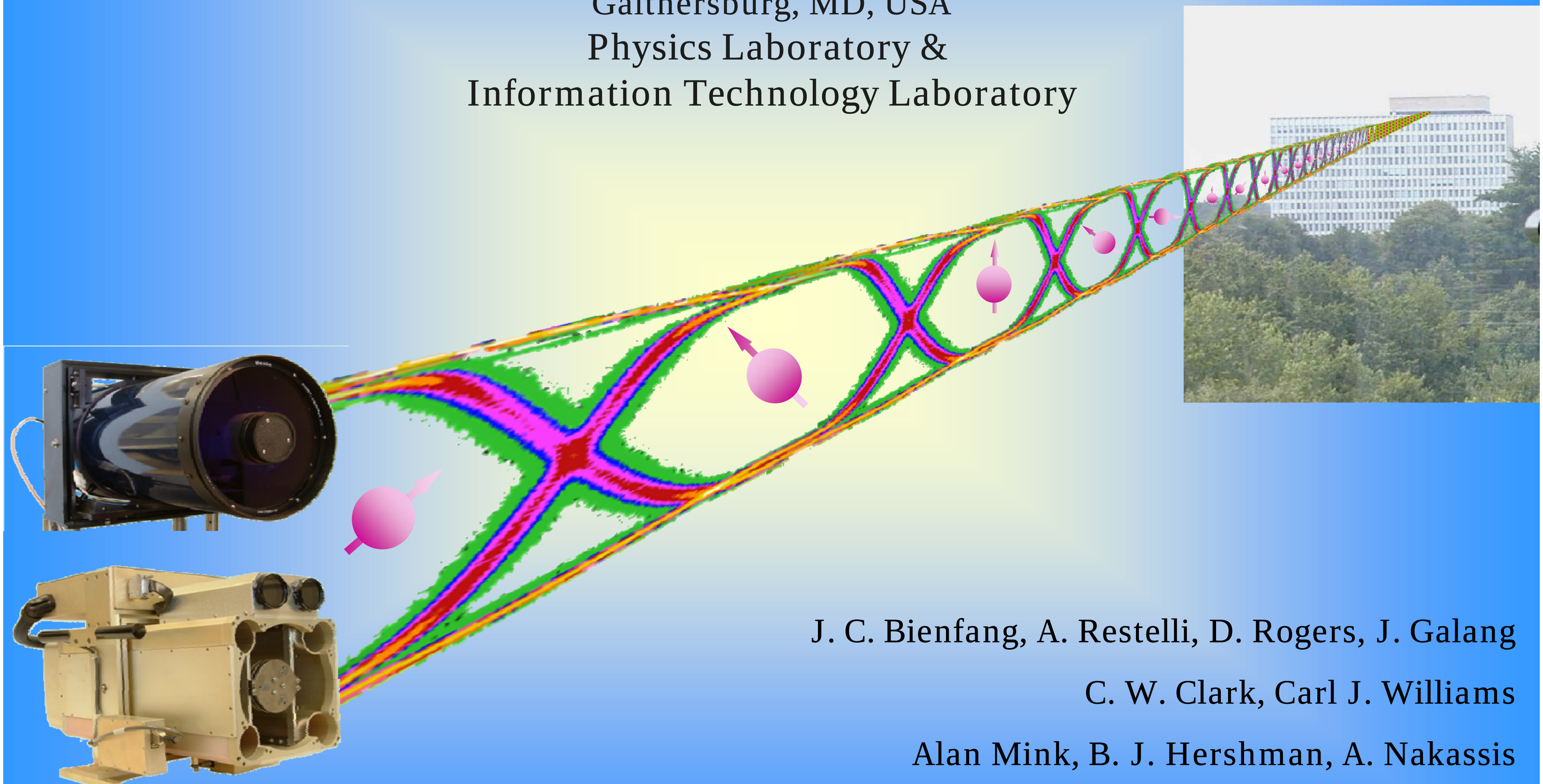
Broadband Quantum Key Distribution

National Institute of Standards and Technology
Gaithersburg, MD, USA
Physics Laboratory &
Information Technology Laboratory



J. C. Bienfang, A. Restelli, D. Rogers, J. Galang

C. W. Clark, Carl J. Williams

Alan Mink, B. J. Hershman, A. Nakassis

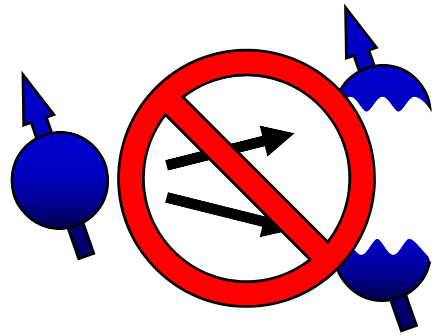
BlackHat 8/7/08

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

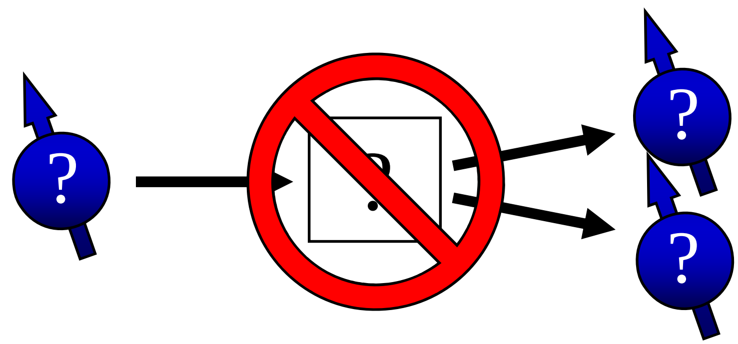
Quantum Capabilities

What properties of quantum mechanics do we exploit?

- Indivisibility



- No arbitrary copying
  [1] Wooters, 1983



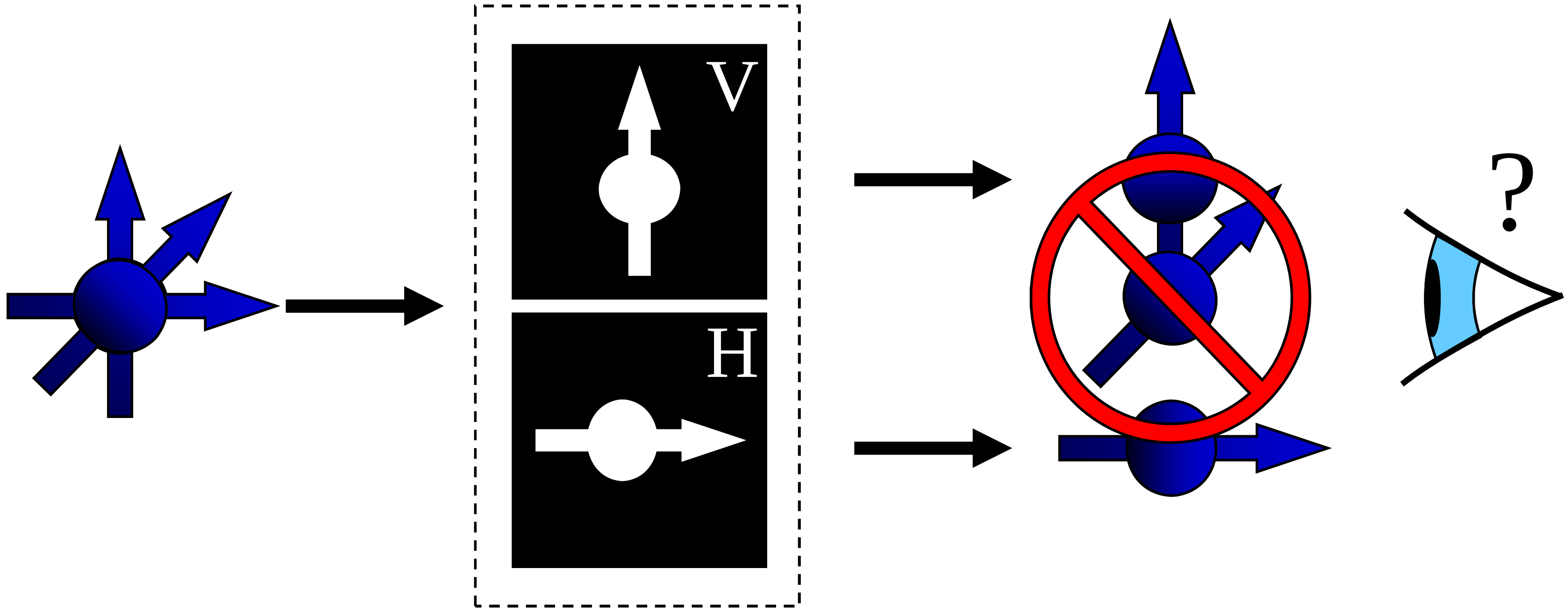
- State Measurement

- … and, in more esoteric schemes, quantum correlation (entanglement)

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Measuring Quantum States

Measure a quantum state that has some property ”↗“…



There is a trade-off between information about an unknown quantum state and disturbance of that state.

