A High-Speed Quantum Communication Testbed

National Institute of Standards and Technology

Carl J. Williams

http://qubit.nist.gov

Contributors

Coordinators: Ron Boisvert, David Su ---- (ITL)
Charles Clark, Carl Williams - (PL)

Hardware group manager
Xiao Tang (895)

Software development
Tassos Nakassis (892)

System Design: Jesse Wen (C), Ed Hagley (C)
Electronic Design: Alan Mink (895), Mikko Heikkero(G),
Barry Hershman (895) Bob Carpenter (895) (C)
Quantum Channel: Richang Lu (G), Andreas Vasilyev (S)
Classic Channel: Julie Rounzaud (G), Mikko Heikkero(G)

C: Contractor; G: Guest Researcher; S: Student

Overall Goals

- Construct a robust quantum communication facility
  - Facility to use single photons to generate quantum key for secure communication – QKD testbed

- Provide standard platform for validation, quantification and comparison of diverse aspects of quantum communication systems
  - Testbed will be used to test single photon sources and detectors developed within NIST and outside
  - Open test-bed to general use by QuIST community
  - Incorporate optical fiber link

NIST QuIST Projects

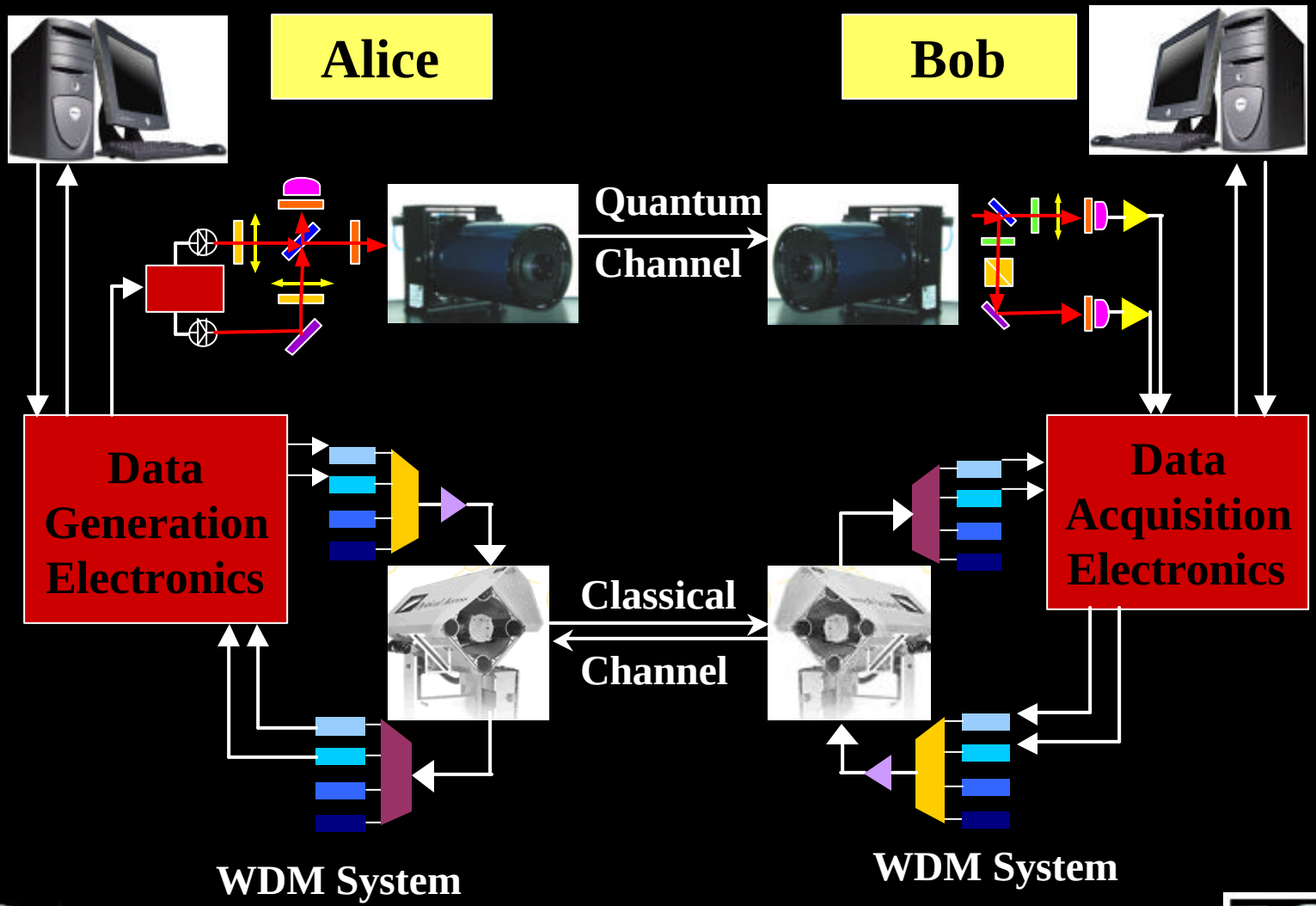
- **Quantum Communications Testbed** (Charles, Clark, Victor McCrary, David Su, Xiao Tang, Carl Williams – ITL, PL)
- **Single Photon Detector** (Sae Woo Nam – EEEL)
  Superconducting Transition Edge Sensors
- **Single Photons on Demand** (Alan Migdall – PL)
  Parametric Down Converters
- **Hybrid Quantum Authentication Protocols** (Rick Kuhn – ITL)
- **Quantum Error Correction, Avoidance, and Compiling** (David Song, Paul Black – ITL)

