

# Quantum Cryptography at Los Alamos National Laboratory: QES & QKarD

Raymond Newell  
Jane Nordholt (P.I.)  
Richard Hughes (P.I.)  
Glen Peterson

**July 28<sup>th</sup>, 2010**

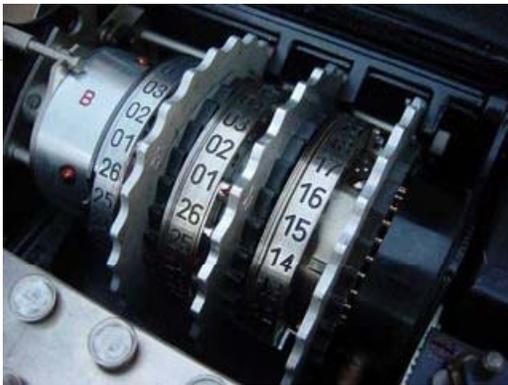
# Outline

- Introduction to Quantum Cryptography
  - Classical vs. Quantum
  - The BB84 Protocol
  - Key generation and encryption
- Quantum Enabled Security (QES)
  - What it is
  - What it is good for
- Quantum Smart Card (QKarD)
  - What it is
  - What it is good for

# The 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<sup>†</sup>

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
- stored
- re-read

indefinitely, and without altering it



Cuneiform tablet,  
ca. 2400 b.c.e.

Quantum information can be

~~• duplicated~~

No-cloning theorem

• stored

Yes, but very hard!

~~• re-read~~

Wavefunction collapse

indefinitely, and without altering it

Quantum systems are very well-suited for secret communication

Not so good for storing secrets

# 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

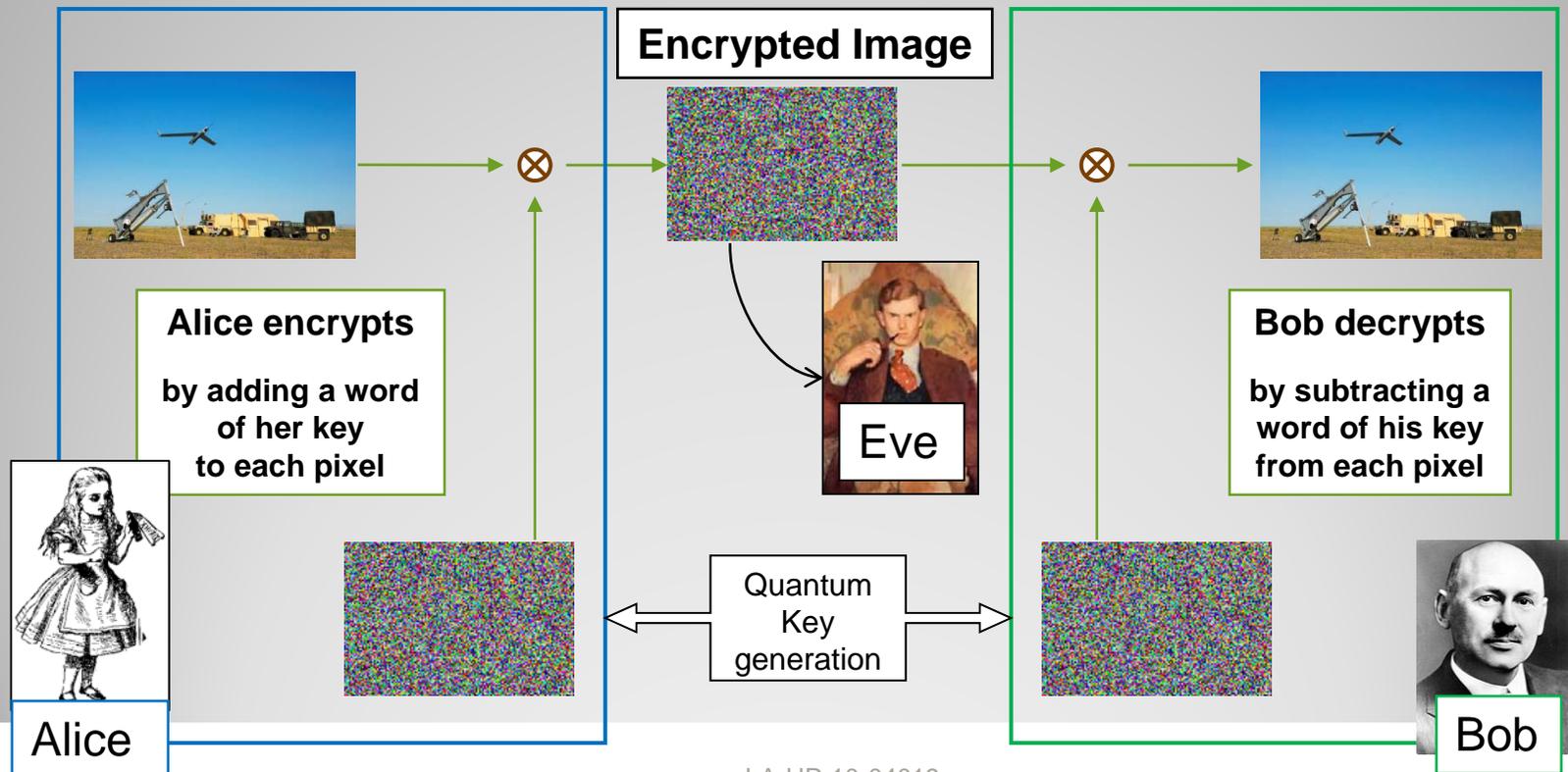
- Encode information onto the **state** of a **quantum system**
- Send quantum **system**
- Measure system's **state**

