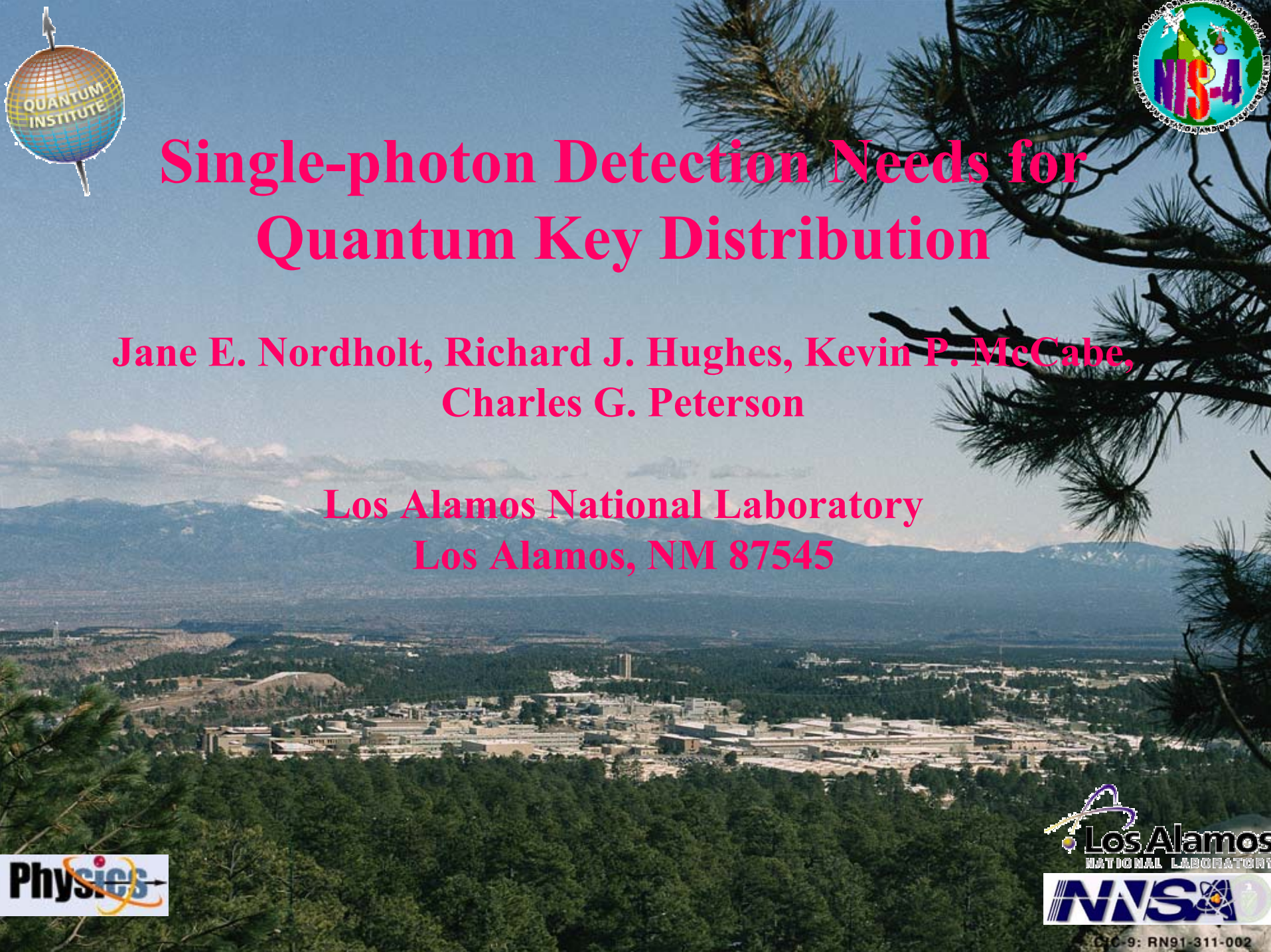
LA-UR-03-2507

Title: SINGLE-PHOTON DETECTION NEEDS FOR QUANTUM KEY DISTRIBUTION

Author(s):
Jane E. Nordholt, 104482, P-21
Richard J. Hughes, 100883, P-21
Charles G. Peterson, 106982, P-21
Kevin P. McCabe, 086754, NIS-4

Submitted to: Workshop on Single-Photon: Detectors, Applications, and Measurement Methods



