Building a QKD Network out of Theories and Devices

December 17, 2005

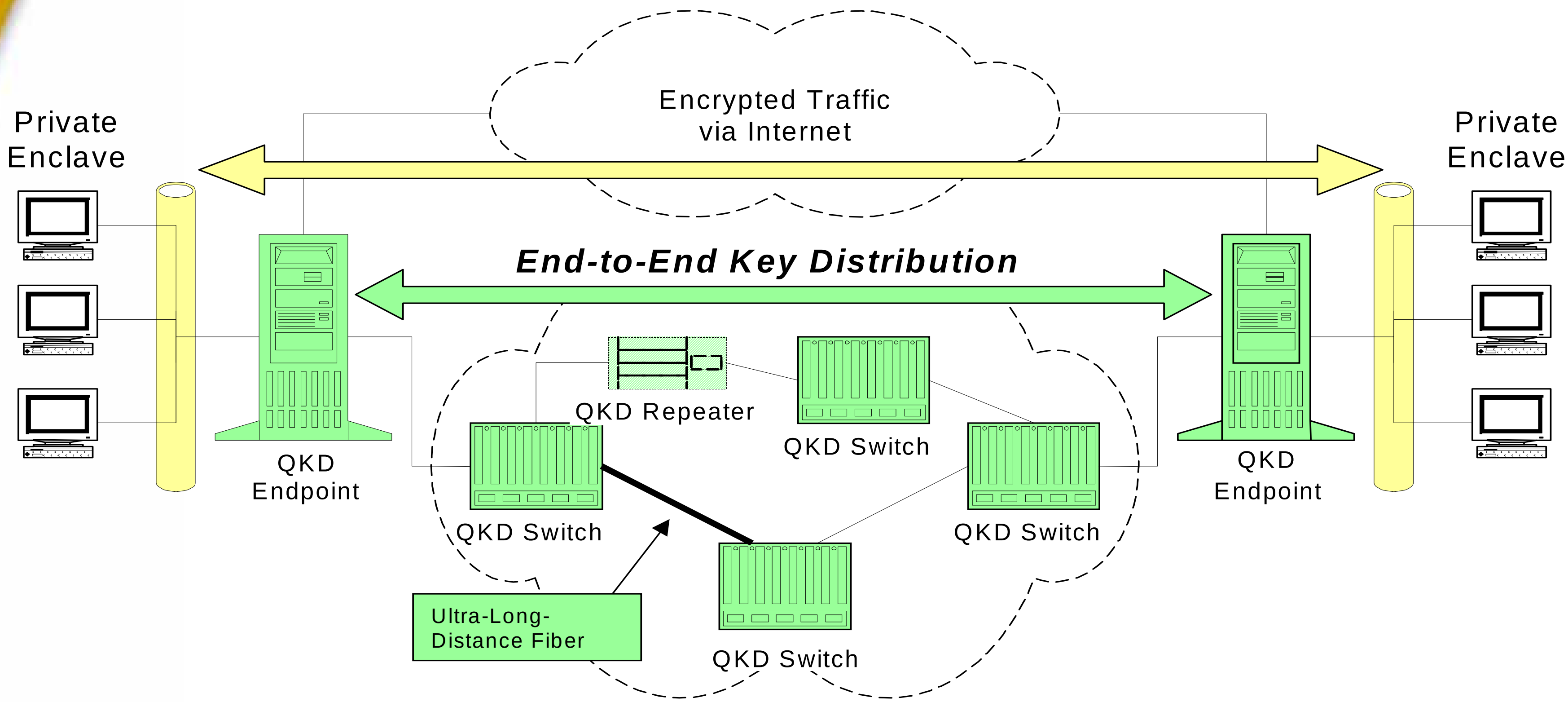
David Pearson
BBN Technologies
dpearson@bbn.com

DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

Why QKD? Why now?

- Unconditional security, guaranteed by the laws of physics, is *very* compelling
- Public-key cryptography gets weaker the more we learn – even for classical algorithms
- If we had quantum computers tomorrow we'd have a disaster on our hands.
- Future proofing – secrets that you transmit today using classical cryptography may become vulnerable next year (RSA '78 predicted 4 x 10^9 years to factor a 200-digit key, but it was done last May)
- The technology of QKD seems to be mature enough that we can start to create usable systems.

DARPA Quantum Network - Goals



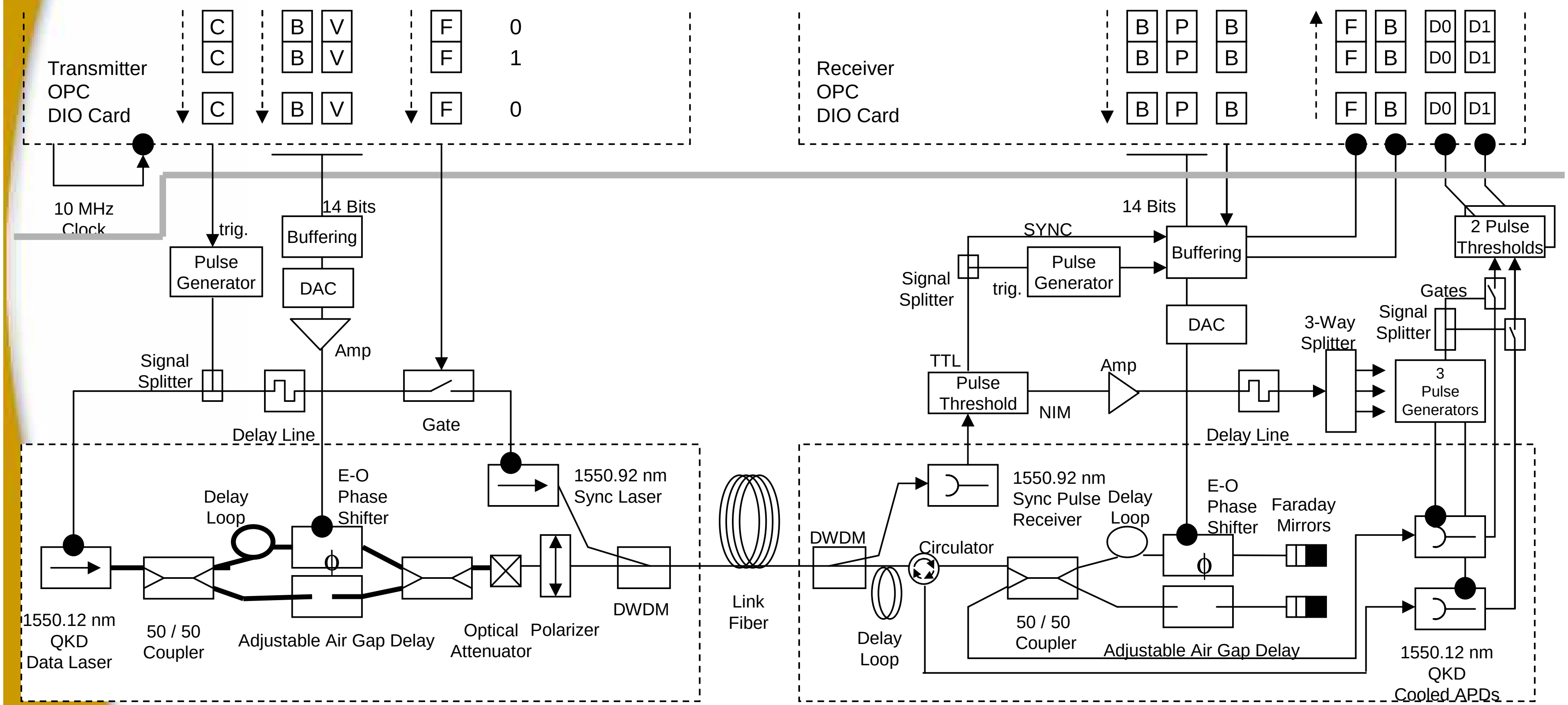
We are designing and building the world's first Quantum Network, delivering end-to-end network security via high-speed Quantum Key Distribution, and testing that Network against sophisticated eavesdropping attacks.

As an option, we will field this ultra-high-security network into commercial fiber across the metro Boston area and operate it between BU, Harvard, and BBN.

'Mark 2' Weak Coherent QKD Links

4 Nodes Continuously Operational Since October 2003

- **Polarization Independent**
- **Sync & Data at 1550 nm**
- **Active Path Length Control**



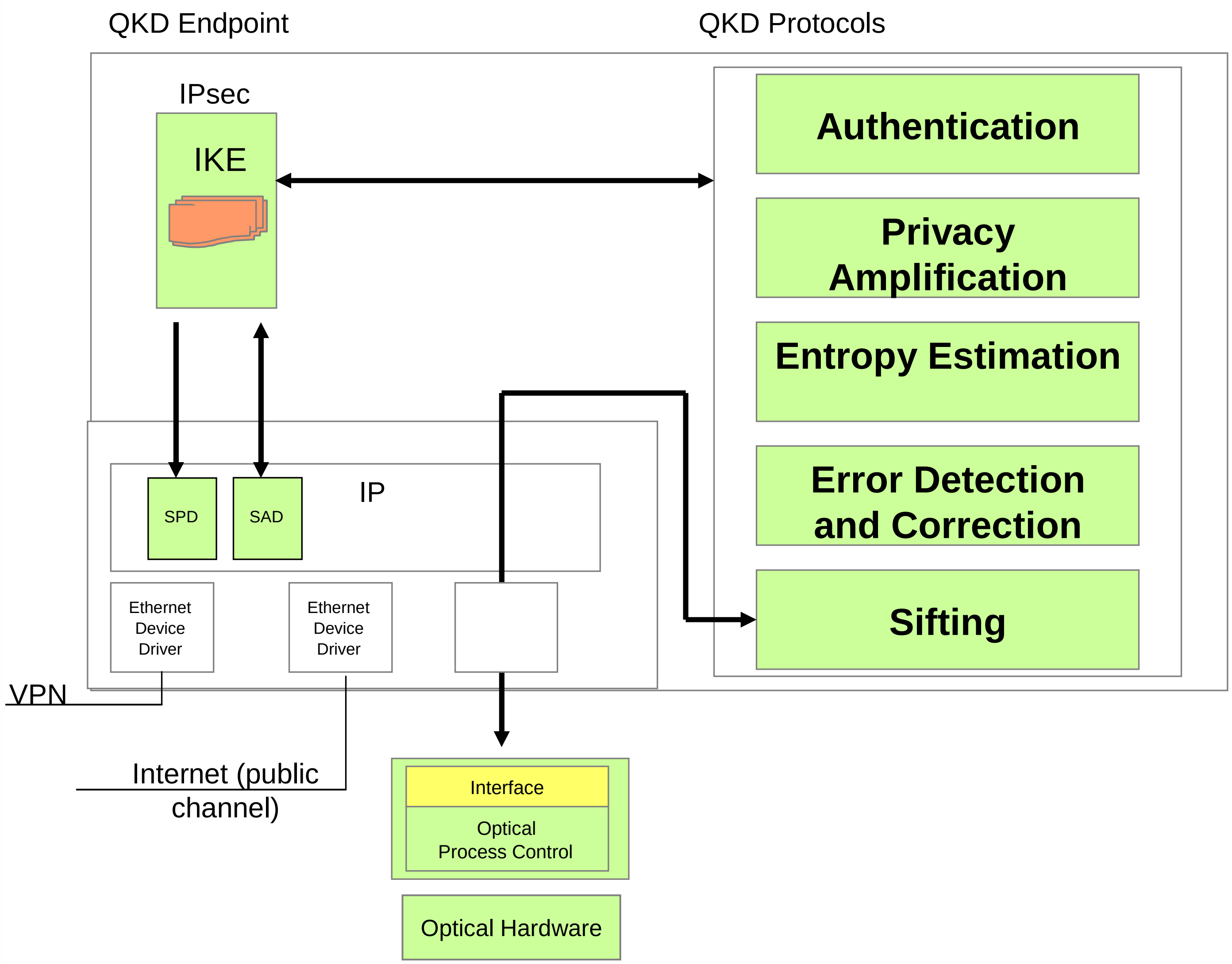
Transmitter (Alice)

Receiver (Bob)