- **Quantum system** – single photons
- **State** – their polarization

# Key generation

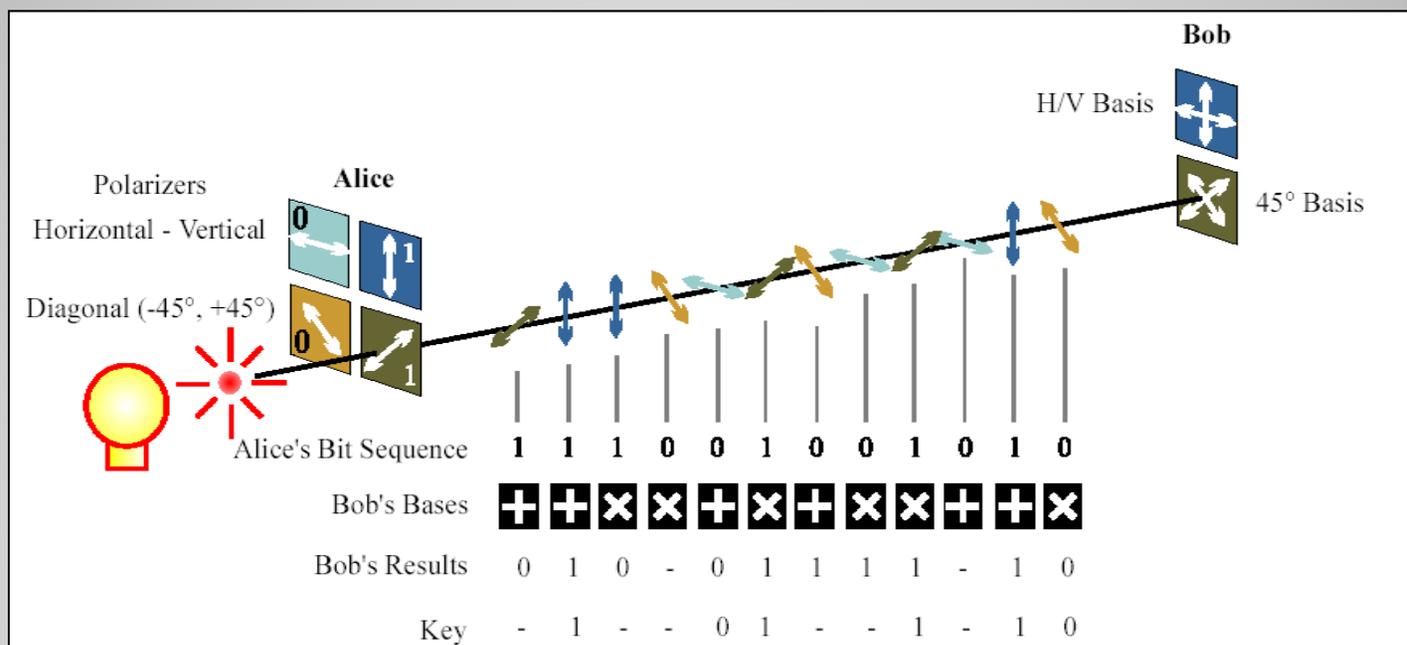
- Goal is to create a shared secret key which is used to encrypt data
- Encrypted data is then transmitted by "Alice" to "Bob"

