Quantum Cryptography

http://tph.tuwien.ac.at/~svozil/publ/2005-qcrypt-pres.pdf

Karl Svozil

Institut für Theoretische Physik, University of Technology Vienna,
Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria
svozil@tuwien.ac.at

16. 3. 2005

References

WIE83 Stephen Wiesner, *"Conjugate coding,"* Sigact News, 15, 78-88 (1983) [manuscript written *circa* 1970]

BBBSS92 Charles H. Bennett and F. Bessette and G. Brassard and L. Salvail and J. Smolin, *"Experimental Quantum Cryptography,"* Journal of Cryptology, 5, 3-28 (1992)

- Charles H. Bennett and Gilles Brassard and Artur K. Ekert, *"Quantum Cryptography,"* Scientific American, 267, 50-57 (1992)

GRTZ02 Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, *"Quantum cryptography,"* Rev. Mod. Phys. 74, 145-195 (2002) http://link.aps.org/abstract/RMP/v74/p145

- David Mermin, *"Lecture Notes on Quantum Computation,"* [Cornell University, Physics 481-681, CS 483; Spring, 2005] http://people.ccmr.cornell.edu/~mermin/qcomp/chap6.pdf

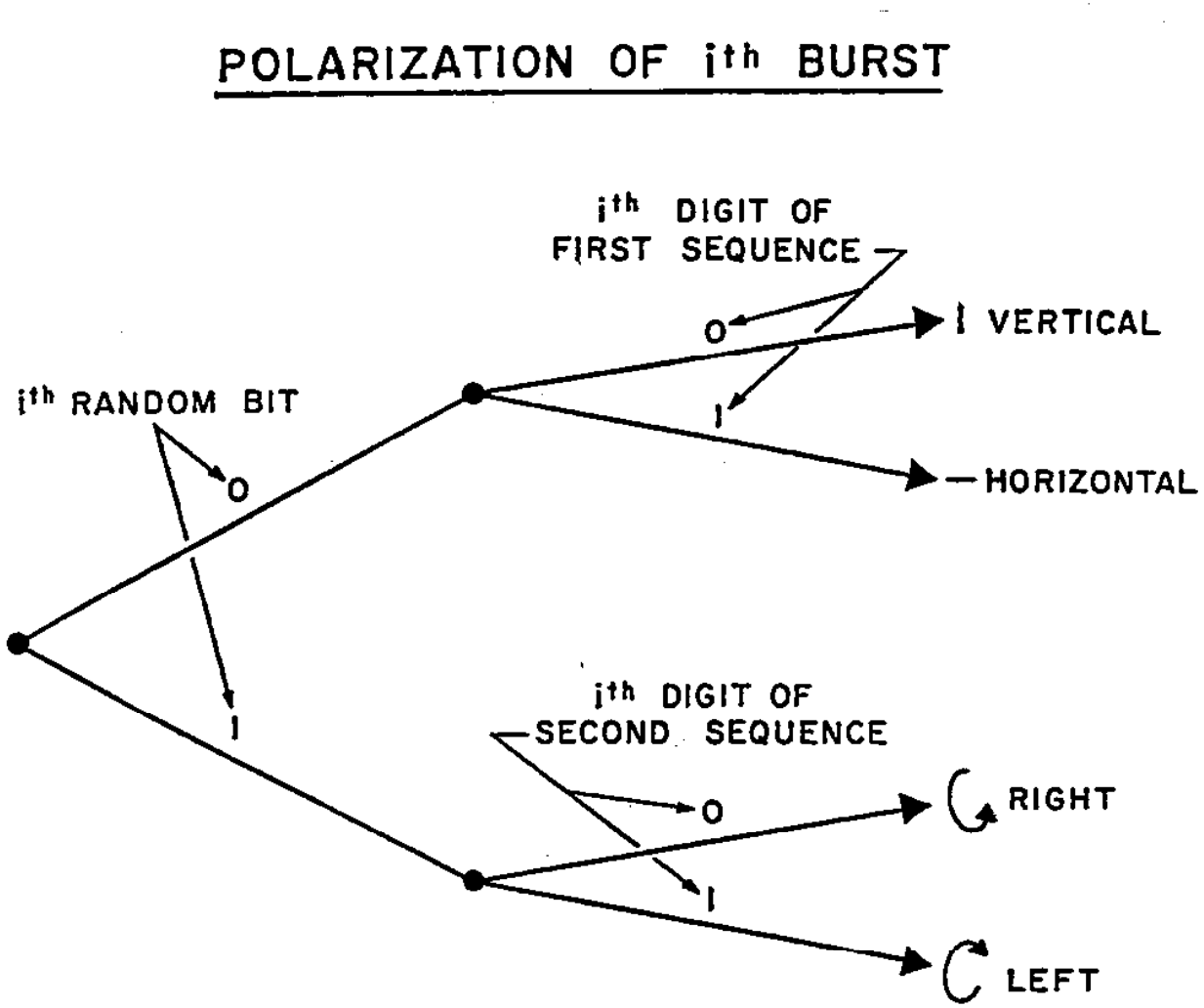
History

1970 Stephen Wiesner, *"Conjugate coding:"* noisy transmission of two or more "complementary messages" by using single photons in two or more complementary polarization directions/bases.

1984 BB84 Protocol: key growing via quantum channel & additional classical bidirectional communication channel