Great for cryptography

Quantum Cryptography

It is possible to send and receive individual quanta and detect if state measurements have been made en route.

➔ *Sensitivity to eavesdropping*

- Source and detect individual quanta *– technology development*
- Requires an additional communications channel
- Evidence of eavesdropping is statistical
- Unpredictability requires randomness
  - *Not transmitting messages from point A to point B on the quantum channel*

➔ Key distribution [2] Gisin (2002)

QKD Protocols

1. Prepare and Measure: [3] Bennett (1984), [4] Weisner (1983).
   - Send photons in a set of non-orthogonal bases:
   - Polarization: (↑, →) & (↗,↖). ← Free-space
   - Relative phase: (0^o, 180^o) & (90^o, 270^o) ← Fiber

2. Quantum Correlations: entangled photon pairs
   - Polarization entanglement: [5] Ekert (1992)

Photon 1 goes to Alice

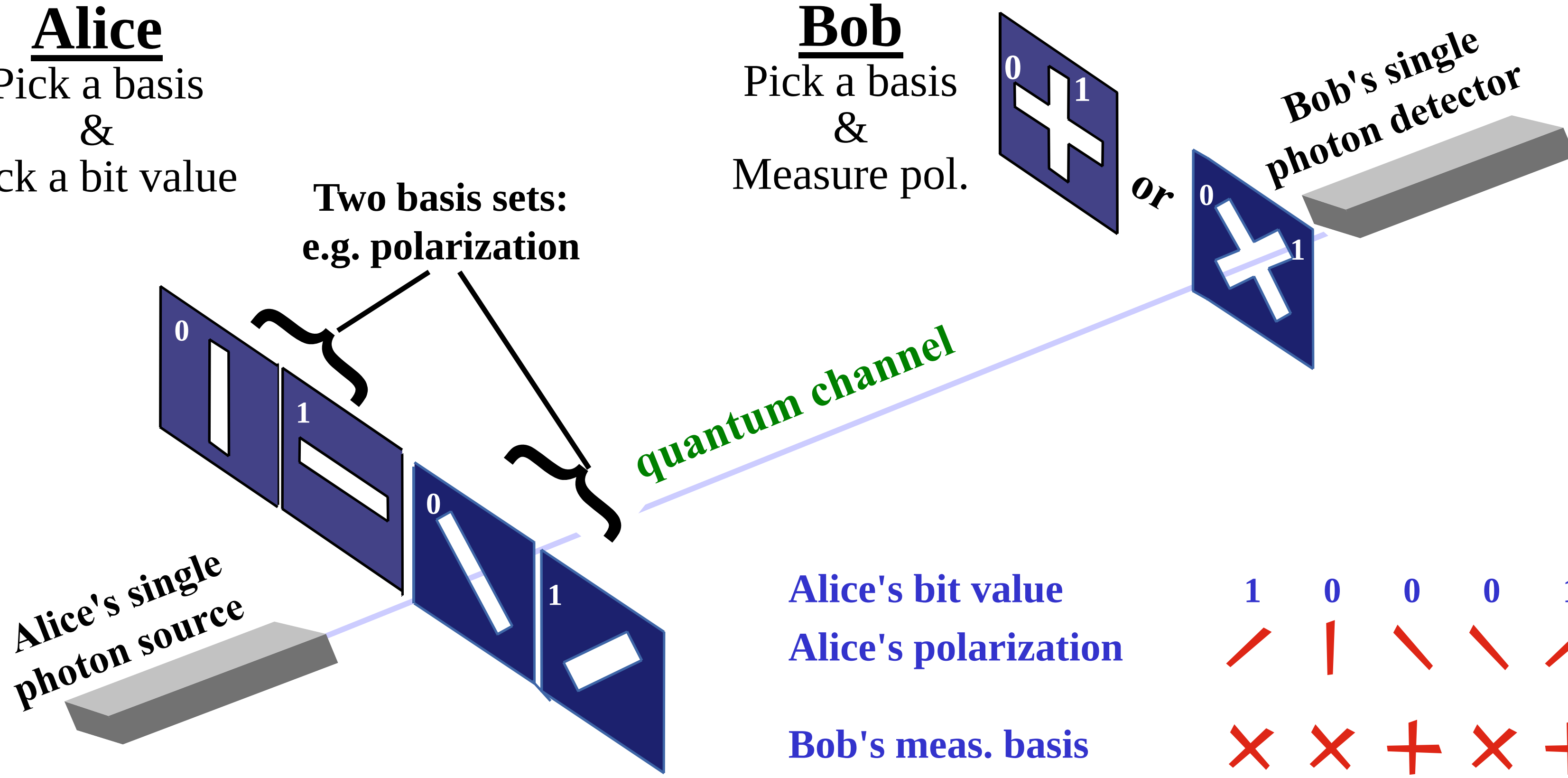
Photon 2 goes to Bob

QKD in the BB84 Protocol

(non-orthogonal bases)

Alice
Pick a basis
&
Pick a bit value

Bob
Pick a basis
&
Measure pol.

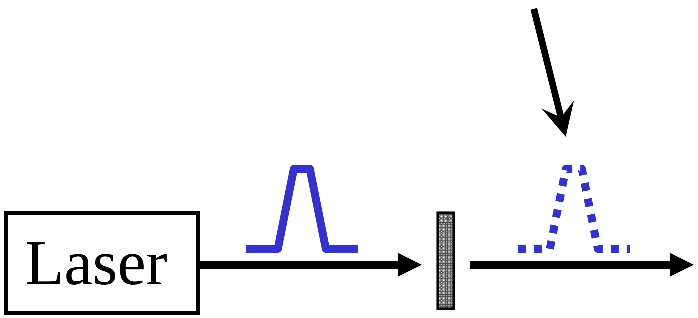


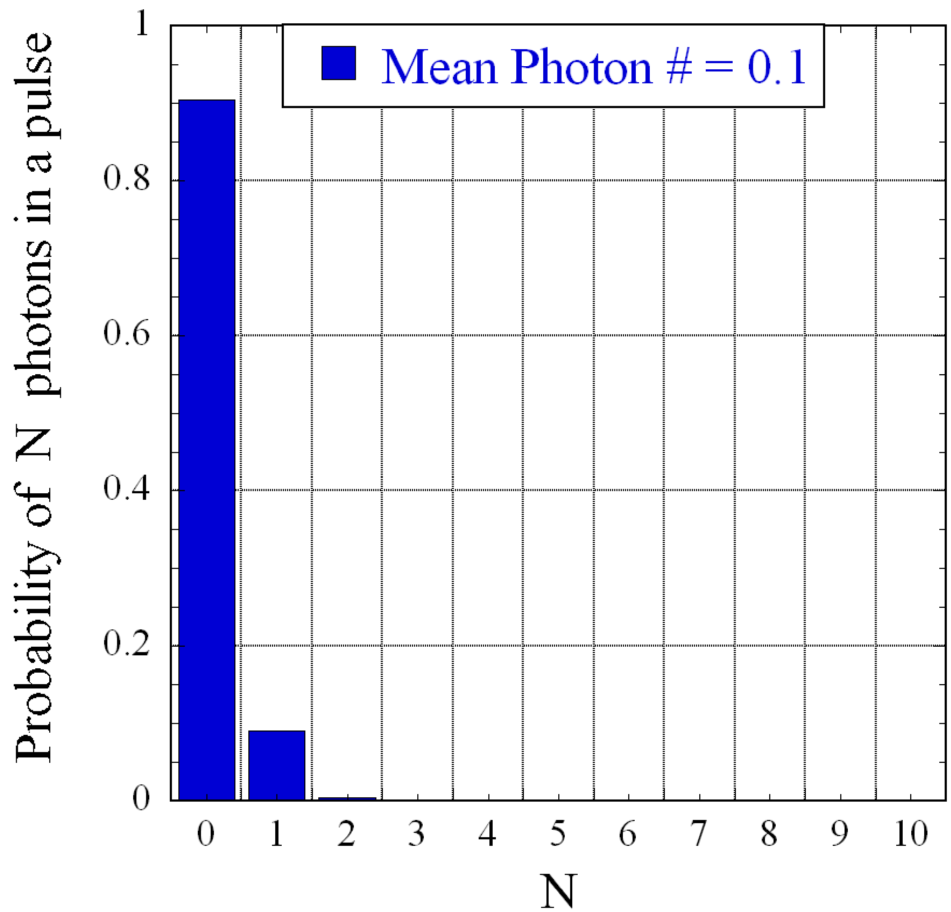
Alice's bit value	1	0	0	0	1	1
Alice's polarization	/	|	\	\	/	—
Bob's meas. basis	×	×	+	×	+	+
Bob's result	1	1	0	0	1	1
Same basis?	Y	N	N	Y	N	Y
SIFTED KEY →	1			0		1

[3] Bennett (1984).

