Quantum Communications

Using physics to keep secrets safe

Raymond Newell, PhD

October 2017

NNSA
National Nuclear Security Administration

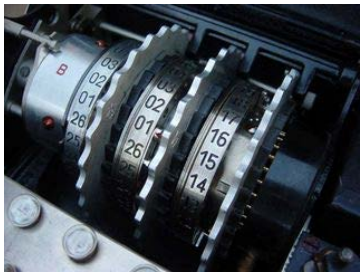
Operated by Los Alamos National Security, LLC for the U.S. Department of Energy's NNSA

LA-UR-1729037

A problem…

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

…maybe it's not as hard as we think

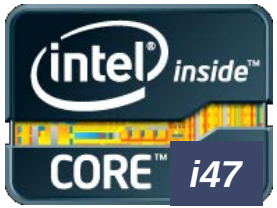


Enigma machine, WWII

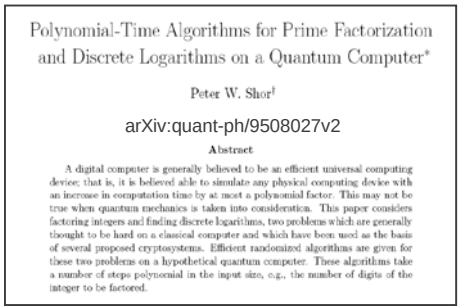
Germans believed it was unbreakable

Cracked by Polish & English intelligence

…the encrypted message could be stored and cracked later



… 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.

…. in any case, you're betting against technology.

…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

No-cloning theorem

No half-photons

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

Difficulties with Today's Public Key Crypto: e.g. RSA

Security lifetime estimates of public keys erode much faster than predicted

1977: "A new cipher which may take millions of years to break", (M. Gardener, Scientific American)

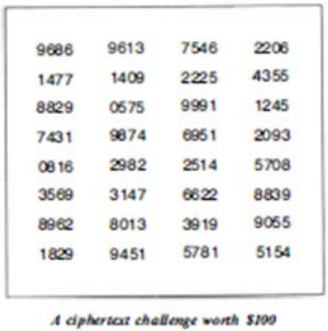
- Predicted to take **40 quadrillion years** to break

1994: Atkins, Graff, Lenstra & Leyland decrypt it in **8 months**

- **Used 1600 computers on "the internet"**

2015: McHugh decrypt in **one day**

- **$30 worth of cloud computing**

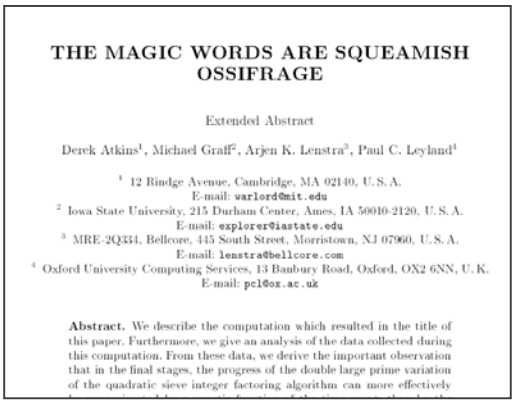


9686	9613	7546	2206
1477	1409	2225	4355
8829	0575	9991	1245
7431	9874	6951	2093
0816	2982	2514	5708
3569	3147	6622	8839
8962	8013	3919	9055
1829	9451	5781	5154

A ciphertext challenge worth $100

Encrypted text 1977

17 years



THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

Extended Abstract

Derek Atkins[1], Michael Graff[2], Arjen K. Lenstra[3], Paul C. Leyland[4]

[1] 12 Rindge Avenue, Cambridge, MA 02140, U. S. A.
E-mail: warlord@mit.edu
[2] Iowa State University, 215 Durham Center, Ames, IA 50010-2120, U. S. A.
E-mail: explorer@iastate.edu
[3] MRE-2Q334, Bellcore, 445 South Street, Morristown, NJ 07960, U. S. A.
E-mail: lenstra@bellcore.com
[4] Oxford University Computing Services, 13 Banbury Road, Oxford, OX2 6NN, U. K.
E-mail: pcl@ox.ac.uk

Abstract. We describe the computation which resulted in the title of this paper. Furthermore, we give an analysis of the data collected during this computation. From these data, we derive the important observation that in the final stages, the progress of the double large prime variation of the quadratic sieve integer factoring algorithm can more effectively

