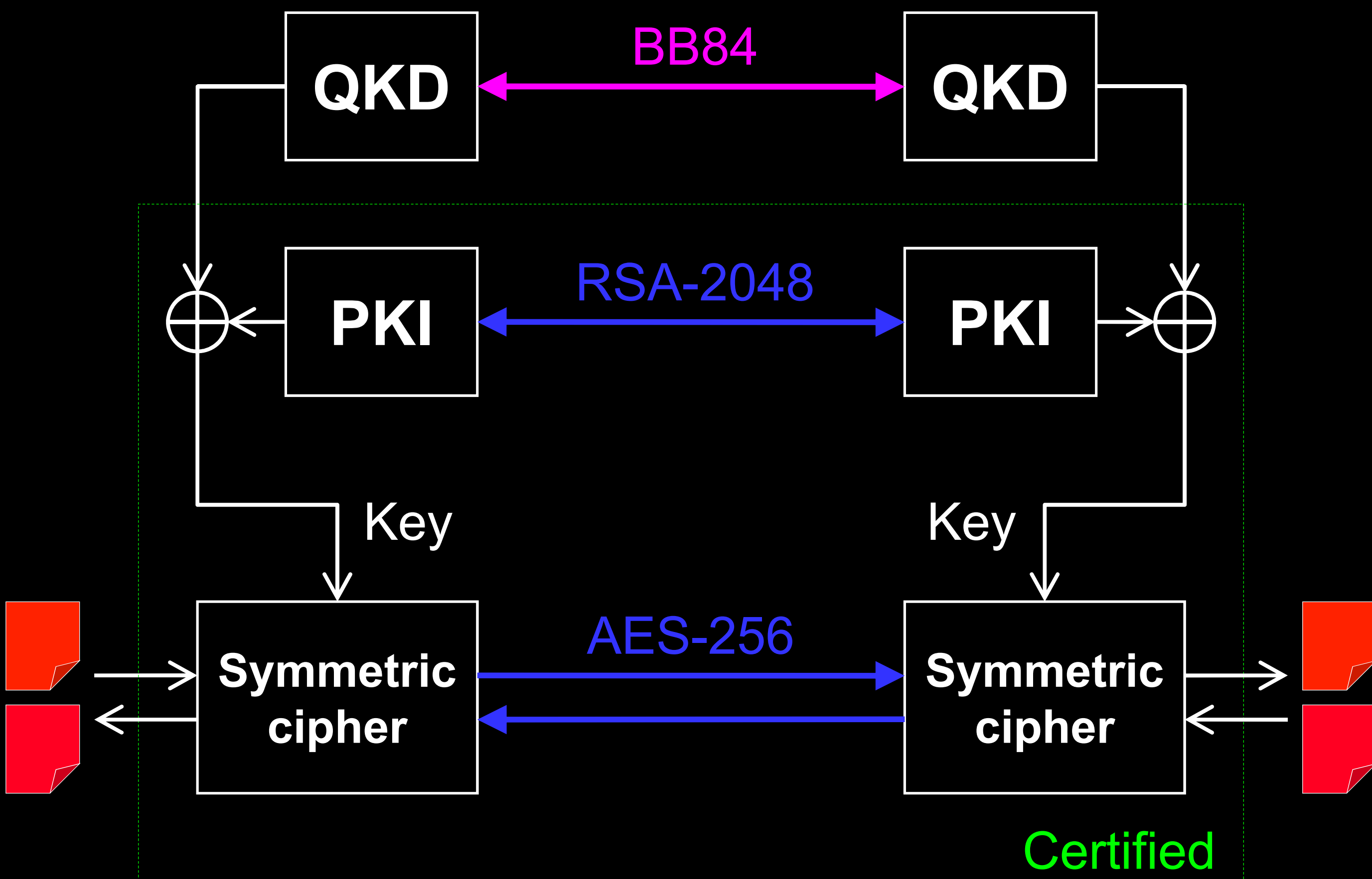
π or $3\pi/2$: 1

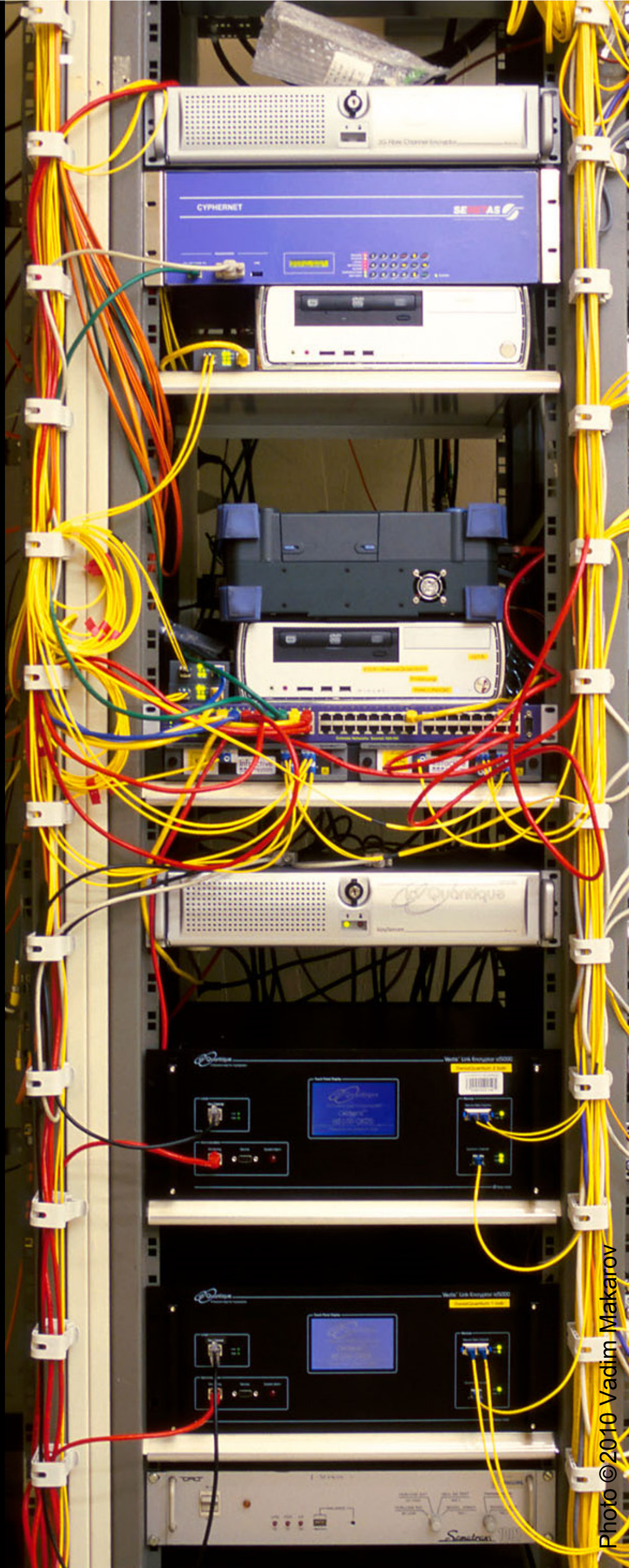
$\varphi_B =$ 0 : X

$\pi/2$: Z


ID Quantique Clavis2 QKD system
Alice
Bob
Photo ©2008 Vadim Makarov. Published with approval of ID Qiantique