Single-Photon Source – Quick & Dirty

Laser Statistics: one can set some average number of photons per pulse.





Pro: Cheap, fast, easy to use
Con: 1/10 Tx rate, security

NIST's Focus to Date

Encryption with QKD requires:

Authentication
Transmission and detection of single photons,
Another (classical) communication channel,
Error Correction,
Privacy Amplification,
and finally, a cipher.

What are the speed limits in single-photon QKD?

→ Physical Layer (the single photon channel)

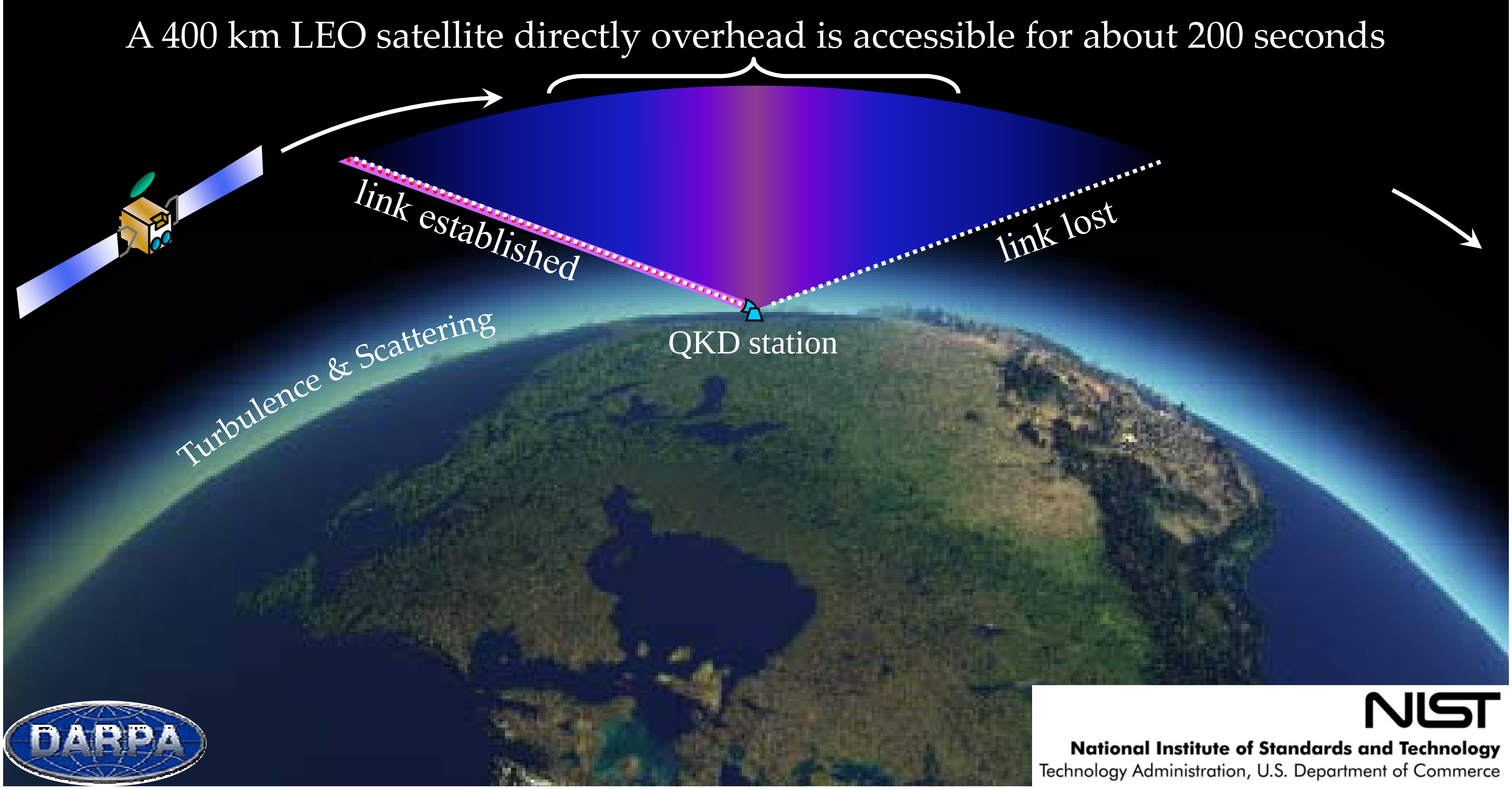
- [6] Rogers (2007).
- [7] Xu (2007).
- [8] Bienfang (2004).

→ Error Correction and Privacy Amplification

- [9] Nakassis (2004).

High-speed QKD in a Global Network

In the absence of a quantum repeater, a LEO QKD satellite can span the globe, but access time is limited by orbit and atmosphere.

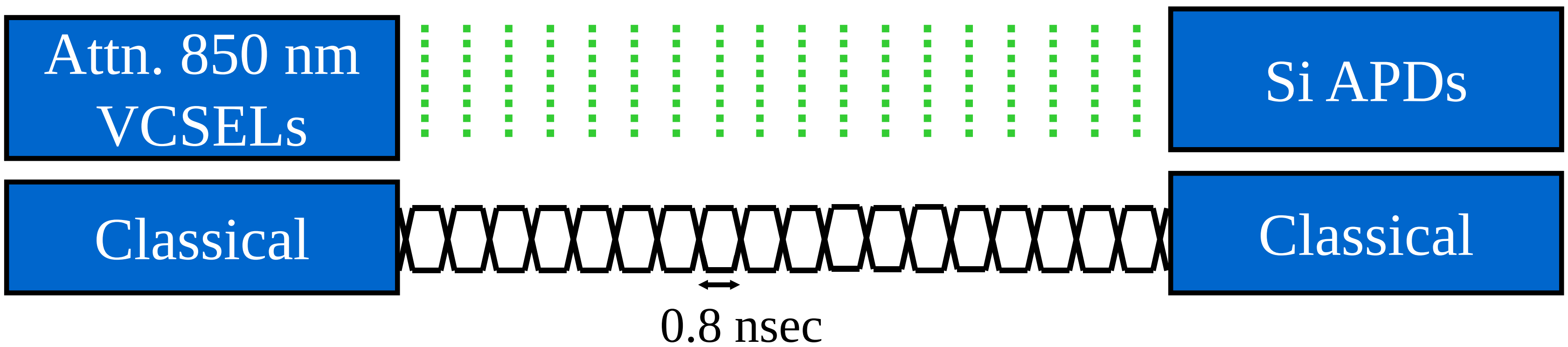


DARPA

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

High-speed Free-space QKD

- SNR is enhanced with spatial & spectral filtering, and temporal gating:

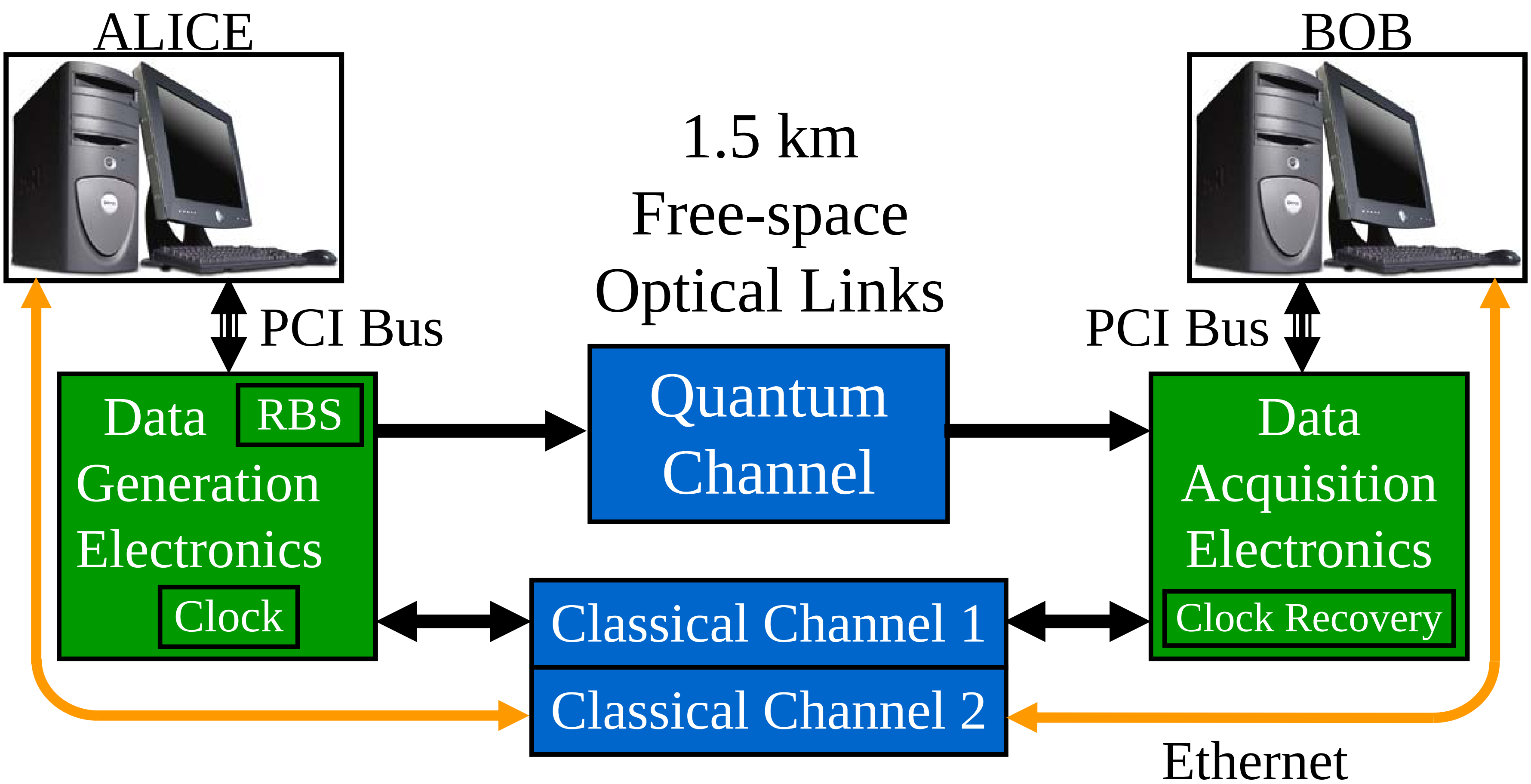


8B/10B encoding/clock recovery

- A 0.8 ns gate is equivalent to 1.25 Gbps signal
  - Limited by detector jitter and recovery time
  - Timing channel is a usable duplex channel for sifting