Bit values in the key don't matter, so long as only Alice & Bob know them

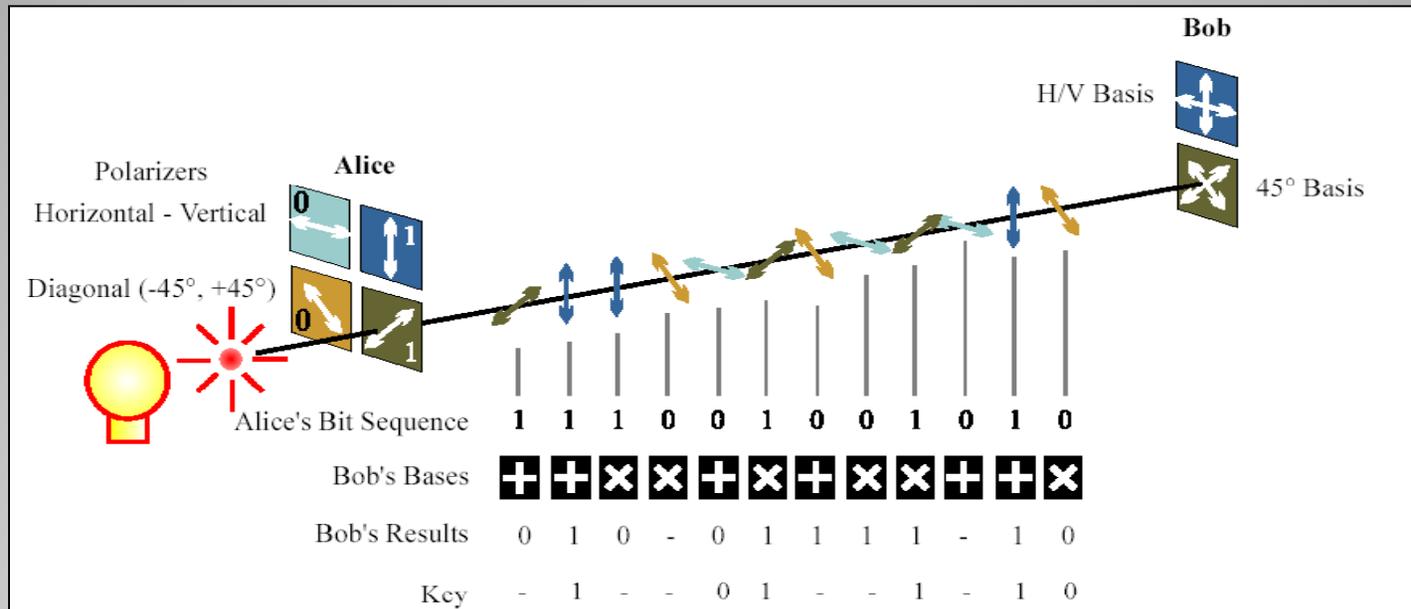


# BB-84 Protocol

- 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:
  - When they used different bases, they discard that bit
  - When they used the same basis, they keep that bit
- The resulting "sifted" bit stream is secure

# An optical technology...

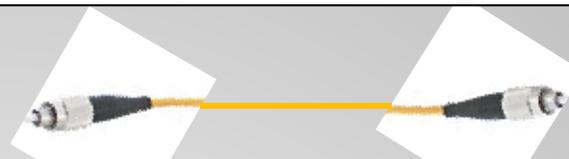
Key generation requires an *optical* connection between Alice and Bob



## Free Space

- Rooftop to rooftop
- Airplane to ground
- Ship to ship
- Satellite to ground
- Etc...