November 5, 2003

DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

QKD Software Suite and Protocols

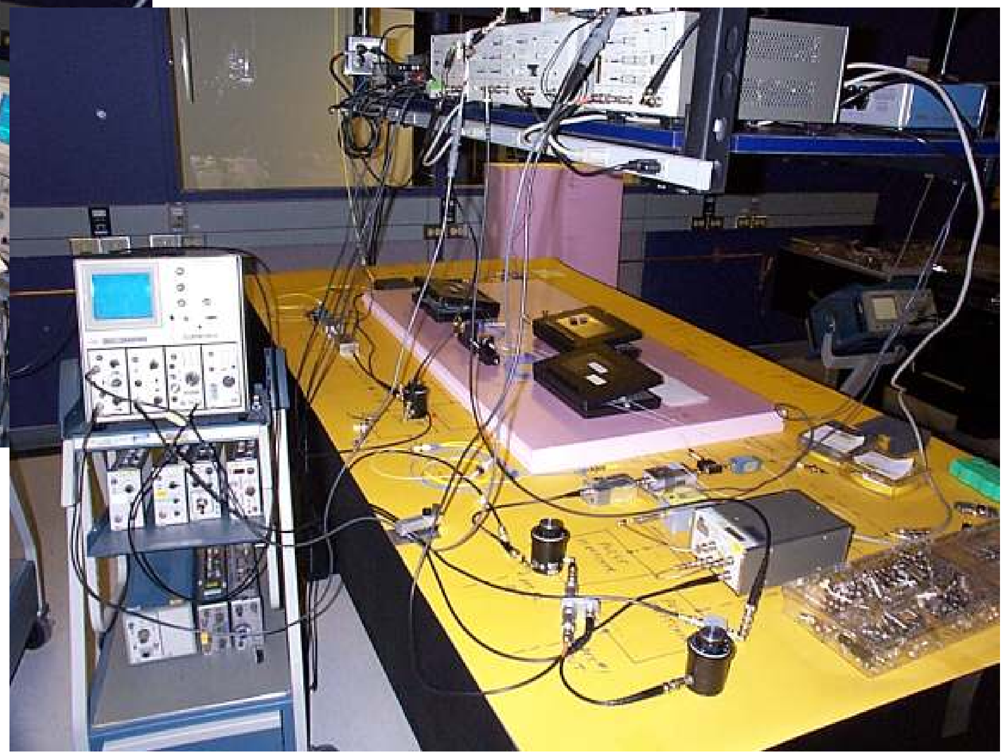


Status as of 3½ Years Ago

The Year 1 Weak-Coherent Link

Alice

Bob



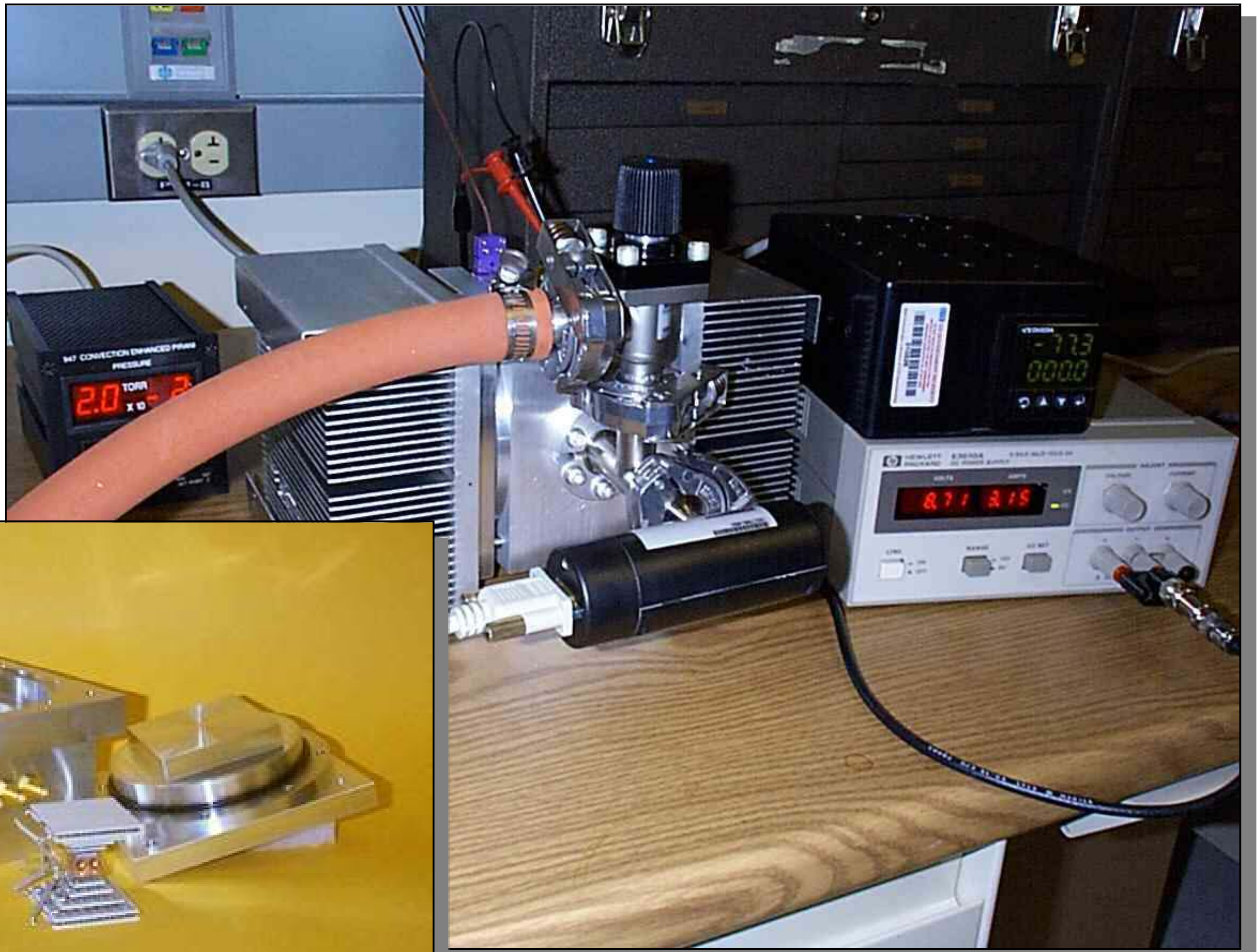
The Cooled Detector Package

2 Epitaxx detectors (EPM 239 AA SS)

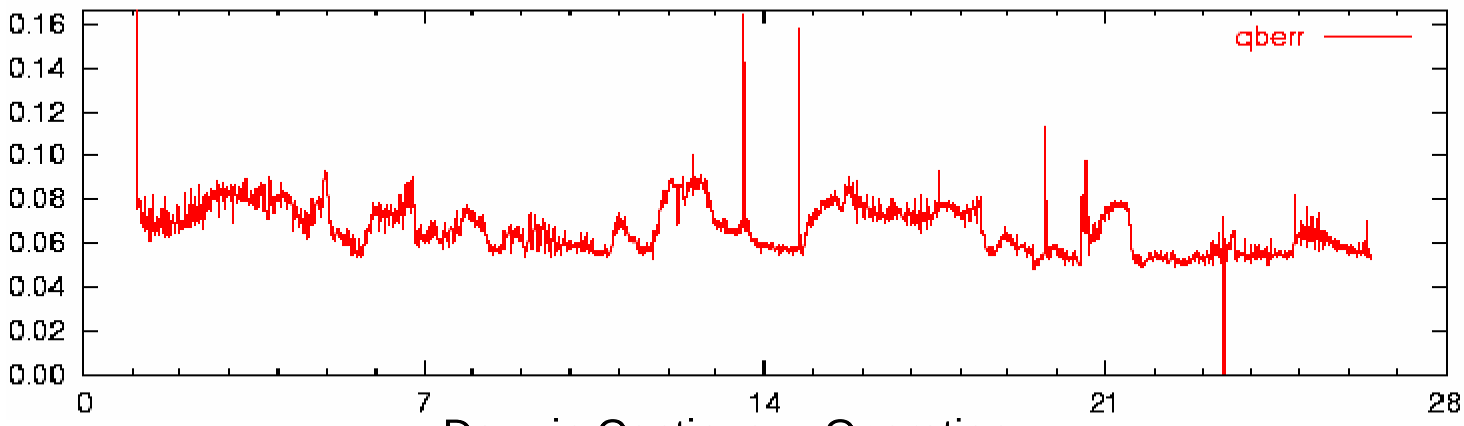
Dual Peltier coolers

Approx. 2 x 10^{-2} Torr

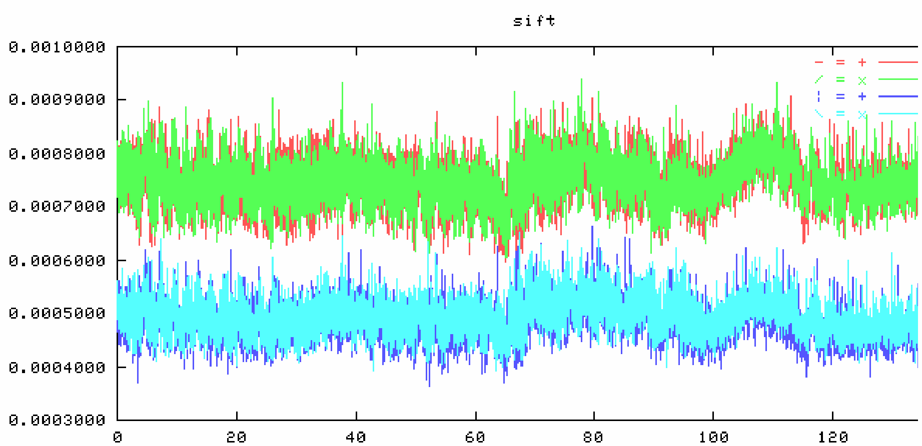
Operates near –60 C, achieves –80 C max

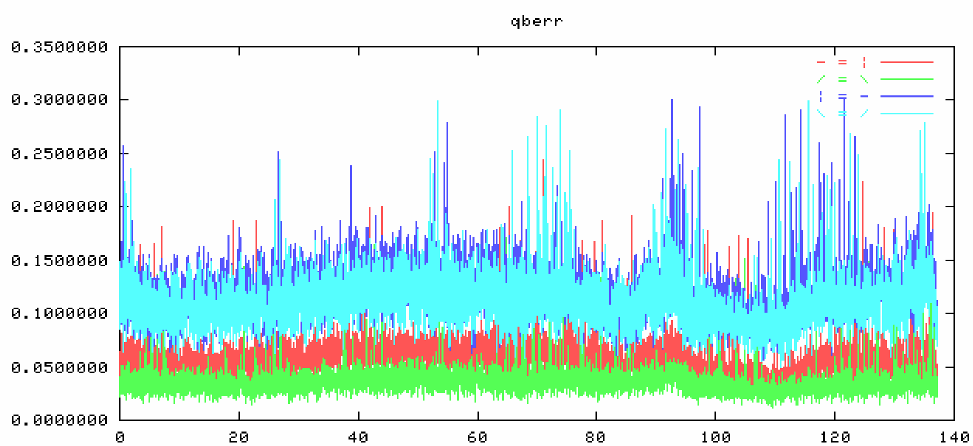


First Days Up and Running



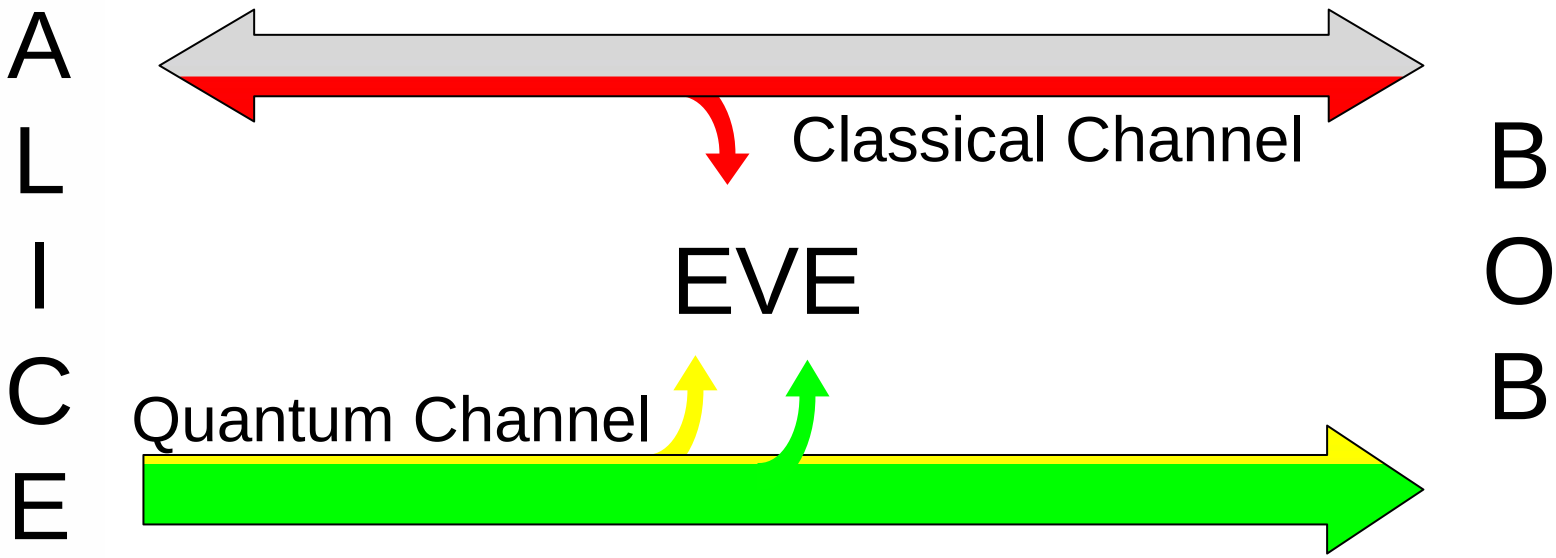
Mean emission = 0.1 photons/pulse;
Perfect results would be 0.05; 10% quant. Eff. would be 0.005





