Quantum Communications

Using physics to keep secrets safe

Raymond Newell, PhD

March 2021

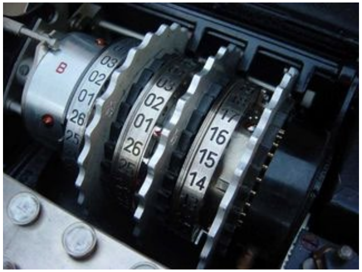
Los Alamos NATIONAL LABORATORY EST. 1943

NNSA National Nuclear Security Administration

A problem…

Current encryption systems rely on *computational difficulty* (often, factoring a large number)

…maybe it's not as hard as we think



Enigma machine, WWII

Germans believed it was unbreakable

Cracked by Polish & English intelligence

…the encrypted message could be stored and cracked later

intel inside
CORE i47

… a Quantum Computer could do it easily

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

arXiv:quant-ph/9508027v2

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

…a solution

Information is physical

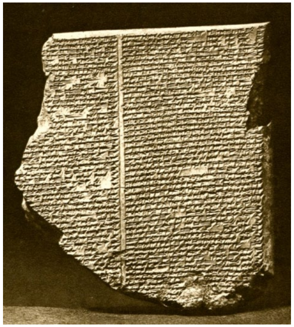
Classical information can be

•duplicated

•divided

•re-read

indefinitely, and without altering it



Epic of Gilgamesh ca. 1800 b.c.e.

Quantum information cannot be

~~•duplicated~~ No-cloning theorem

~~•divided~~ No half-photons

~~•re-read~~ Wavefunction collapse

Quantum systems are well-suited for secret communication

Security is based on *fundamental laws of physics* rather than assumptions about adversary's abilities

Quantum Mechanics for secure communication

How do you build a system which obeys quantum laws, not classical ones?

Get small

Charles H. Bennett

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

International Conference on Computers, Systems & Signal Processing Bangalore, India December 10-12, 1984

Gilles Brassard

The BB-84 Protocol

- Encode information onto the state of a quantum system
- Send quantum system
- Measure system's state

- Quantum system – single photons
- State – their polarization

An Optical technology…

Quantum communication requires an *optical* connection between terminals

Free Space

- Rooftop to rooftop
- Airplane to ground
- Ship to shore
- Satellite to ground
- Etc…