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



## Fiber Optics

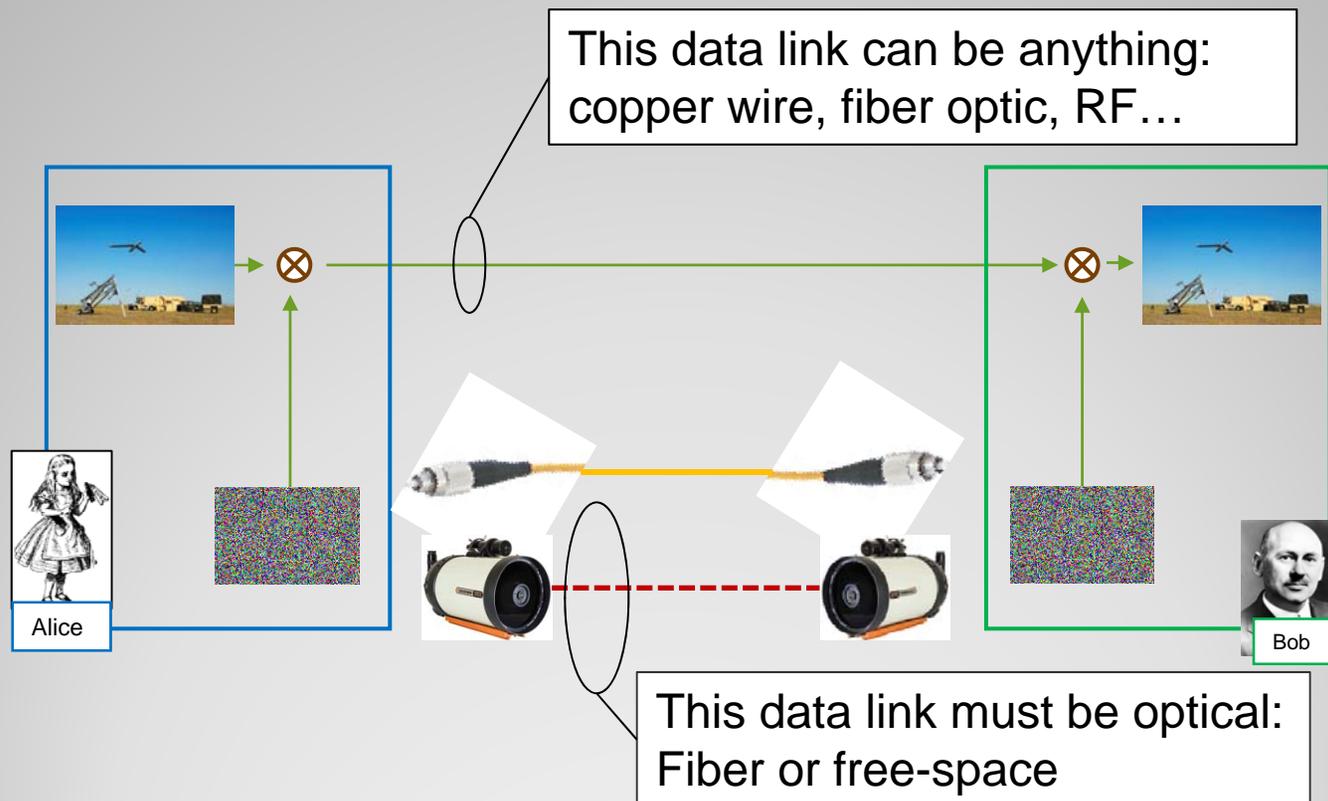
- Standard telecom fibers
- Coexist with DWDM data
- Within a building
- FTTx link
- Metro
- Up to 200 km