Time in Hours, Data Segment ended 2 Jan 03

Bounding Eve's Information
(the heart of QKD)



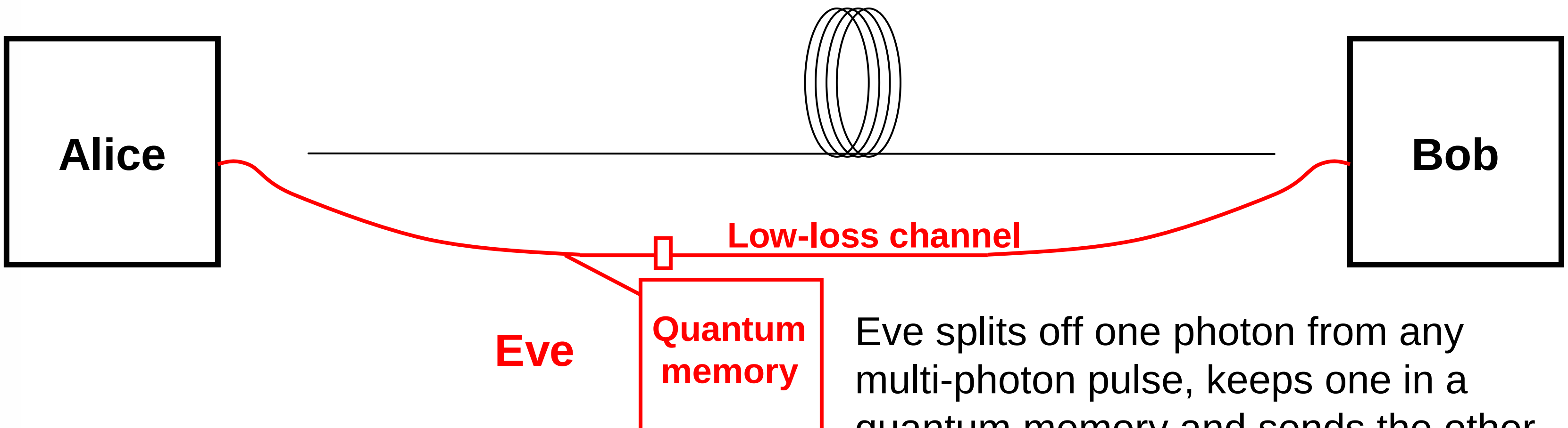
Information Eve learns:

- t Bits from probing single-photon pulses
- q Classical bits leaked
- ν Bits from imperfect quantum channel

After we get the bound, we use privacy amplification to reduce Eve's knowledge to $\varepsilon << 1$

Imperfections in the Quantum Channel (taking security proofs w/ a grain of salt)

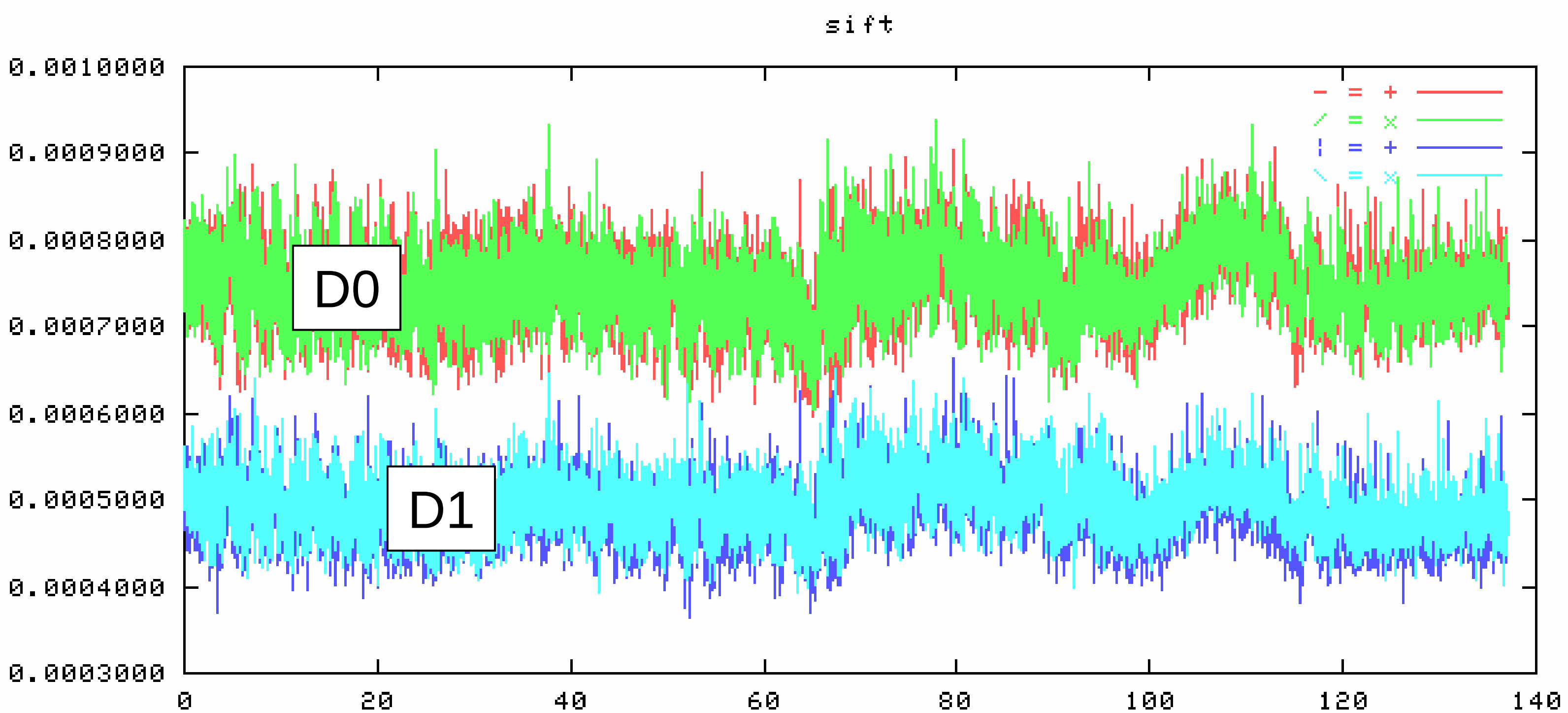
- Multi-photon pulses (weak coherent ≠ single photon)



Eve splits off one photon from any multi-photon pulse, keeps one in a quantum memory and sends the other through to Bob over a special low-loss channel. If she doesn't get a photon, she blocks the pulse. When bases are announced she measures her stored qbit in the correct basis

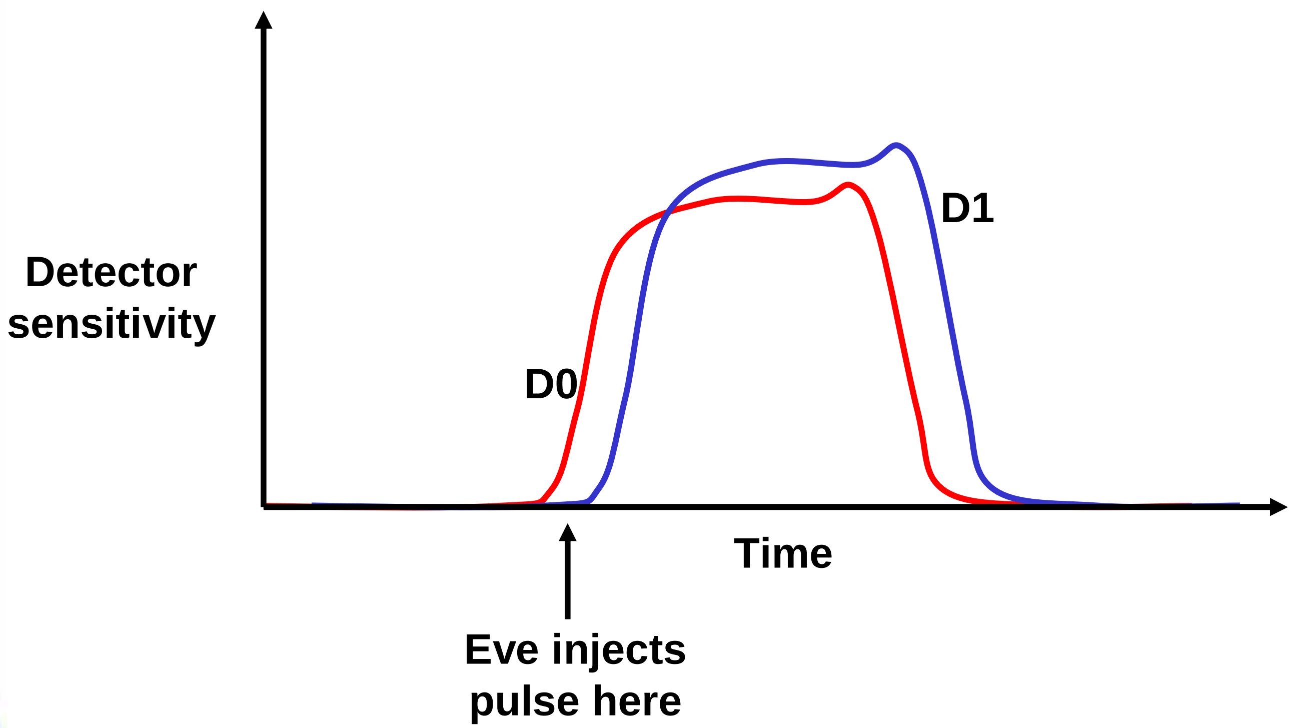
Imperfections in the Quantum Channel (taking security proofs w/ a grain of salt)