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Link Topology

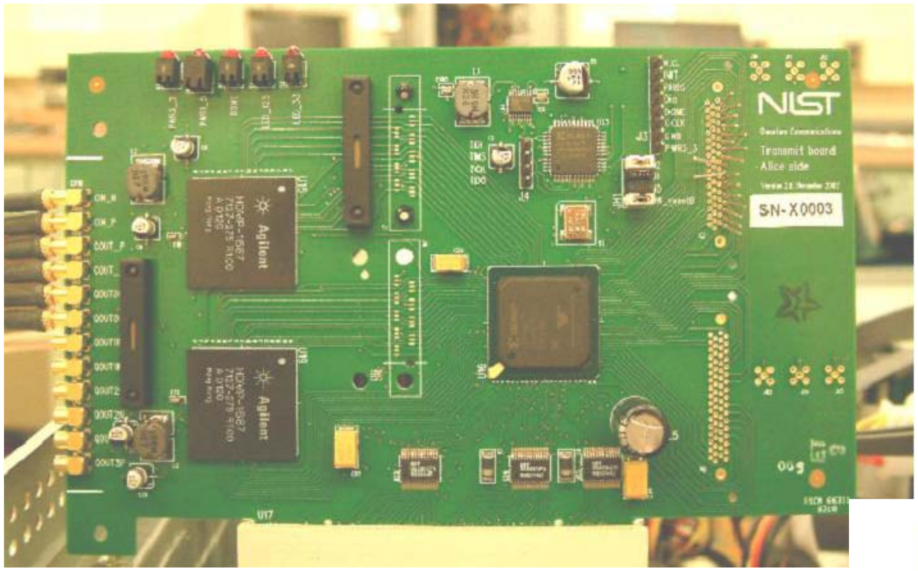


Ch.1: Defines 2048-bit q-channel frames, Sifting

Ch.2: Error Correction, Privacy Amplification

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

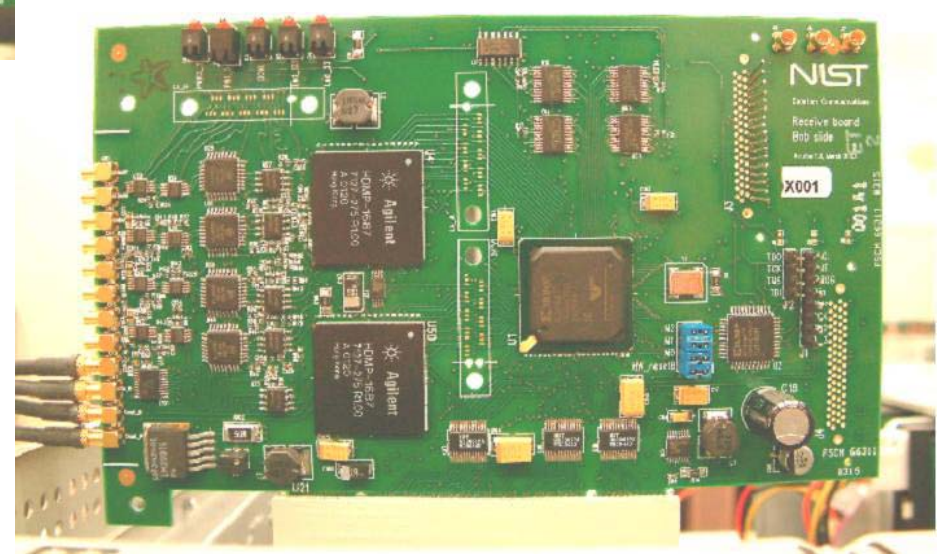
Rev. 1.0 Boards



Operating in Linux
with custom drivers

Alice

Bob

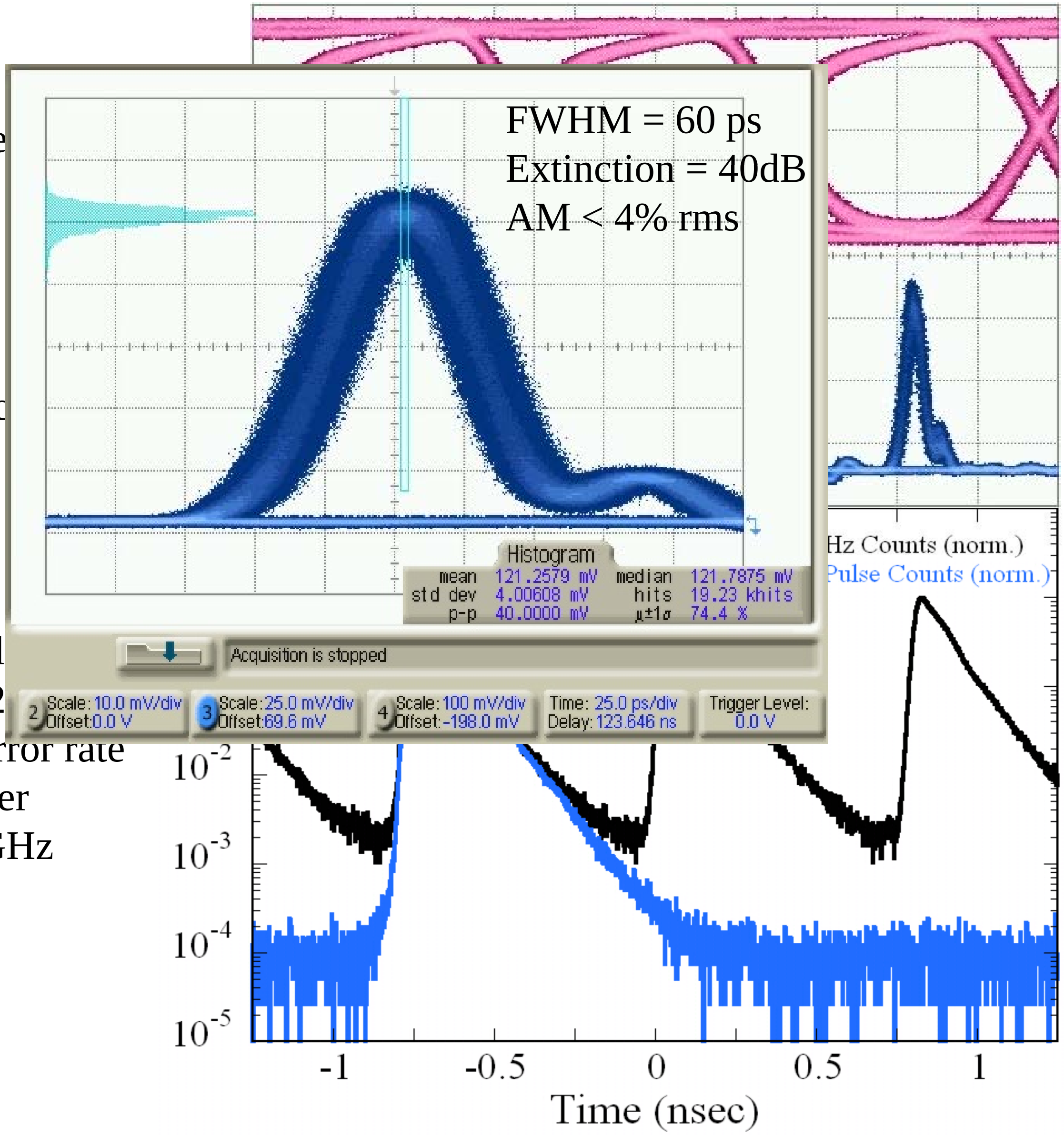


Signal diagnostics at 1.25GHz

1.25Gbps NRZ ele
from Alice

1.25 Gbps optical
Alice – Gain switc
VCSELs

Histogram of singl
arrival times at 1.2
→ Quantum bit error rate
due to detector jitter
<0.01% @ 1.25 GHz
< 1% @ 2.5 GHz



Institute of Standards and Technology
ninistration, U.S. Department of Commerce

High-Speed Error Correction

To expedite EC, we (A. Nakassis) incorporated forward error correction (Hamming codes):

1. Segment and parity exchange
→ Estimate error rate.
→ Optimize segmentation:
50% have 0 errors
35% have 1 error
13% have 2 errors
4% have 3…

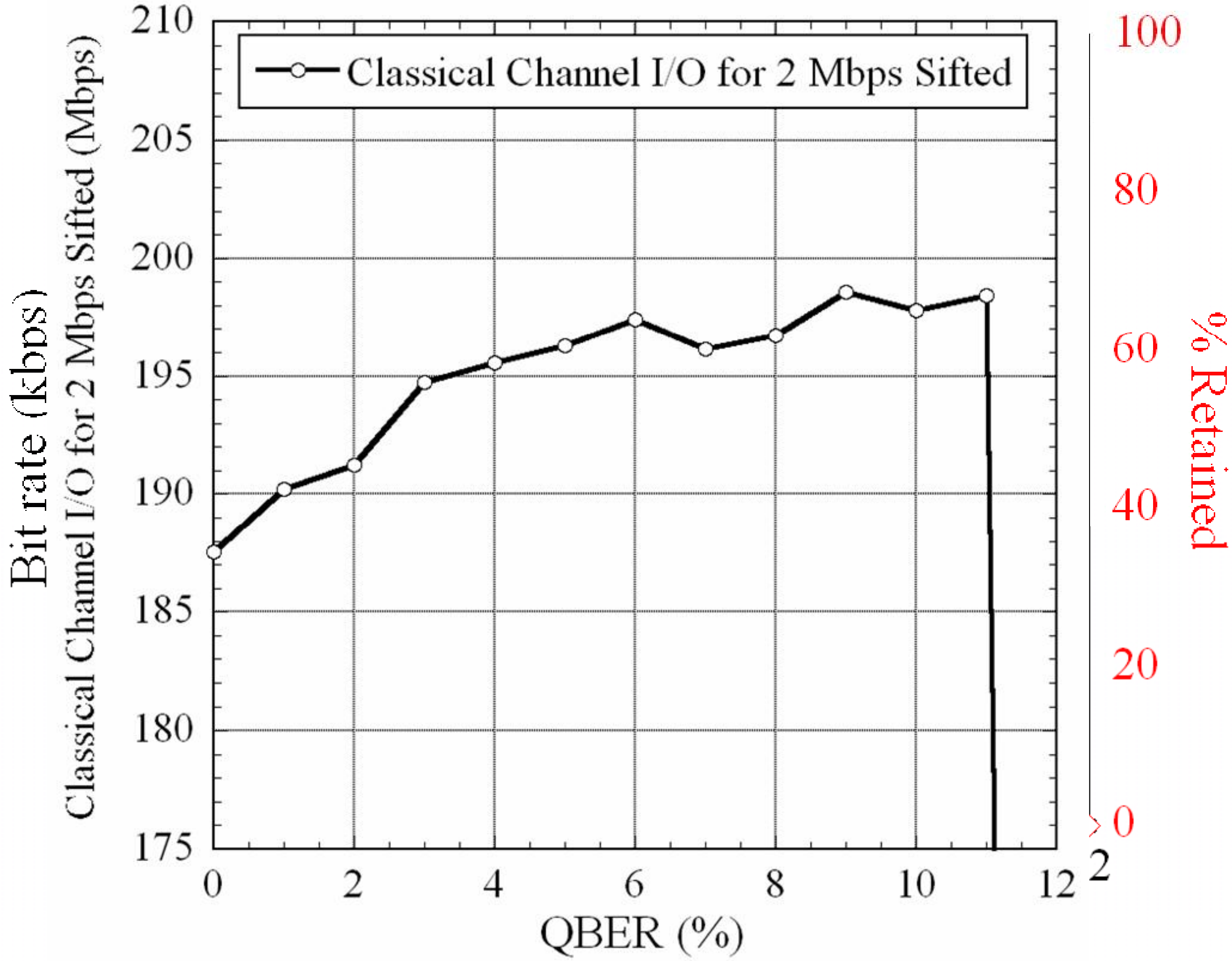
2. FEC round
→ Token holder generates & sends FEC code for those segments with odd numbers of errors.
→ FEC applied, token switched. Some high-error segments are identified & discarded.

3. Reset
→ Privacy maintenance
→ Shuffle bits
→ Estimate error rate

→ If $\varepsilon > 10^{-4}$ return to step 2.

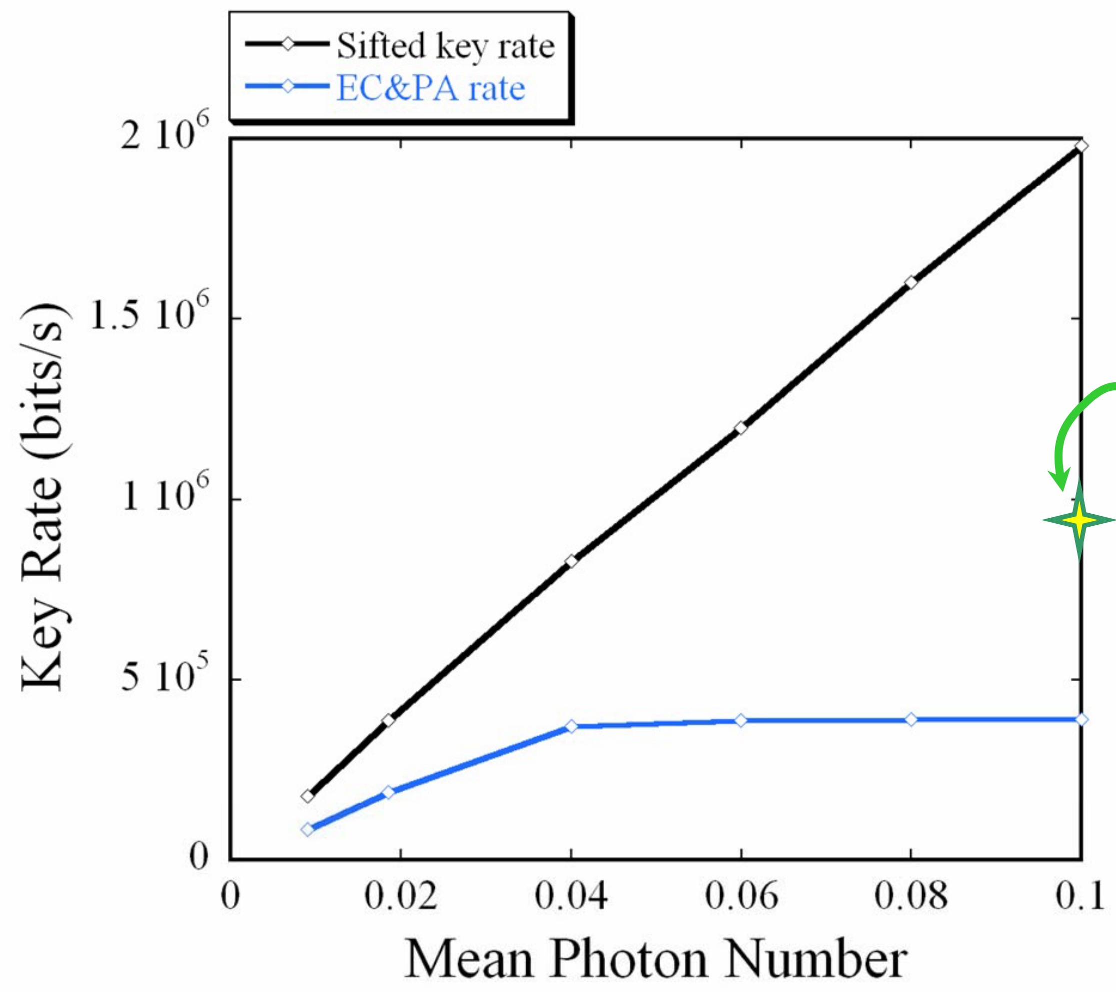
If $\varepsilon < 10^{-4}$ (~ 6 cycles) we apply a final round of FEC → $\varepsilon < 10^{-9}$