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

**LANL team leads the world in both types**

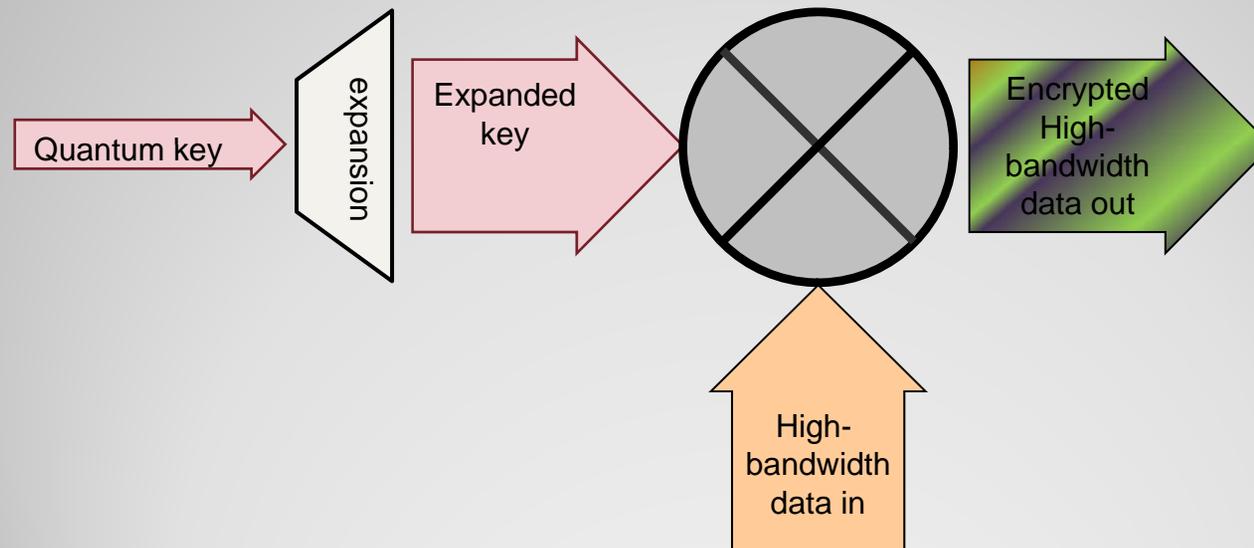
# ...use is not restricted to optics

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



# Quantum keys can secure high-bandwidth links

- Current systems generate quantum keys at 1 to  $\sim 10$  kbit/sec
- These keys can be “expanded” with cryptographic algorithms to much larger bit sequences
- Bandwidth of secure channel can be much higher than key generation rate



# What makes quantum keys better?

- Classical keys are generated with algorithms
  - Must assume the algorithm is known to all
- If a small portion of key is compromised (guessed, leaked, whatever) the whole thing is compromised
  - Run algorithm backwards to find the preceding key
  - Run algorithm forward to find following key
- Quantum keys have no algorithmic heritage
  - “backward security”: can’t compute preceding values
  - “forward security”: can’t compute following values

# What makes quantum keys *even better*?

- Quantum keys are Future Proof\*
  - Do not rely on computational complexity
  - Storing quantum-encrypted data to crack the code later won't work
  - Inventing a quantum computer wouldn't help

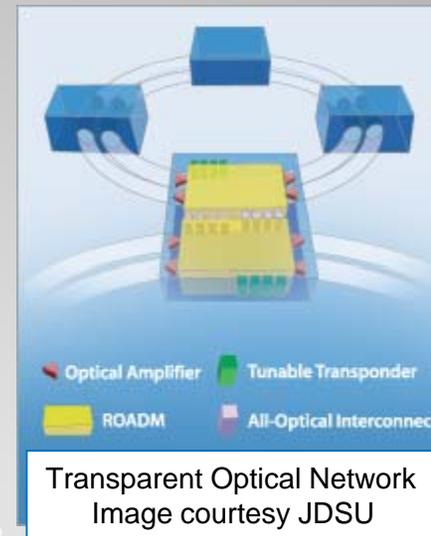
\* Certain types of time travel have been shown to break quantum keys

# Quantum Enabled Security (QES)

- Synthesis of fiber-optic data comm with real-time quantum key generation
  - Quantum keys used to generate secret codes
  - Transmitter uses secret codes used to spread data signals in wavelength and time
  - Receiver de-spreads using same secret code
  - Eavesdropper unable to reconstruct original data
- Provides telecommunications security at the *physical* layer
  - Eavesdropper can't even tell what a bit is