- Multi-photon pulses (weak coherent ≠ single photon)
- Unbalanced detectors



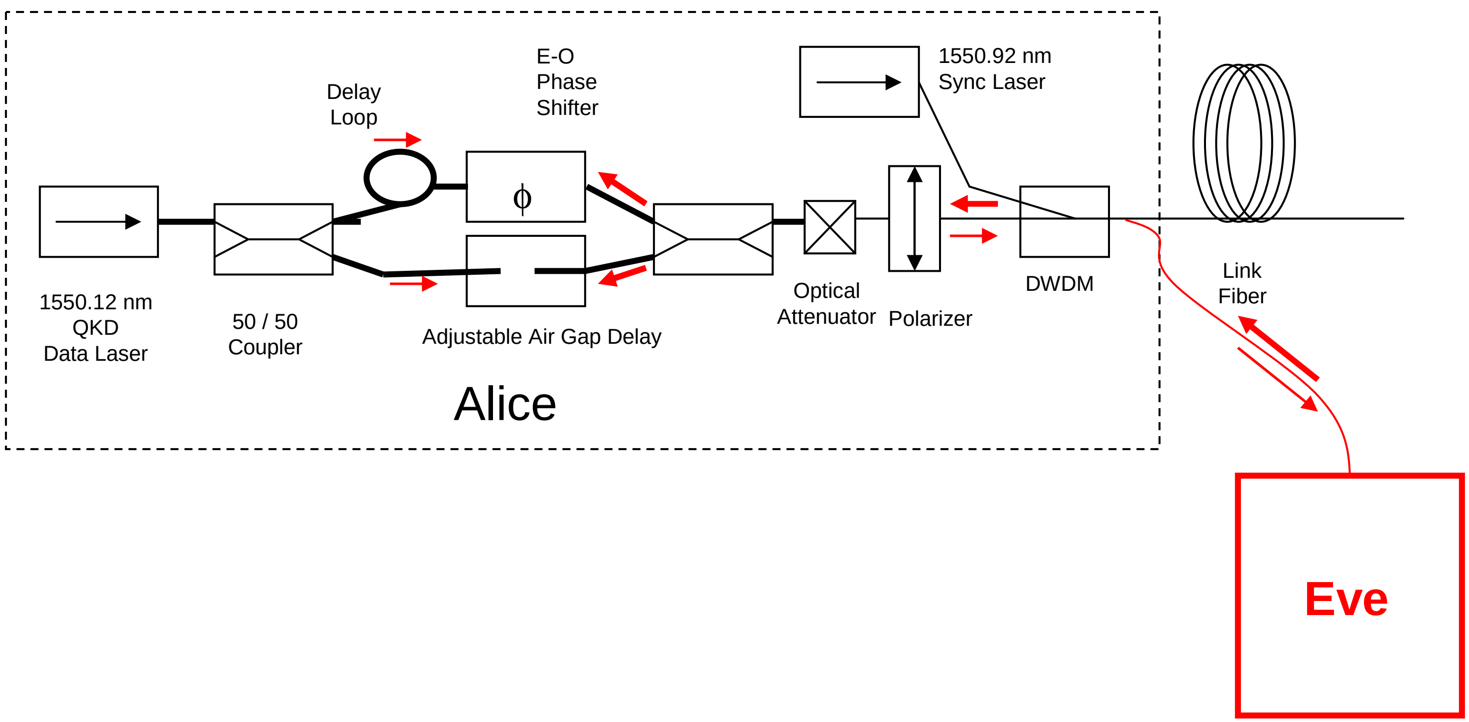
Imperfections in the Quantum Channel
(taking security proofs w/ a grain of salt)

- Multi-photon pulses (weak coherent ≠ single photon)
- Unbalanced detectors
- Timing imperfections in detectors



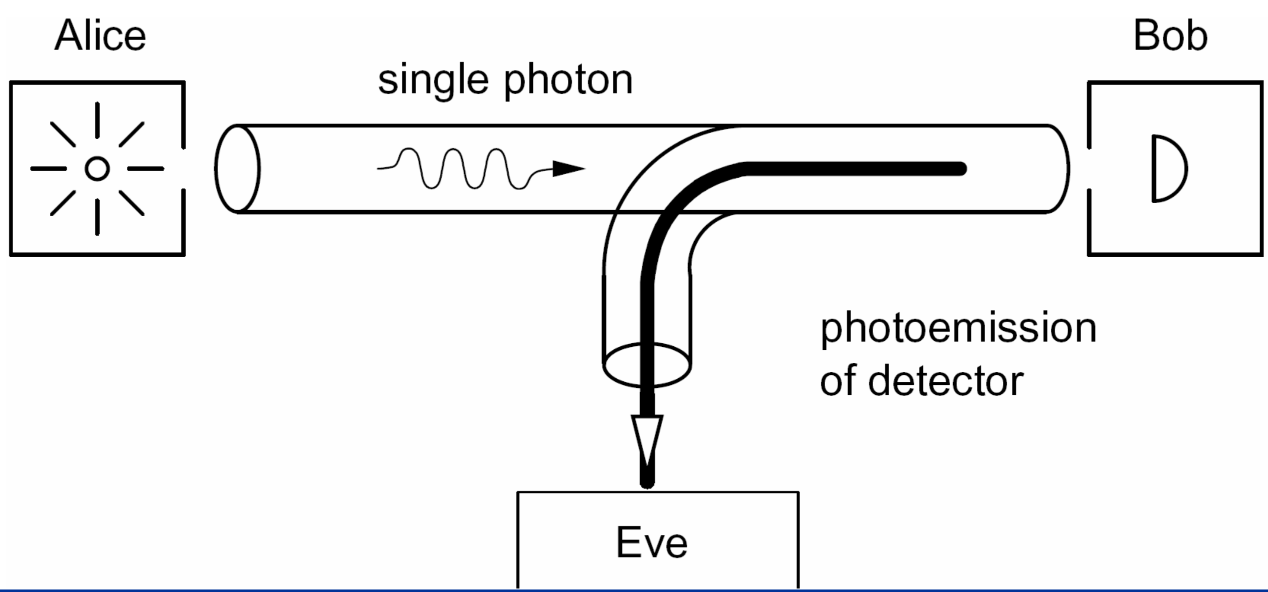
Imperfections in the Quantum Channel
(taking security proofs w/ a grain of salt)

- Multi-photon pulses (weak coherent ≠ single photon)
- Unbalanced detectors
- Timing imperfections in detectors
- Active probes of Alice/Bob interferometers (OTDR)



Imperfections in the Quantum Channel (taking security proofs w/ a grain of salt)

- Multi-photon pulses (weak coherent ≠ single photon)
- Unbalanced detectors
- Timing imperfections in detectors
- Active probes of Alice/Bob interferometers (OTDR)
- Breakdown flash from APDs



Imperfections in the Quantum Channel (taking security proofs w/ a grain of salt)

- Multi-photon pulses (weak coherent ≠ single photon)
- Unbalanced detectors
- Timing imperfections in detectors
- Active probes of Alice/Bob interferometers (OTDR)
- Breakdown flash from APDs
- Memory effects of APDs

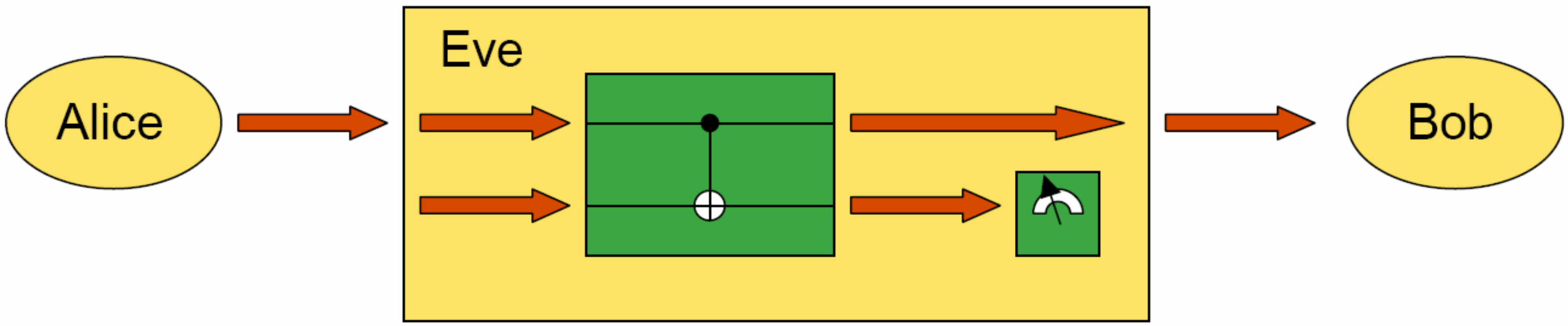
⋮

A consensus list of vulnerabilities would be a very valuable thing!

Some of the vulnerabilities we want to fix in the optics, some by monitoring, and some by privacy amplification (with extensions to the proofs)

Howard Brandt's entangling probe for BB84

(quant-ph/0509088)



Uses an entangling probe with a POVM which can *sometimes* unambiguously discriminate between 0 (in either basis) and 1. With loss, allows PNS-type attack for true single-photon source

Shapiro showed that Brandt left out part of the error rate (thank goodness!)

But it was plausible that the attack worked, despite the proofs

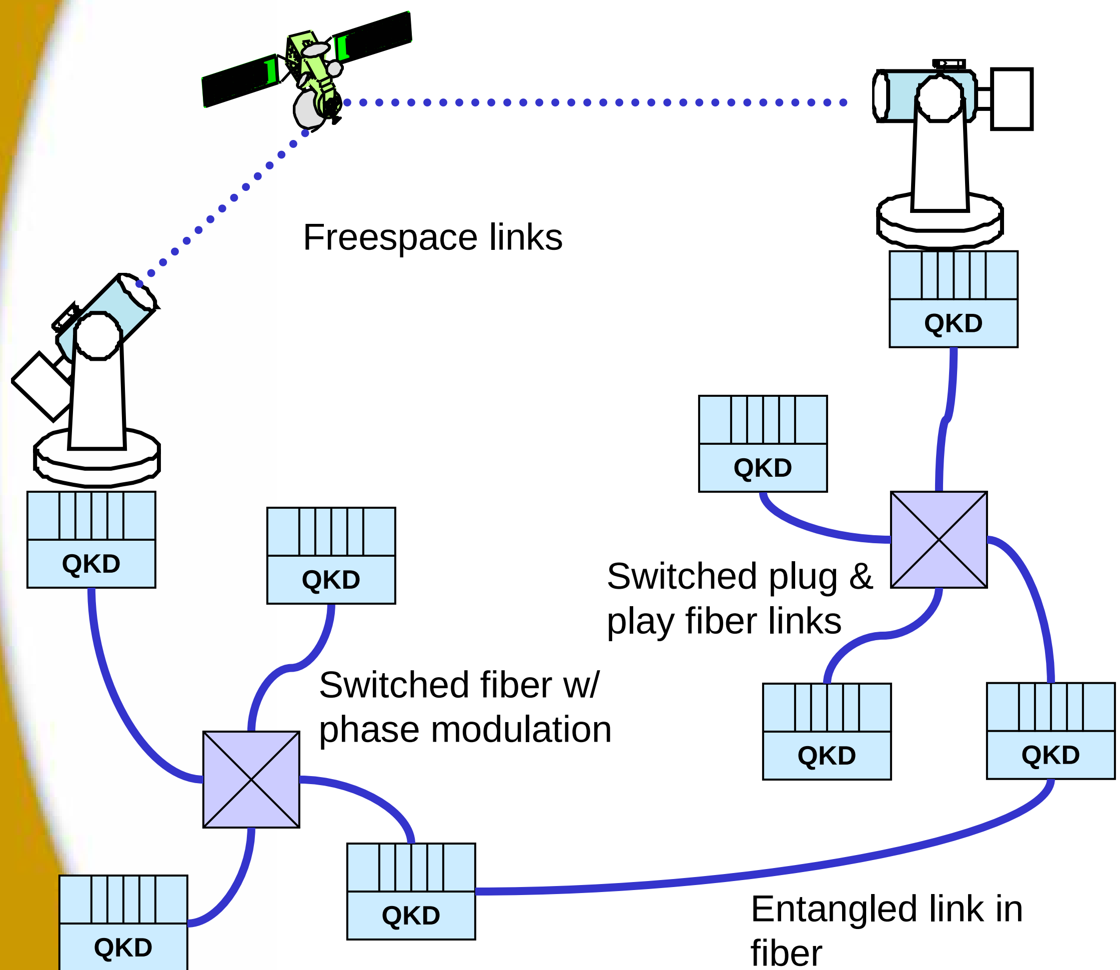
Quantum Networking

Quantum Networking

- Without a network, QKD will never “take off”
- The holy grail: using quantum teleportation and quantum memory to switch qbits
  - Could extend range of quantum communication through entanglement purification
  - At least 10 years off
- An interim solution: circuit-switched quantum links using optical switches
- Another useful technology: key relay through trusted intermediate nodes