1991 EPR-Ekert protocol: maximally entangled state, three complementary polarization directions; additional security confirmation by violation of Bell-type inequality through data which cannot be directly used for coding

Wiesner's conjugate coding scheme



BB84 Protocol

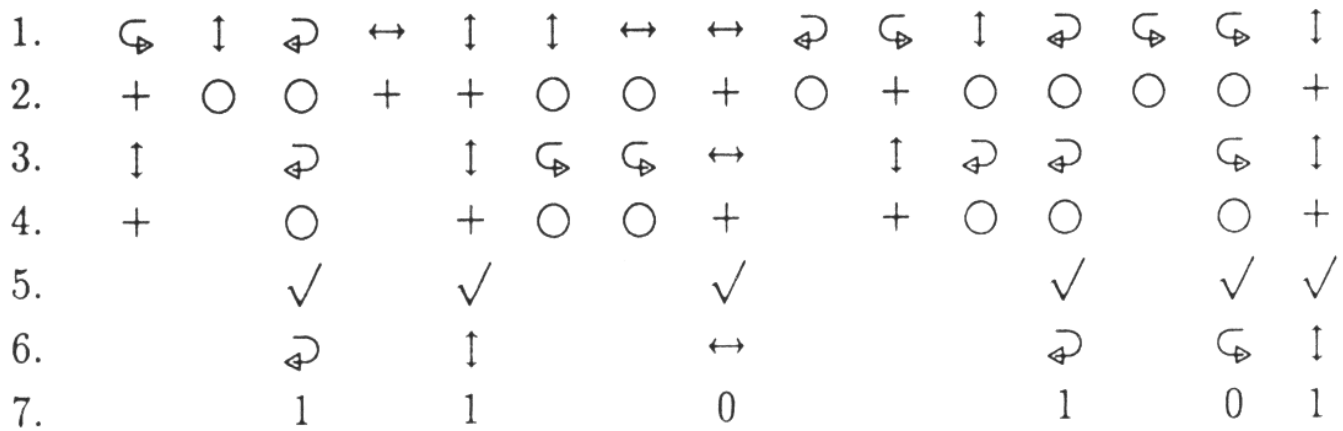


Fig. 1. Basic quantum key distribution protocol.

1. Alice sends a random sequence of photons polarized horizontal (↔), vertical (↕), right-circular (↻) and left-circular (↺);
2. Bob measures the photons' polarization in a random sequence of bases, rectilinear (+) and circular (◯).
3. Results of Bob's measurements (some photons may not be received at all).
4. Bob tells Alice which basis he used for each photon he received;
5. Alice tells him which bases were correct;
6. Alice and Bob keep only the data from these correctly-measured photons, discarding all the rest.
7. This data is interpreted as a binary sequence according to the coding scheme ↔ = ↺ = 0 and ↕ = ↻ = 1.

from [BBBSS92]

EPR-Ekert protocol

Parametrization of $|\psi\rangle = x|+\rangle + y|-\rangle$ by two angles $0 \leq \theta \leq \pi$ (azimutal) and $0 \leq \varphi \leq 2\pi$.

Let the expectation value measured by a pair of particles along the directions a_i and b_j be

$E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{+-}(a_i, b_j) - P_{-+}(a_i, b_j)$.

Consider the Clauser-Horne-Shimony-Halt (CHSH) term

$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3)$.