# QES can be added to transparent optical networks

- Older fiber optic networks use *electrical* amplifiers and routers
  - Don't preserve quantum information
  - Incompatible with QES
- Modern networks use *optical* amplifiers and routers
  - EDFA for amplifiers
  - Gratings, prisms, MEMs for switches
  - These preserve quantum states
  - Compatible with QES

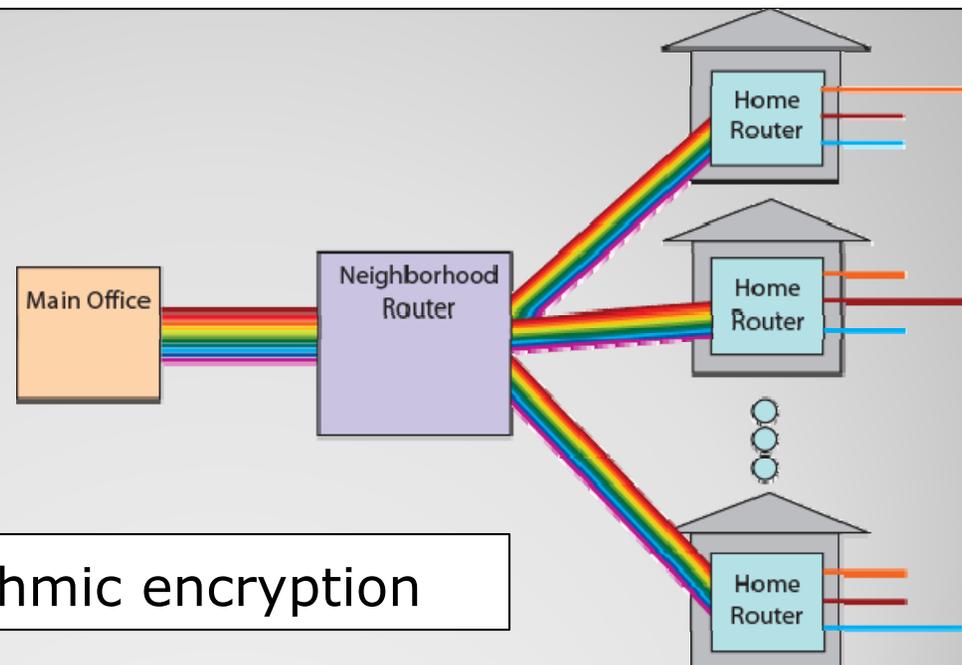


Verizon FiOS



# Fiber to the home

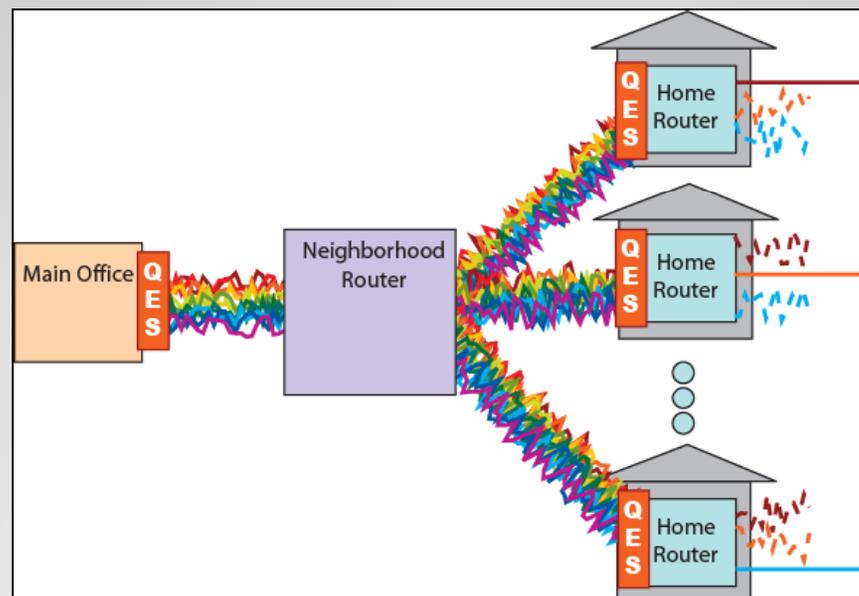
- Transparent fiber network from core to the home
- 32 wavelengths assigned to 32 users
- Wavelength demultiplexing takes place *in the home*
- All your data go to 31 neighbors; 31 neighbors' data goes to you!



