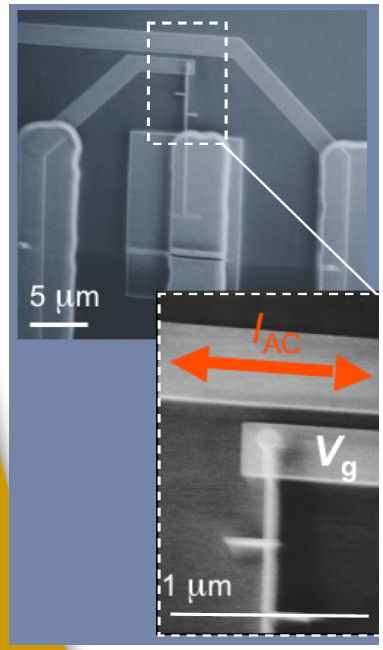
The DARPA Quantum Network

Chip Elliott
Principal Engineer, BBN
celliott@bbn.com

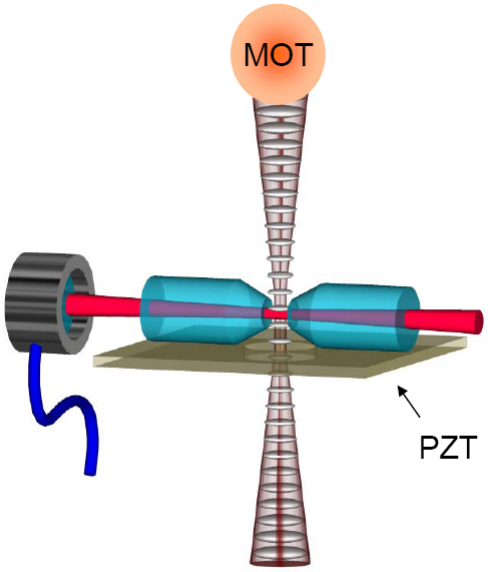
DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

Physics Today

- Routine manipulation of single particles / waves
  - Photons, atoms, electron spins, . . .
- Now starting to engineer quantum states and quantum interactions (e.g. entanglement)