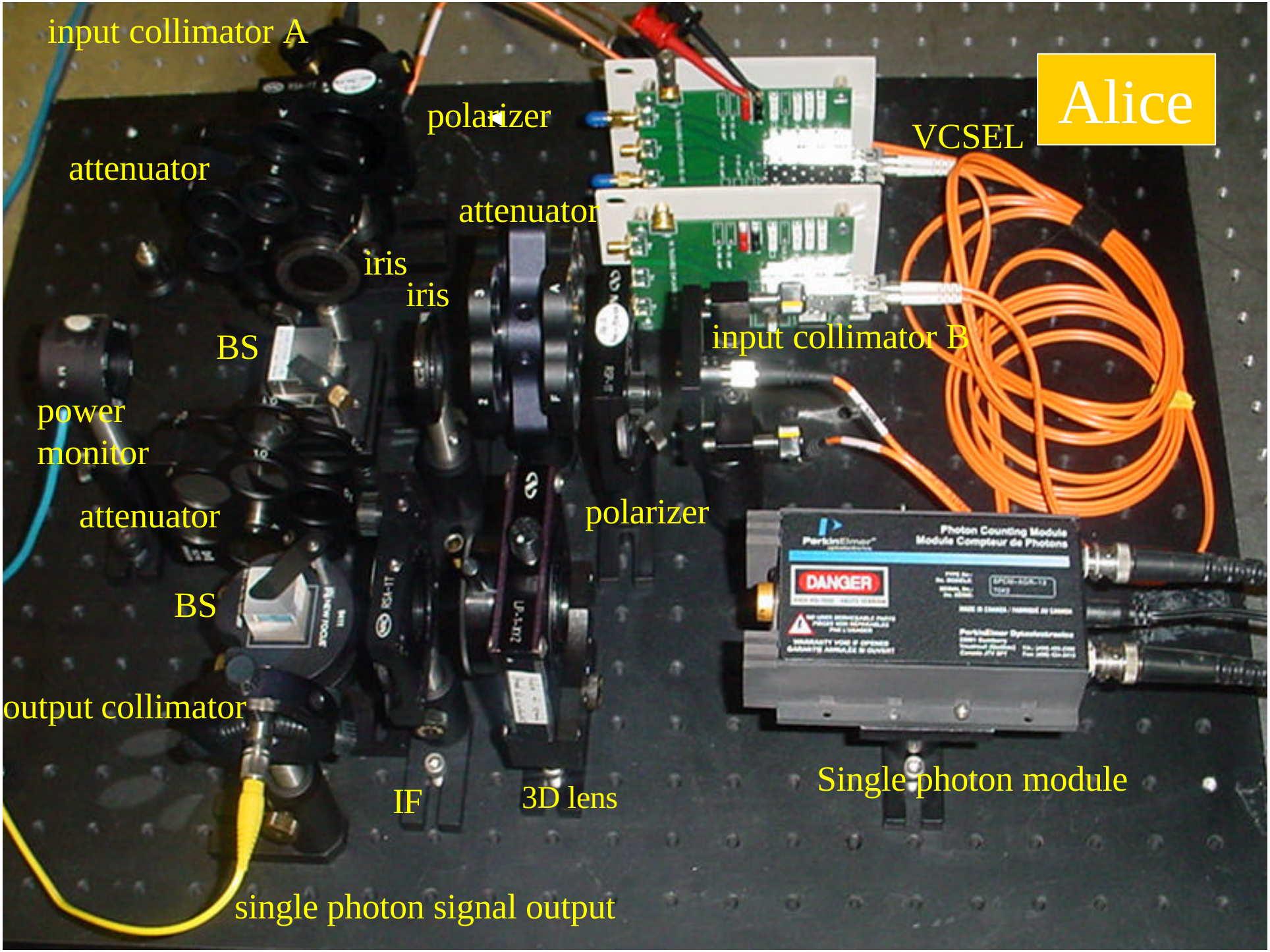
Overview of Testbed Hardware

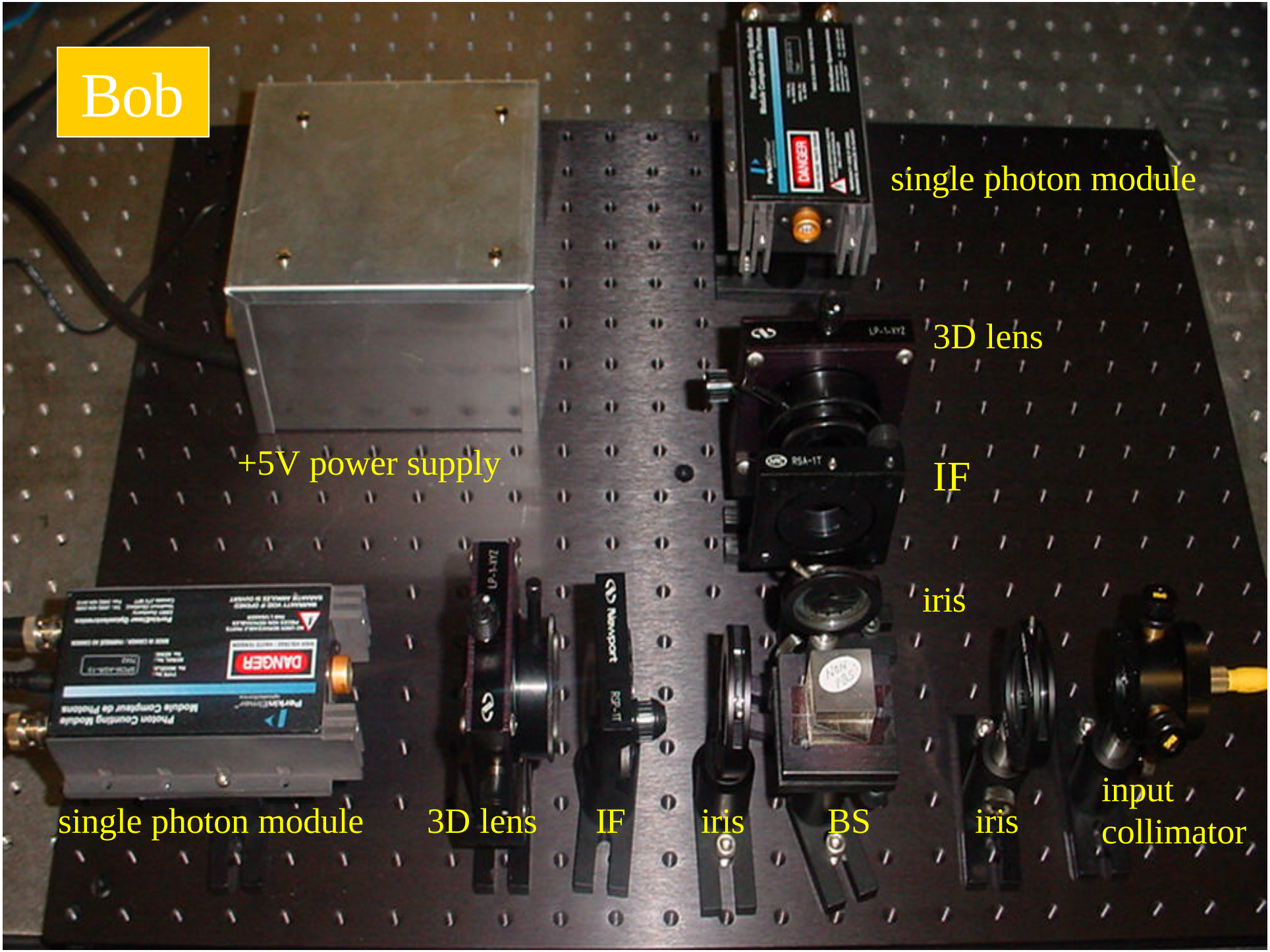
- **Quantum Link**
  - **Attenuated VCSEL transmitters (initially)**
  - **850 nm free space optics**
  - **Si avalanche detectors**
  - **1.25 Gb/s wire rate**
- **Two classical links operating near 1550 nm**
  - **8B/10B encoded path for timing/framing**
  - **Dedicated gigabit ethernet channel**
    - Sifting
    - Error correction/Reconciliation
    - Privacy amplification

Mikko Heikkero, Julie Rouzaud, Richang Lu, Alan Mink, Andreas Goedecke, Jesse Wen, Ed Hagley, Leticia Pibida, Xiao Tang, Tassos Nakassis, Charles Clark, Carl Williams