- Verizon uses algorithmic encryption

# Fiber to the home with QES

- Each data channel hops between one of 32 wavelengths and one of 32 time bins
- Spreading code generated from quantum keys
- Eavesdroppers don't know keys; can't unscramble the hopping



# Fiber taps

- Optical fibers are easy to tap
  - COTS taps readily available
  - Not hard to DIY, either
- Even if standard encryption remains unbroken, vulnerabilities exist
  - Traffic flow analysis
  - Authentication
  - Jamming



# QES defeats taps

By spreading the signals in wavelength and time, *average* signal power can be set below the noise floor

## Authorized Receiver

- Knows the spreading code
- Always looks in the right place at the right time
- Gains a signal-to-noise advantage

## Eavesdropper

- Does not know the spreading code
- Has to measure at all wavelengths and all timeslots
- Must accept large input noise
- Cannot even see the bits, much less unscramble them

# Domain of use

Any location with transparent optical network

- FTTx
- Avionics
- Data center
- Corporate campus
- Industrial site
- Embassy abroad
- Etc...

- Compatible with existing fiber optic infrastructure
- No need to lay new fiber, or dedicate existing fiber
- Dedicated hardware package installed at each sender/receiver
- Hardware design leverages existing telecom devices

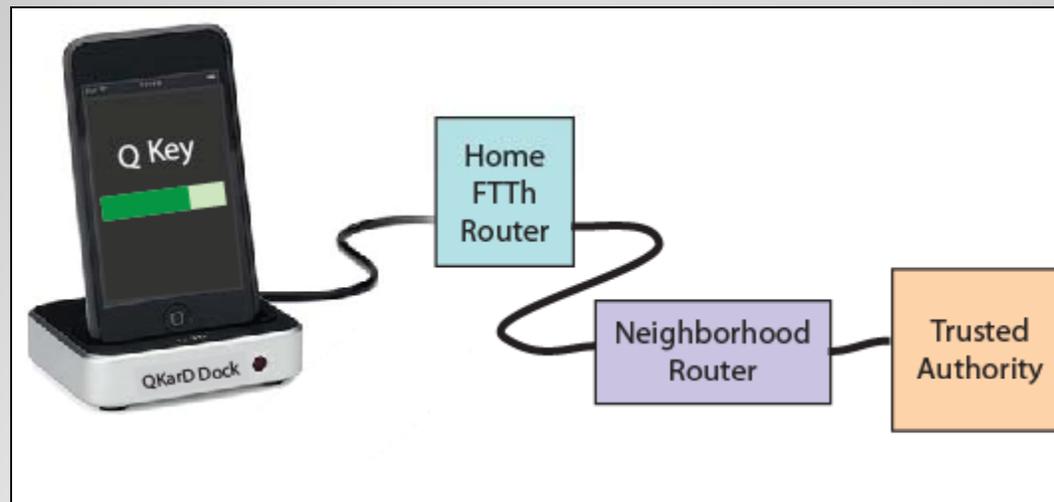
# Quantum Smart Card: QKarD

- Handheld Quantum Key generator for the end-user
- Offers unconditional security for any digital transfer:

Cell phone call	Bank transfer	Facility access	and on and on..
VoIP	Finance	Vehicle access	
Videoconference	E-commerce	E-voting	
Telepresence	Digital media	Database protection	
- Periodically connect to optical network to generate quantum keys
- Device stores quantum keys in secure memory
- Keys used for on-the-fly encryption over any network