N. J. Phys. 4, 43.1 **(2002)**

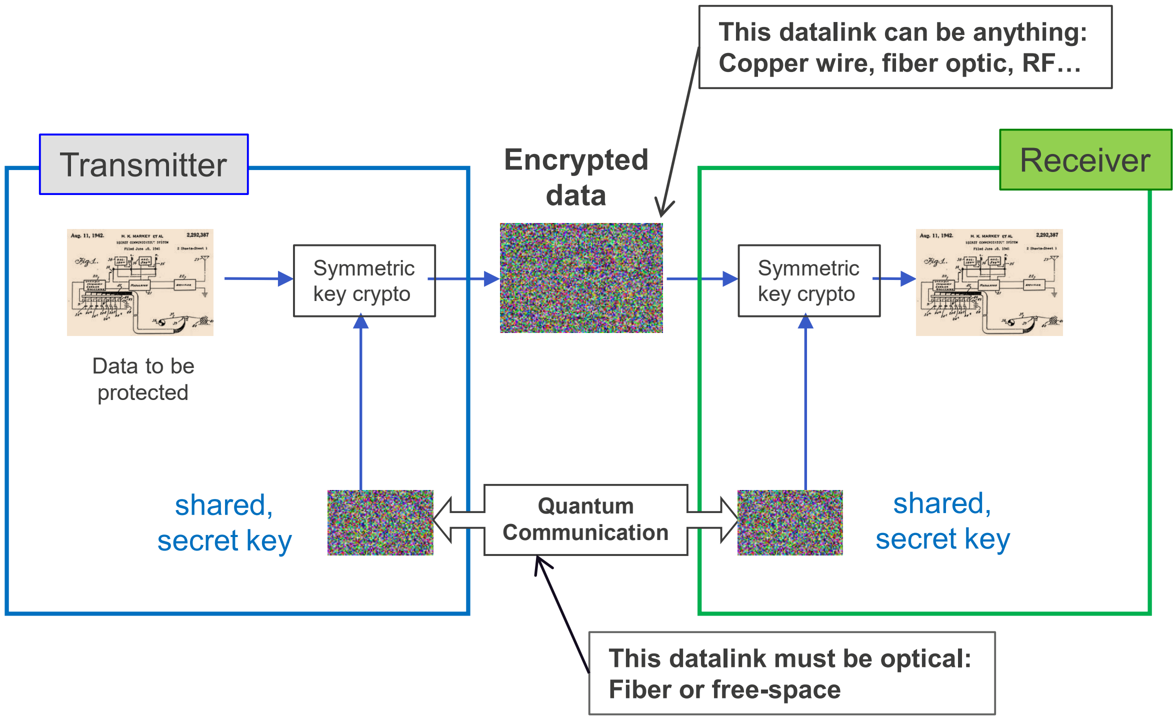
Fiber Optics

- Standard telecom fibers
- Coexist with telecom data
- Within a building
- Within a base or enclave
- Metro area
- Up to 200 km

N. J. Phys. 8, 193 **(2006)**

…use is not restricted to optics

Once keys are generated; encryption can be used over *any* data link



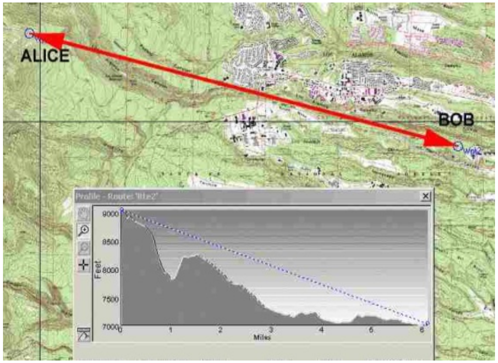
Example system: 10-km through the air link (1999)

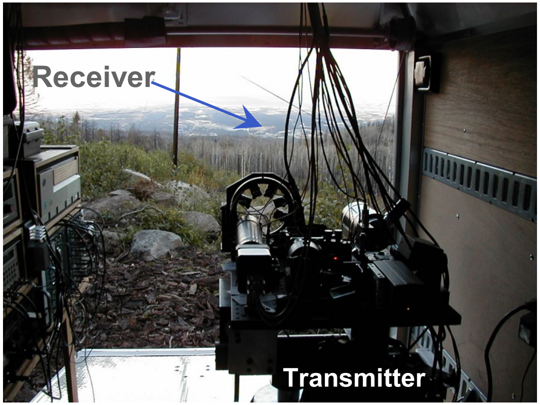
Sample of key material at 10-km range in daylight one-airmass path: comparable optics to satellite-to-ground

A: 01110001 01111010 00100001 01100100 10100110
B: 01110001 01111010 00100001 01100100 10100110

A: 11100010 00111101 10011111 10000111 11001111
B: 11100010 00111101 10011111 10000111 11001111

- key transferred by 772-nm single-photon communications
- 1-MHz sending rate; ~600-Hz key rate
- day: 45,576 secret bits/hour ; night: 113,273 secret bits/45 mins