Decrypted text 1994

Quantum Mechanics for secure communication

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

Get small

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

Charles H. Bennett

Gilles Brassard

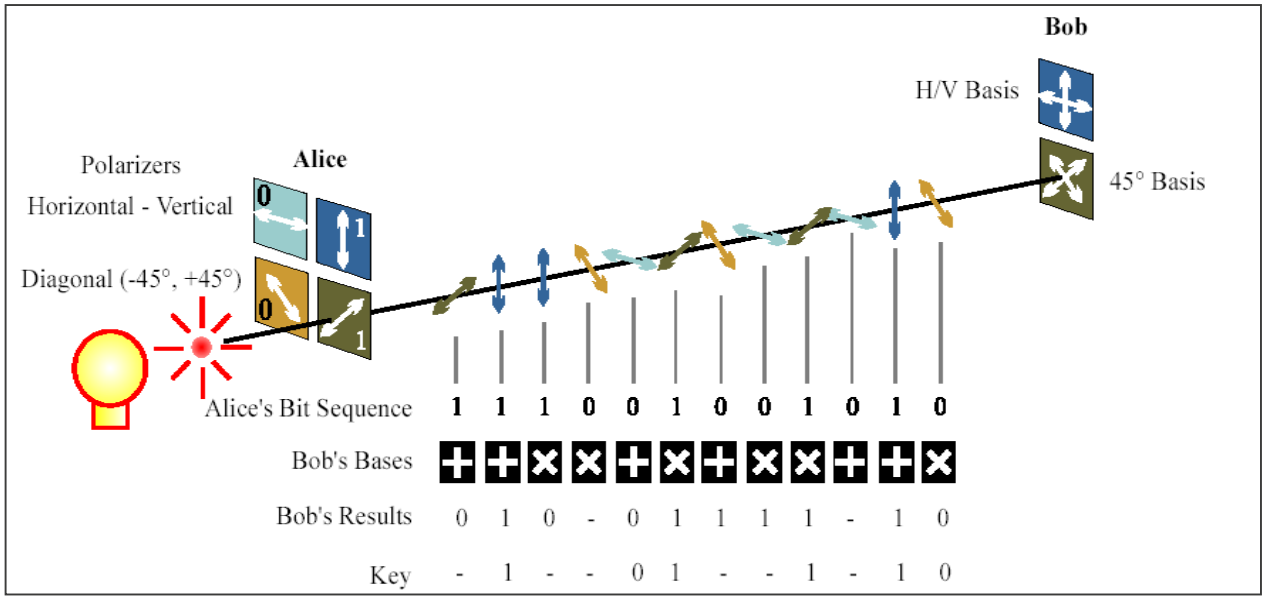
The BB-84 Protocol

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

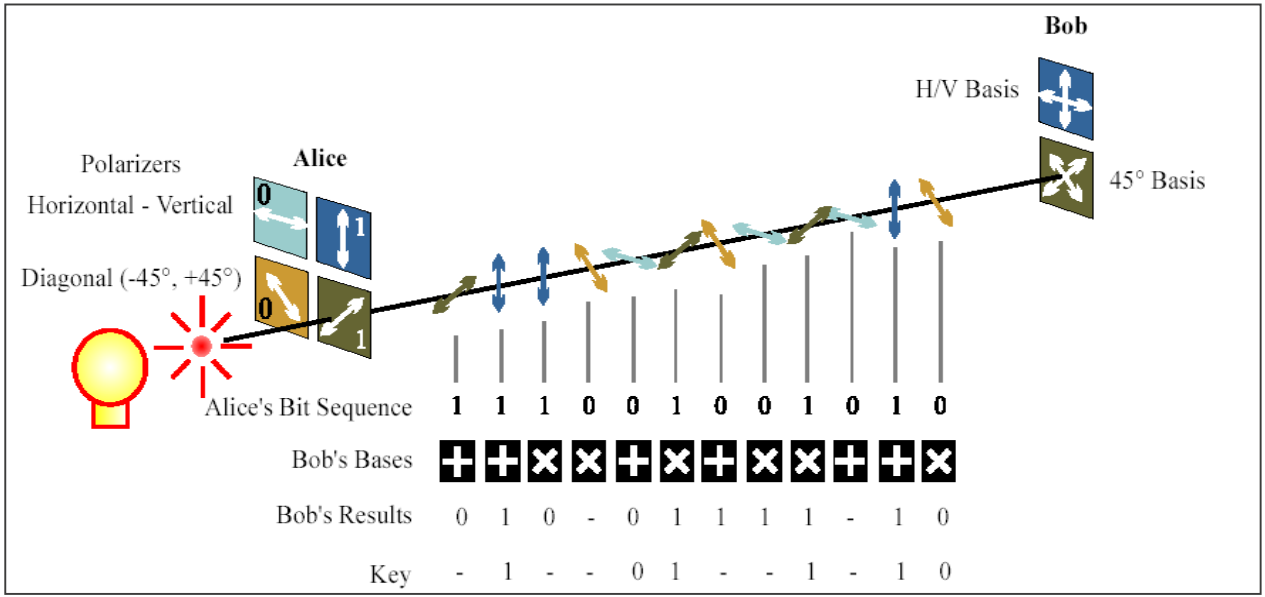
- Quantum system – single photons
- State – their polarization