Dual key agreement





www.swissquantum.com
ID Quantique *Cerberis* system (2010)

Commercial QKD

Classical encryptors:

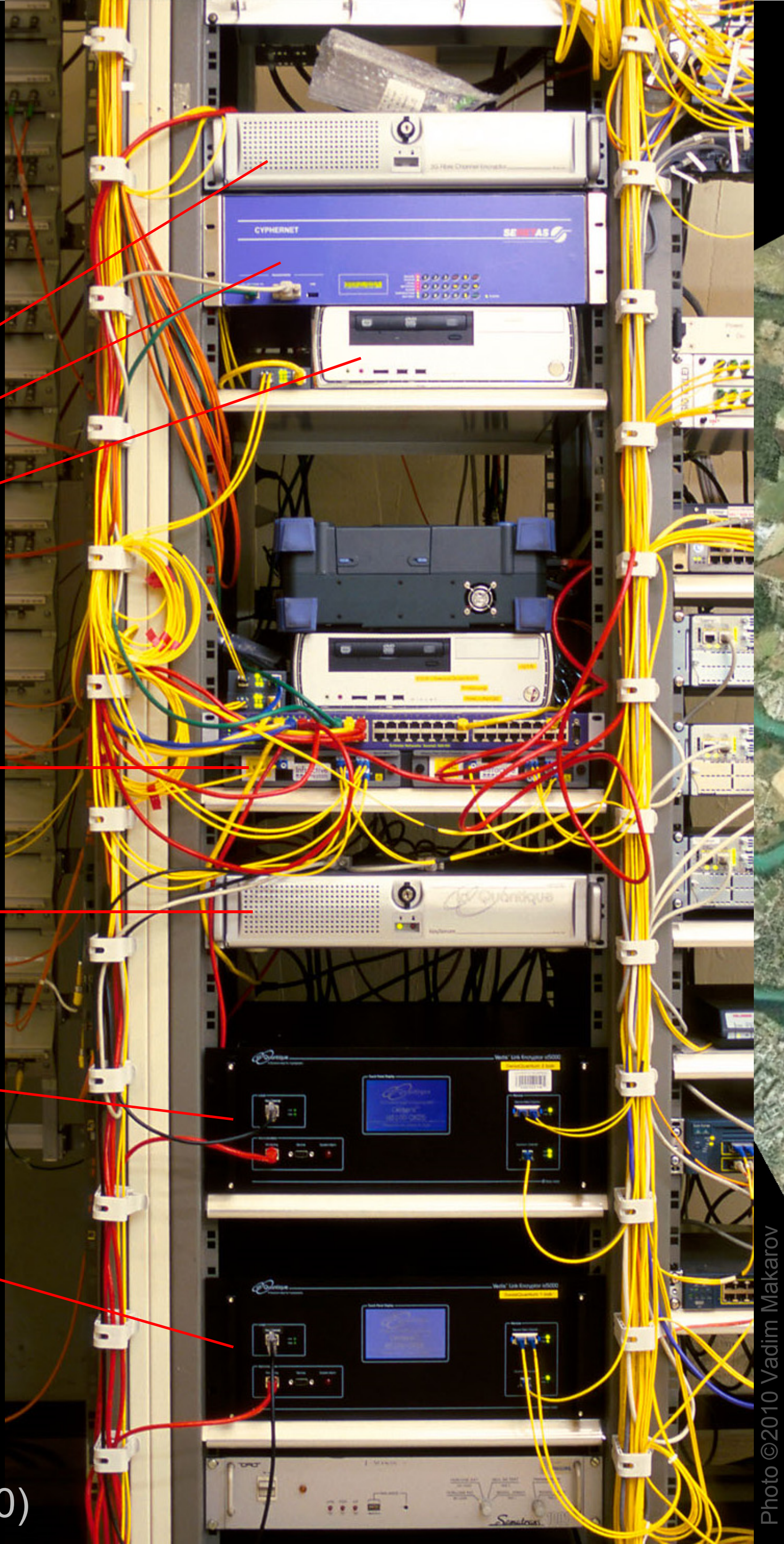
L2, 2 Gbit/s
L2, 10 Gbit/s
L3 VPN, 100 Mbit/s