Single-photon Detection Needs for Quantum Key Distribution

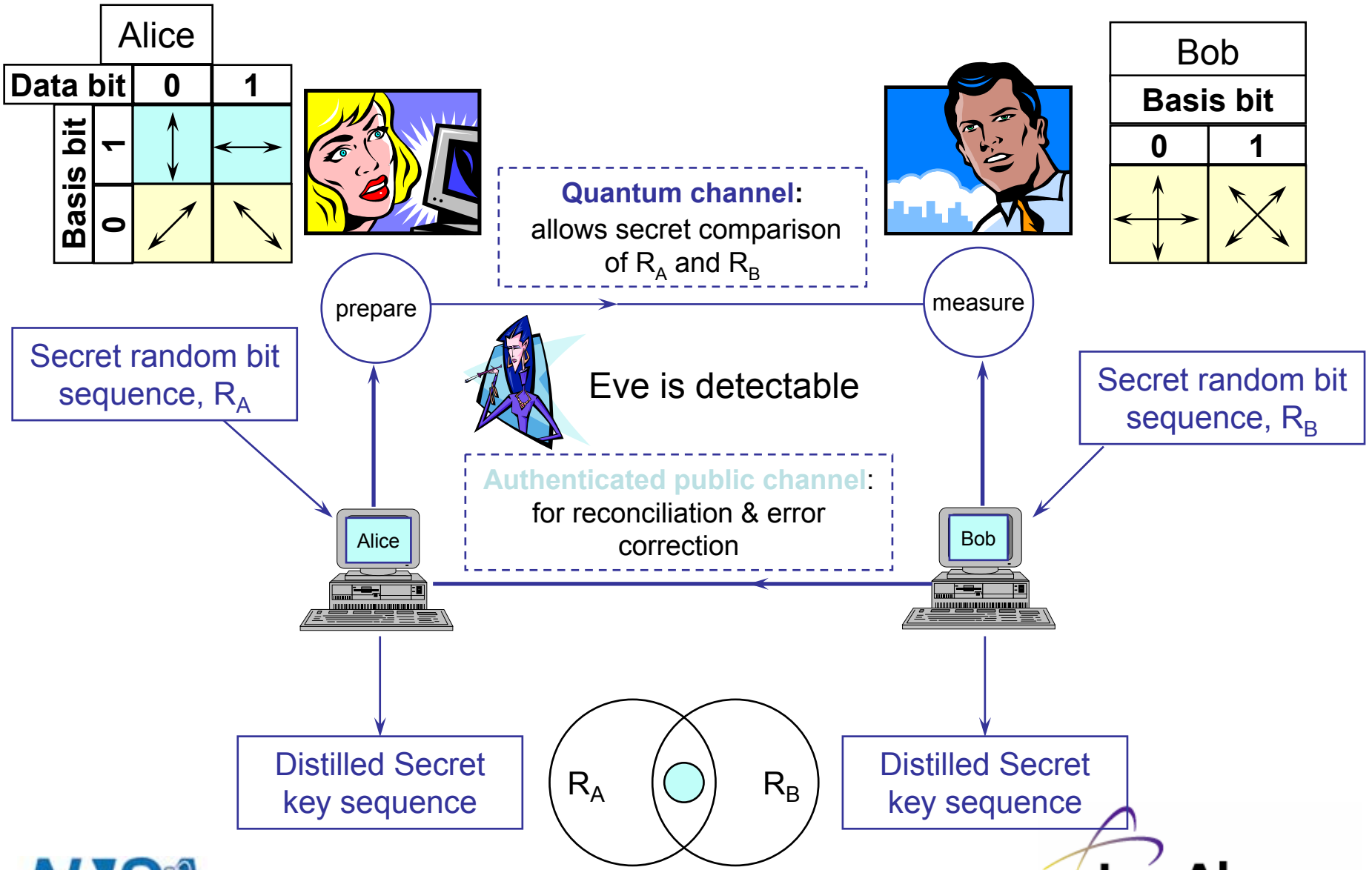
Jane E. Nordholt, Richard J. Hughes, Kevin P. McCabe,
Charles G. Peterson