EC & PA Processing Rates



National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Bit Rates at 625 MHz (2006)



Machine dependent
→ 400 kbps on 2.4 GHz Pentium IV

Dual 3.0 GHz Xeon
0.950 Mbps at α = 0.15

One-time-pad encrypted streaming video at 512 kbps, 64 kbps audio.

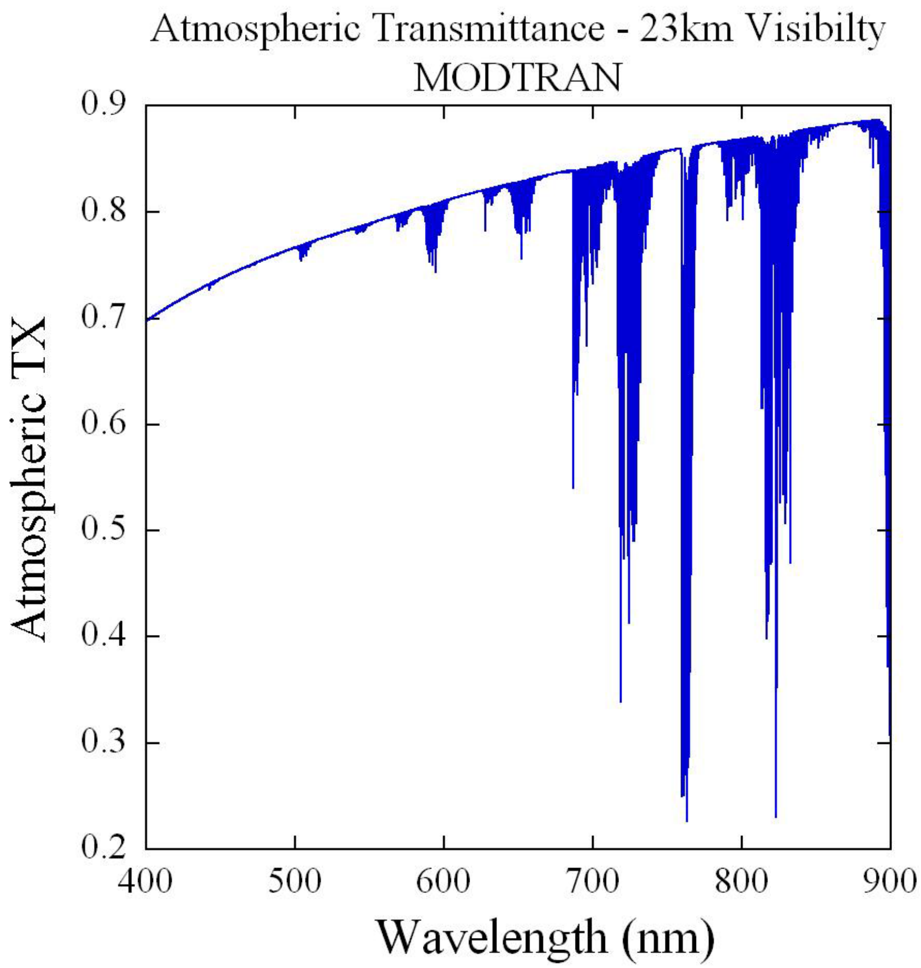
More work to be done to achieve Daylight operation

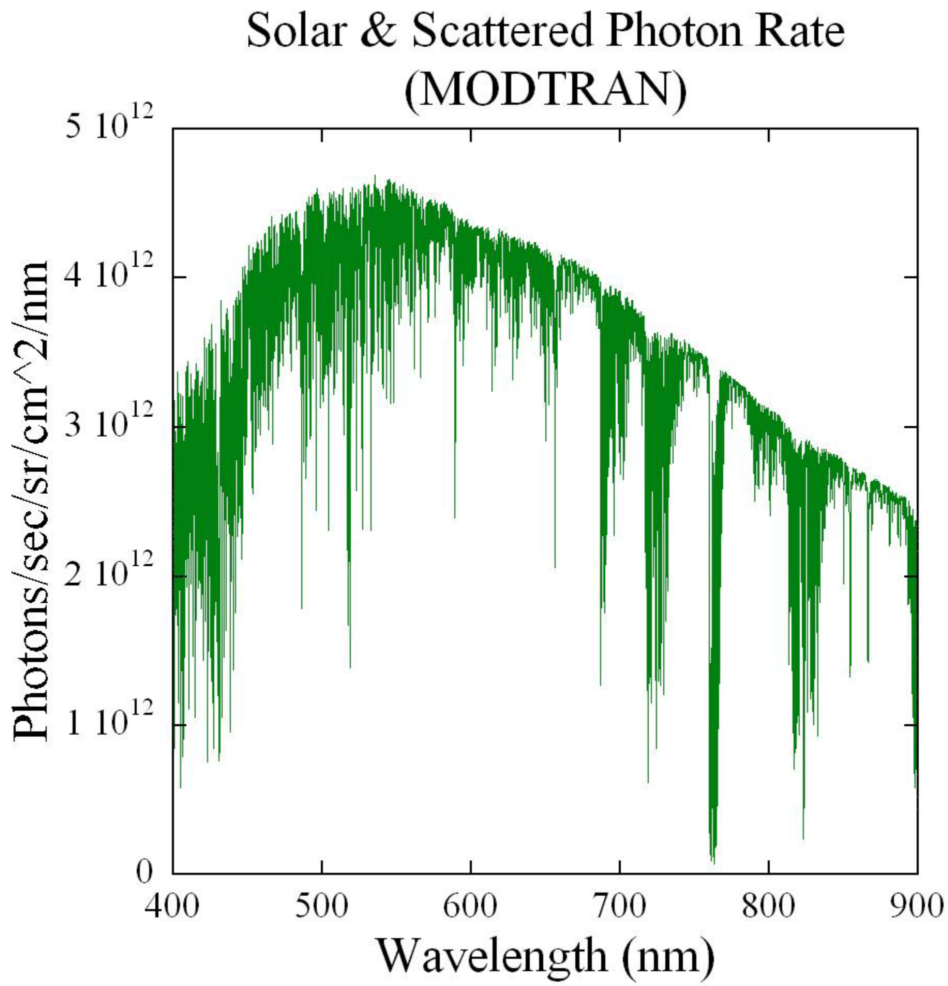
[I. Rech, S. Cova, *et al. Politecnico di Milano*]