BB-84 Protocol

- Transmitter “Alice” has an attenuated laser and four polarizers
  - Polarizers are oriented Horizontal, Vertical, Diagonal (+45°), and Anti-diagonal (-45°)
- Horizontal and Vertical form one basis (HV), Diagonal and Anti-Diagonal another (45°)
- Alice randomly chooses a bit value, 0 or 1, and a basis value, HV or 45°, and sends that photon



BB-84 protocol, continued



- **Receiver "Bob" randomly chooses a basis to measure, HV or 45°**
- **Bob measures bit values in that basis**
- **Alice and Bob compare basis choices ("sifting")**
  - **When they used different bases, they discard that bit**
  - **When they used the same basis, they keep that bit**
- **Use Forward Error Correction to estimate bit error rate**
- **Use Privacy Amplification to distill out the truly secret fraction**
  - **If error rate is too high, secret fraction is zero**

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)**

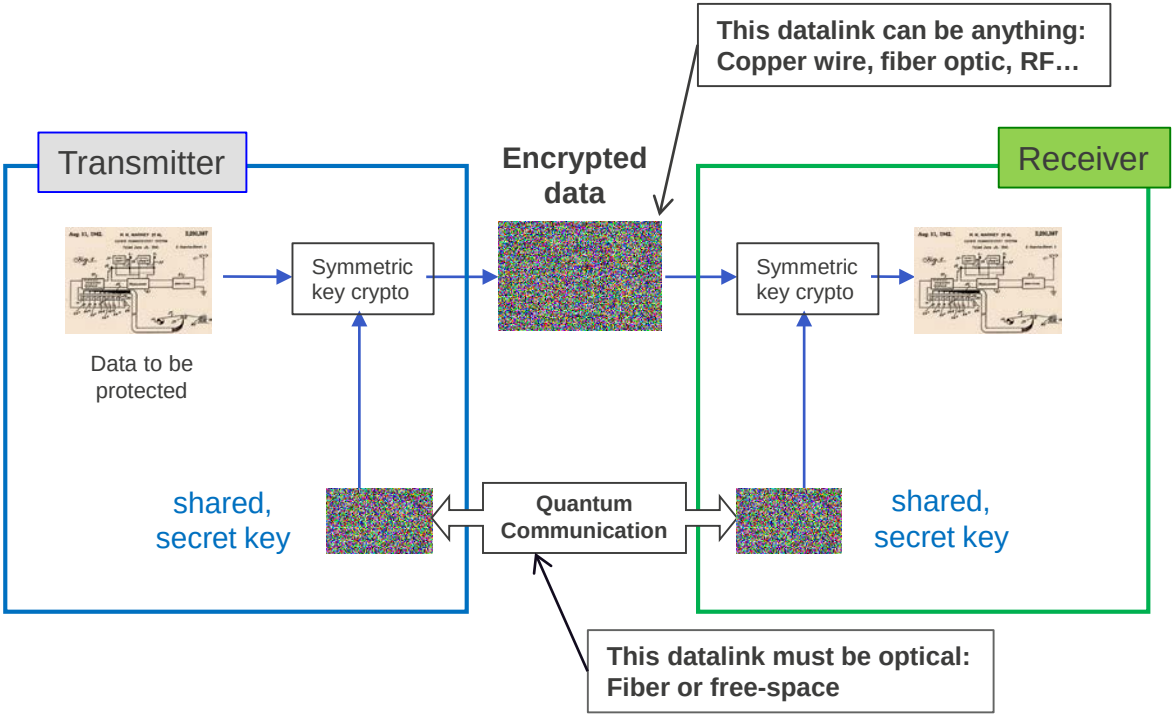
Fiber Optics

- 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