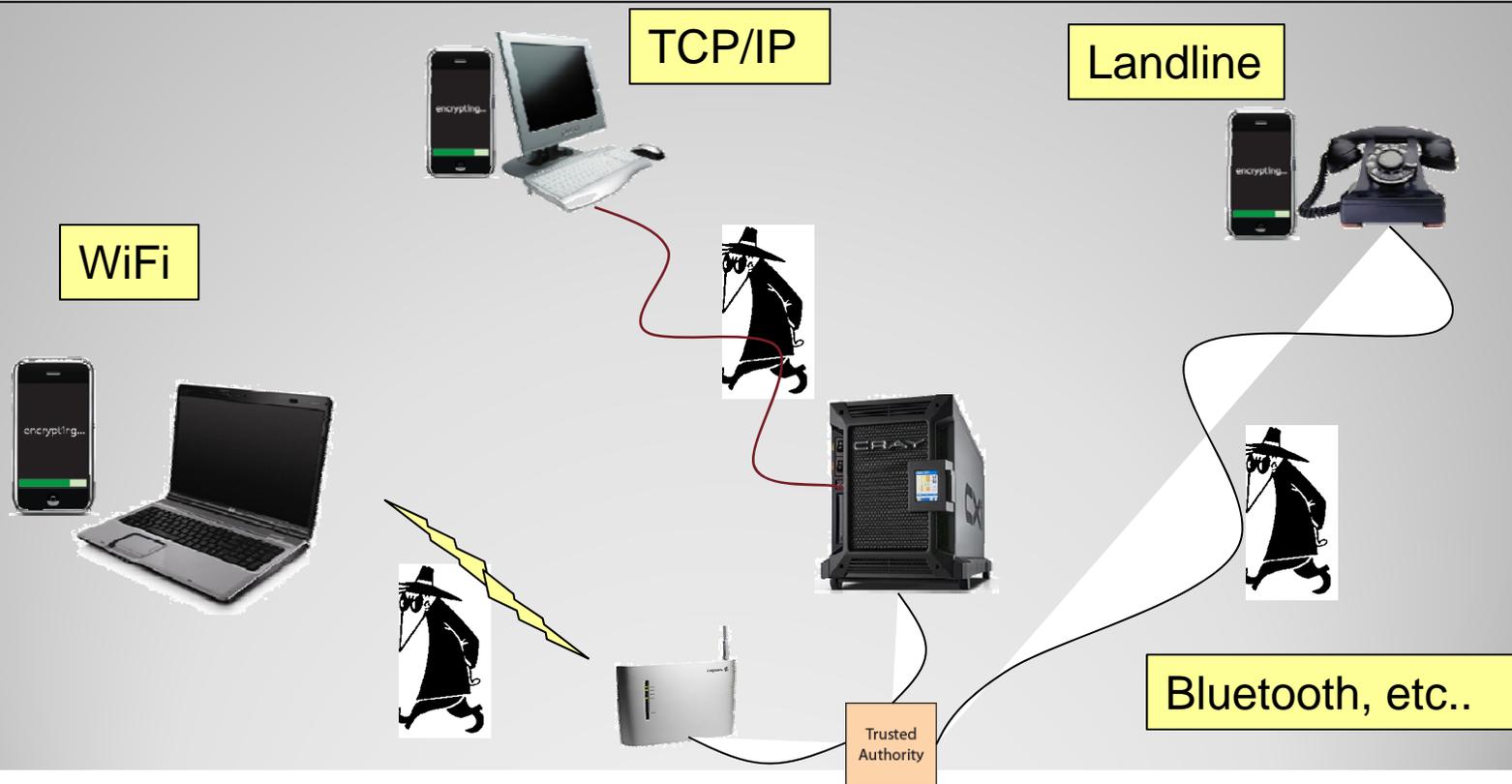
# Docking

- QKarD dock has fiber optic connection to central Trusted Authority
- Performs QKD to establish quantum keys on QKarD
- Keys stored for later use in secure memory



# Unconditionally secure communication

Quantum keys stored in QKarD are used to encrypt communications on other devices



LA-UR 10-04019

# Quantum secure smartphone

Possible to incorporate QKarD technology into a smartphone





# Summary

- Quantum cryptography changes the game: security comes from laws of physics, not hard math problems
- QES is a demonstrated, functioning technology which transmits quantum-encrypted data over existing telecom infrastructure
- QKarD is a buildable technology for a handheld personal electronic device which generates and stores quantum keys for secure transmission of any data