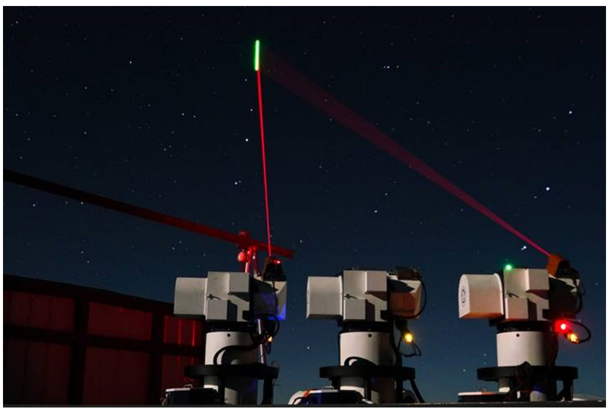


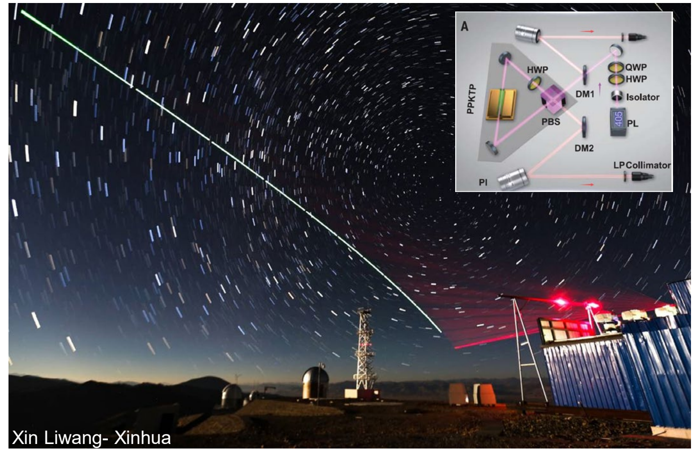
Example system: 1200-km through the air link (2017)

QUANTUM OPTICS

Satellite-based entanglement distribution over 1200 kilometers

Juan Yin,[1,2] Yuan Cao,[1,2] Yu-Huai Li,[1,2] Sheng-Kai Liao,[1,2] Liang Zhang,[2,3]
Ji-Gang Ren,[1,2] Wen-Qi Cai,[1,2] Wei-Yue Liu,[1,2] Bo Li,[1,2] Hui Dai,[1,2] Guang-Bing Li,[1,2] Qi-Ming Lu,[1,2] Yun-Hong Gong,[1,2]
Yu Xu,[1,2] Shuang-Lin Li,[1,2] Feng-Zhi Li,[1,2]
Ya-Yun Yin,[1,2] Zi-Qing Jiang,[3] Ming Li,[3] Jian-Jun Jia,[3] Ge Ren,[4] Dong He,[4] Yi-Lin Zhou,[5] Xiao-Xiang Zhang,[6] Na Wang,[7] Xiang Chang,[8] Zhen-Cai Zhu,[5]
Nai-Le Liu,[1,2] Yu-Ao Chen,[1,2] Chao-Yang Lu,[1,2] Rong Shu,[2,3] Cheng-Zhi Peng,[1,2]* Jian-Yu Wang,[2,3]* Jian-Wei Pan[1,2]*





LETTER

doi:10.1038/nature23675

Ground-to-satellite quantum teleportation

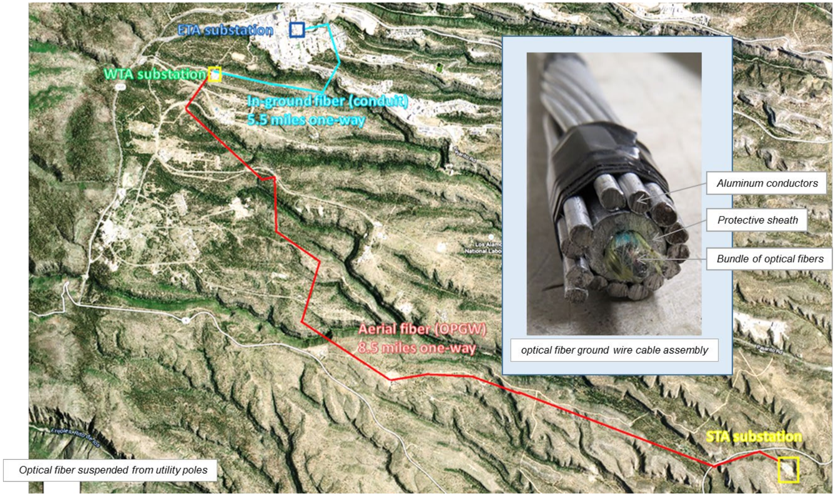
Ji-Gang Ren[1,2], Ping Xu[1,2], Hai-Lin Yong[1,2], Liang Zhang[2,3], Sheng-Kai Liao[1,2], Juan Yin[1,2], Wei-Yue Liu[1,2], Wen-Qi Cai[1,2], Meng Yang[1,2], Li Li[1,2], Kui-Xing Yang[1,2], Xuan Han[1,2], Yong-Qiang Yao[4], Ji Li[5], Hai-Yan Wu[5], Song Wan[6], Lei Liu[6], Ding-Quan Liu[3], Yao-Wu Kuang[3], Zhi-Ping He[3], Peng Shang[1,2], Cheng Guo[1,2], Ru-Hua Zheng[7], Kai Tian[8], Zhen-Cai Zhu[6], Nai-Le Liu[1,2], Chao-Yang Lu[1,2], Rong Shu[2,3], Yu-Ao Chen[1,2], Cheng-Zhi Peng[1,2], Jian-Yu Wang[2,3] & Jian-Wei Pan[1,2]