WDMs

Key manager

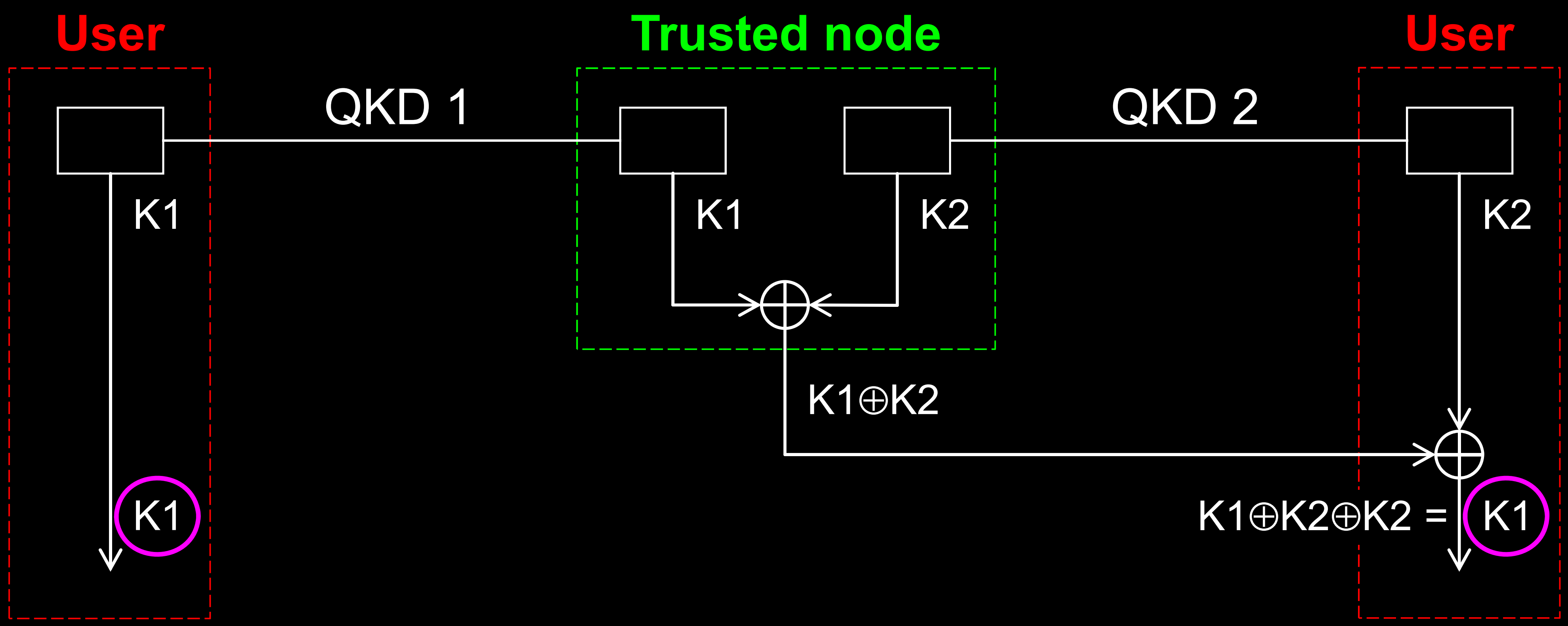
QKD to another node (4 km)

QKD to another node (14 km)