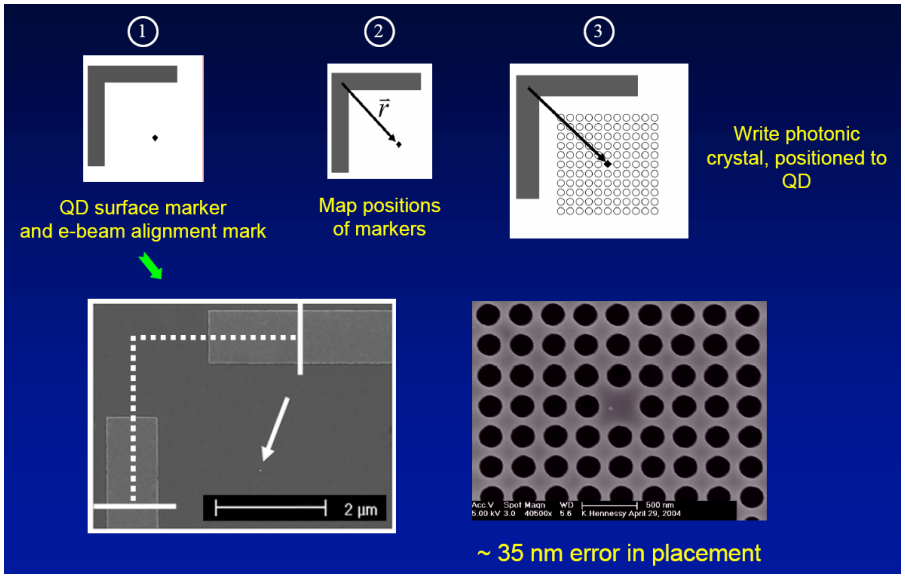


Electron Spins



Optical dipole trap

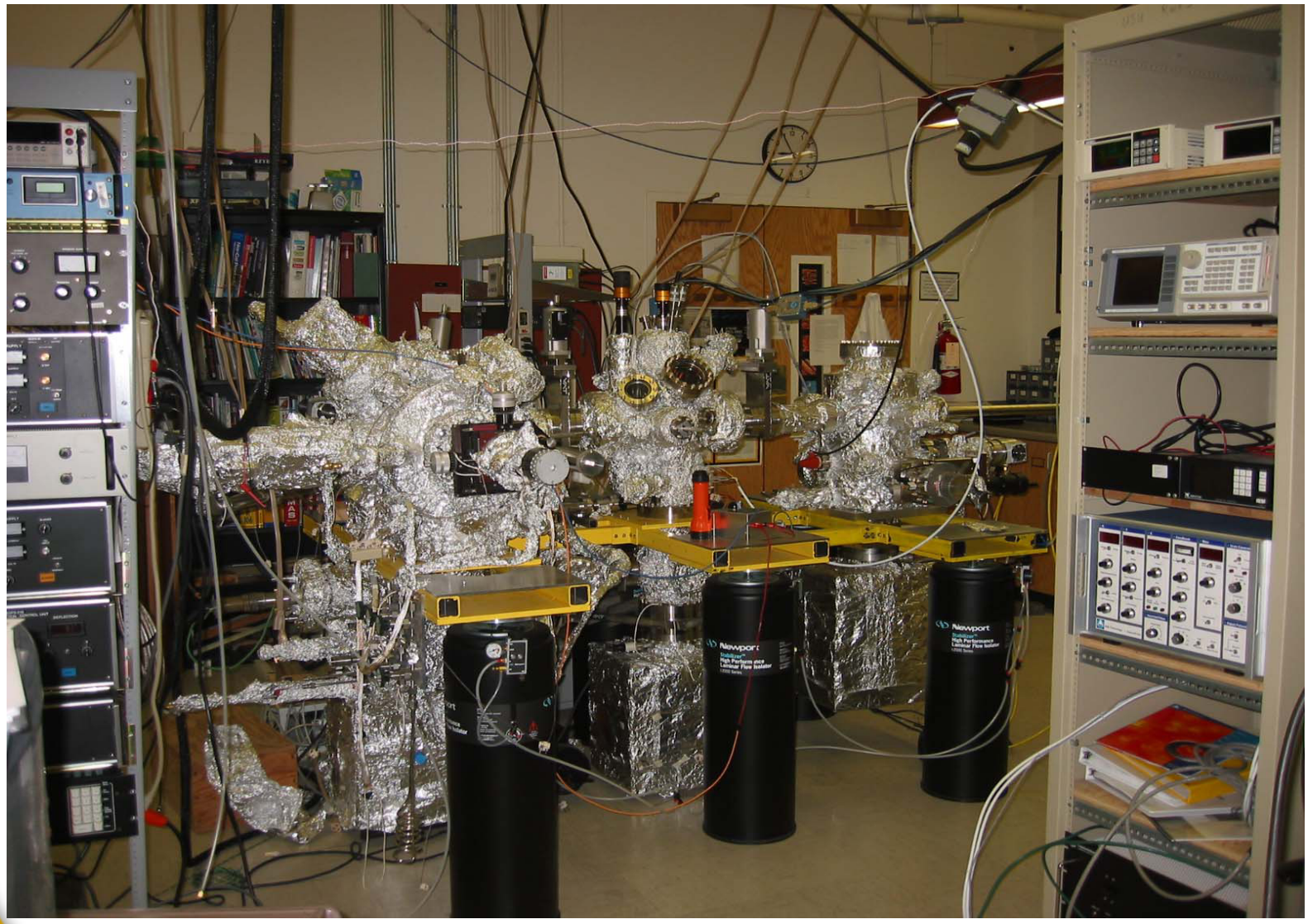
Rubidium Atom



Quantum Dot in Photonic Crystal

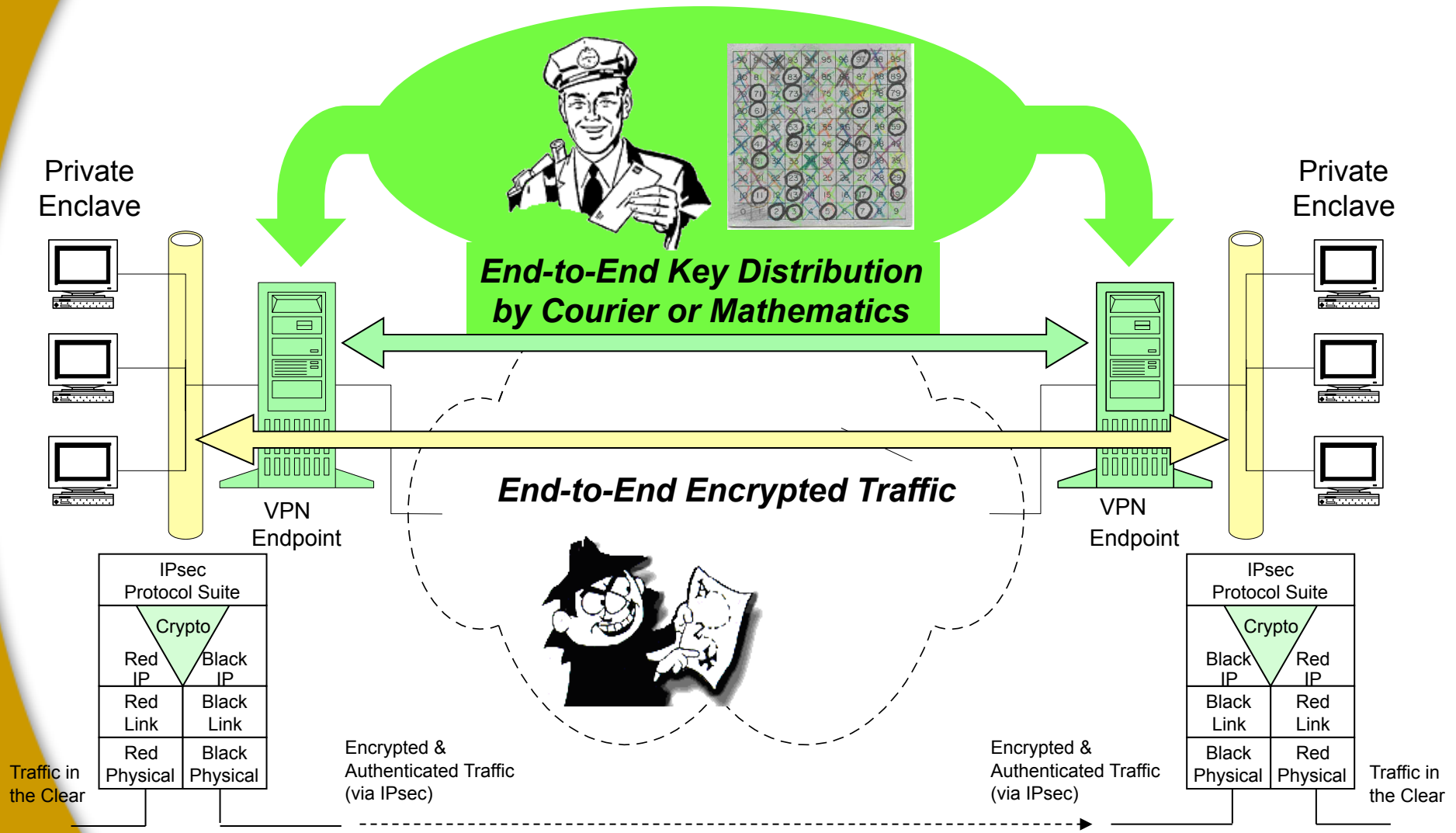
DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