With the six measurement directions corresponding to $\varphi = 0$ (for all six), and $\theta_1^a = 0$, $\theta_2^a = \pi/4$, $\theta_3^a = \pi/2$, $\theta_1^b = \pi/4$, $\theta_2^b = \pi/2$, and $\theta_3^b = 3\pi/4$ (three per side), $S = -2\sqrt{2}$ is maximally violated by the Tsirelson bound.

Constant monitoring of S certifies the absence of an eavesdropper.

Interferometric protocols

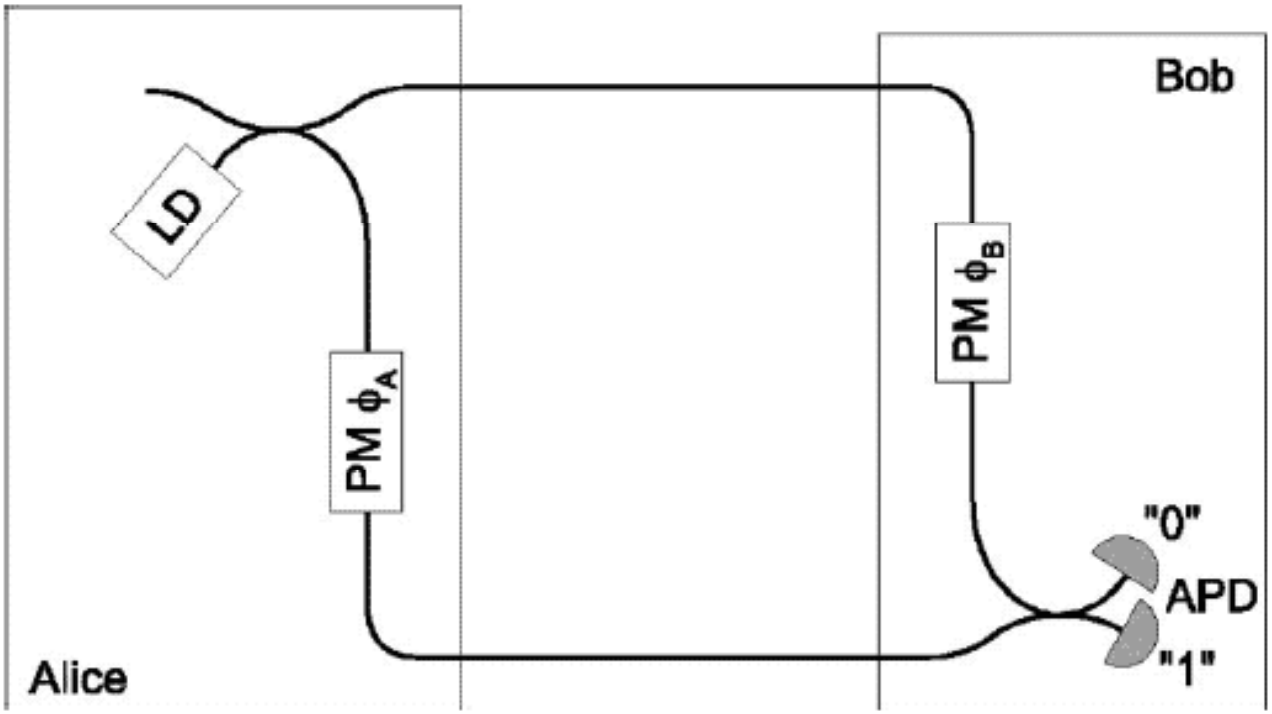


FIG. 14. Conceptual interferometric setup for quantum cryptography using an optical fiber Mach-Zehnder interferometer: LD, laser diode; PM, phase modulator; APD, avalanche photodiode.

from GRTZ02

Single particle production, manipulation & detection

It is essential to use single particle states, otherwise "Eve" could eavesdrop on the extra particles.

Complementarity

Eavesdropping randomizes the state transmitted from Alice to Bob.