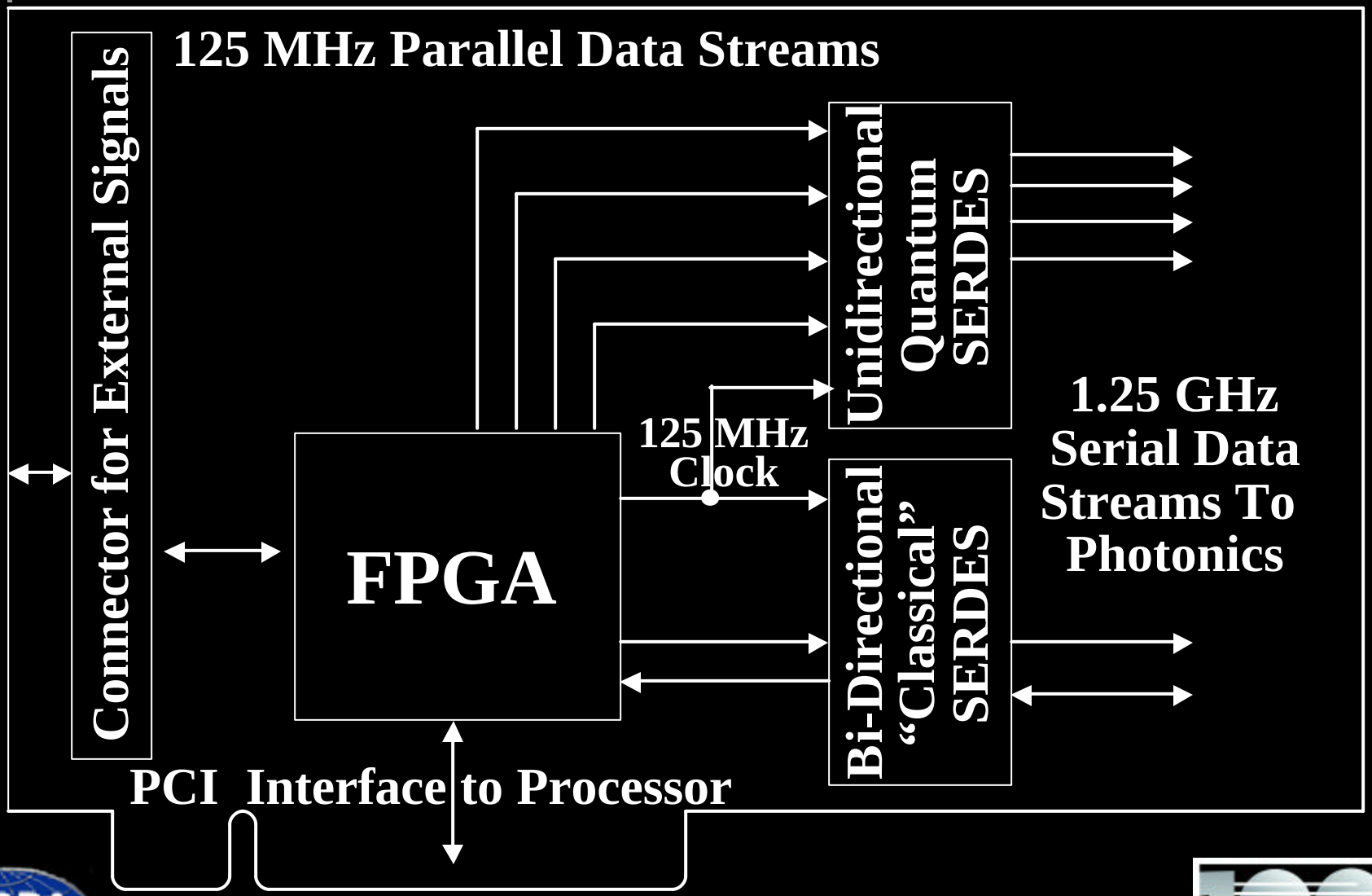
Testbed Structure



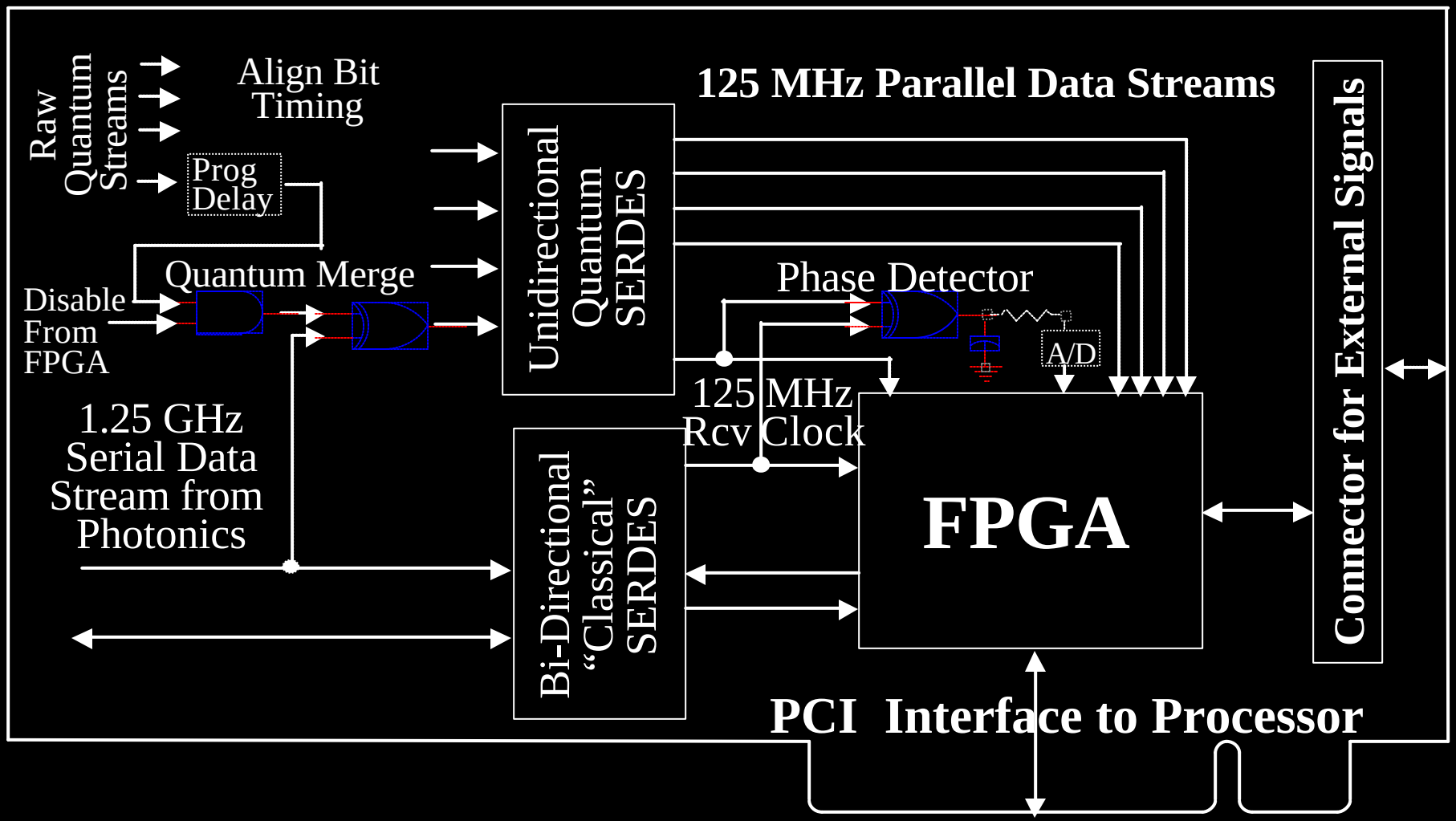

input collimator A
polarizer
Alice
VCSEL
attenuator
attenuator
iris
iris
input collimator B
BS
power
monitor
attenuator
polarizer
BS
output collimator
IF
3D lens
Single photon module
single photon signal output


Bob
single photon module
3D lens
+5V power supply
IF
iris
single photon module
3D lens
IF
iris
BS
iris
input collimator