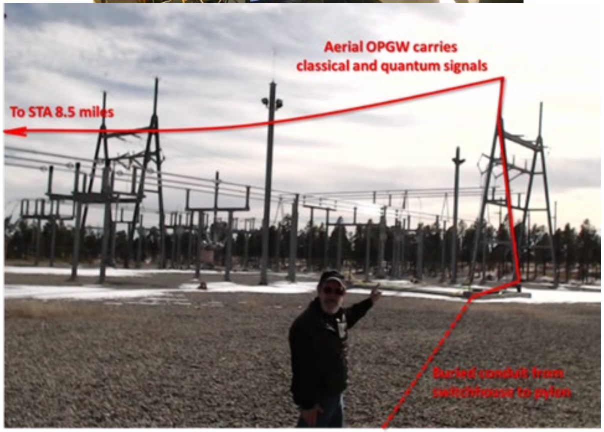
[1] Yin, Pan et al (2017), Ren et al (2017)

Example system: QC for Electric Grid Security (2020)

Quantum systems can be used as a bump-in-the-wire retrofit on existing control systems and networks

Invisible to end-user, but with much stronger security now and in the future





Achievable range depends on detectors

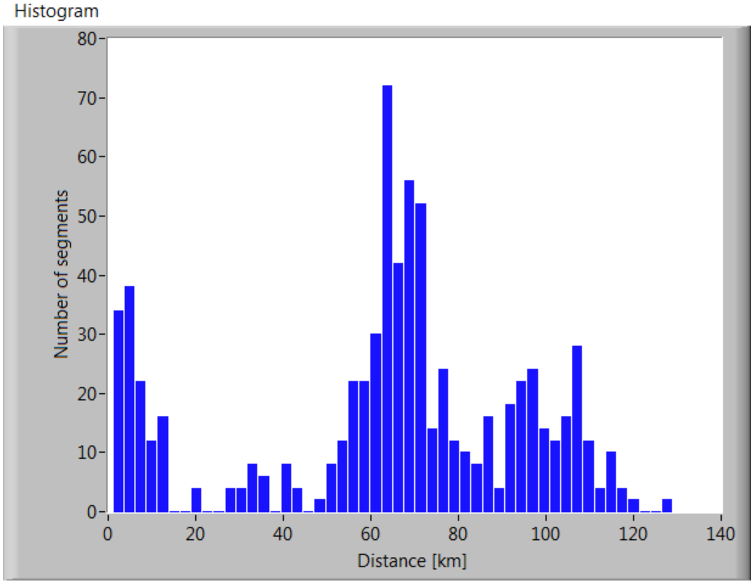
- **The security of a Quantum communication system is contingent on the transmitter sending only one photon at a time (or at most, a few)**

- **Maximum transmitted power is fixed (a few femtowatts)**
- **Loss in the channel is fixed (0.2 dB/km for fiber)**
- **Maximum range is determined by the detectors**

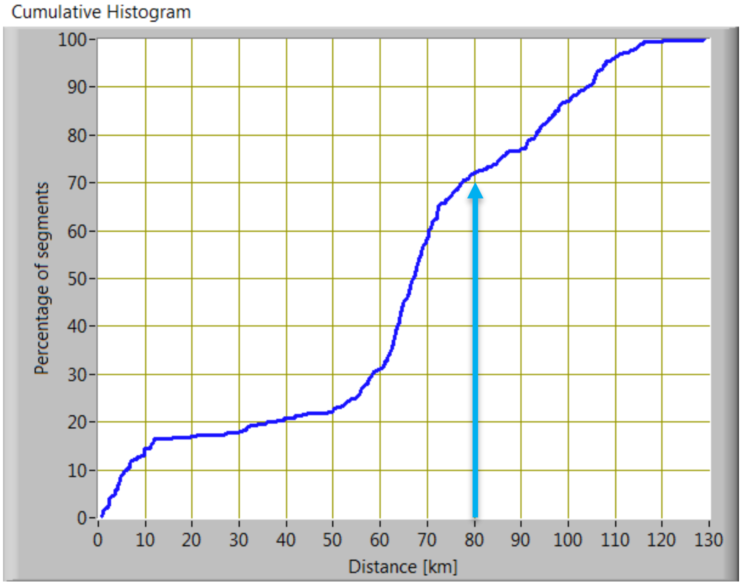
	Avalanche photodiode	Superconducting nanowire	Transition edge sensor
Efficiency @1550 nm	20%	80%	>95%
Mechanism	Electron-hole pairs avalanche in an over-biased p-n junction	Heat from photon warms a superconductor above critical temperature	Heat from photon warms a superconductor above critical temperature
Cryogenics?	No	Yes	Yes
Cost per system	$10k	$200k	No COTS product
Achievable range	80 km	150 km	200 km