No-cloning (no-copy) theorem

- Ideally, a perfect Qcopy device A, acting upon an arbitrary state ψ and some arbitrary blank state b, would do this:

$$\psi \otimes |b\rangle \otimes |A_i\rangle \longrightarrow \psi \otimes \psi \otimes |A_f\rangle.$$

- Suppose it would copy the two "quasi-classical" state "+" and "−" accordingly:

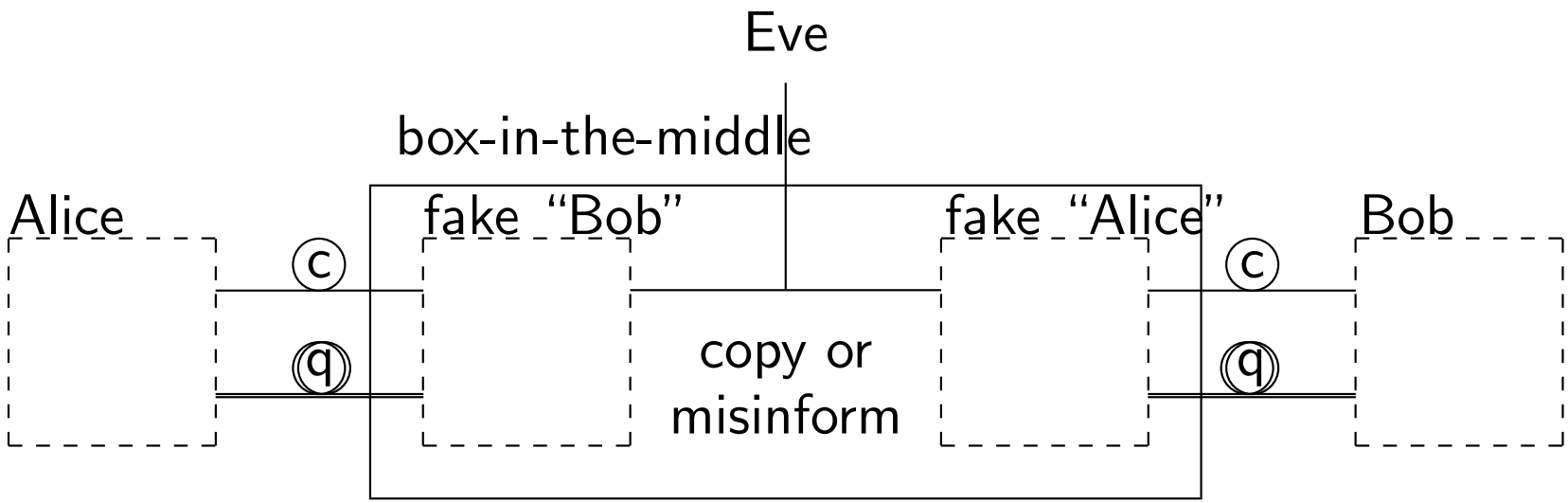
$$|+, b, A_i\rangle \longrightarrow |+, +, A_f\rangle, \qquad |-, b, A_i\rangle \longrightarrow |-, -, A_f\rangle.$$

- By the linearity of quantum mechanics, the state $\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ is copied according to

$$\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \otimes |b, A_i\rangle \longrightarrow \frac{1}{\sqrt{2}}(|+, +, A_f\rangle + |-, -, A_f\rangle)$$

$$\neq \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \otimes \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \otimes |A_i\rangle.$$

Man-in-the-middle attack using both the classical & quantum channels



from http://arxiv.org/abs/quant-ph/0501062

Man-in-the-middle attack using both the classical & quantum channels

- Compare: "Standard quantum key distribution protocols are provably secure against eavesdropping attacks, if quantum theory is correct." (from http://arxiv.org/abs/quant-ph/0405101).
- To: "The need for the public (non-quantum) channel in this scheme to be immune to active eavesdropping can be relaxed if the Alice and Bob have agreed beforehand on a small secret [[classical cryptographic]] key,.."(from BB84: C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE Computer Society Press, 1984), pp. 175-179.)
- "In accordance with our general philosophy that QKD forms a part of an overall cryptographic architecture, and not an entirely novel architecture of its own, the DARPA Quantum Network currently employs the standardized authentication mechanisms built into the Internet security architecture (IPsec), and in particular those provided by the Internet Key Exchange (IKE) protocol." (from http://arxiv.org/abs/quant-ph/0503058)

Techniques & gadgets

- Photon sources: faint laser pulses, photon pairs generated by parametric downconversion, photon guns, ...
- Quantum channels: single-mode fibers, free-space links, ...
- Single-photon detection: photon counters, ...
- (Quantum) Random number generators: calcite prism, ...