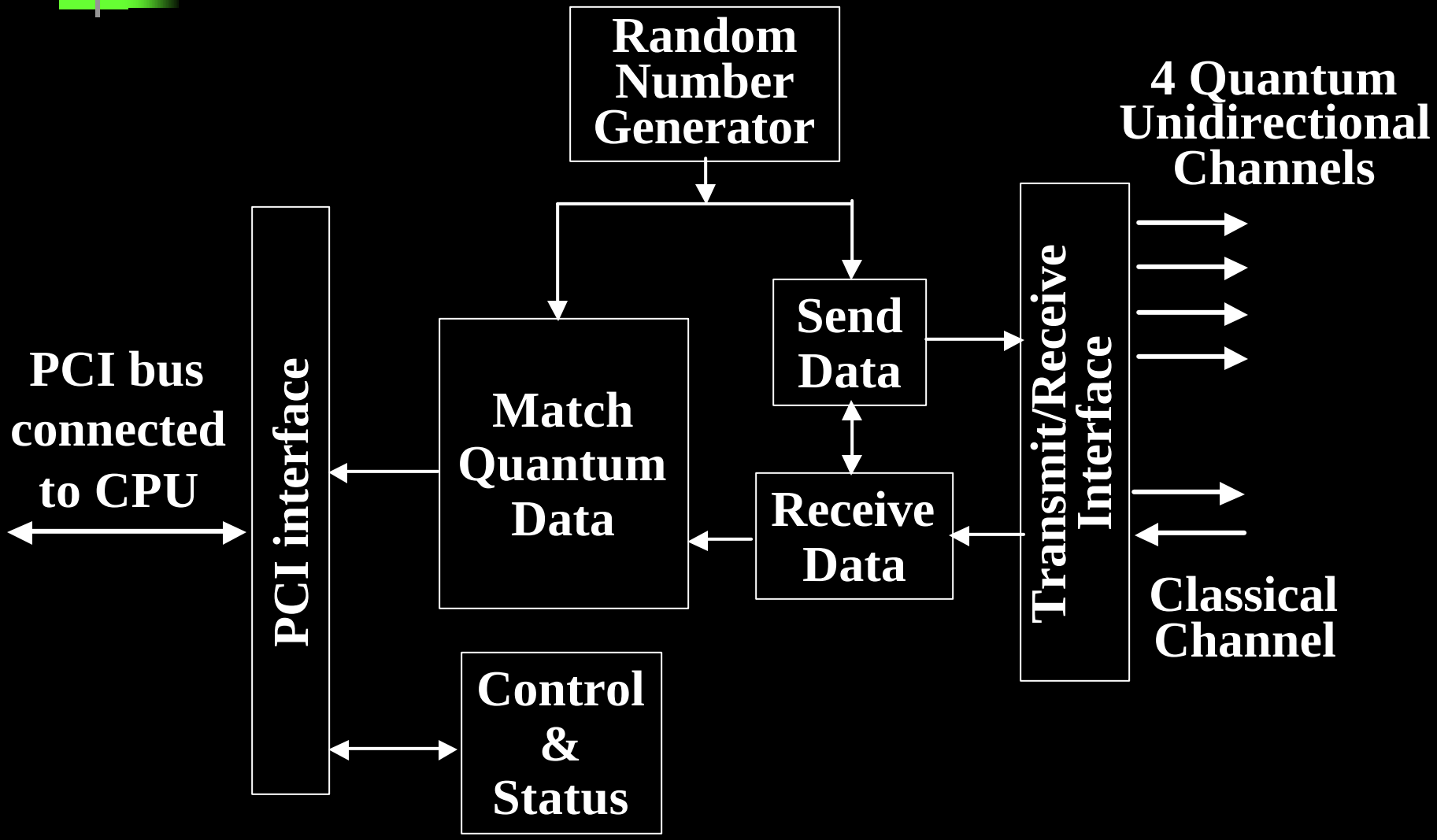
Alice's Circuit Board Block Diagram



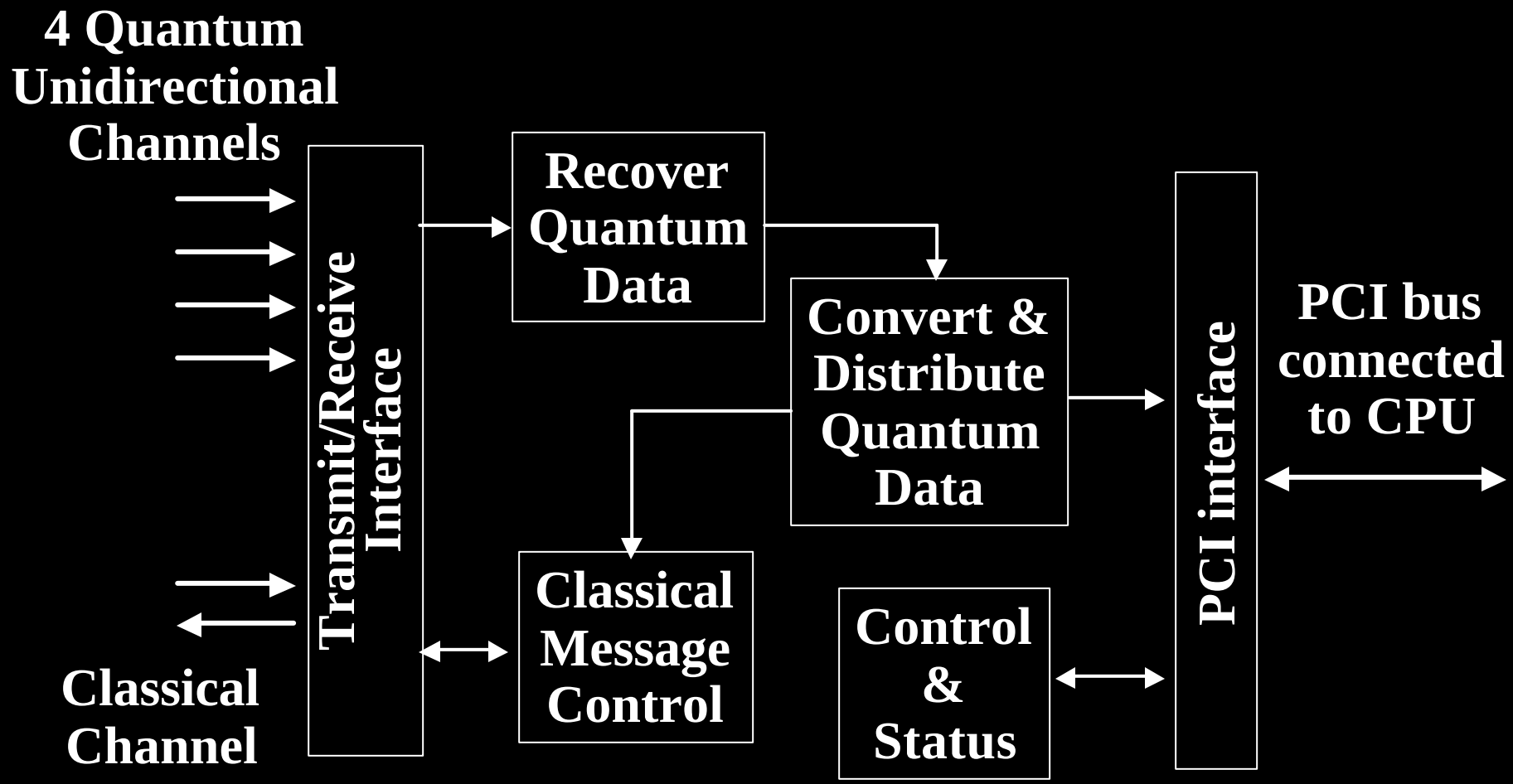
Bob's Circuit Board Block Diagram



Alice FPGA Block Diagram



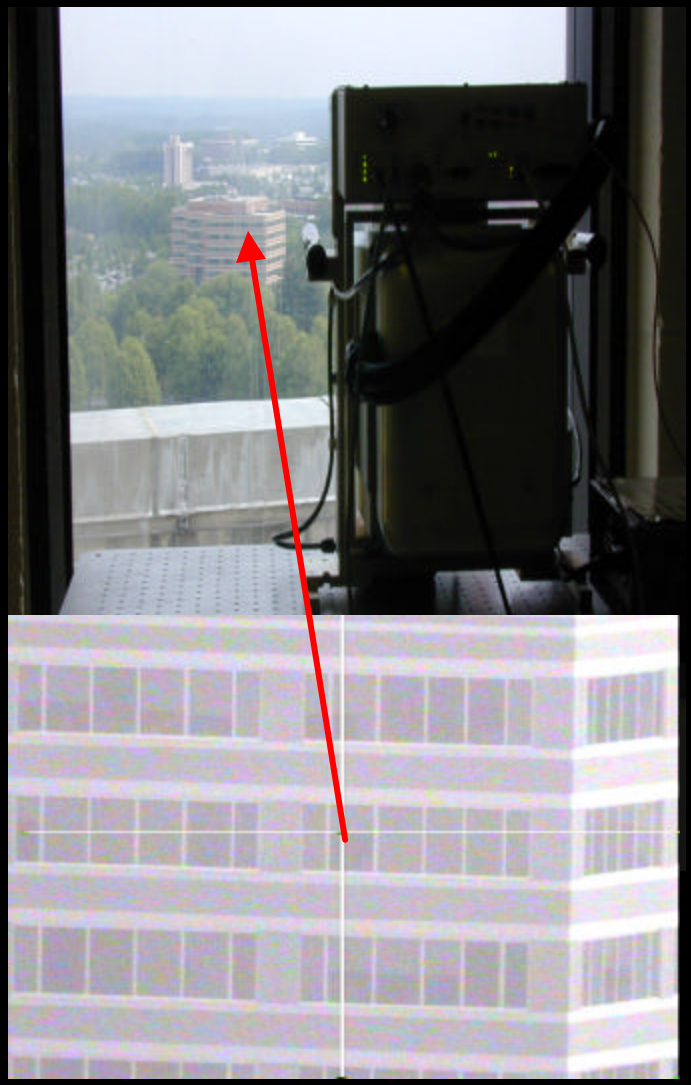
Bob FPGA Block Diagram



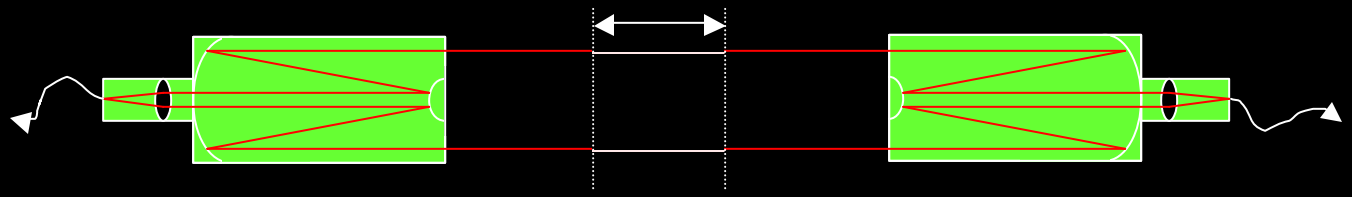
Technical Accomplishments (1)

Classical Channel Telescopes

- View from Administration Building (Bob) to NIST North (Alice) – 600 m
- Computer-controlled aiming and tracking
- Linked with NIST network
- Tested open air link efficiency

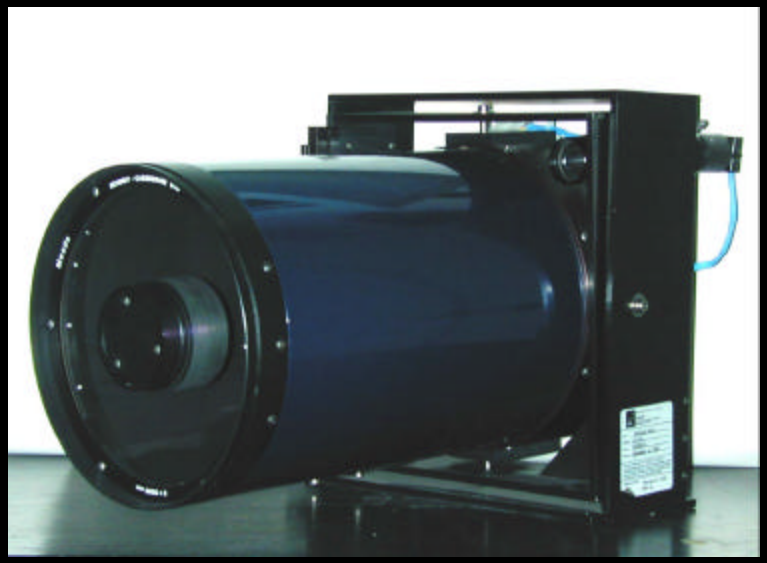