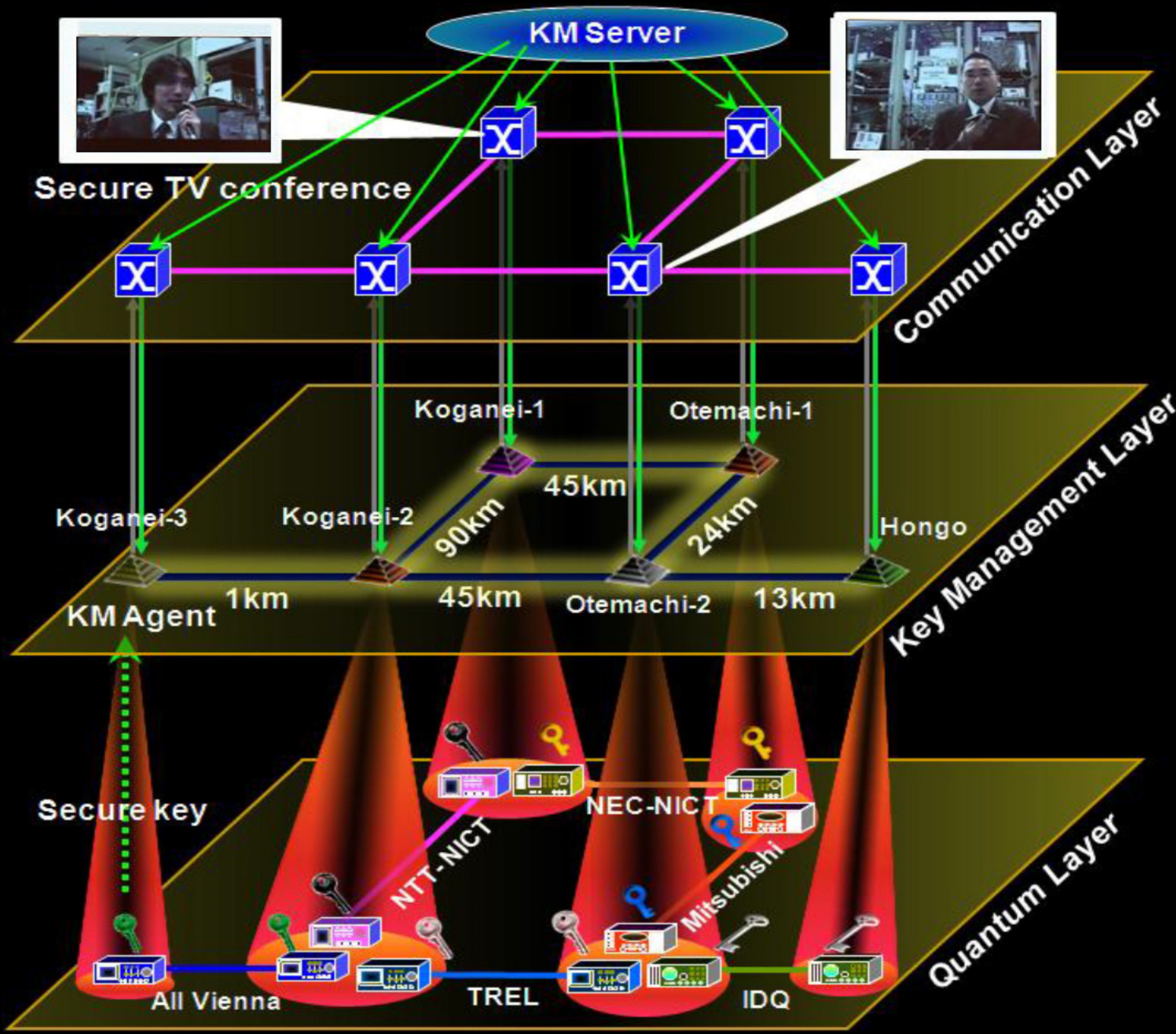


www.swissquantum.com
ID Quantique *Cerberis* system (2010)

Trusted-node repeater



Trusted-node network



M. Sasaki *et al.*, Opt. Express **19**, 10387 (2011)

Quantum Backbone

- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes

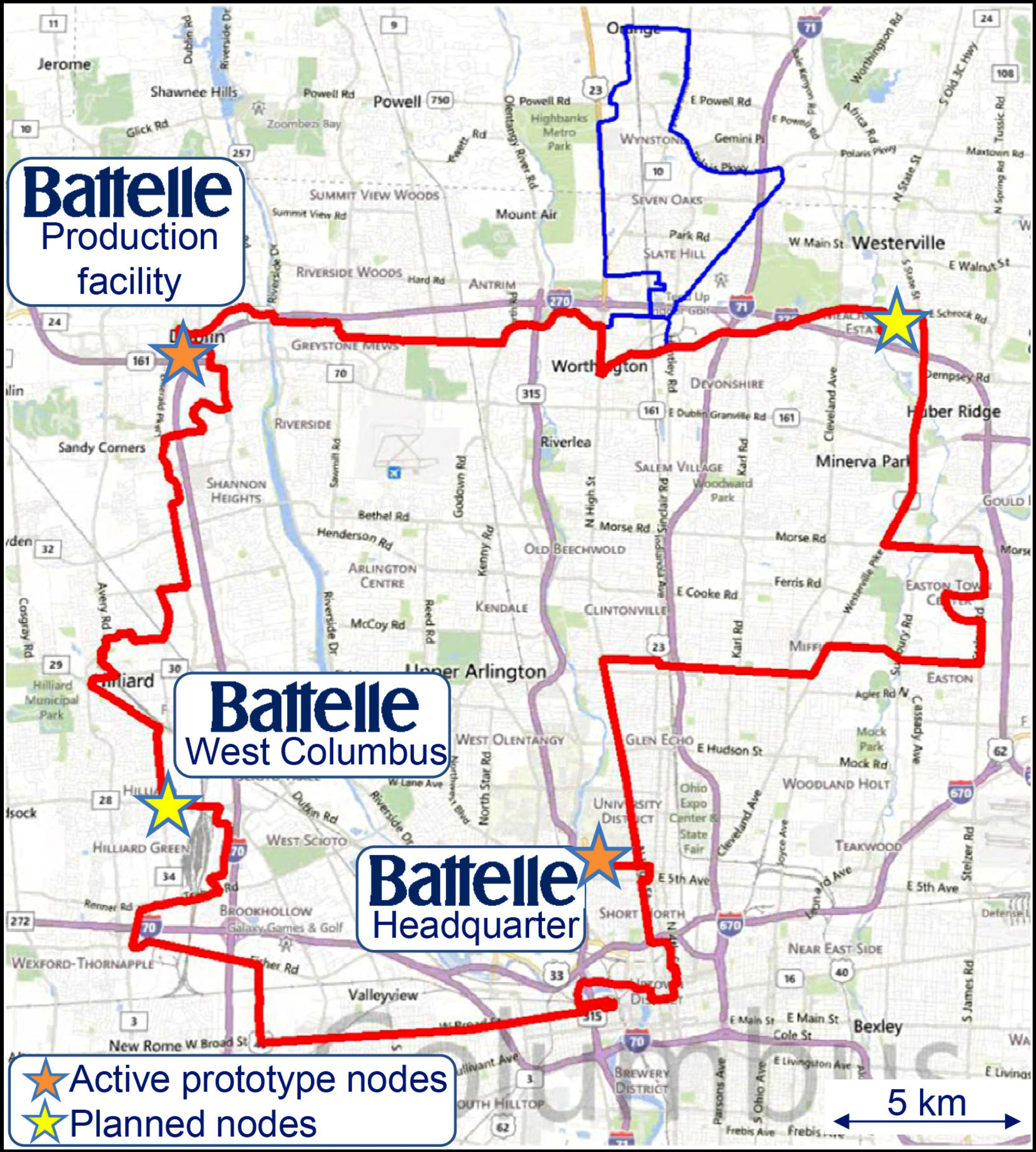
  31 fiber links
- Metropolitan networks