Two Kinds of QKD Networking

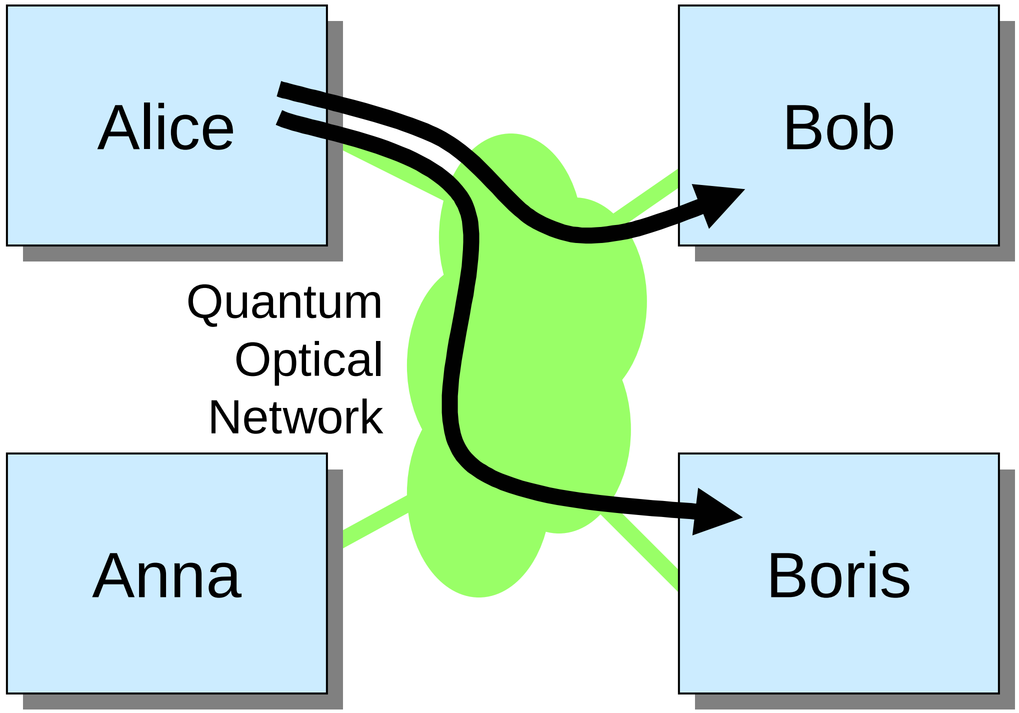
Currently Operational in DARPA Quantum Network



- Switched networks
  - Share infrastructure
  - Quite secure
  - Requires compatible technology
  - Limited in range
- Trusted networks
  - Can extend range
  - Allow different kinds of QKD to play together
  - Robust and redundant
  - Nodes *must* be kept secure

Optical Switching in DARPA Quantum Network

Nodes *Do Not* Need to Trust the Switching Network



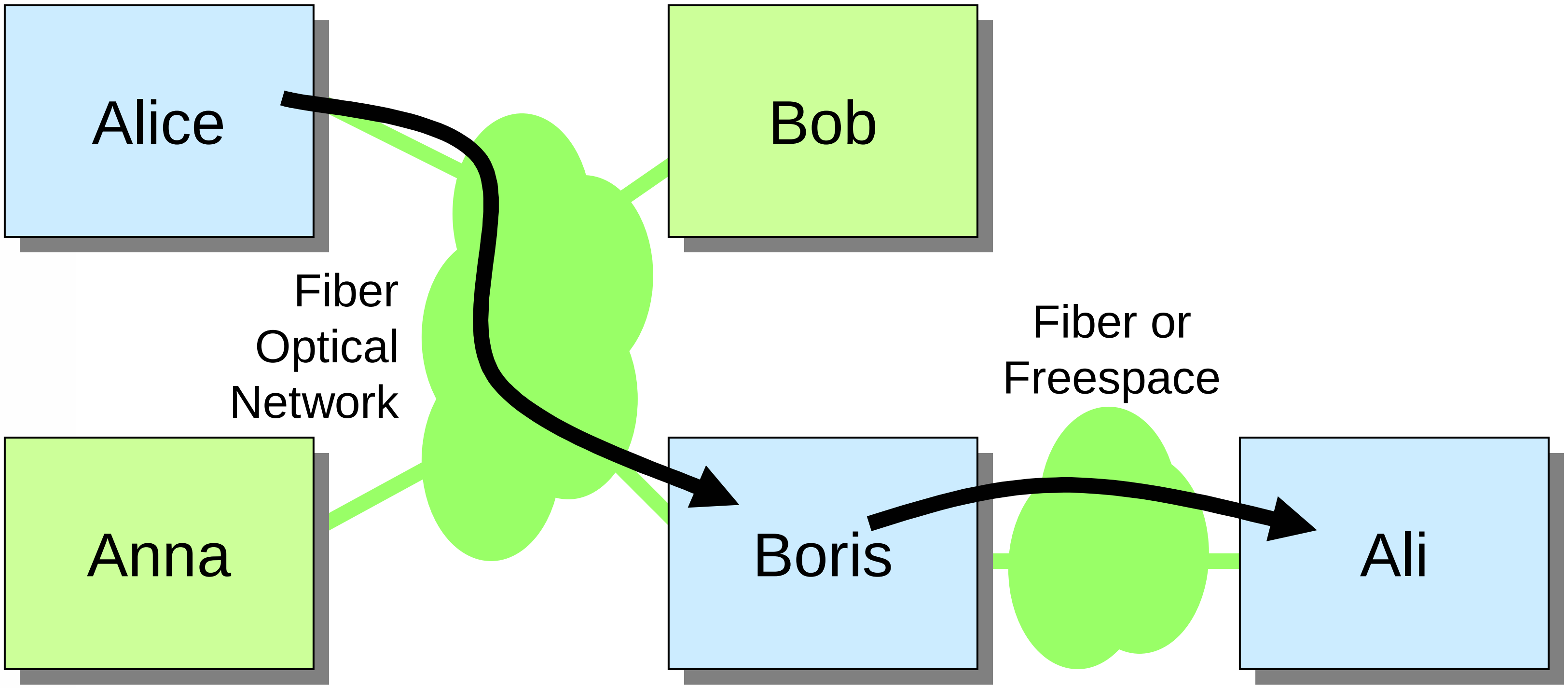
Pairwise QKD Key Material Built Up Between . . .

Alice & Bob	Alice & Boris
Anna & Bob	Anna & Boris

Suitable for Compatible QKD Nodes at Metro Distances

Key Relay in DARPA Quantum Network

Nodes *Do* Need to Trust the Relays

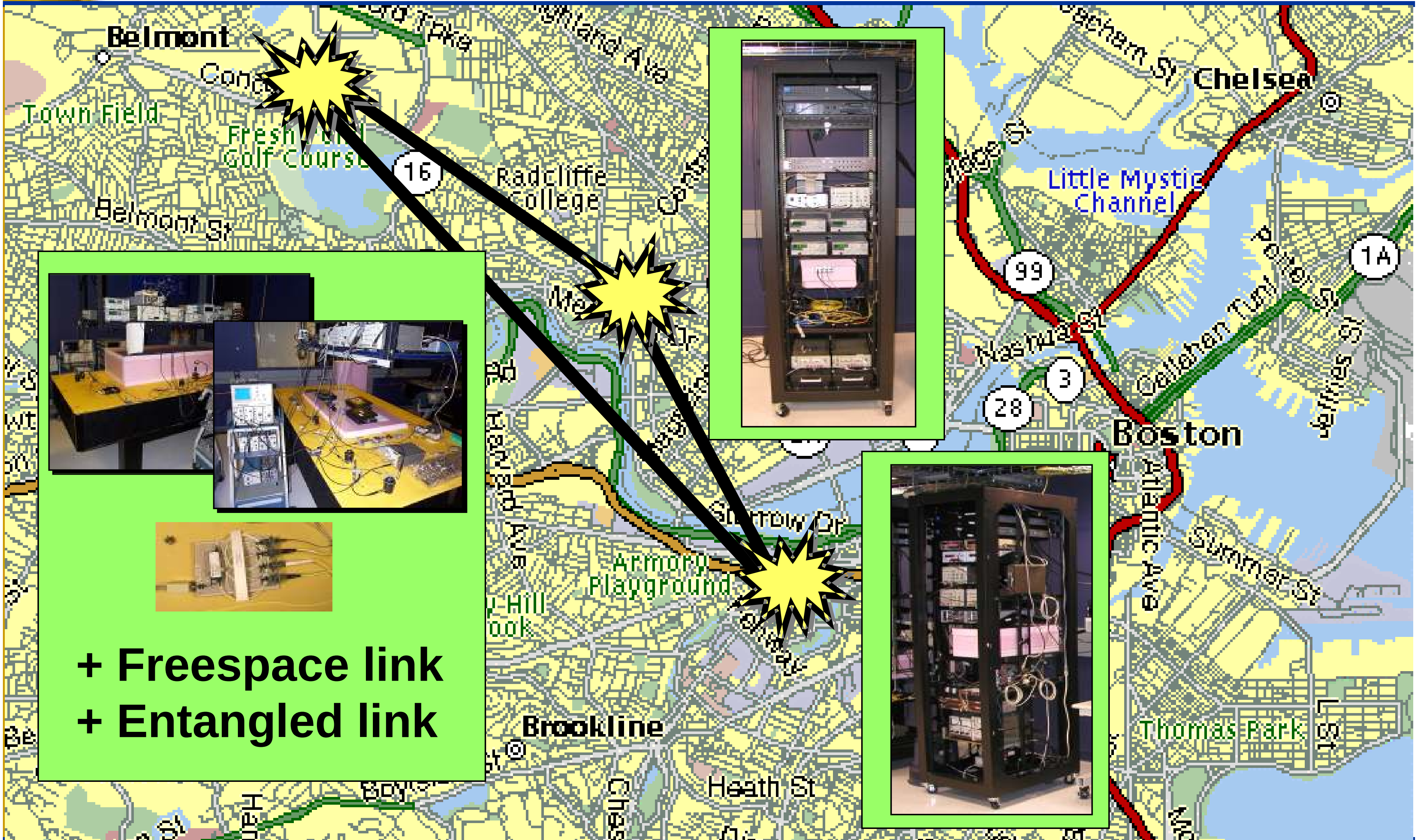


Pairwise QKD Key Material Built Up Between . . .

Alice & Ali	(via Boris as relay)
Bob & Boris	(via Alice or Anna as relay)

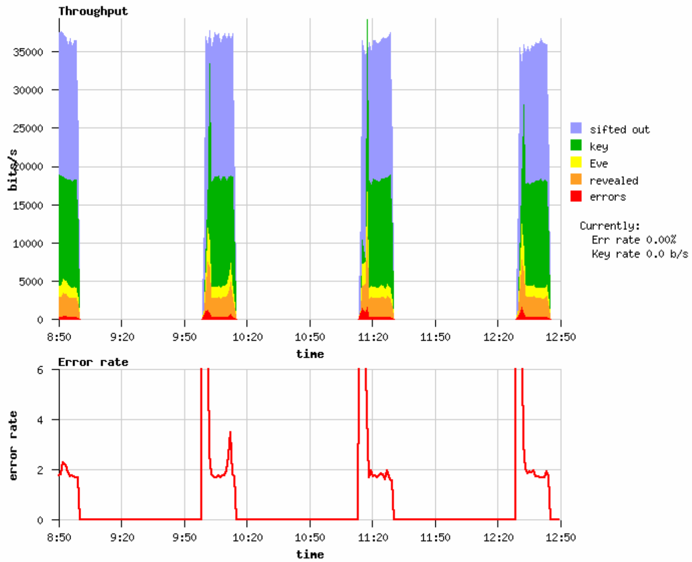
Suitable for Incompatible QKD Nodes or Long Distance Relay