DARPA

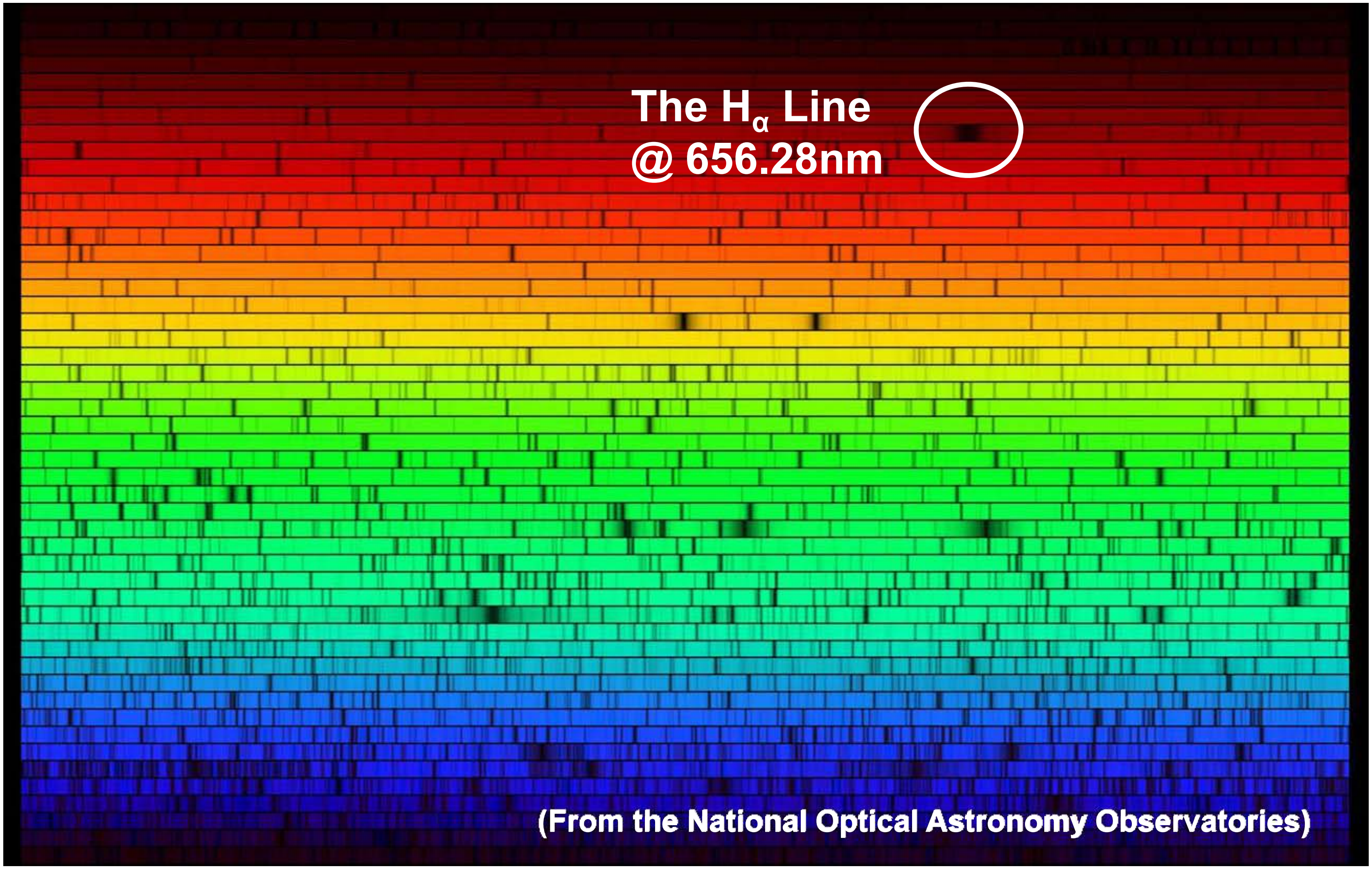
NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Single Photon Channels in Vis.