Technical Accomplishments (2)



Quantum Channel Telescopes

- **Installed computer-controlled aiming & tracking**
  Accuracy » 51mrad
- **Installed fiber interface**
- **Overall receiving efficiency: »30% (short distance)**



Technical Accomplishments (3)

WDM System Upgraded

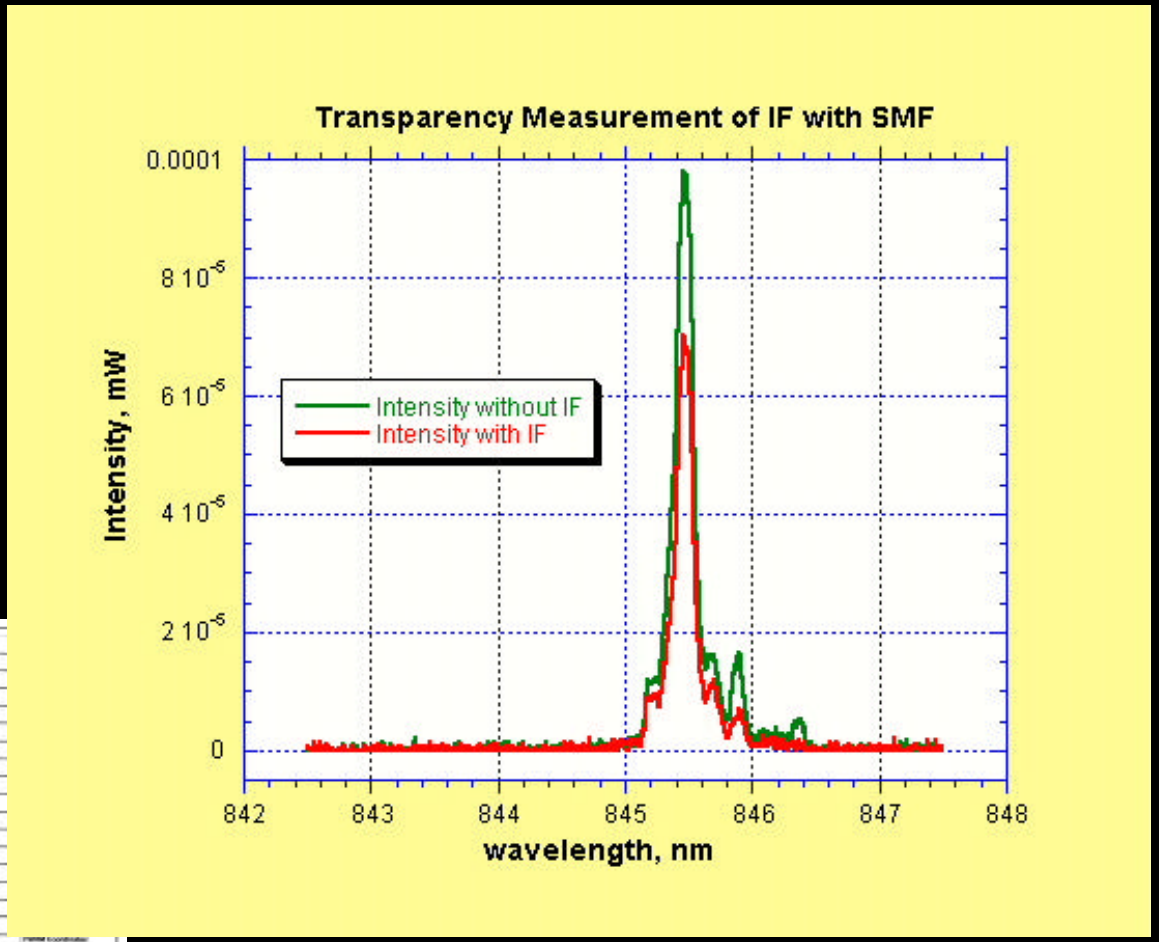
- NIST Base System operated at 625 Mbit/s at 4 wavelengths near 1550 nm
- WDM System Upgraded to:
  - Enables the receivers to run at 1.25 Gbit/s
  - Enables the Multiplexer and Demultiplexer to work with multimode fiber that will connect to the telescopes.