1989 IBM Yorktown Heights

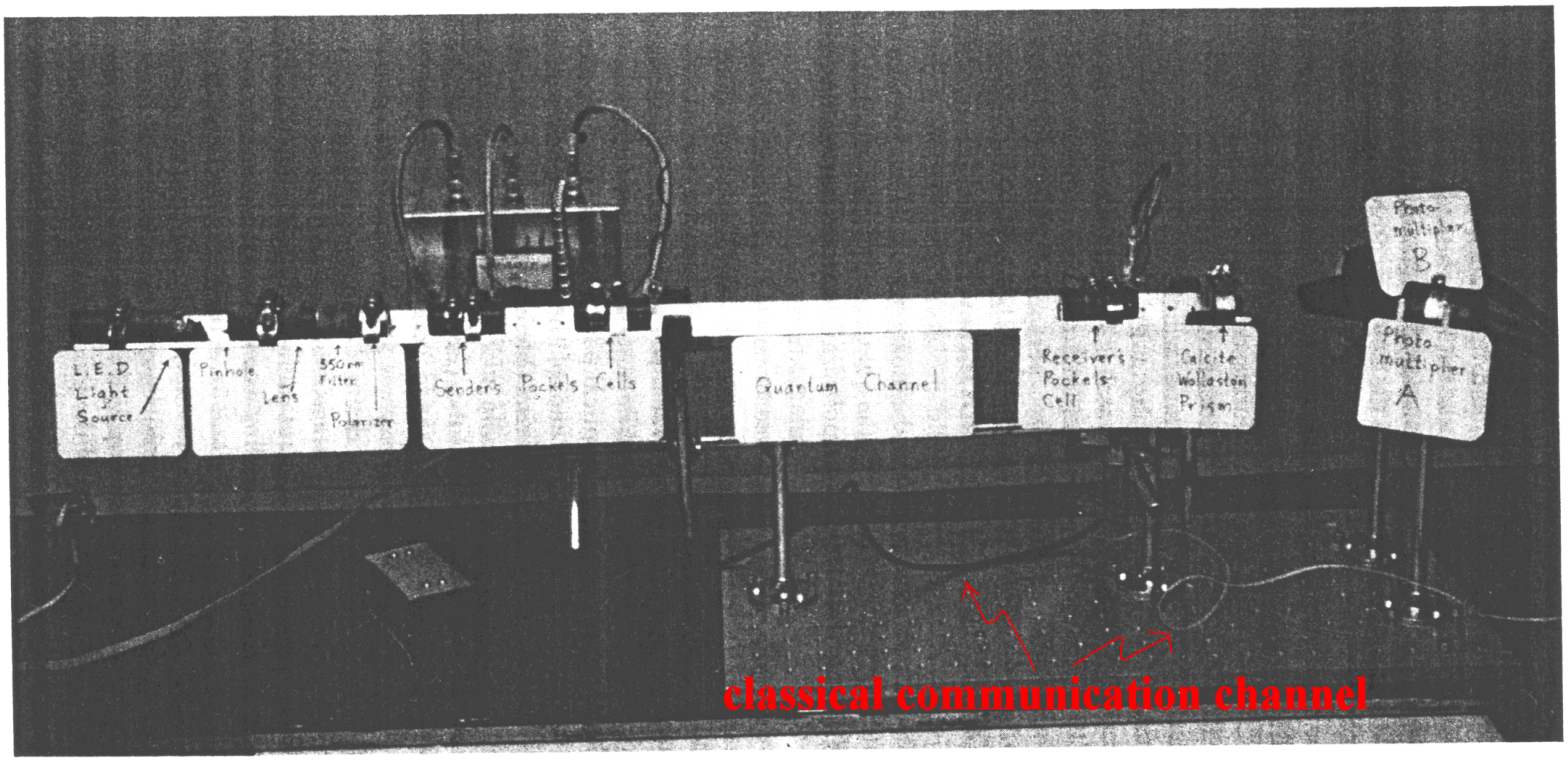


Fig. 2. Photograph of the apparatus.