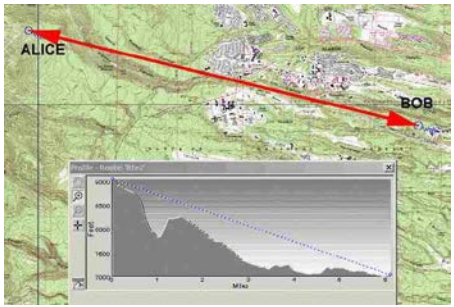
Example system: 10-km through the air link

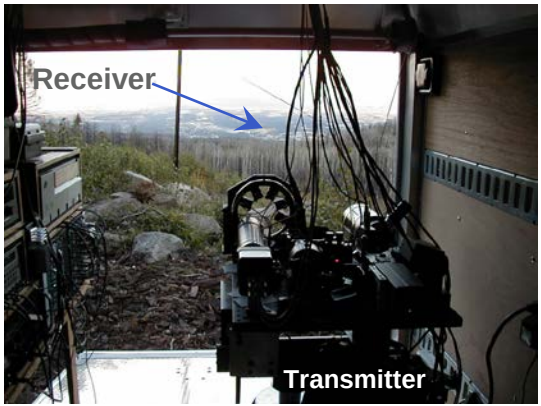
Sample of key material at 10-km range in daylight one-airmass path: comparable optics to satellite-to-ground

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: QC for Electric Grid Security

- **Objective**

  Use quantum cryptography to secure PMU/PDC data packets with acceptable latency
  - *Existing crypto cannot authenticate within latency requirement*

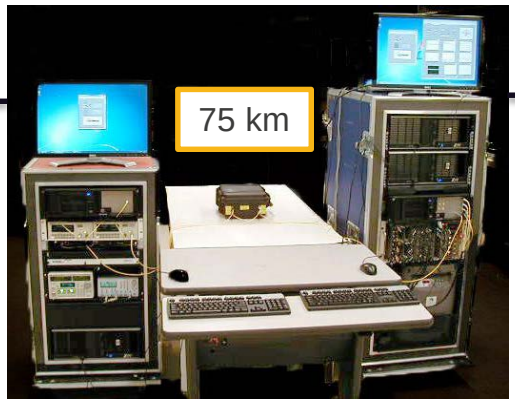
- **Bump-in-the-wire retrofit on an existing comm system**

- **Result**

  Fully operational with existing SCADA hardware

  Multicast authentication within latency requirement

Industry-standard phasor measurement unit



Industry-standard phasor data concentrator

Achievable range depends on detectors

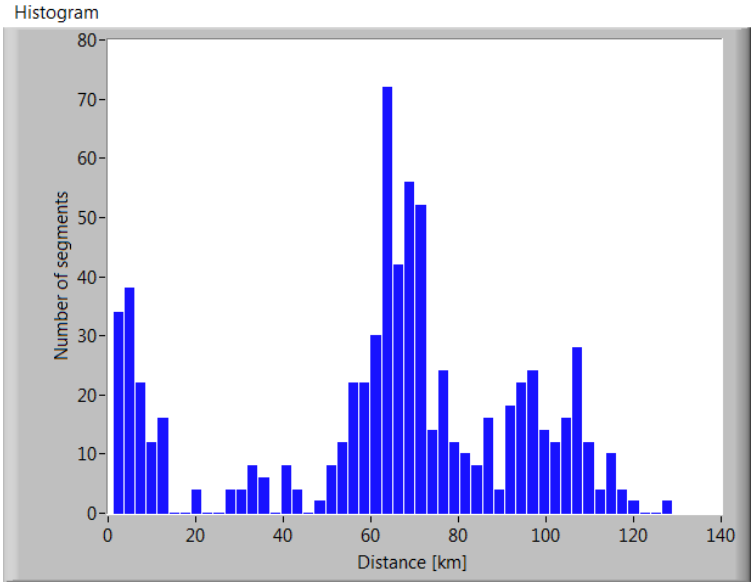
- **The security of a Quantum communication system is contingent on the transmitter sending only one photon at a time (or at most, a few)**