The DARPA Quantum Network
Operating Continuously Across Cambridge Since 6/2004

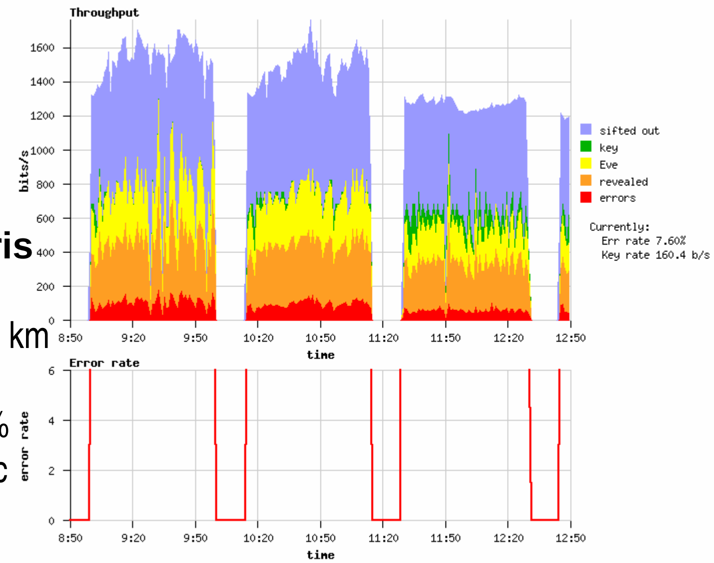


DARPA Quantum Network in Operation

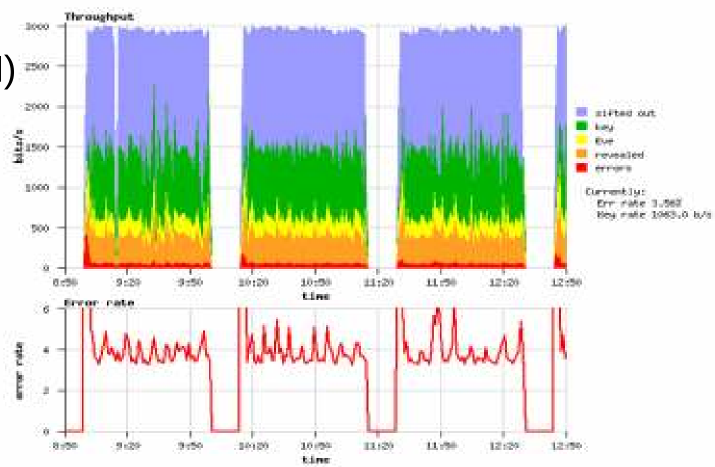
Alice / Bob
(Within BBN)
0 dB, 0 km
mu = **1.0**
QBER ~ 2%
~ 13,000 bits/sec



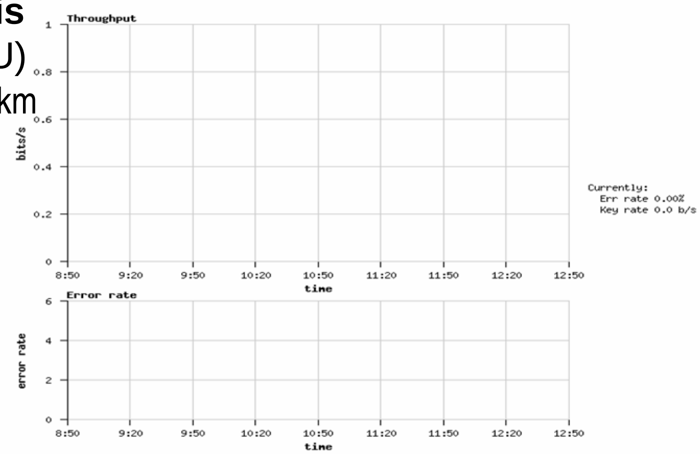
Alice / Boris
(BBN-BU)
11.5 dB, 19.6 km
mu = **1.0**
QBER ~ 7.6%
~ 160 bits/sec



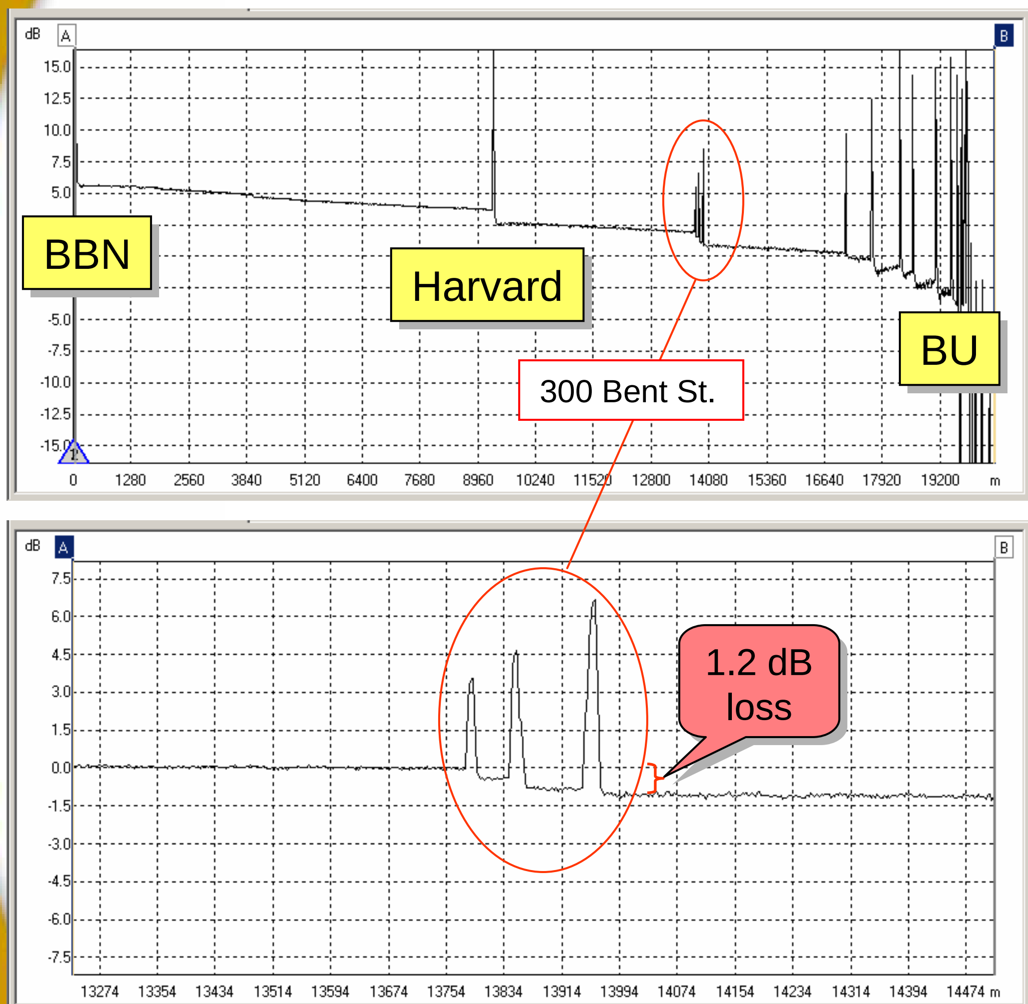
Anna / Bob
(Harvard-BBN)
5.1 dB, 10.2 km
mu = **0.5**
QBER ~ 3.5%
~ 1,000 bits/sec



Anna / Boris
(Harvard-BU)
16.6 dB, 29.8 km
mu = **0.5**
QBER: N/A
0 bits/sec



Cambridge Dark Fiber



Distances & Attenuations

	BBN	Harvard	BU
BBN		10.2 km 5.1 dB (a)	19.6 km 11.5 dB (b)
Harvard	10.2 km 5.1 dB		
BU	19.6 km 11.5 dB		

(a) Equivalent to 24.3 km fiber span at 0.21 dB/km
(b) Equivalent to 54.8 km fiber span at 0.21 dB/km
Both measurements include 2x2 fiber switch in path (~1 dB).

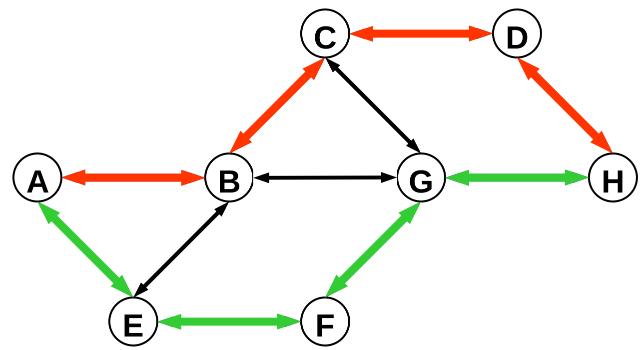
Many connectors in current path to BU (Boris) resulting in high atten. Will splice in coming months, but this gives a preview of mid-distance (~50 km) performance.

Routing and Key Relay

- Determines topology of network
- Chooses paths with small number of nodes, and ample key material
- Uses one-time-pad encryption of new key
- Transports *keys*, not *data*

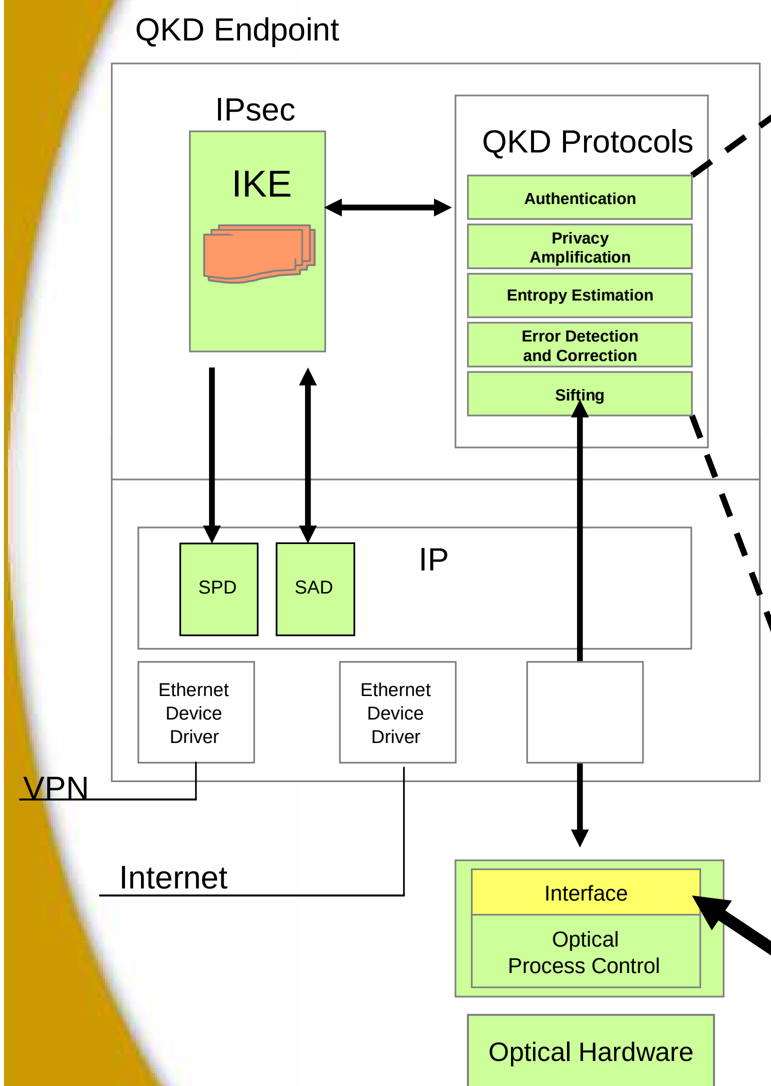
- Each node knows full network topology
- Can choose shortest path
- Or multiple independent shortest paths