80 km range would enable 70% of Dept. of Energy's links

This is a histogram of all 734 fiber spans that comprise ESnet, sorted according to span length.

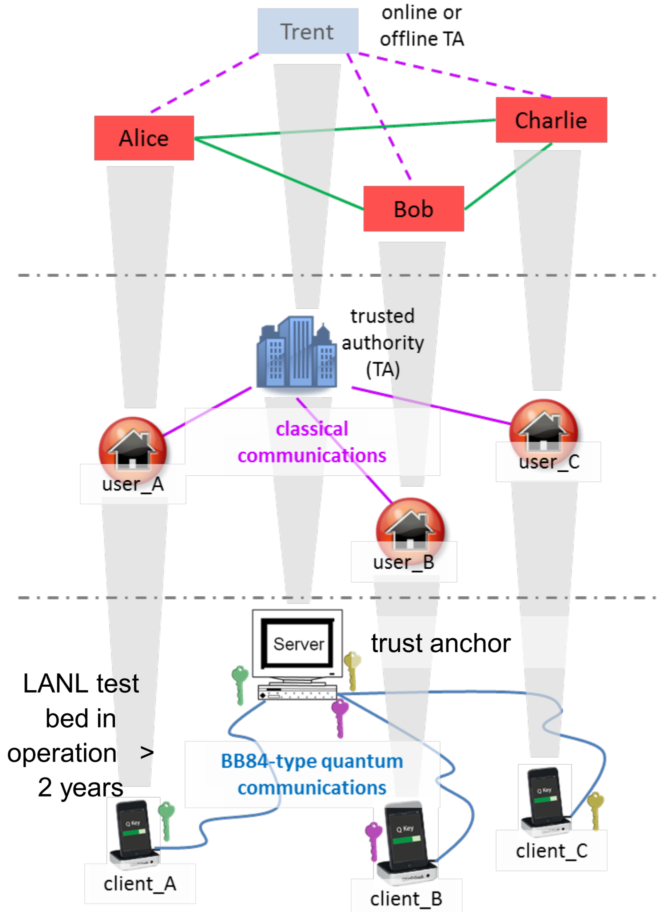


A cumulative histogram of the same data set shows that 70% of all spans are 80km or less.



Do you have a similar data set to share?
raymond@lanl.gov

ID management for lightweight crypto with forward security
Network-Centric Quantum Communications



application layer:
- confidentiality
- authenticity
- integrity
- non-repudiation
- without direct user-to-user QC

quantum key management layer:
- classical protocols built from quantum primitives
- authenticated key establishment
- one-time signatures
- certificates

quantum protocol layer:
- identification (QID)
- key distribution (QKD)
- secret splitting (QSS)

quantum physical layer:

Quantum science provides unparalleled security assurances in many different contexts

- **Powerful Quantum Computers don’t exist yet, but are under intense development worldwide**
  - Someday, a quantum computer could be able to break many popular crypto protocols
  - Someday even sooner, could do lots of other useful things: optimization, efficient search…
- **One form of defense: Quantum Communications**
  - Quantum signals cannot be copied, split, or examined by an eavesdropper
  - Compatible with existing fiber optic infrastructure, especially utilities
  - Earth – space – earth quantum entanglement
- **Another form of defense: Quantum-Safe Cryptography**
  - Lots of active research by cryptographers worldwide
  - It takes a long time to get from mathematics to implemented systems