  Existing: Hefei, Jinan

  New: Beijing, Shanghai
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC

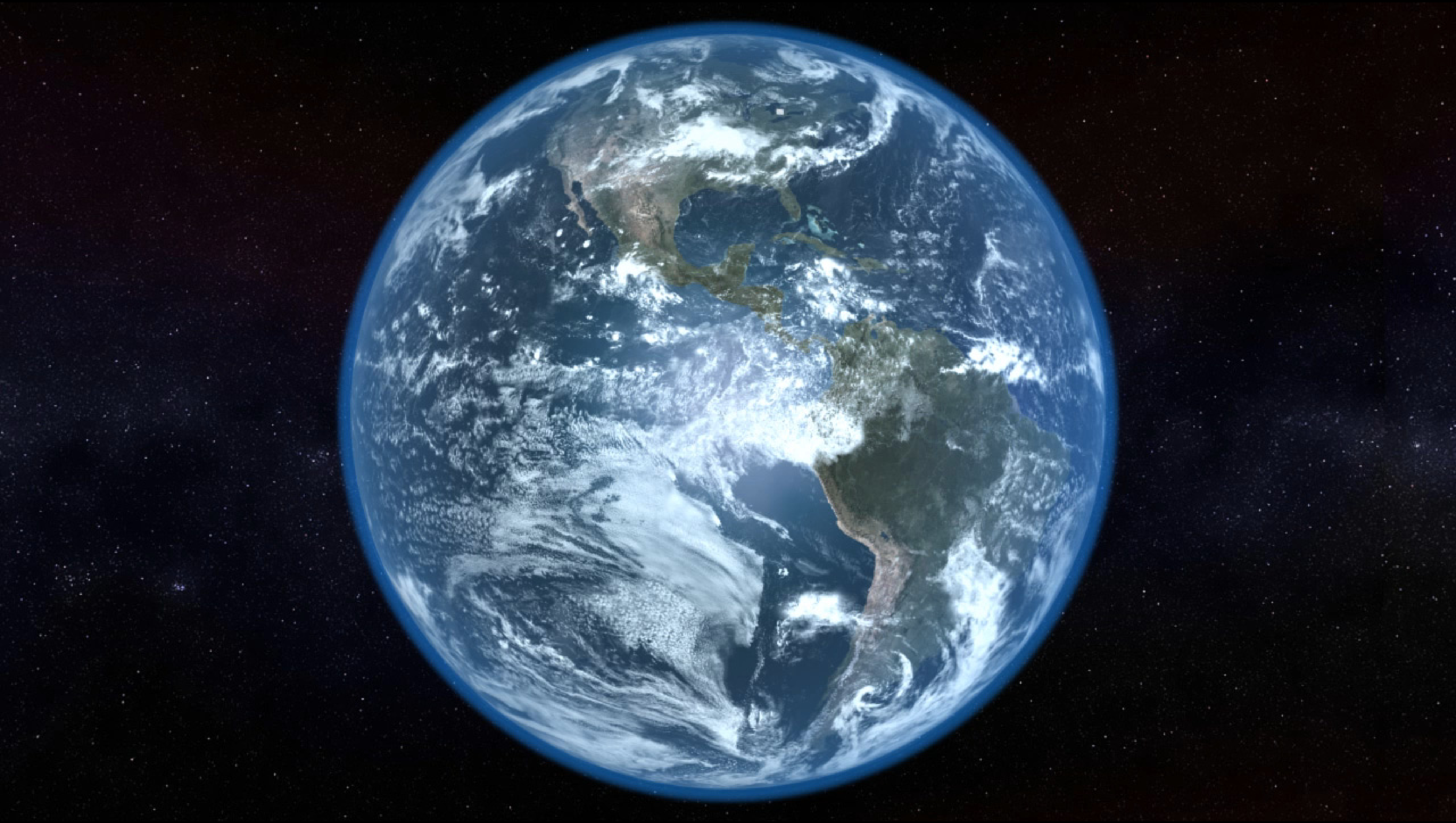
Q. Zhang, talk at QCrypt 2014

The Battelle quantum network



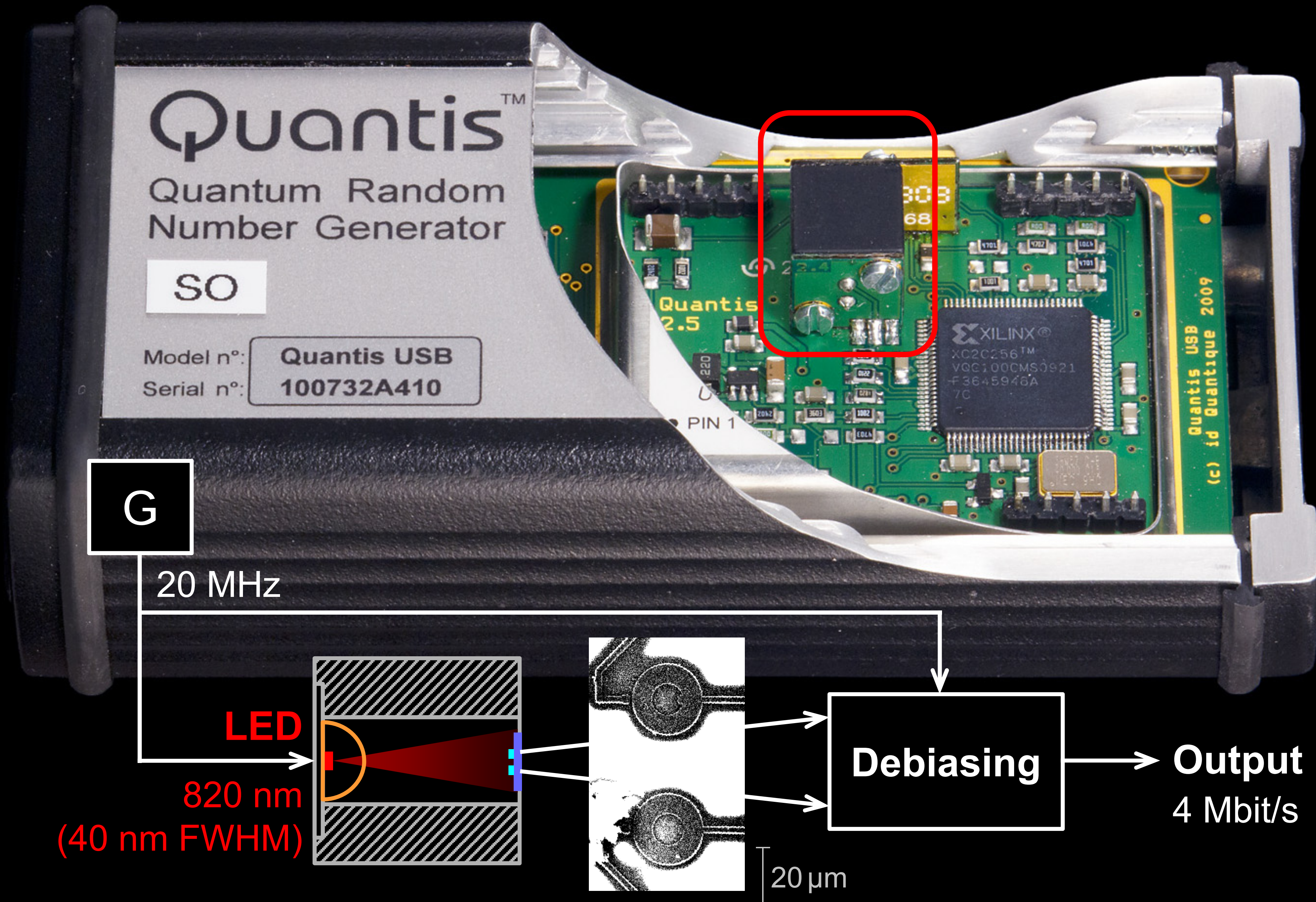
Plans:

N. Walenta *et al.*, poster at QCrypt 2014



Quantum communication primitives	Advantages over classical primitives:		
	Unconditionally secure?	Less resources?	Other quantum advantages?
Key distribution	●		
Secret sharing	●		
Digital signatures	●		
Superdense coding		●	
Fingerprinting		●	
Oblivious transfer	Impossible		●
Bit commitment	Impossible		●
Coin-tossing	●		
Cloud computing	●		
Bell inequality testing	(no classical equivalent)		
Teleportation	(no classical equivalent)		
Entanglement swapping	(no classical equivalent)		
Random number generators	●		

Quantis RNG: what's inside?



G. Ribordy, O. Guinnard, US patent appl. US 2007/0127718 A1 (filed in 2006)
I. Radchenko *et al.*, unpublished

Quantum digital signatures

Alice:

1. Distributes latent signatures

"0" $|$↕↔⤢↕⤡⤡$\rangle$ "1" $|$↔⤡↔↕↕⤢$\rangle$

Bob: measures

× + + + × + ...

Charlie: measures

+ × × + + × ...