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

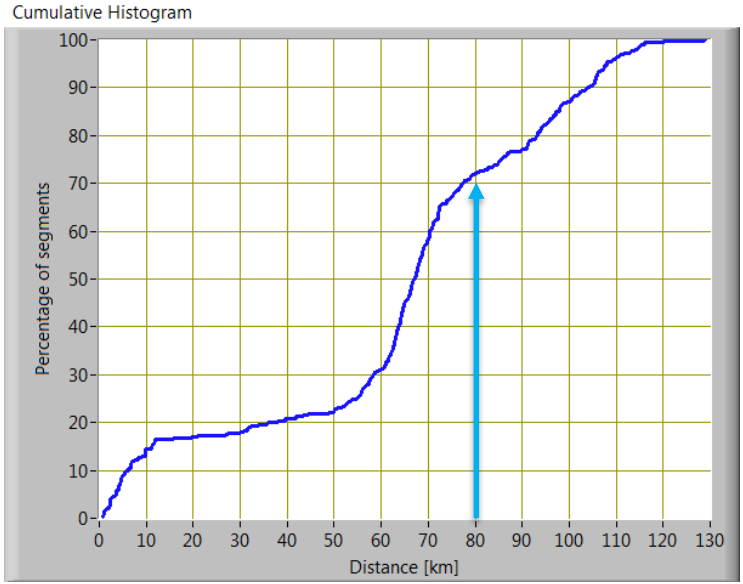
	Avalanche photodiode	Superconducting nanowire	Transition edge sensor
Efficiency @1550 nm	20%	80%	>95%
Mechanism	Electron-hole pairs avalanche in an over-biased p-n junction	Heat from photon warms a superconductor above critical temperature	Heat from photon warms a superconductor above critical temperature
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 ESnet'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.



Data courtesy of Christopher Tracy, ESnet LBNL

Quantum communication ≠ quantum computing

Quantum computing is **offense**

A quantum computer could be used to break most existing cryptography

Quantum computers don't exist yet, but are under development worldwide

Quantum communication is **defense**

Quantum communication could not be broken by a quantum computer

But quantum comms could still be vulnerable to bad implementations

The other defense against quantum computers is a new type of math-based cryptography called **Post-Quantum Cryptography,** also called **Quantum-Safe Cryptography**

Security is based on a different set of difficult math problems, which are believed to remain difficult even for a quantum computer

The NSA has publicly endorsed this approach

Quantum Comm in USA & The World

Worldwide many governments are making significant investments in quantum communications

- **Europe**
  - €1B Initiative on Quantum Technology program, start 2018. Part of the H2020 R&D framework
- **UK**
  - £120M 6-year project to build quantum technology hubs, started 2014
- **Canada**
  - $140M Transformative Quantum Technologies initiative, started 2016
- **China**
  - Several $100M investment over past five years
  - Launched world's first quantum communications satellite in July 2016
  - Quantum com satellite successful, published several papers summer 2017
  - Building 2,000 km QC link from Beijing to Shanghai
    - Major portions complete summer 2017

In contrast, domestic programs have been smaller scale, shorter duration, and not coordinated

- **Commerce**
  - NSF EFRI ACQUIRE – $13M program to develop chip-scale quantum repeaters 2017-2020
- **Energy**
  - Office of Electricity Cybersecurity for Energy Delivery Systems project $12M 2010- 2020
- **Defense**
  - DARPA QUINESS - $24M program to extend range and rate of QC 2013-15
  - DARPA InPho $19M program to increase bit density 2012-14
  - ONR Free-Space Optical program 2013-15
  - ONR Applied Research in Quantum Information Science 2015-18
- **DNI/DTO/IARPA**
  - Various programs 2001 – 2009 estimate $60M

Quantum science provides unparalleled security assurances in many different contexts

- **QC is forward-secure; compromises in the future do not retroactively compromise today's data**
  - Free space: satellite to ground, ship to shore, UAV to terminal…
  - Fiber optic: metro-area, site-wide, LAN, campus…
  - Once keys are made, any communication can be secured
- **Recent inventions expand QC to fiber network environments**
  - Vital cryptographic functions built on quantum primitives
  - Enables scalable, deployable, and affordable QC networks
- **Free-space QC is under active development throughout the world**
  - Keyserver in the sky
  - LPI/LPD communications
  - High-bandwidth comms where RF environment is unworkable
- **Must develop these capabilities *before* we need them**