That Single Particle in Context



DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

Today's Secure Networks



DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

Potential Weakness in Math-Based Key Distribution Techniques

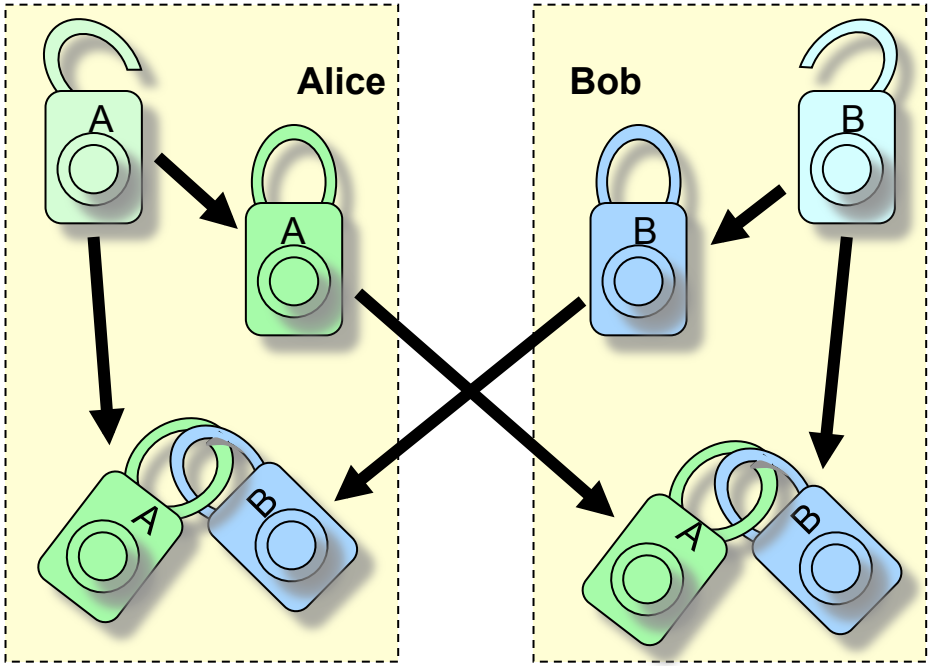
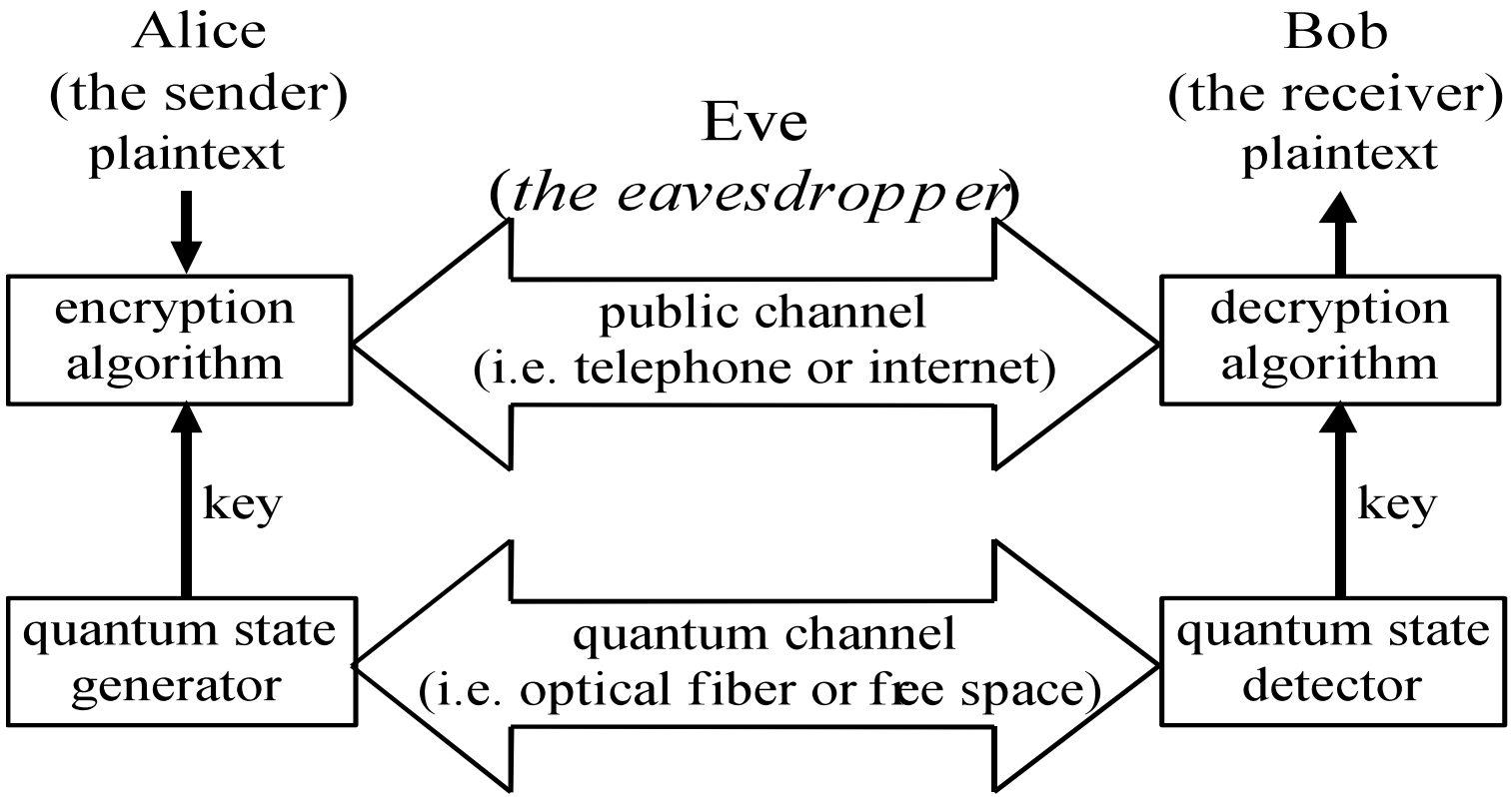


Diagram from Ueli Maurer

- Basic Idea
  - 2 Keys: Public, Private
  - Encrypt with Public Key
  - Decrypt with Private Key
- Variants
  - RSA (Large Prime #s)
  - Elliptic Curve
- Enabling Technology
  - Some math function that is easy to do but hard to undo

But . . . No Known Proofs of "One-Way" Property

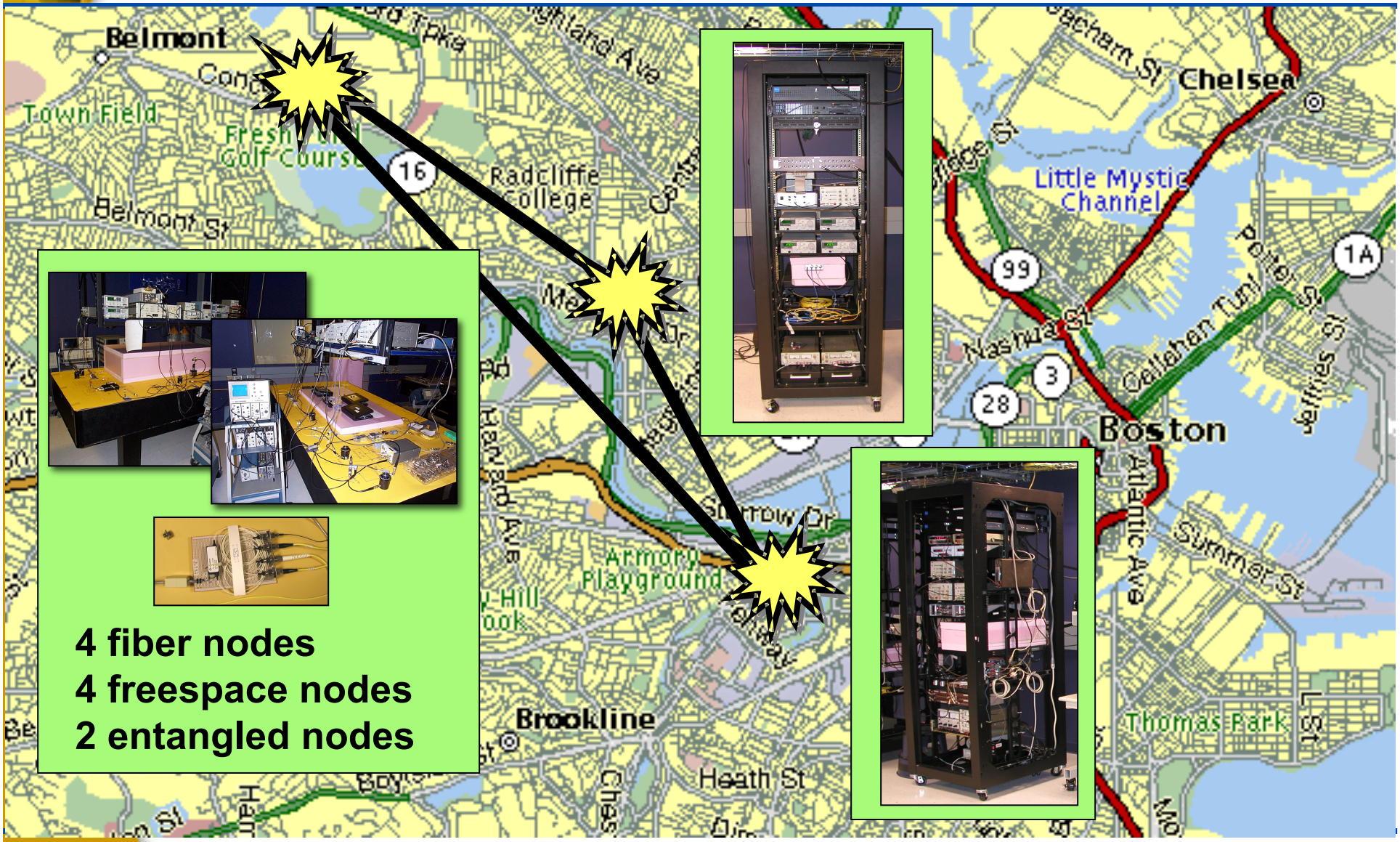
A New Kind of Key Distribution - Quantum Key Distribution



DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

The DARPA Quantum Network

Operating Continuously Across Cambridge Since 6/2004



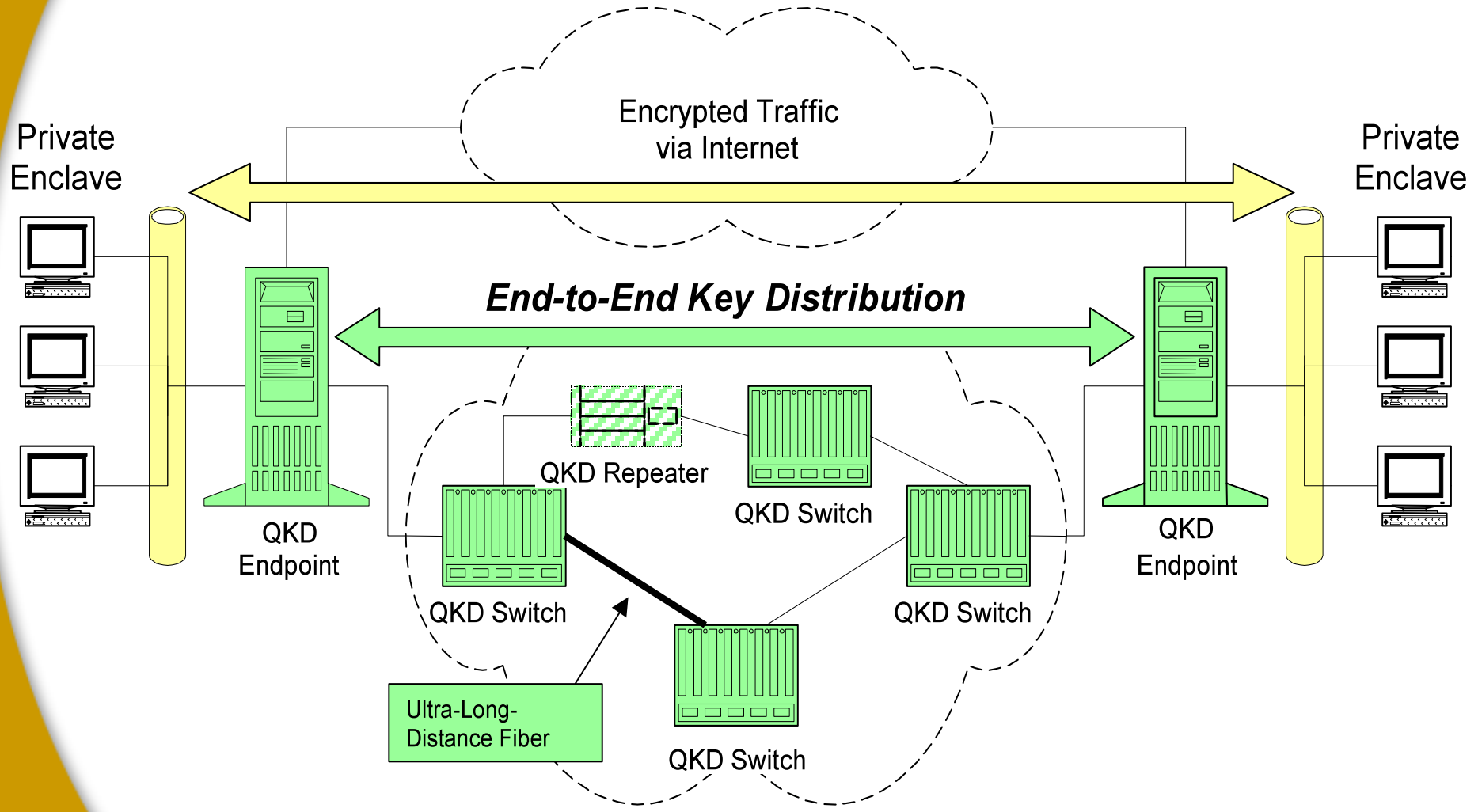
DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

Project 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.

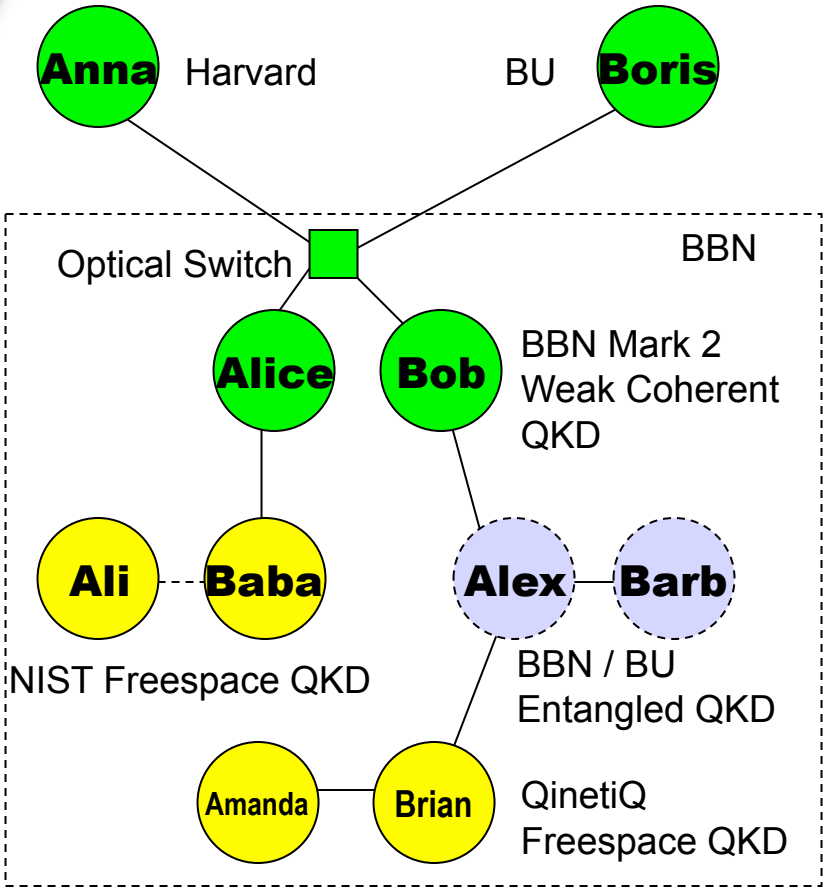
We have fielded this ultra-high-security network into commercial fiber across the metro Boston area and are now operating it 24x7 between BU, Harvard, and BBN.