⋮

2. Signs: reveals bit and latent sequence

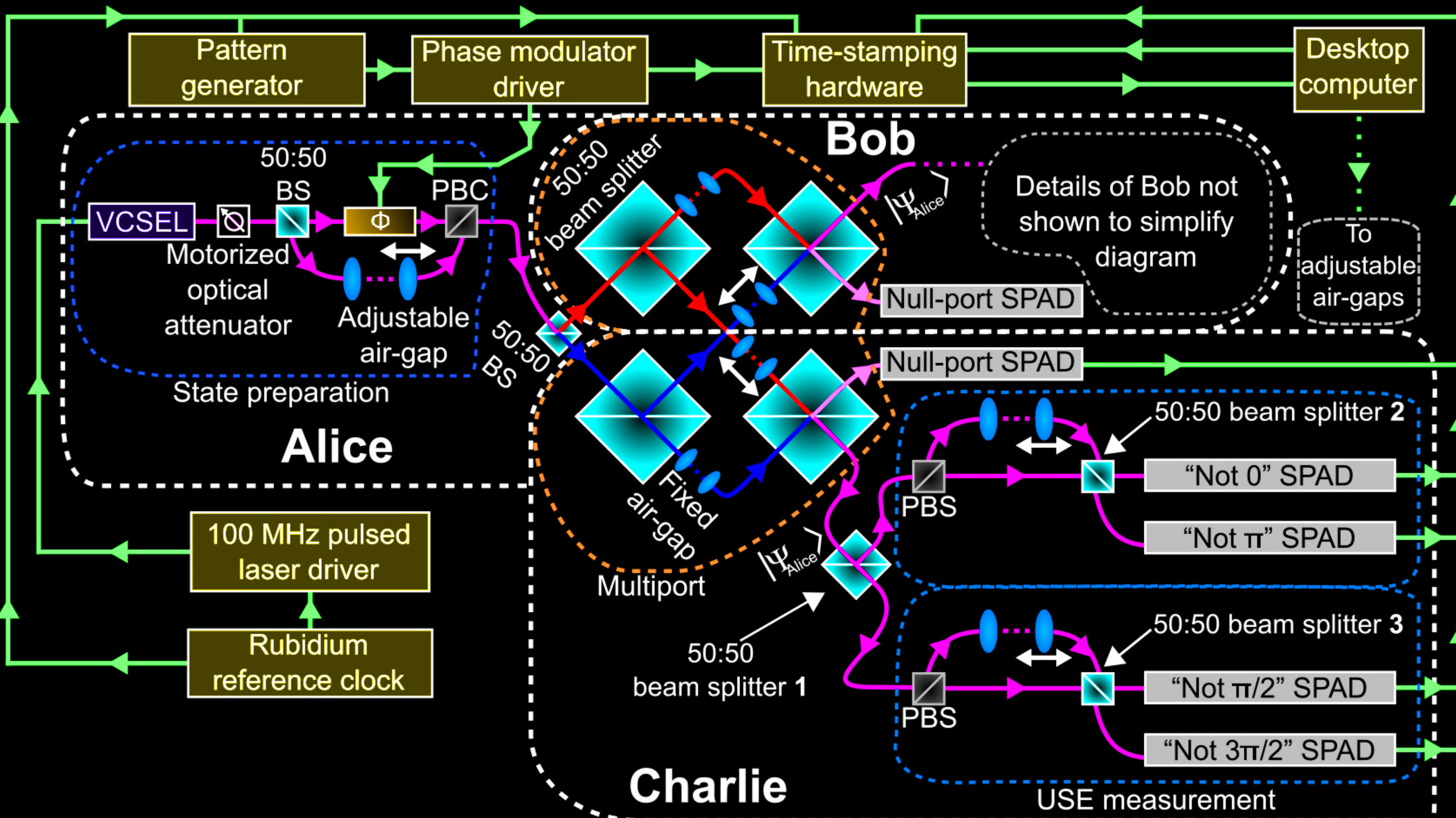
1, ↔⤡↔↕↕⤢

Bob: verifies measurement results

Charlie: verifies measurement results

R. Collins *et al.*, Phys. Rev. Lett. **113**, 040502 (2014)

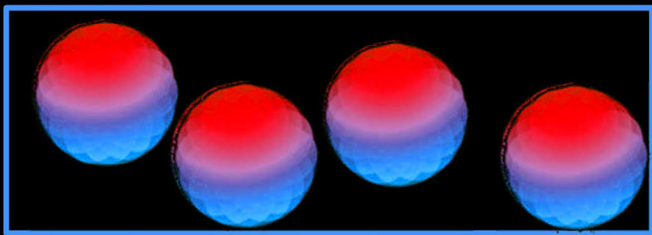
Quantum digital signatures



R. Collins *et al.*, Phys. Rev. Lett. **113**, 040502 (2014)

Blind quantum computing

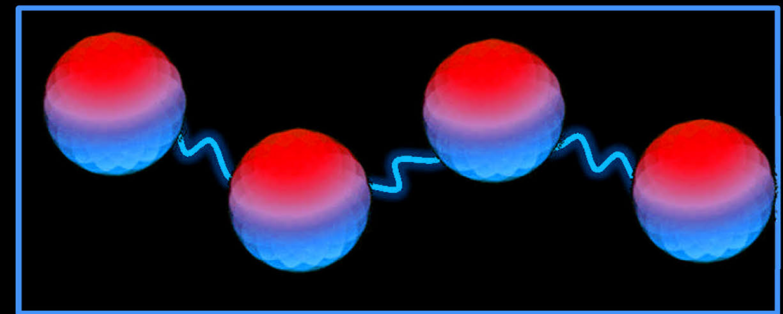
Client



Prepares qubits and sends them to quantum server

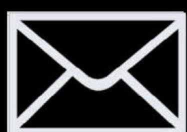
„sends single parts of computer“

Quantum Server