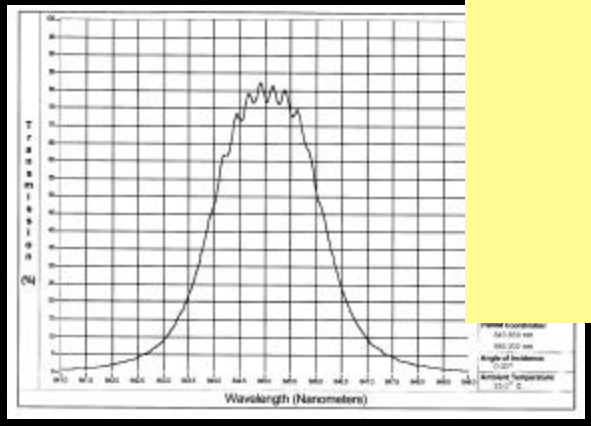
Technical Accomplishments (4)

Alice and Bob Bodies

- **Observed VCSEL's spectra**
- **Determined parameters for interference filters and other parts**
- **Built the bodies of Alice and Bob**

VCSELs and Interfence Filters





Status Hardware

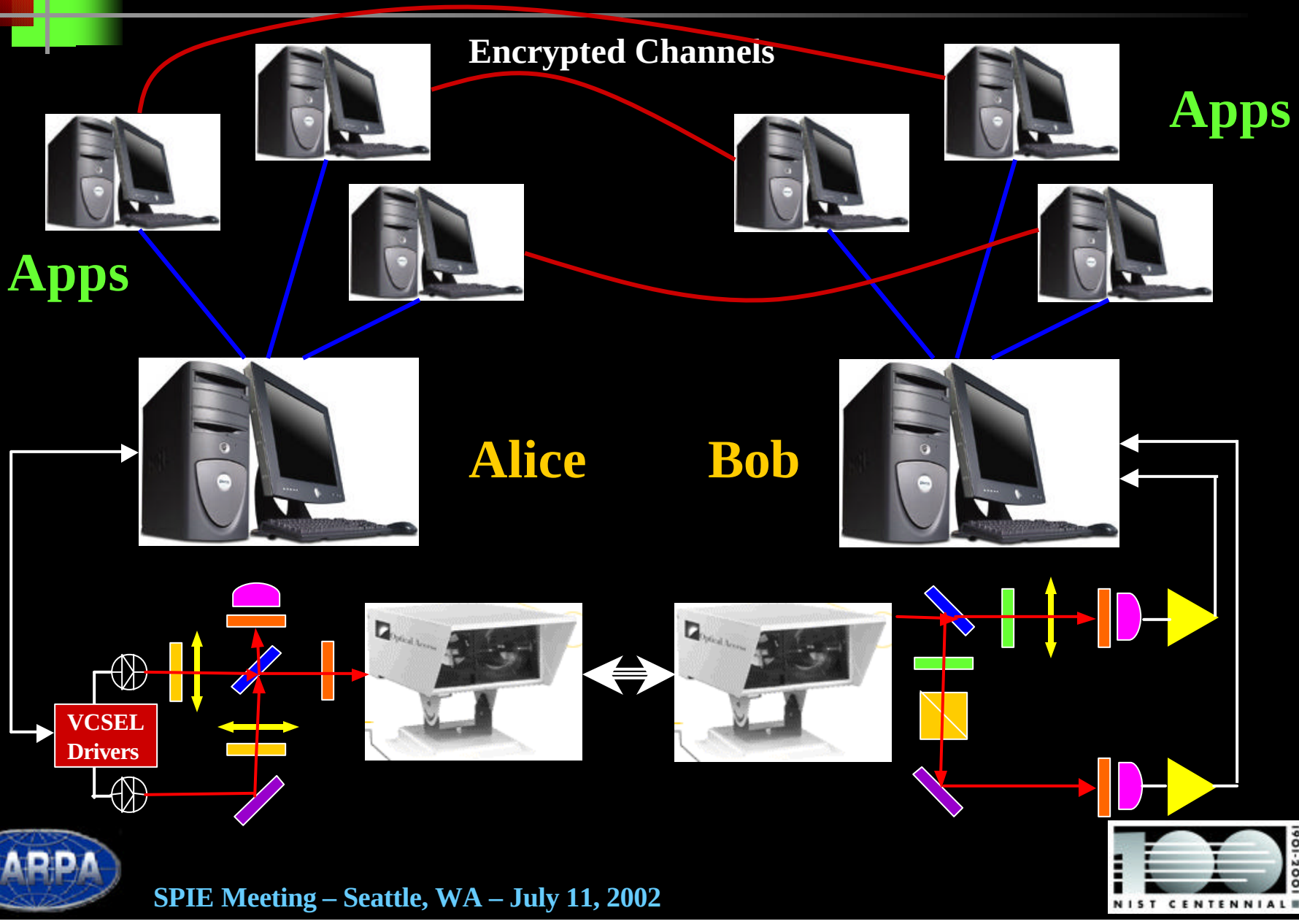
- Classical Channel and Telescope
  - WDM System Upgraded to 1.25GHz
  - LVDS Circuit Designed
  - Quantum Scopes Tracking and Linked to Network
- High Speed Electronics
  - Random Number Generator Completed
  - 8/10 bit Encoding Chipset Received
  - High Speed Board Designed and Parts Ordered
  - FPGA Layout Complete
- Quantum Telescopes
  - Developed Computer Controlled Tracking
  - Installed Fiber Interface
- VCSEL's Characterized and Filters Obtained
- Alice and Bob Bodies Built

Software Philosophy

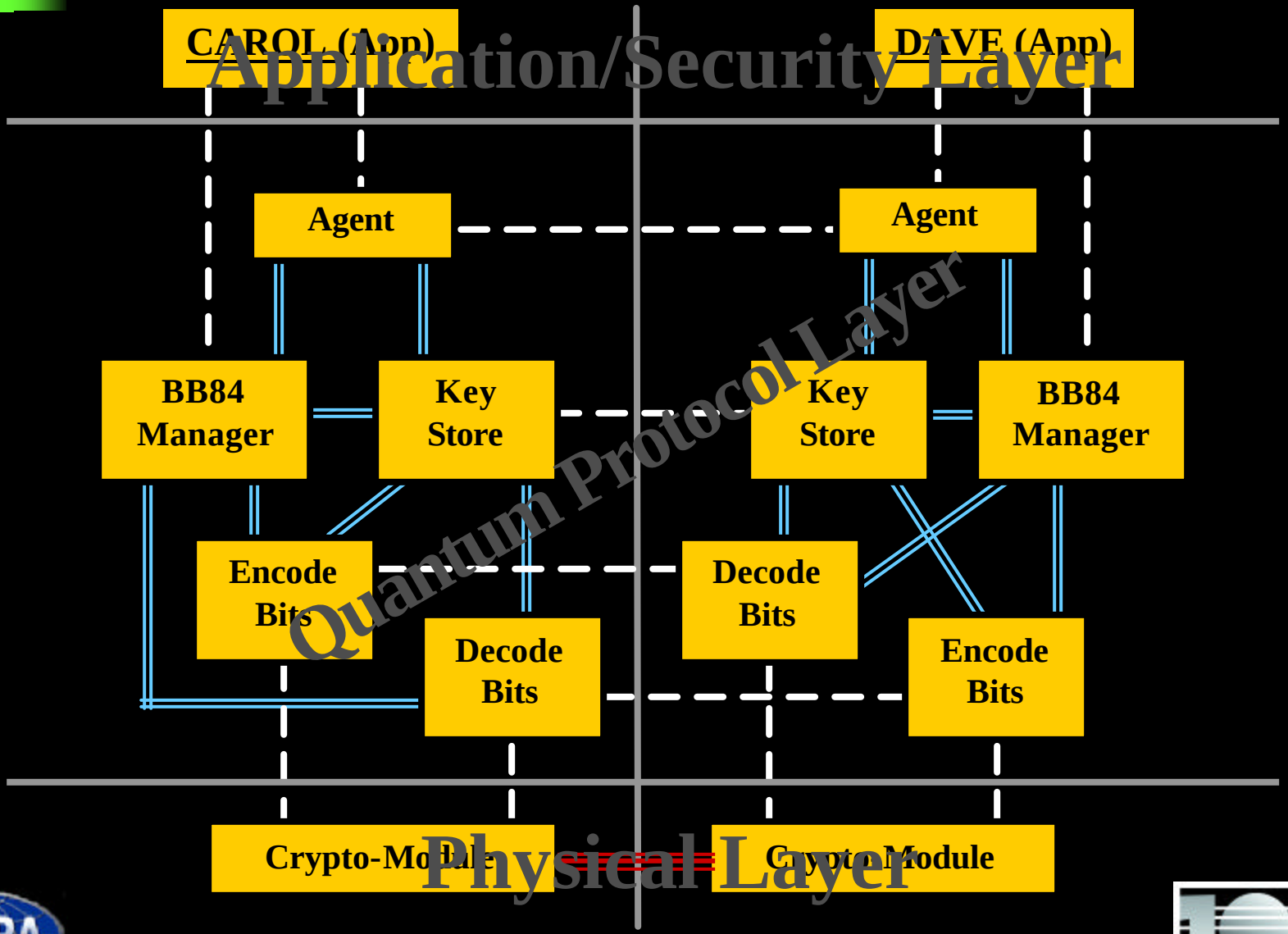
- Develop public-domain java prototype of BB84 protocol with necessary cryptographic services
  - Forward error correction – Reed-Solomon Codes
  - Privacy amplification
  - Key store protocols
  - Hybrid authentication protocols
  - Internet Key Exchange, IPSec
- Implement BB84 with cryptographic services and characterize system
- Implement alternatives and variants to BB84
  - Explore engineering tradeoffs
  - Explore enhancements of basic functionality
- Work with others to develop standardized interfaces and integrated cryptographic modules