The DARPA Quantum Network



DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

Building the DARPA Quantum Network

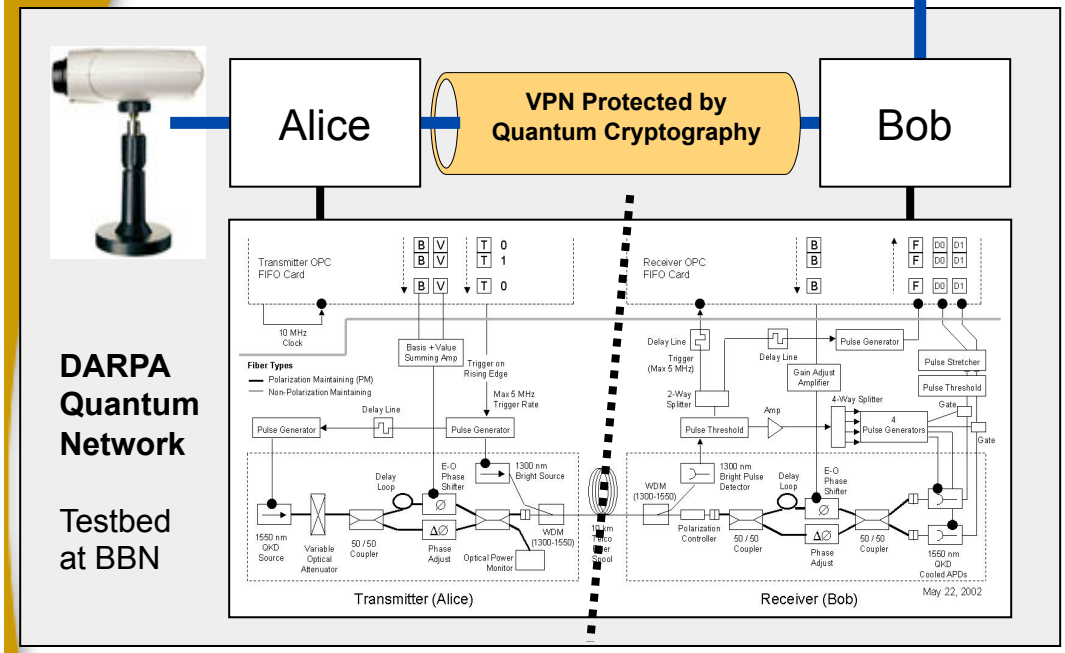


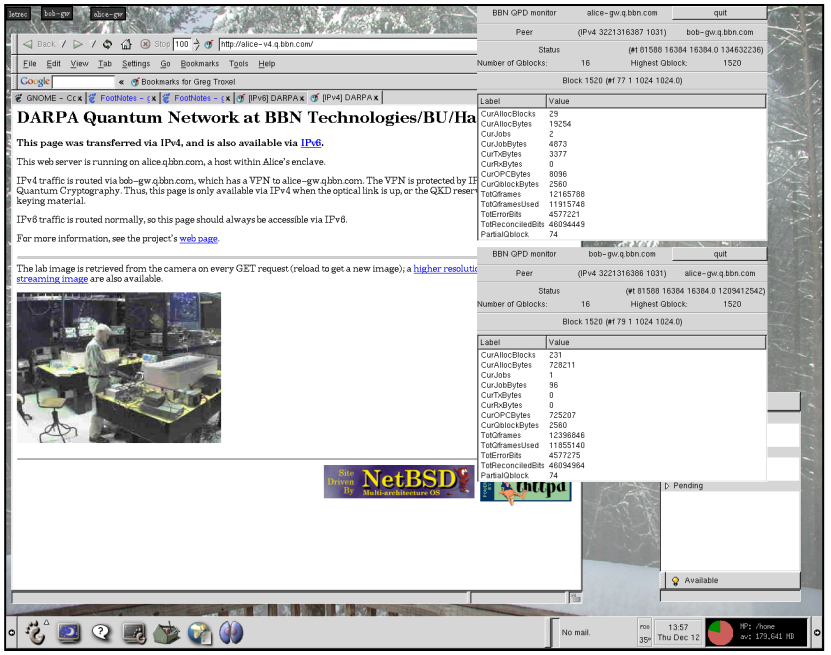
- End-to-End Architecture
  - Multiple QKD technologies
  - Shared software protocol stack
  - Allows graceful evolution
- QKD Networking
  - Key Relay via trusted intermediaries for distance & bridging incompatible technologies
  - Passive optical switches for compatible endpoints