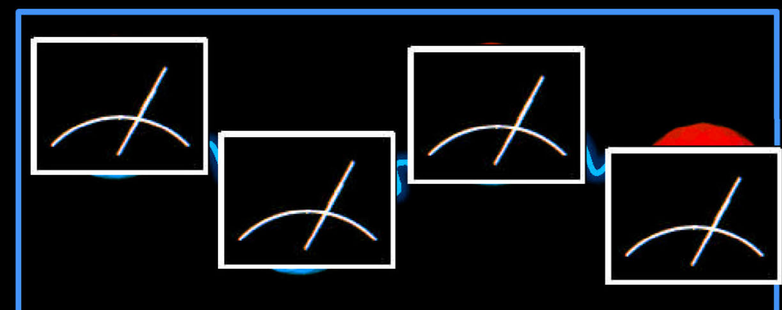
Entangles qubits

„assembles computer“



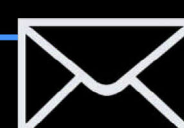
Computes and sends measurement instructions (adapted to state of the qubits)

„sends computer program“



Qubits are unknown, instructions seem like random operations

„computes, but does not know computer“

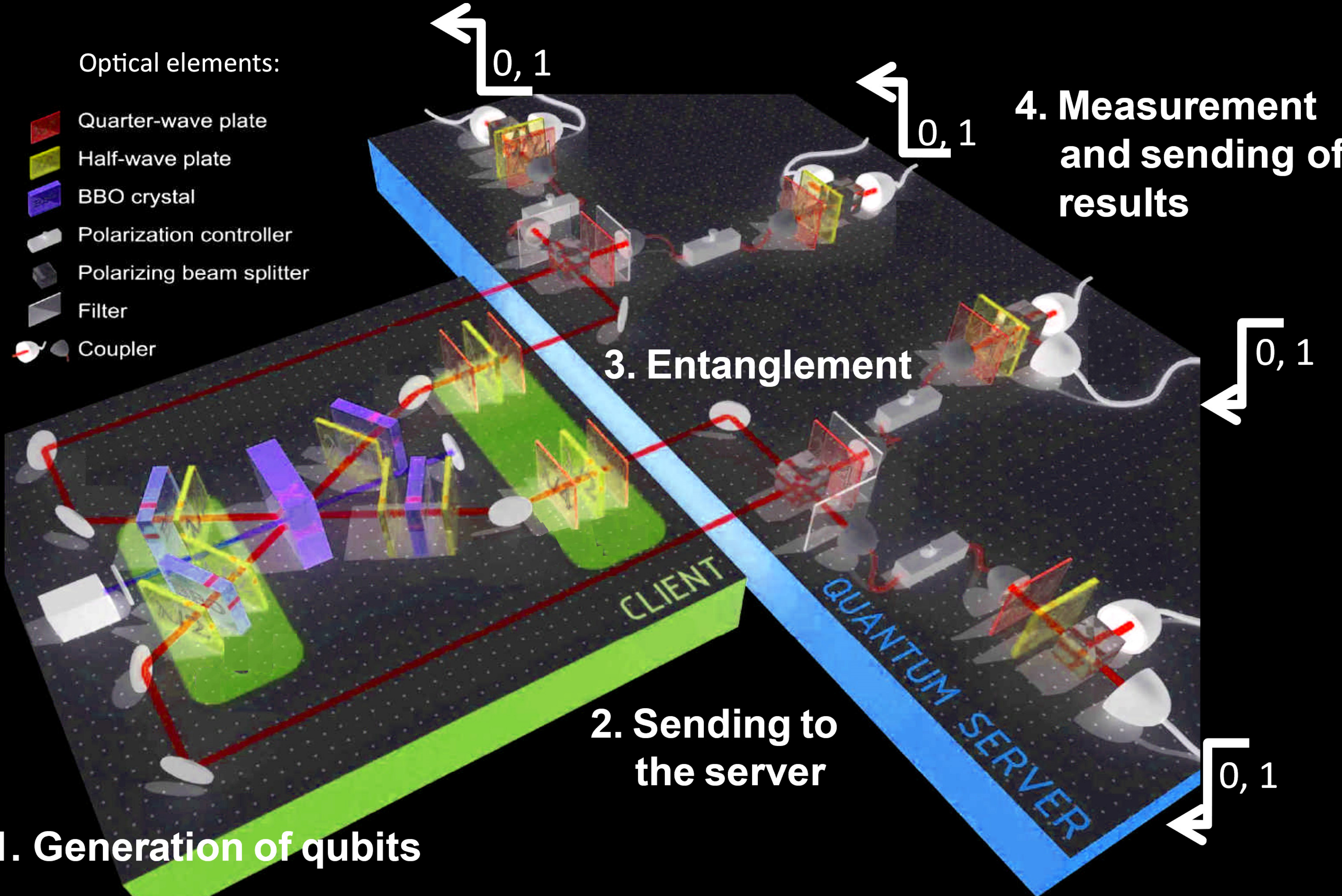


Results

Client can interpret and use the results

Slide courtesy S. Barz

Blind quantum computing



S. Barz *et al.*, Science **335**, 303 (2012)

The future is quantum


NRK 1
NRK
Nyheter
23:03