Tassos Nakassis, David Su

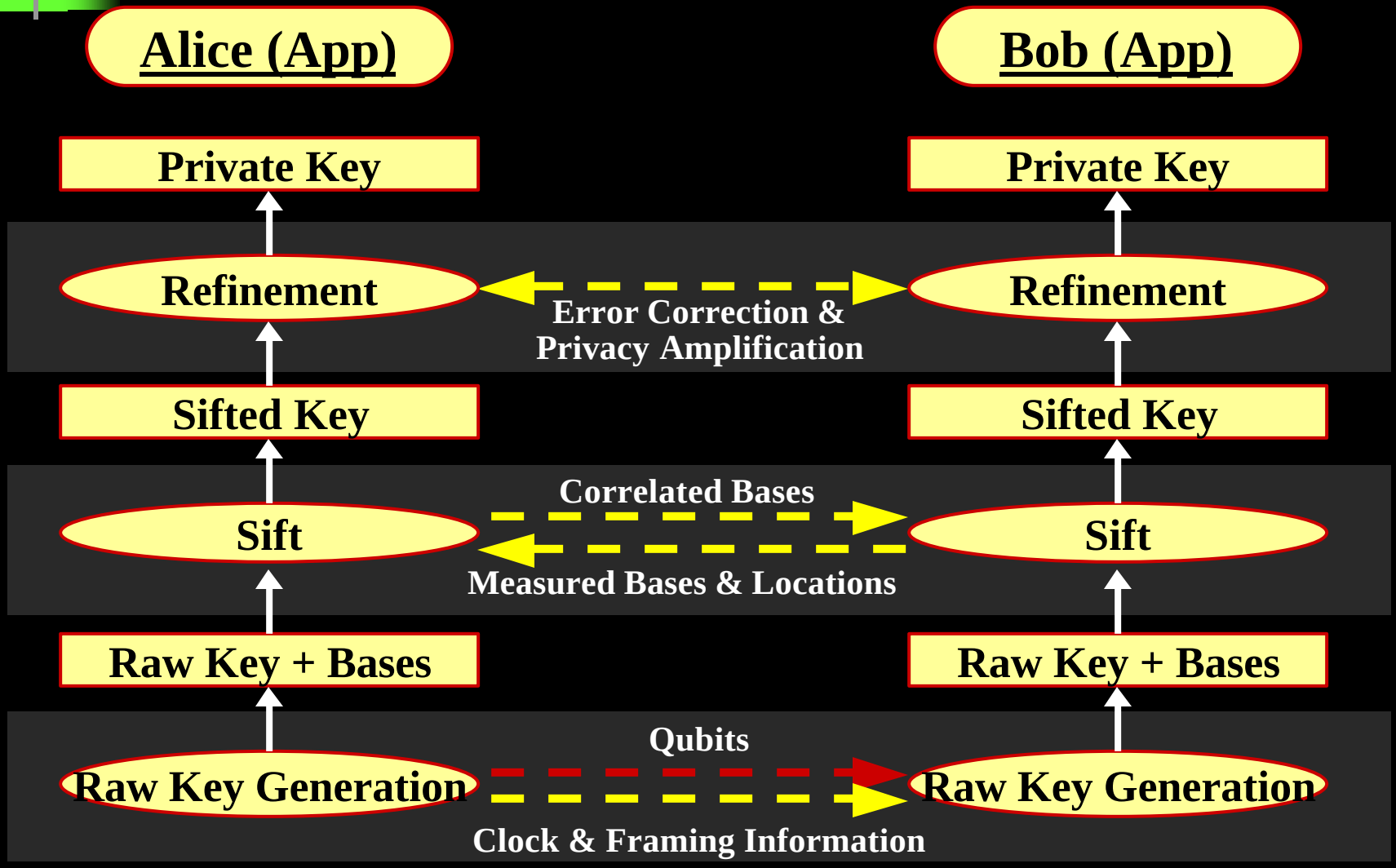
Software Overview/Topology



Software Layers

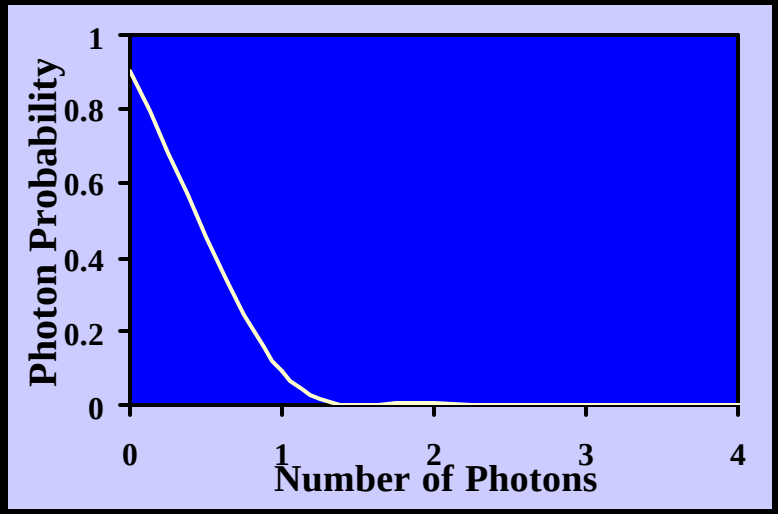


Crypto Module / Qubit Generator

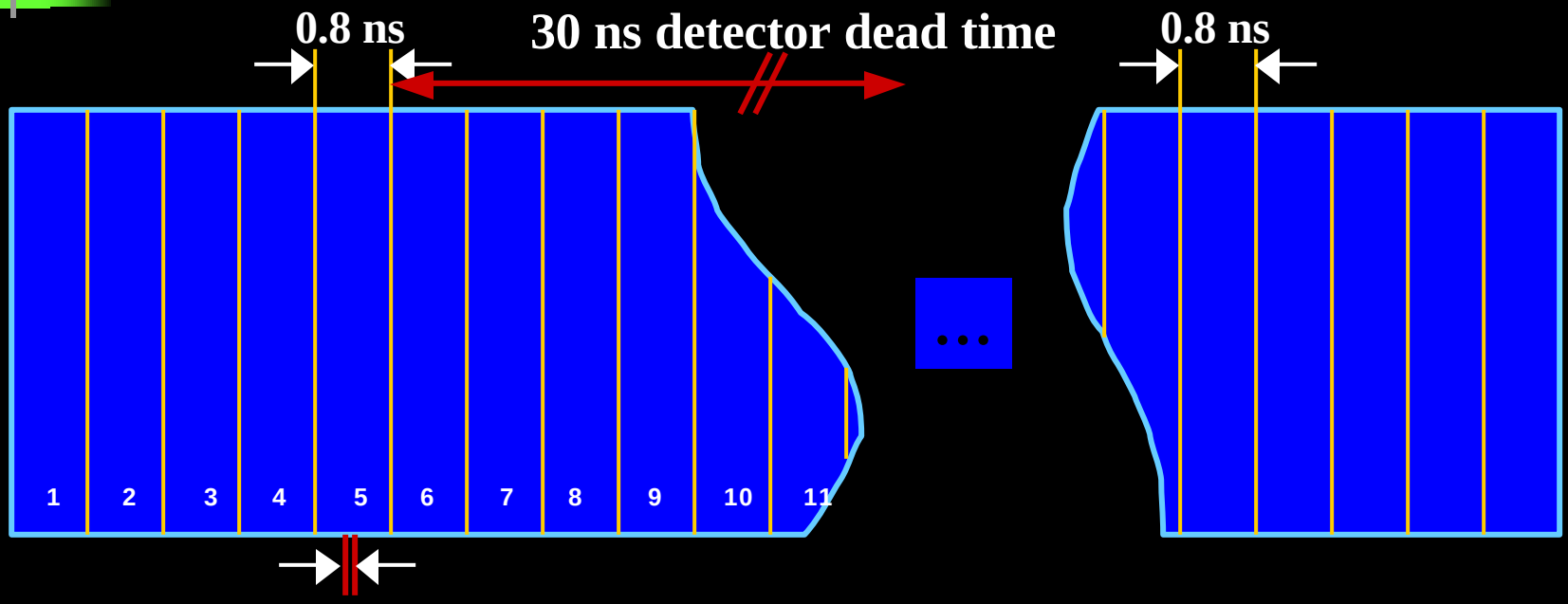


Timing Considerations

- Photon travel time (600m/3´10^{8}m/s): 2 ms
- Mean photon number: 0.1 photons
- Detector efficiency: 50%
- Detector recovery (dead-time): 30 ns
- Detector jitter: ~ 0.1 ns
- Quantum link budget: ~ -20 dB
- Pulse rate: 1.25 GHz
- Count rate: 3 MHz
- Frame size: "1250"
- Frame length: 1 ms
- Counts/Frame: ~ 3



Timing for a Single Frame

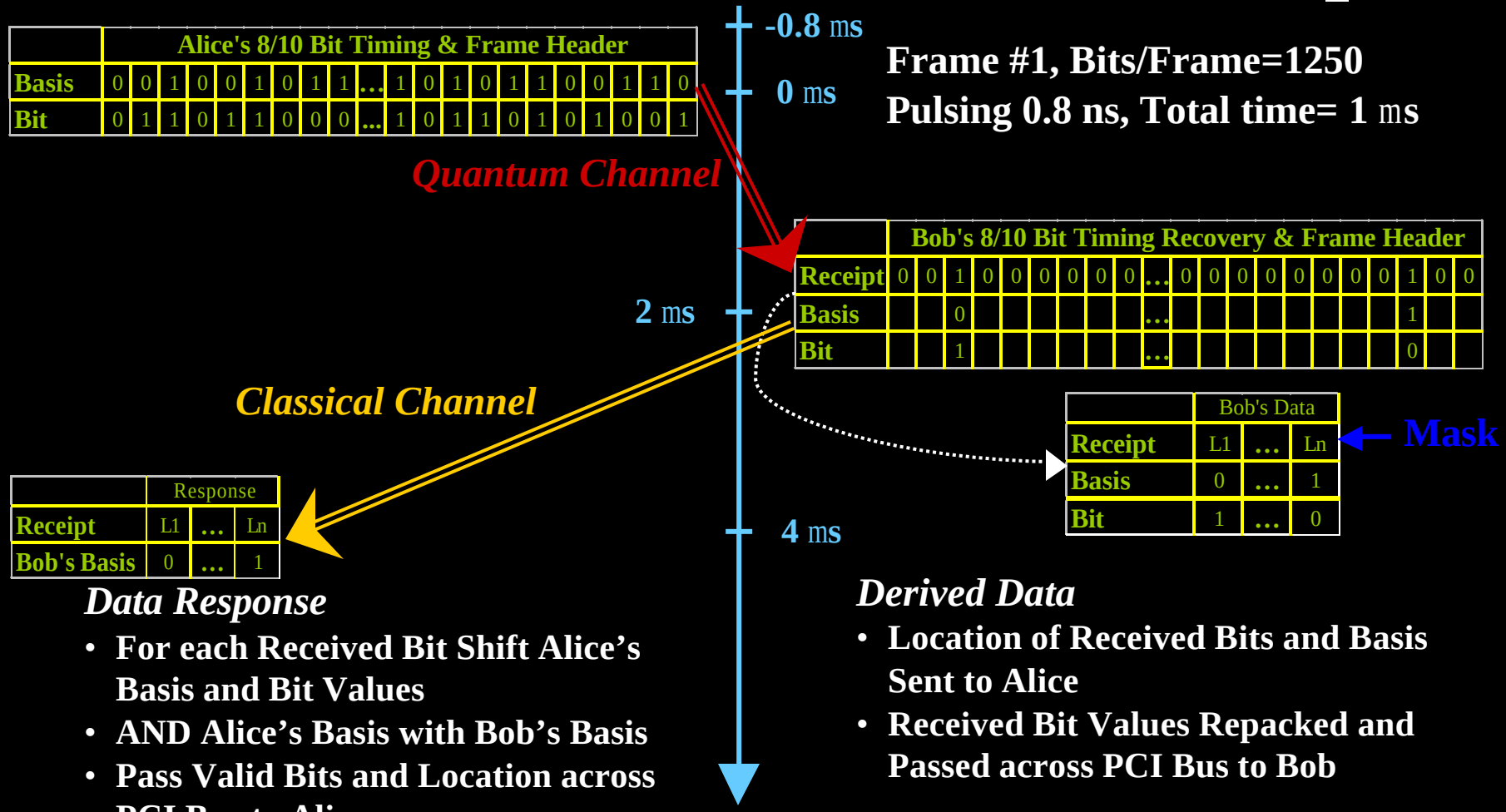


1250 Bits/Frame « ~ 1 ms

Roughly 1 in 400 Bits are received $(0.1*0.5*0.05)^{-1}$

Data Streams and Timing

Random Number Generator Fills Alice's Basis and Bit Buffer - 16´622



Data Response

- For each Received Bit Shift Alice's Basis and Bit Values
- AND Alice's Basis with Bob's Basis
- Pass Valid Bits and Location across PCI Bus to Alice

Derived Data