A simple network



Open Testbed for QKD Networking

BBN's QKD Protocols
Modular Suite of QKD Protocols



Authentication

IPsec Based
- ✓ Public Key
- ✓ Secret Key

Privacy Amplification

- ✓ GF[2^n] Universal Hash

Entropy Estimation

- ✓ BBBSS 92
- ✓ Slutsky
- ✓ Myers / Pearson
- ✓ Shor / Preskill

Error Detection and Correction

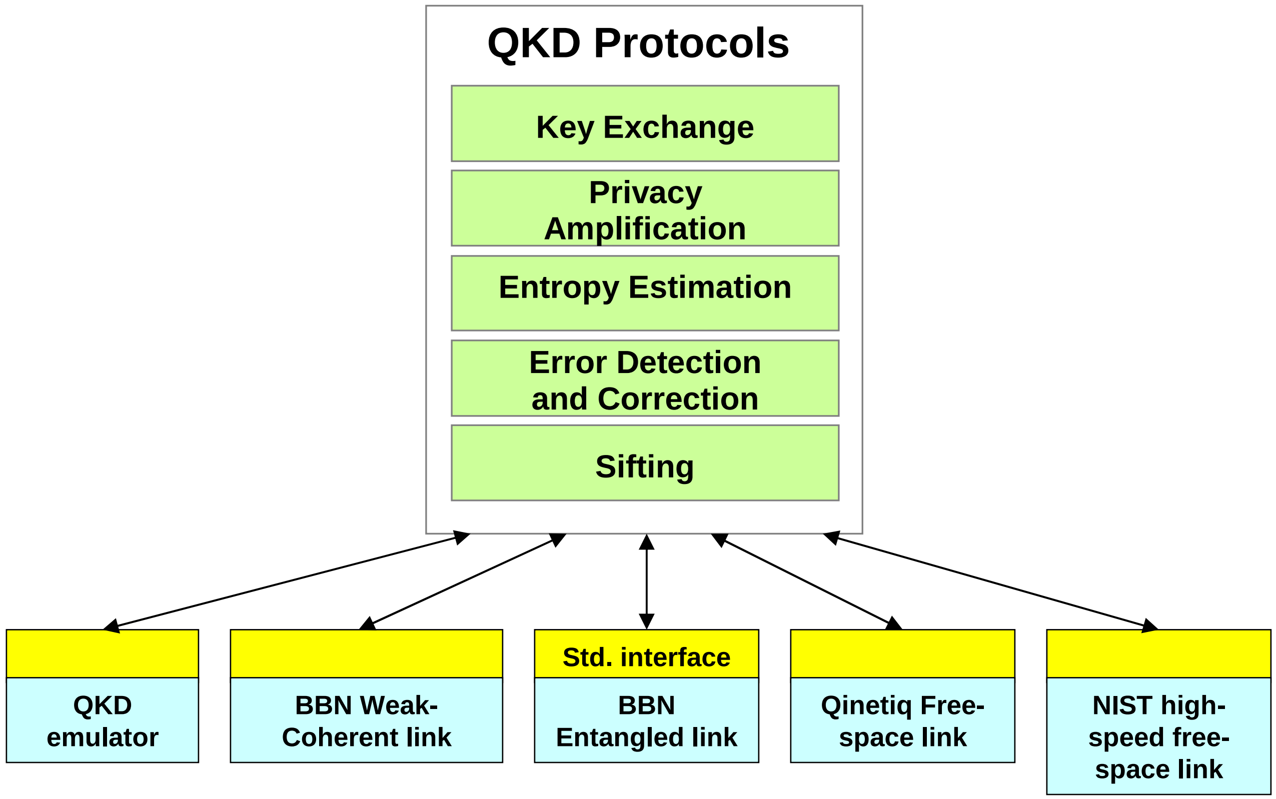
- ✓ BBN Cascade
- ✓ BBN 'Niagara' FEC

Sifting

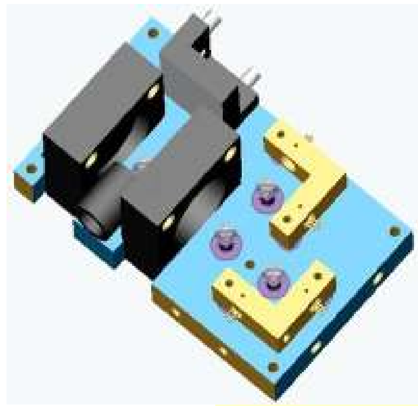
- ✓ Traditional
- ✓ 'SARG' Sifting

Simple, Open Interface Makes It Easy To "Plug In" Other Teams' QKD Systems

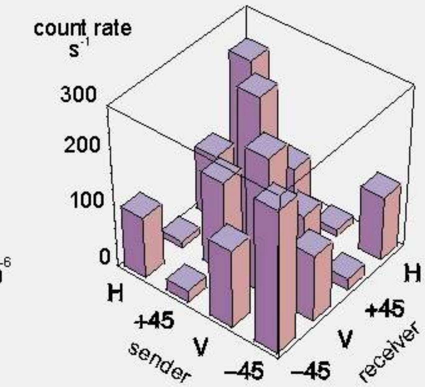
Open Interfaces
Enable a wide range of Quantum channels



The ‘Mark 2’ QinetiQ Freespace Link



- pulse rate: 10MHz
- 0.1 photons per pulse
- wavelength: 840nm
- overall attenuation: <30dB
- detection time jitter: 300ps
- detected pulse width: 1ns
- detection window: 1.4ns
- gated dark count probability: $7x10^{-6}$
- raw key rate: 1kHz
- bit error rate: 5%



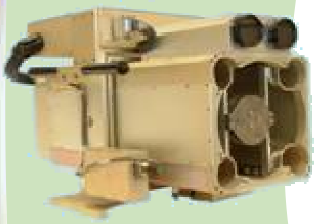
23 km demonstrated through free space

- **Background Information**
  - Based on Successful QinetiQ / Munich Freespace System
  - New QinetiQ Transmitter, with Subcontract for Improved Munich Detector
- **Current Status**
  - Brassboard Transmitter Demo’d with Old Receiver
  - BBN Software Integrated with QinetiQ System
  - Continuous Operation across QinetiQ Laboratory
  - Delivered and operational March 23, 2005

NIST / BBN Freespace Collaboration

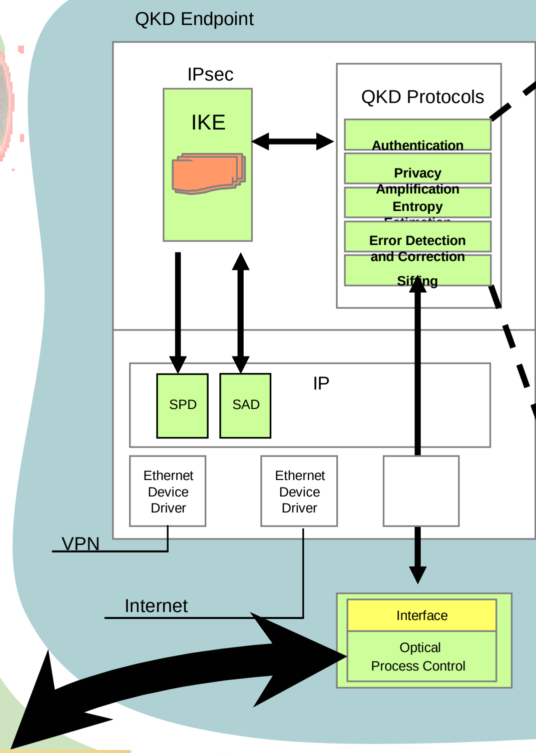
Ali & Baba – What is Currently Integrated in BBN's Lab

Quantum Telescope
840nm (don't have)



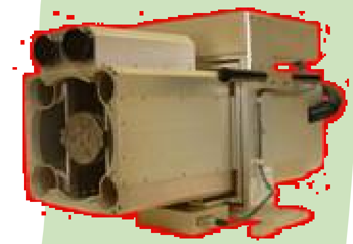
Classical Telescope
1550nm (not yet)

Ali



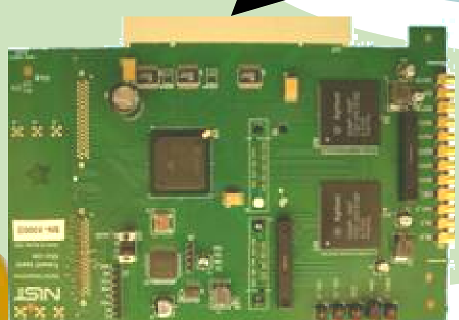
Authentication	**IPsec Based** ✓ Public Key ✓ Secret Key
Privacy Amplification	✓ GF[2^n] Universal Hash
Entropy Estimation	✓ BBBSS 92 ✓ Slutsky ✓ Myers / Pearson ✓Shor / Preskill
Error Detection and Correction	✓ BBN Cascade ✓ BBN 'Niagara'
Sifting	✓ Traditional ✓ 'Geneva' Sifting

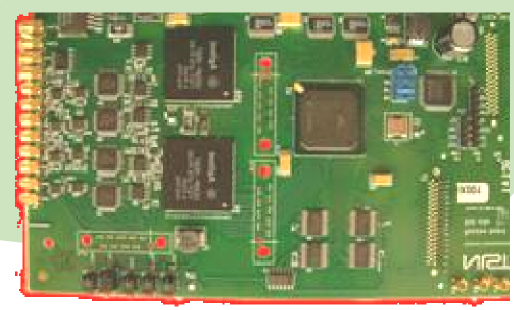
Quantum Telescope
840nm (don't have)



Classical Telescope
1550nm (not yet)

Baba

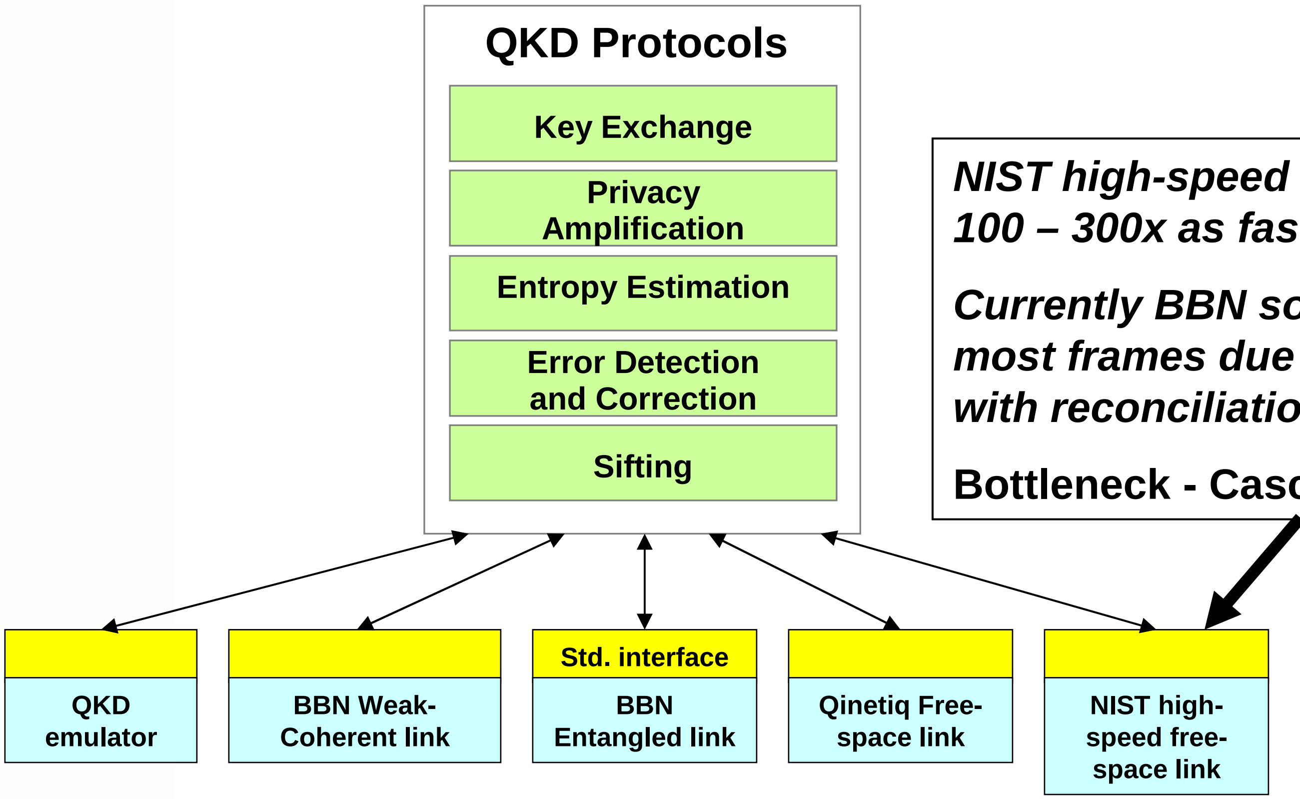




Quantum and Classical Channels running through Coax

Open Interface to Optics

Enables a wide range of Quantum channels



NIST high-speed free-space link:
100 – 300x as fast as other systems.