8 Nodes Running 24x7 in DARPA Quantum Network
And 2 More Running in Hardware Emulation

Secure Network Protected by Quantum Cryptography

Full system continuously operational since Dec 2002



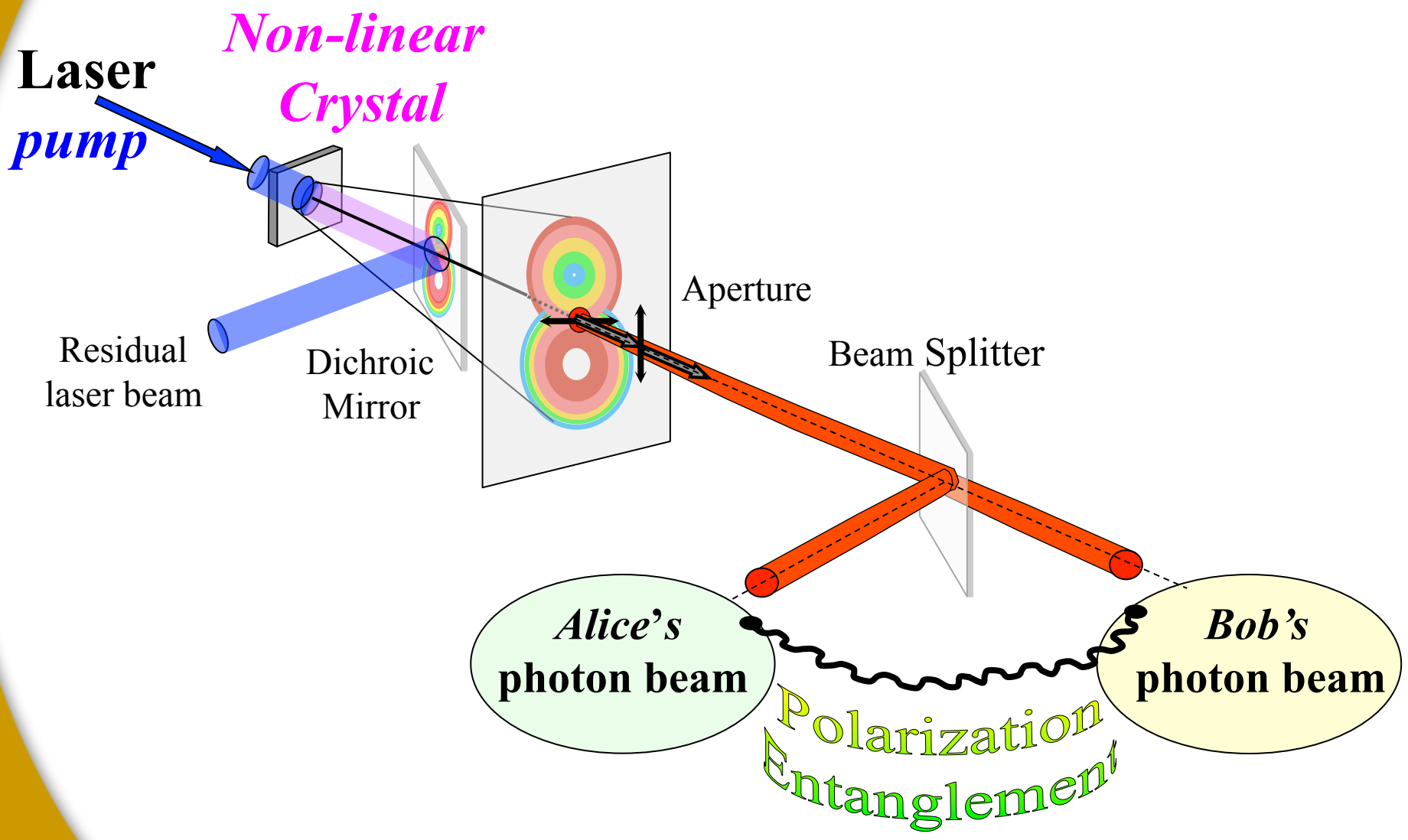


- 5 MHz pulse rate, 0.1 photons / pulse, 1550 nm
- TEC cooled APDs
- Full system measured long term QBER approx. 3% in 10 km Cambridge network
- Full suite of QKD Protocols operational

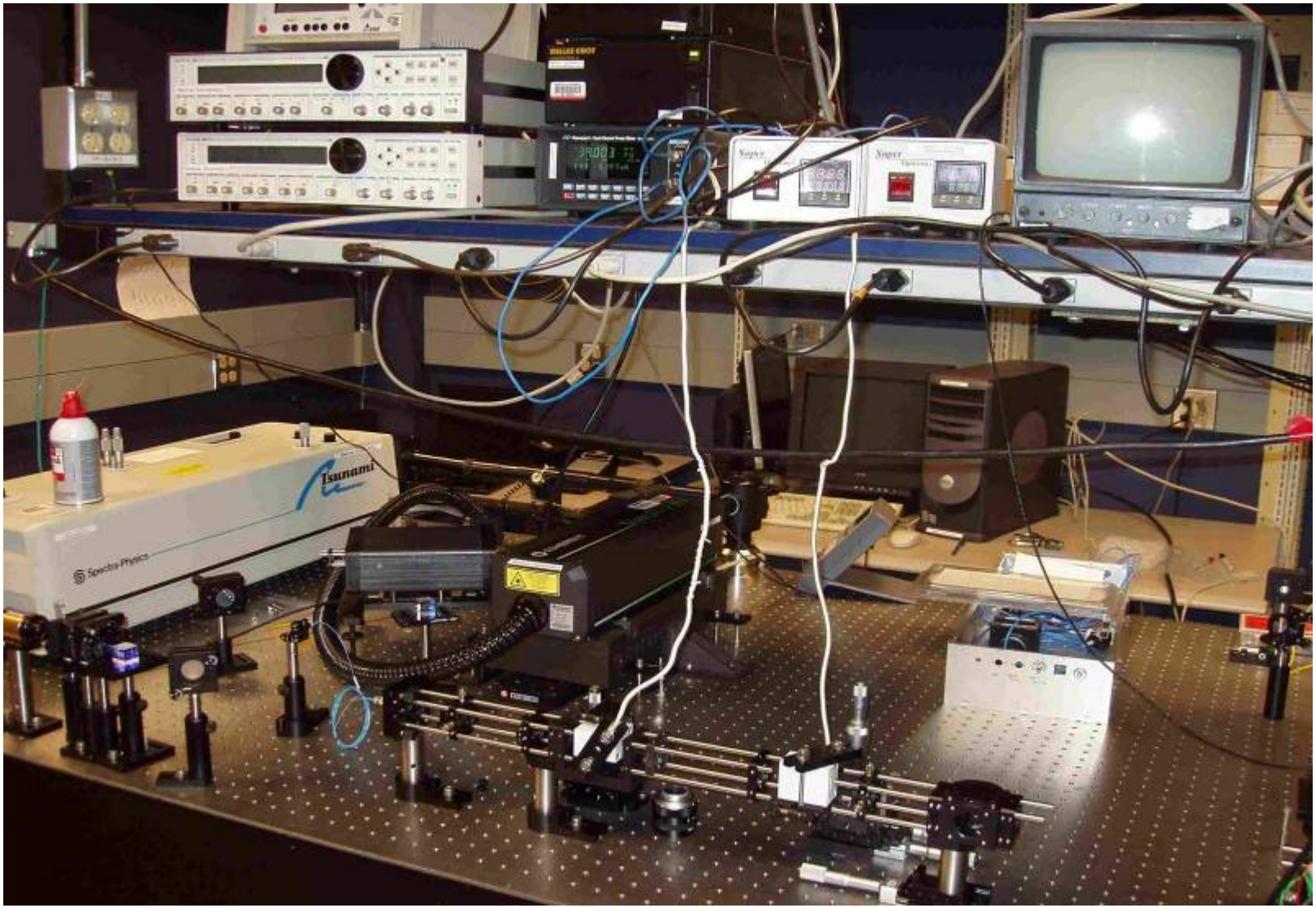
- Privacy-amplified “secret bits” output approx 700 bits / sec.
- Fully integrated with Internet Protocols for both rapid rekeying (AES, 3DES) and one-time pad

DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

Telecom-Ready Source of Entangled Photons



1st Build of Entangled Source



DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

Alex and Barb

Transmitter and Receiver for the Entangled Link

Alex

Barb

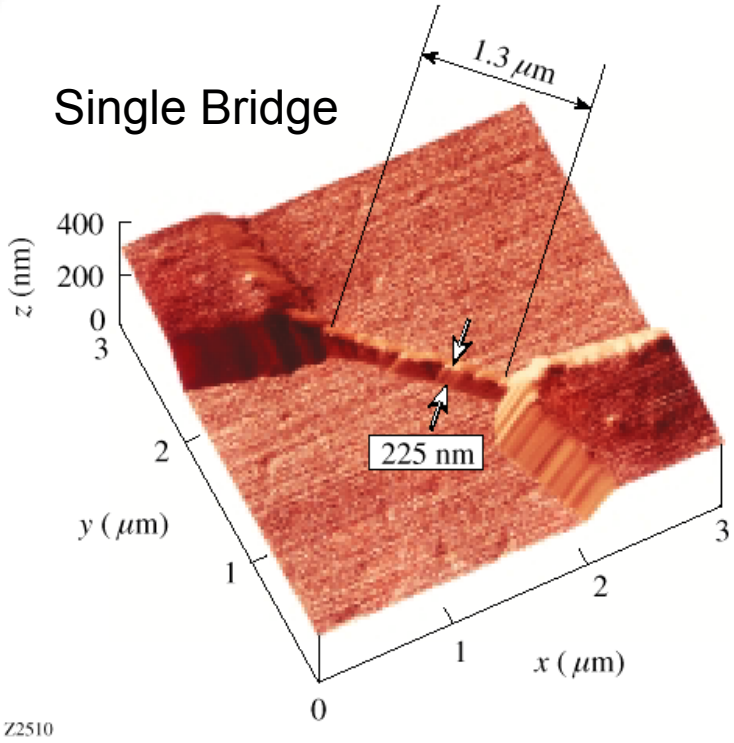
- Opto-Electronics
  - External polarization-entangled 1550 nm source for use in (dark) telecom fiber
  - Uses 4 IBM Almaden detector pairs!
  - 1 MHz pulse rate, InGaAs detector limited
  - Asynchronous link operation based on Alice's detects
- System Design
  - Interfaces with BBN's protocol stack
  - Currently employs BB84 protocol
  - Eventual upgrade to Ekert
- Current Status
  - Testing with Emulated SPDC Source
  - Running 24x7 in shakedown
  - Connected via PM fiber in lab, will introduce polarization control once full system is operating well

BBN / U. Rochester / NIST Detector Collaboration

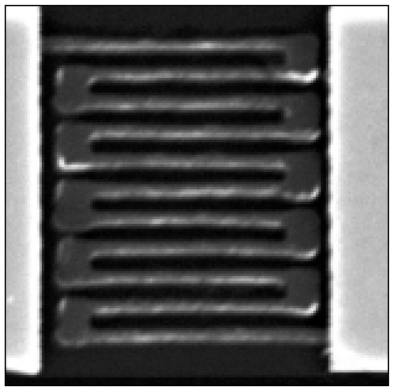
From University Demonstration to the Telecom Closet

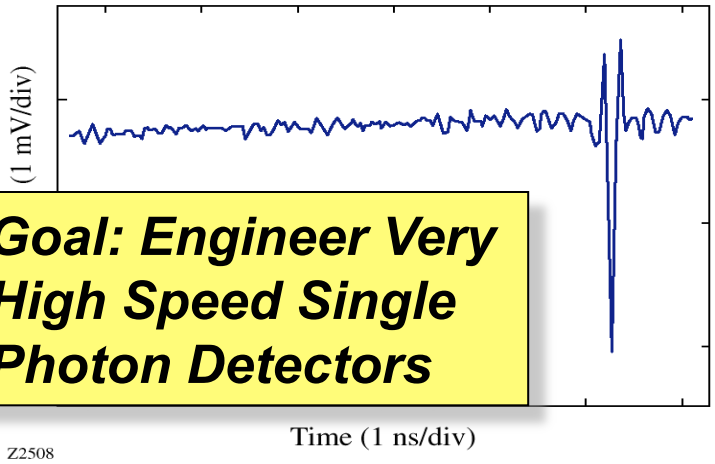
Fabrication and Properties of an Ultrafast NbN Hot-Electron Single-Photon Detector," R. Sobolewski, LLE Review, Volume 85, p. 34.

Single Bridge



Meander Structure





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.

Goal: Engineer Very High Speed Single Photon Detectors

DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

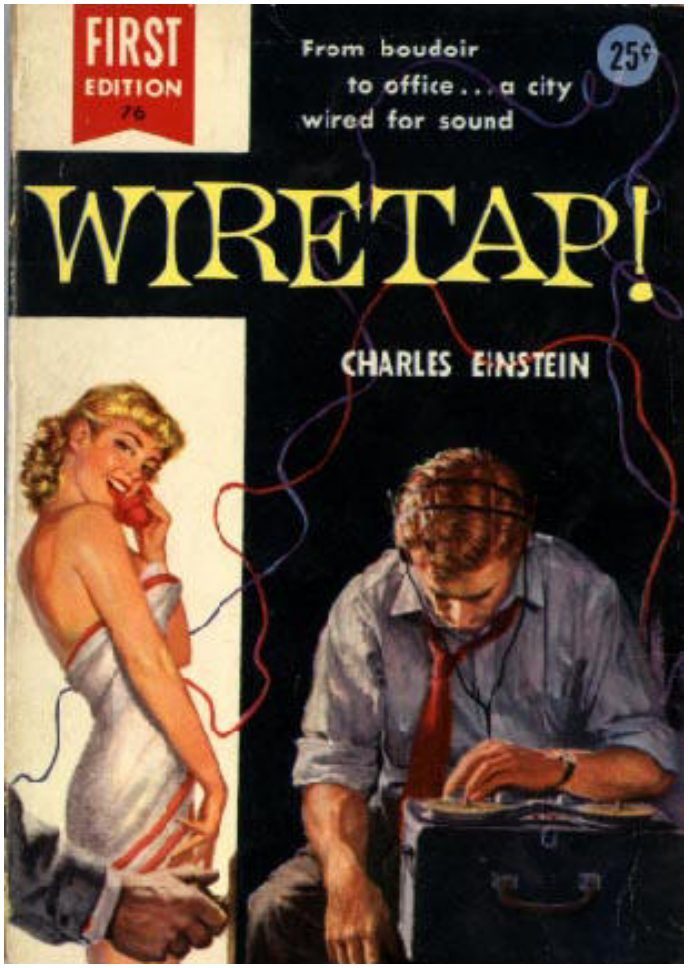
NbN Detector Packaging for Network Operation

Closed-Cycle Cryocooler with 10,000 hr maintenance

Successful QKD trials at BBN in June 2005, Experimentation and continuous operations since.

DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

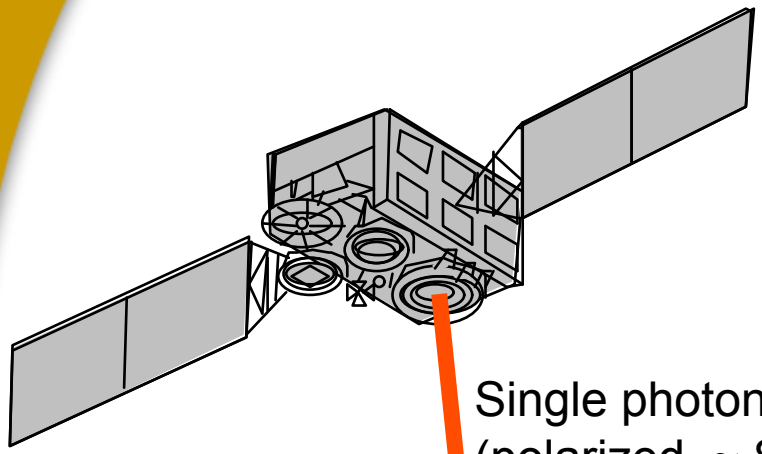
‘Eve’ Collaboration with MIT



rle AT MIT RESEARCH LABORATORY OF ELECTRONICS AT MIT

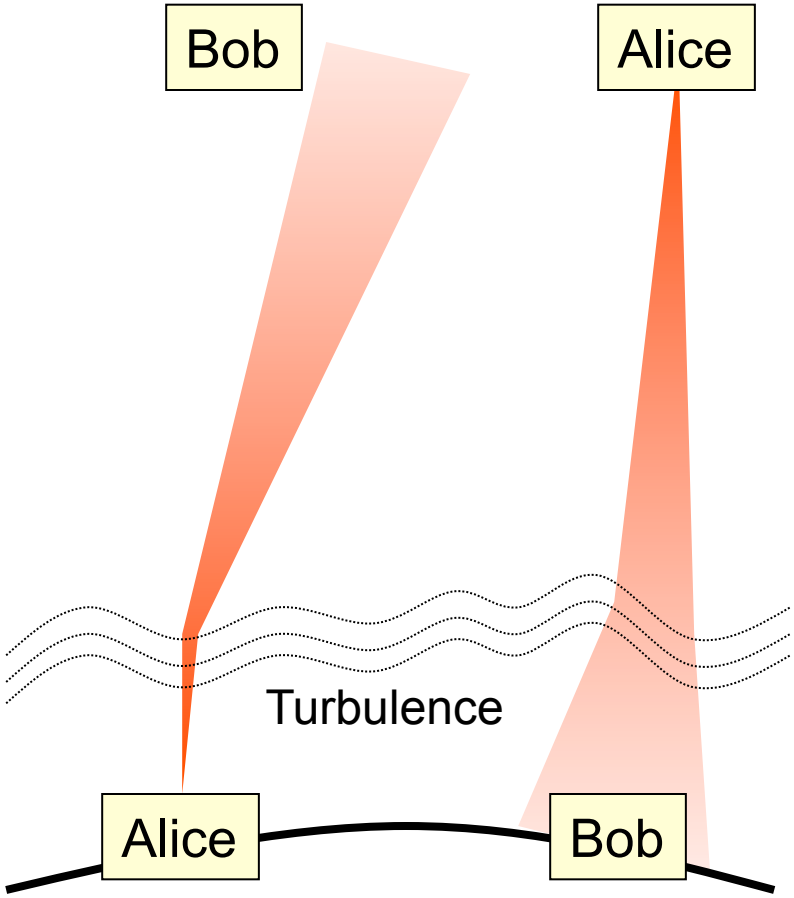
- Goal
  - Demonstrate Fuchs-Peres (Brandt) optimal entangling probe on polarization-based BB84 protocol
- Investigators
  - Prof. Jeffrey Shapiro, Dr. Franco Wong
- Planned Approach
  - Proof of principle, not actual eavesdropping system
  - MIT builds combined Alice-Bob-Eve to eliminate all extraneous problems (such as synchronization)
  - MIT perform experiments varying degree of entanglement
  - BBN post-processes with BB84 protocol engine, reports QBER, etc.

Quantum Cryptography for Space Systems



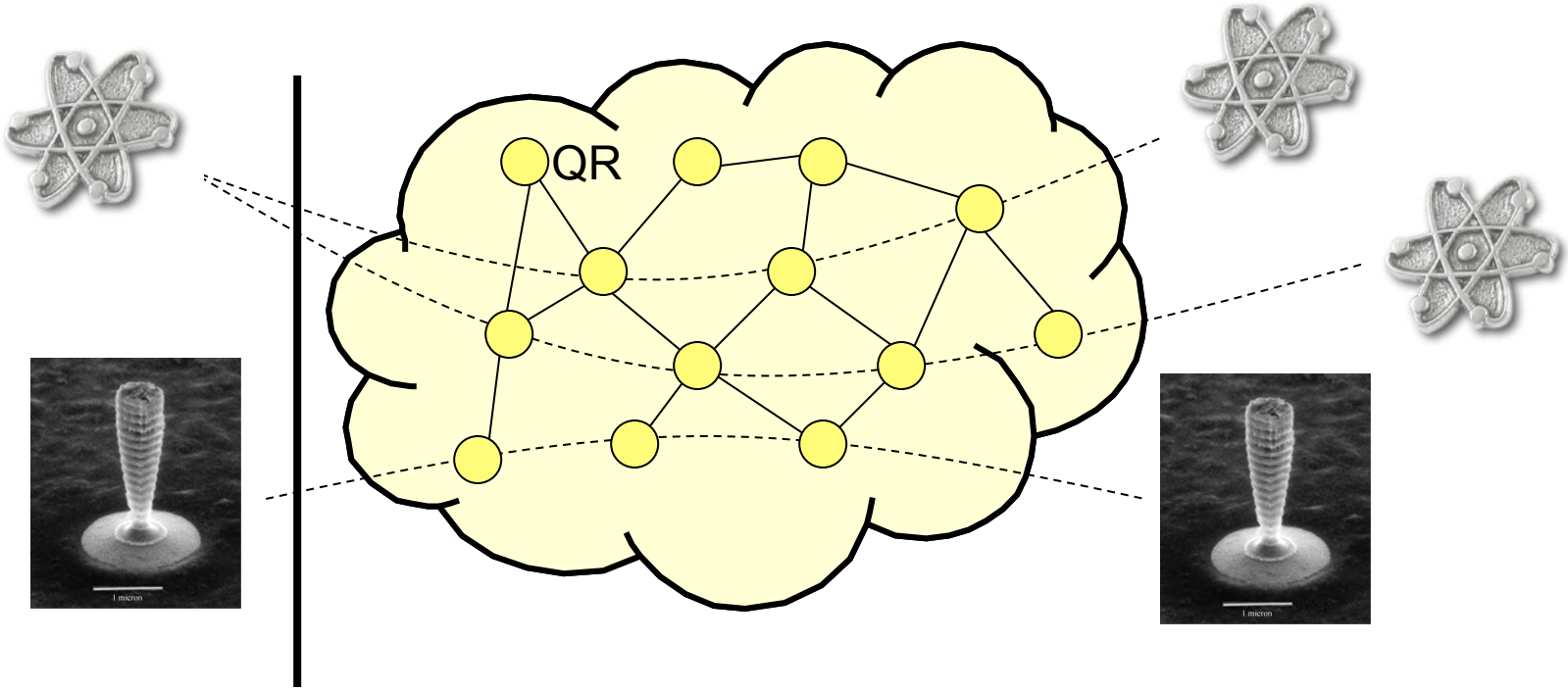
Single photons
(polarized, ~ 800 nm)

Alice in space is probably preferable for various reasons.



DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

Building the Quantum Internet



"Edge" interface is polarized photon

Transport is via end-to-end teleportation

Transport is fundamentally analog, not digital (fidelity guarantees)

DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

Thank You !

Chip Elliott
celliott@bbn.com

quantum.bbn.com