- Location of Received Bits and Basis Sent to Alice
- Received Bit Values Repacked and Passed across PCI Bus to Bob

Data Streams Details

Alice's Data Stream

FrameID	N_{bits}	(A_1,B_1)	…	(A_{Nbits},B_{Nbits})

Data Generation Electronics

FrameID	N_{recd}	(L_1,A_{B1})	…	(L_{nrecd},A_{BNrecd})

Shift and AND Operations

FrameID	N_{valid}	(J_1,B_1)	…	(J_{Nvalid},B_{Nvalid})

Send Across PCI

FrameID	N_{valid}	B_1	…	B_{Nvalid}

Bob's Data Stream

Data Acquisition Electronics

FrameID	N_{recd}	$(L_1,A_{B1},B_{1'})$	…	$(L_{nrecd},A_{Nrecd},B_{Nrecd'})$

FrameID	N_{recd}	$B_{1'}$	…	$B_{Nrecd'}$

Across PCI

FrameID	N_{valid}	J_1	…	J_{Nvalid}

Shift

FrameID	N_{valid}	B_1	…	B_{Nvalid}

time

Error Correction + Privacy Amplification

Undiscussed Issues

- De-skew Quantum and Classical Channel
- Fill Buffer of Alice's Basis and Bit using Random No.
- Gate Quantum Channel Serdes off Classical Clock
- Buffer Fill and Flushing Across PCI
- Interface w Software Code (Operating System)
- BB84 vs B92