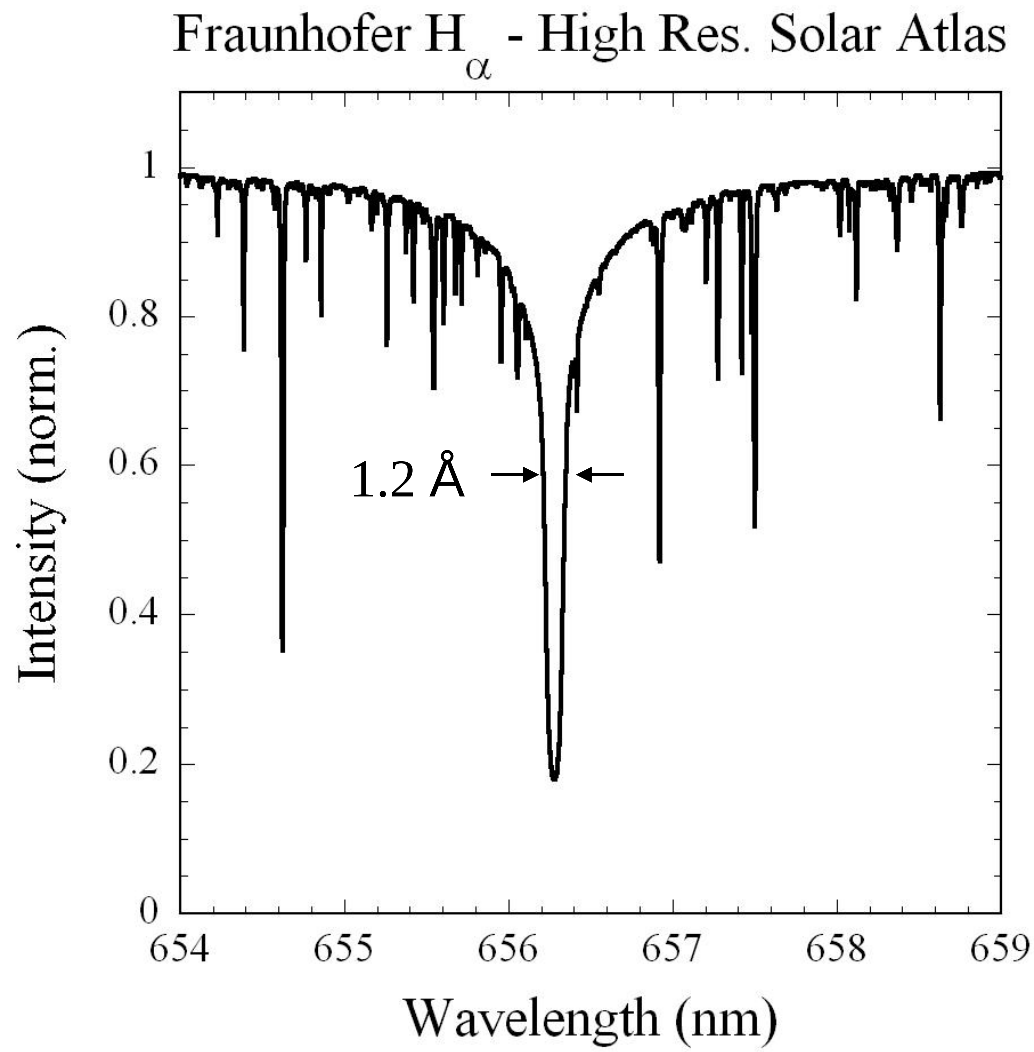


The Visible Solar Spectrum

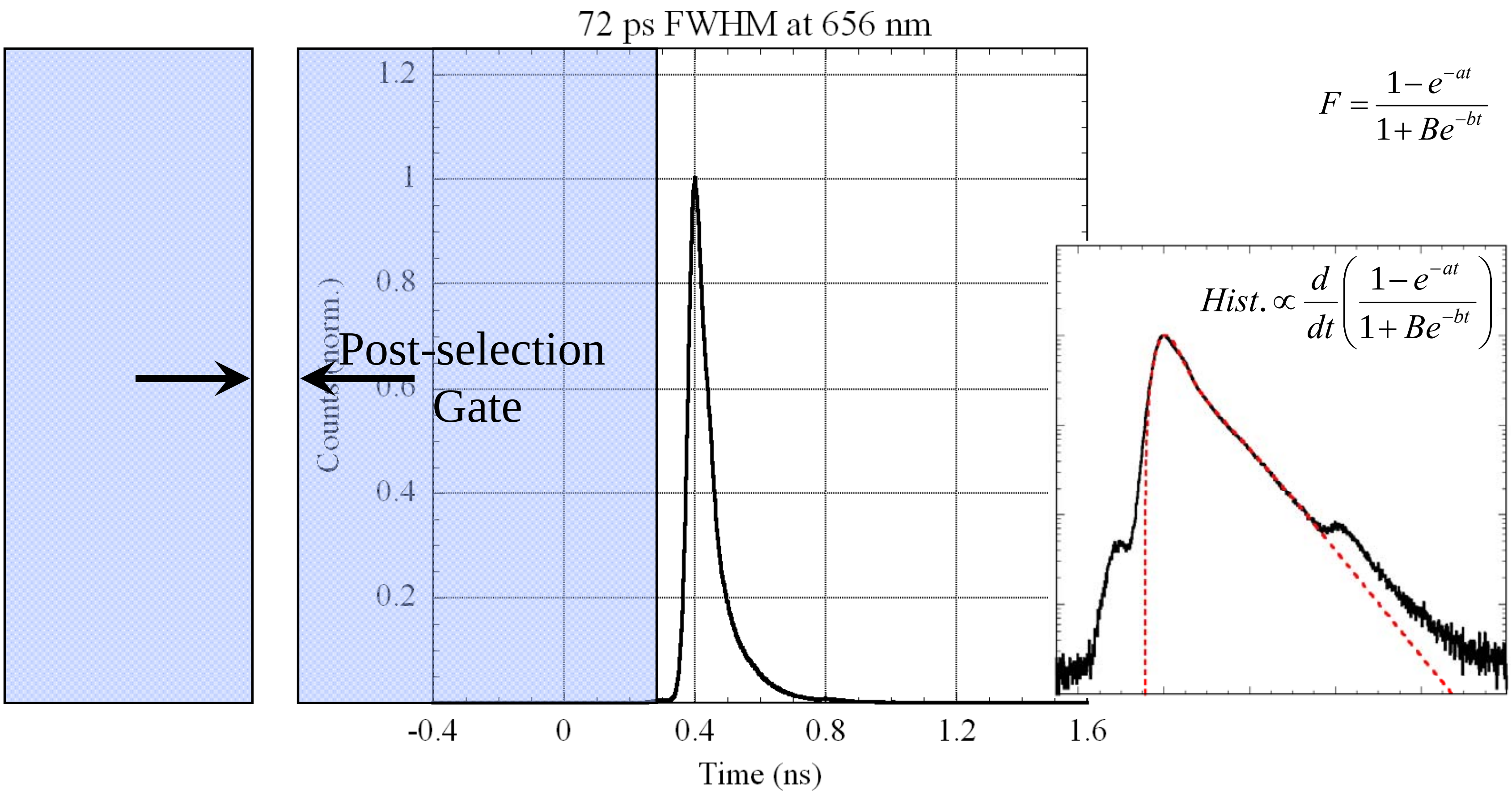


H_α Fraunhofer Window

- At the center of the H_α line background noise is reduced by ~7.5 dB.
- Filters are excellent.

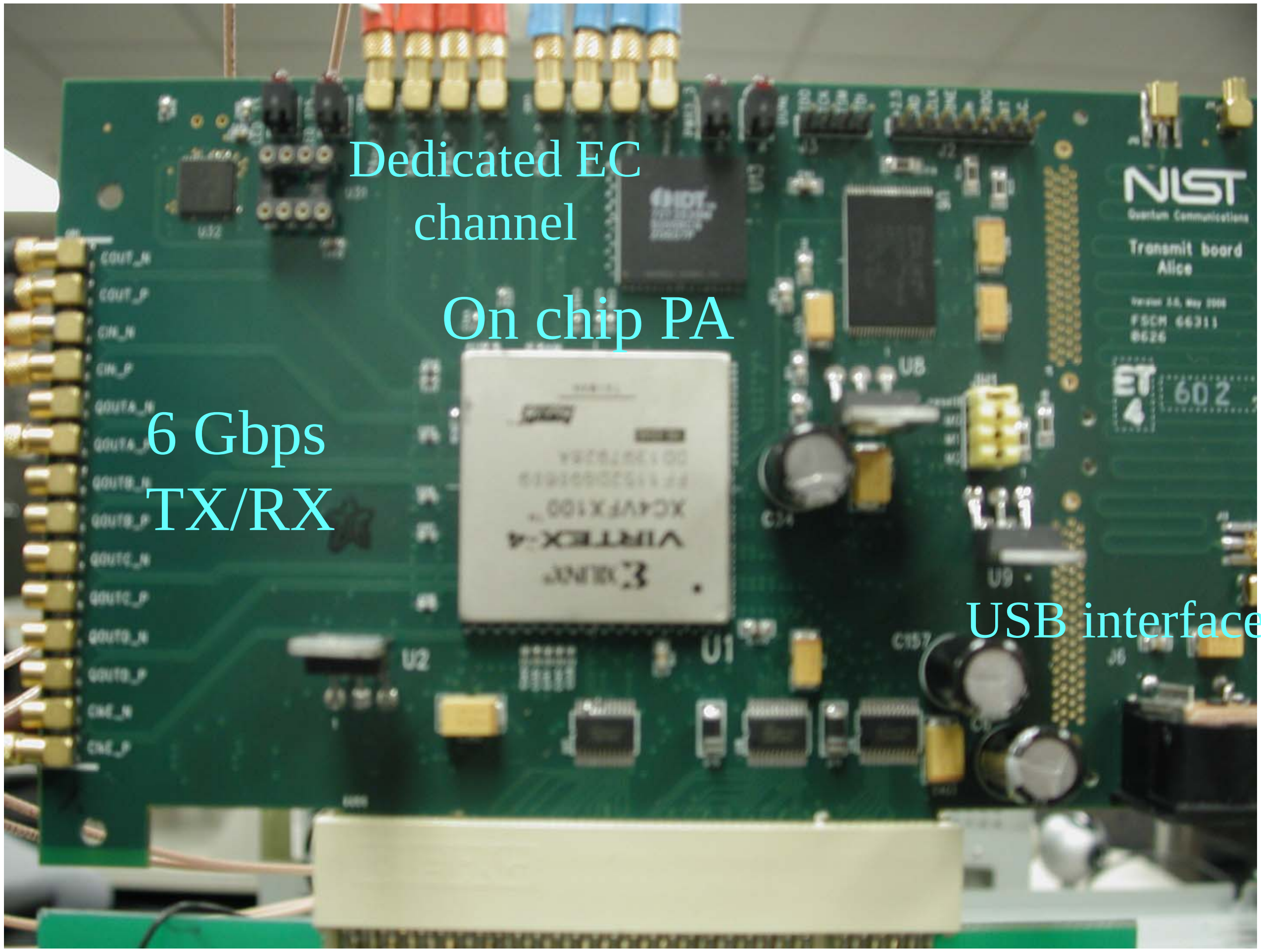


Timing Resolution of Si-APDs



Improved FWHM → 1/8 × Exposure to background noise

Faster QKD – Rev. 2.0 Board



Transceiver rates variable up to 6 GHz (166 ps)

Dedicated EC channel & PA processor
➔ up to 20 Mb/s input

Memory for > 200 km

Non-PCI interface (!)
➔ Portable

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Conclusion

- Bandwidth of BB84 QKD systems can be maximized with clock recovery techniques
- Detectors will enable operation > 2.5 GHz
- Improved timing resolution reduces QBER and extends the range of a FSO QKD system
- High-bandwidth one-time-pad encryption services can be provided with quantum-generated key

References

[1] Wooters, W., *et al.*, "A single quanta cannot be cloned," *Nature* **299**, 802-803 (1982).

[2] Gisin, N., *et al.*, "Quantum cryptography," *Rev. Mod. Phys.* **74**, 145-195 (2002).

[3] Bennett, C.H., *et al.,* "Quantum Cryptography: Public key distribution and coin tossing," Proceedings of the Int. Conf. on Computers, Systems & Signal Processing, Bangalore, India, Dec. 10-12, 175-179 (1984).

[4] Weisner, S., "Conguate coding," *Sigact news* **15:1**, 78-88 (1983).

[5] Ekert, A., "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**, 661-663 (1991).

[6] Rogers, D., *et al.*, "Detector dead-time effects and paralyzability in high-speed quantum key distribution," *New J. Phys.* **9**, 319 (2007).

[7] Xu, H., *et al.*, "1310-nm quantum key distribution system with up-conversion pump wavelength at 1550 nm," *Optics Express* **15**, 7247-7260 (2007).

[8] Bienfang, J.C., *et al.*, "Quantum key distribution with 1.25 Gbps clock synchronization," *Optics Express* **12**, 2011 (2004).

[9] Nakassis, A., *et al.*, "Expeditious reconciliation for practical quantum key distribution," Quantum Information and Computation II, Proc. SPIE **5436** (2004).

An incomplete list of attacks on realistic quantum key distribution:

Scarani, V., *et al.*, "Quantum cryptography with finite resources: Unconditional security bound for discrete variable protocols with one-way post-processing," *Phys. Rev. Lett.* **100**, 200501 (2008).

Gottesman, D., *et al.*, "Security of quantum key distribution with imperfect devices," *Quant. Inf. and Computation* **4**, 325-360 (2004).

Lo, H. K., *et al.*, "Decoy state quantum key distribution," *Phys. Rev. Lett.* 94, 230504 (2005).

An incomplete list of side-channel attacks on realistic quantum key distribution systems:

Kurtsiefer, C., *et al.*, "The breakdown flash of silicon avalanche photodiodes – backdoor for eavesdropper attacks," *J. Mod. Opt.* **48**, 2039-2047 (2001).

Lamas-Linares, A., *et al.*, "Breaking a quantum key distribution system through a timing side channel," *Optics Express* **15**, 9388-9393 (2007).

Vakhitov, A., *et al.*, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," *J. Mod. Opt.* **48**, 2023-2038 (2001).

Some other attacks on quantum key distribution systems:

Makarov, V., *et al.*, "Faked states attack on quantum cryptosystems" *J. Mod. Opt.* **52**, 691–705 (2005).

Cederlof, J., *et al.*, "Security aspects of the authentication used in quantum cryptography," *IEEE Trans. Inf. Theory* **54**, 1735-1741 (2008).