Incoherent green light flashes are produced by Light Emitting Diode (LED) on the left, collimated into a beam by Pinhole and Lens, then pass through a 550 nm Filter and a horizontal Polarizer. Sender's Pockels Cells convert the horizontal polarization into an arbitrary sequence of the four polarization states (horizontal, vertical, left-circular, and right-circular). After traversing the quantum channel, a 32 cm free air optical path, the beam passes through Receiver's Pockels Cell, which, if energized, converts rectilinear into circular polarizations and vice versa. Finally, a calcite Wollaston prism splits the beam into horizontally and vertically polarized components, in which individual photons are detected by Photomultiplier tubes A and B, respectively.

from [BBBSS92]

1993 Lake Geneva

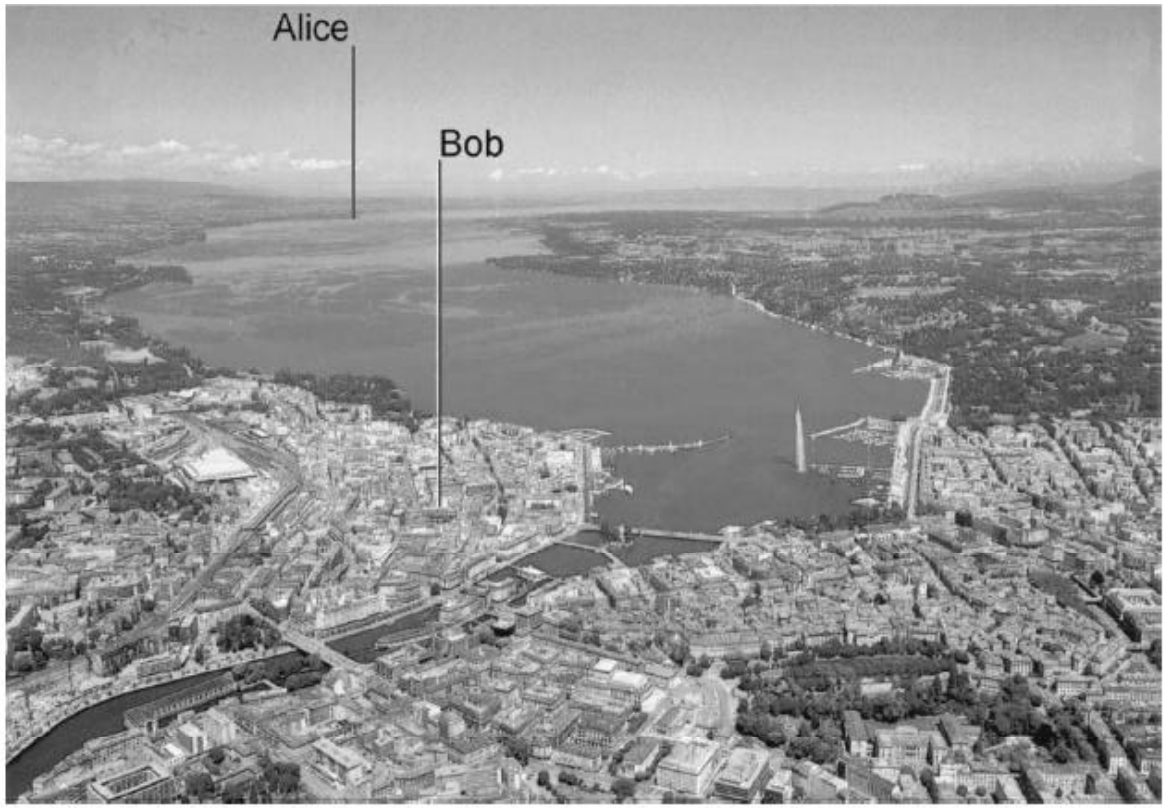


FIG. 13. Geneva and Lake Geneva. The Swisscom optical fiber cable used for quantum cryptography experiments runs under the lake between the town of Nyon, about 23 km north of Geneva, and the center of the city.