Currently BBN software discards most frames due to rate mismatch with reconciliation

Bottleneck - Cascade Error Correction

BBN's 'Niagara' LDPC Forward Error Correction

40x Less Comms Overhead, 16x Less CPU than Cascade

Inputs

historic error rate

noise margin

margin for suboptimal code

Pseudo-random seed

k (block size)

D – density profile

p – number of parity constraints (revealed bits)

Code

A low-density parity-check matrix

$$\begin{matrix} 1, & 0, & 0, & \ldots & 1 \\ 0, & 0, & 1, & \ldots & 0 \\ & & \vdots & & \\ 0, & 1, & 0, & \ldots & 0 \end{matrix}$$

Random, with constraints on row/column weights

A promising alternative to adding a safety margin is to add more parity bits when decoding fails

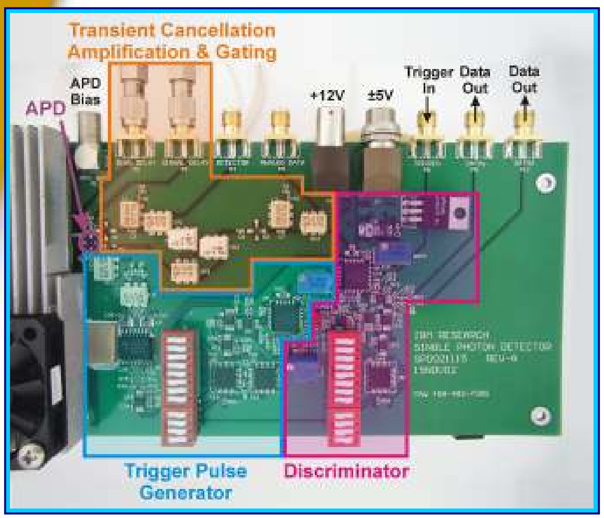
Average for 4096 bit blocks, 3% error rate	BBN Cascade	LDPC
Revealed bits	958	1006
% of Shannon limit	120%	126%
Delay (round trips)	68	**1**
Communication (bytes)	19200	**480**
CPU usage (secs / Mb, 800MHz x86)	17.4	**1.1**

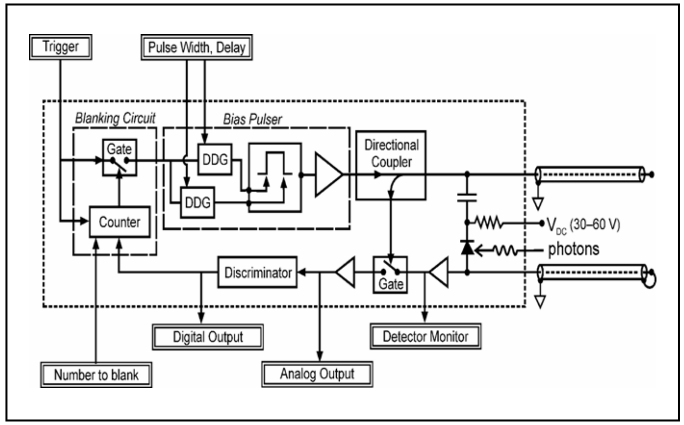
Detectors

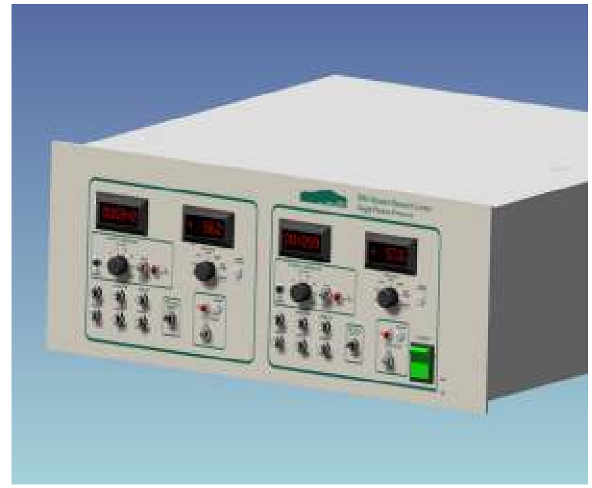
IBM Almaden Collaboration

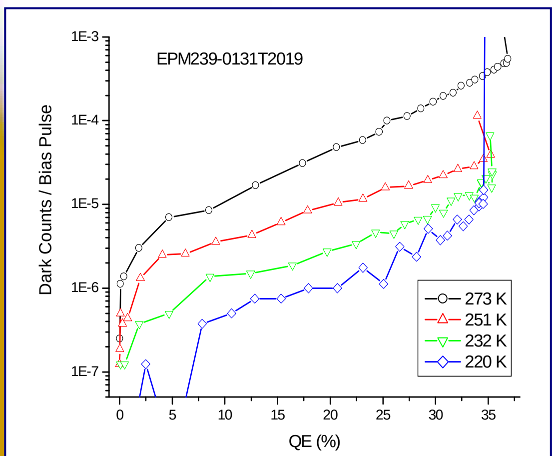
Newest BBN QKD Systems Incorporate IBM Detectors

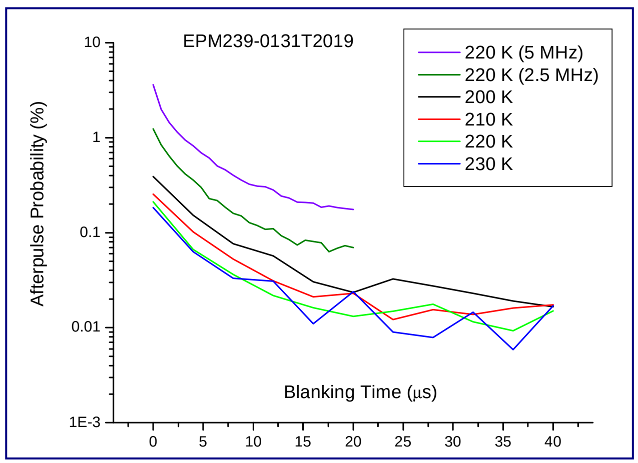
Donald S. Bethune, William P. Risk and Gary W. Pabst
IBM Almaden Research Center
San Jose, CA











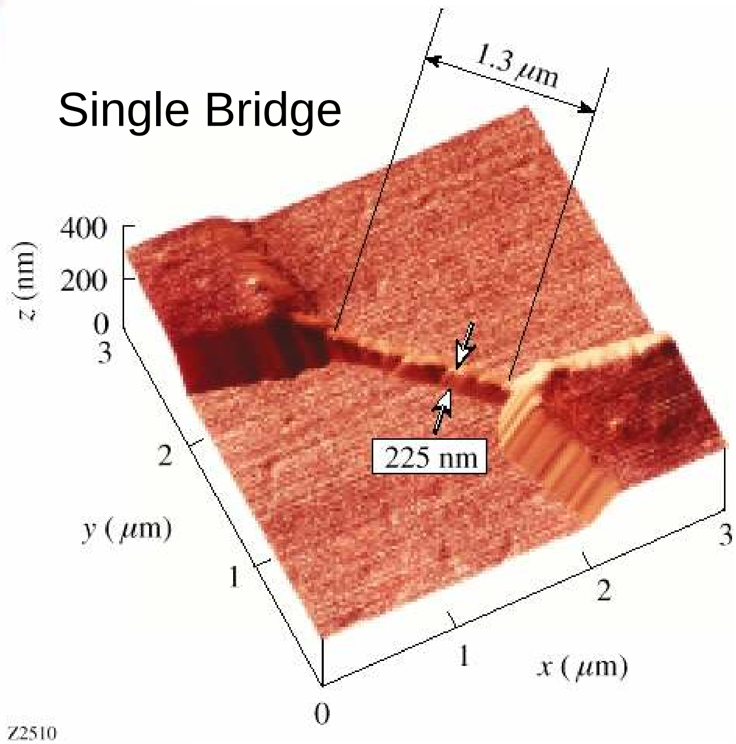
IBM Almaden supplied Detectors for DARPA Quantum Network QKD systems

BBN / U. Rochester / NIST Detector Collaboration

From University Demonstration to the Telecom Closet

Fabrication and Properties of an Ultrafast NbN Hot-Electron Single-Photon Detector," R. Sobolewski, LLE Review, Volume 85, p. 34.

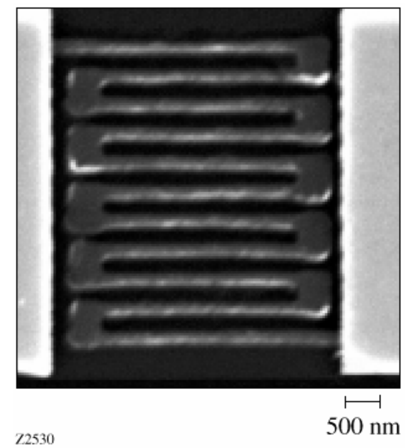
Single Bridge

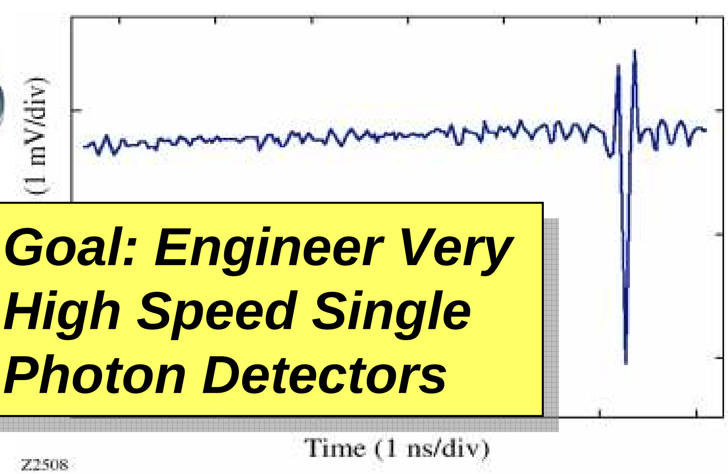


Superconducting (4.2 K) NbN hot-electron photodetector (HEP) with picosecond response time, high intrinsic quantum efficiency, negligible dark counts, and the capability to detect single photons from the ultraviolet to the infrared wavelength range.

Sumitomo

Meander Structure





Goal: Engineer Very High Speed Single Photon Detectors

Why Develop this Detector?

Detector Model	Count rate(Hz)	QE %	Jitter (ps)	Dark Counts (per ns)
InGaAs PFD5W1KS APD (Fujitsu)	5×10^6	>20	>200	6×10^{-6}
R5509-43 PMT (Hamamatsu)	9×10^6	1	150	1.6×10^{-5}
Si APD SPCM-AQR-16 (EG&G)	5×10^6	0.01	350	2.5×10^{-8}
Mepsicron-II (Quantar)	1×10^6	0.01	100	1×10^{-10}
Transition Edge Sensor (NIST)	2×10^4	>80	N/A	~0
SSPD projection (R. Sobolewski)	3×10^9	>10	18	1×10^{-11}

Ideal Characteristics for Quantum Key Distribution

Very Fast (> 1 GHz), Low Dark Count (< 1/s), Good QE (>10%)

Theories vs. Devices

When you sit down to engineer a QKD system to meet those security guarantees, you constantly have to bridge the abstract world of the proofs and the messy world of devices

Justice? You get justice in the next world, in this world you get the law. – William Gaddis

Proofs? You get proofs in the next world, in this world you get devices. – Chip Elliott

Active Collaborations in Year 4

BOSTON UNIVERSITY

UNIVERSITY OF ROCHESTER OFFICIAL SEAL · MELIORA · 1850

Harvard University

DARPA

QinetiQ

BBN TECHNOLOGIES
A Verizon Company

IBM®

MITRE

NIST

The Team

Boston University

Prof. Alexander Sergienko
Prof. Mal Teich
Prof. Bahaa Saleh
Prof. Gregg Jaeger
Dr. Martin Jaspan
Dr. Gianni Di Giuseppe
Dr. Hugues De Chatellus

Harvard University

Prof. Tai Tsun Wu
Dr. John M. Myers
Dr. Dionisios Margetis
Dr. F. Hadi Madjid
Margaret Owens

Visitors

Rich Cannings (U. Calgary)

University of Rochester

Prof. Roman Sobolewski

NIST Boulder

Dr. Aaron Miller
Dr. Sae Woo Nam
Dr. Robert Schwall

BBN Technologies

Dr. Alex Colvin
Chip Elliott
Dr. Chris Lirakis
John Lowry
Dr. David Pearson
Oleksiy Pikalo
John Schlafer
Dr. Greg Troxel
Henry Yeh