from GRTZ02

2004 Vienna

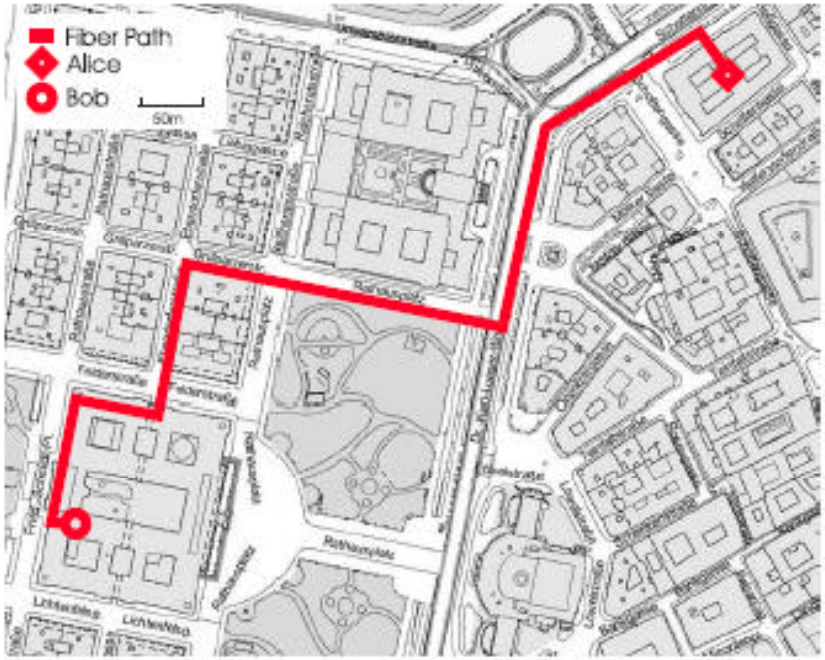


Figure 1: A quantum cryptography system is installed between the headquarters of a large bank (Alice) and the Vienna City Hall (Bob). The beeline distance between the two buildings is about 650m. The optical fibers were installed some weeks before the experiment in the Vienna sewage system and have a total length of 1.45 km.

from Zeilinger et al. http://arxiv.org/abs/quant-ph/0404115

2003-present DARPA Network Boston

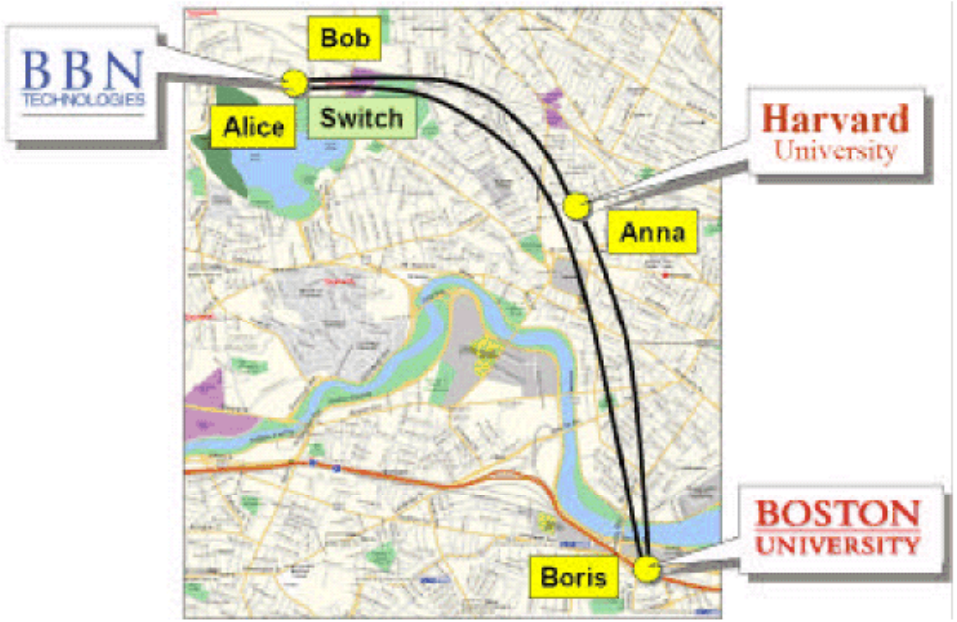


Figure 11: Logical Map of the Cambridge-Area Fiber Network.

Figure 12 presents the distances and attenuations for the current fiber spans across Cambridge. As can be seen, the BBN-Harvard spans are 10.2 km (5.1 dB) and the BBN-BU spans are 19.6 km (11.5 dB). These attenuations are quite high, being equivalent to 24.3 km and 54.8 km respectively of standard fiber at 0.21 dB/km, and are incurred by a large number of connectors along the current fiber paths. A sample Optical Time Domain Reflectometry (OTDR) trace for the BU-BBN path, at the left, illustrates the effects of these connectors.

from http://arxiv.org/abs/quant-ph/0503058

Thank you for your attention!