Los Alamos National Laboratory
Los Alamos, NM 87545

CIC-9: RN91-311-002

Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

BB84 Quantum Key Distribution (QKD) Protocol

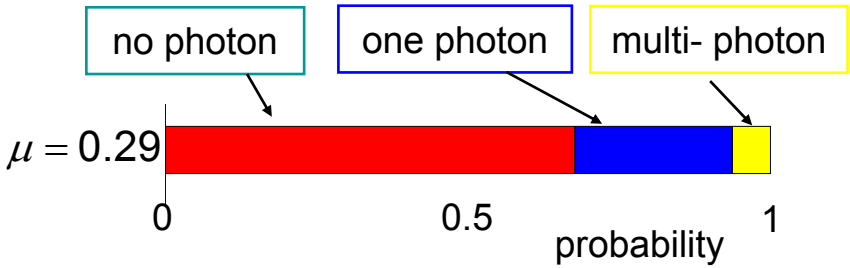


Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

"Realistic Security": BBBSS91 Privacy Amplification

From Sifted Bits to Secret Bits

cf. Bennett et al. (1991)



- Assume eve identifies all multi-photon signals
- Attribute all errors to intercept/resend on single-photon signals
- Eve gains error correction information

privacy amplification

- Eve's collision entropy per bit is

$$R \approx 1 - \mu - 4\varepsilon \log_2 1.5 + 1.19\left[\varepsilon \log_2 \varepsilon + (1-\varepsilon)\log_2 (1-\varepsilon)\right]$$

- Alice and Bob extract ~ R secret bits/sifted bit by universal hashing
  - Random Boolean matrix
- No secrecy in certain parts of parameter space
  - Optimal choice of μ

NNSA

Los Alamos

Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

Secrecy efficiency: ideal system

secrecy efficiency = transmission & detection x protocol efficiency x error correction x privacy amplification

secret bits per initial bit

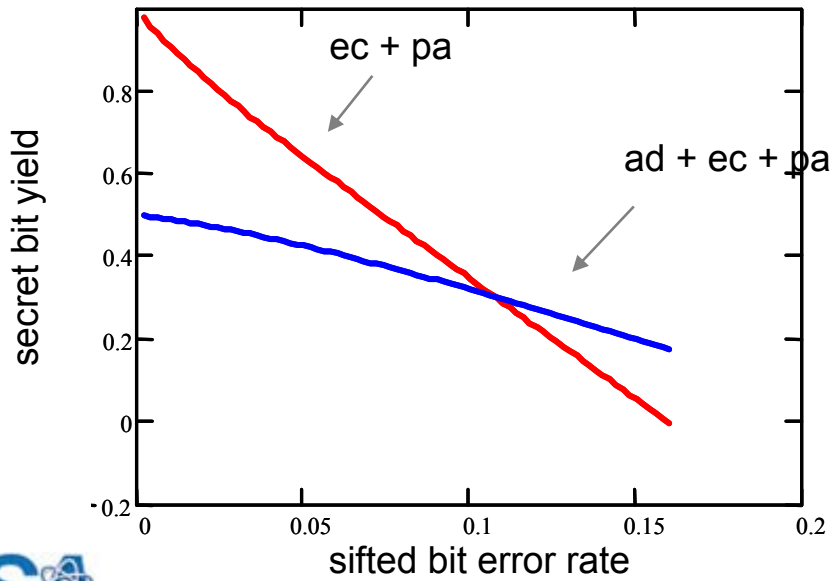
physics
introduce errors

physics

information theory
reveals side information

information theory
collision entropy – side information

secrecy efficiency after error correction and privacy amplification against intercept/resend



QKD may not be possible EVEN IF photons can be transmitted and detected

NNSA

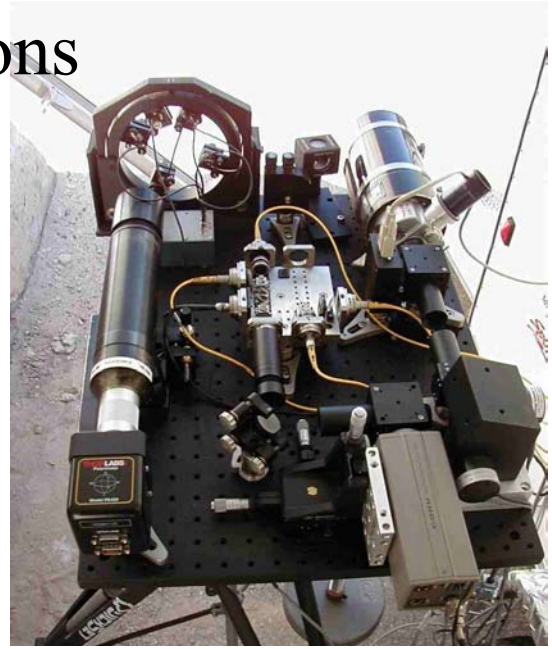
Los Alamos

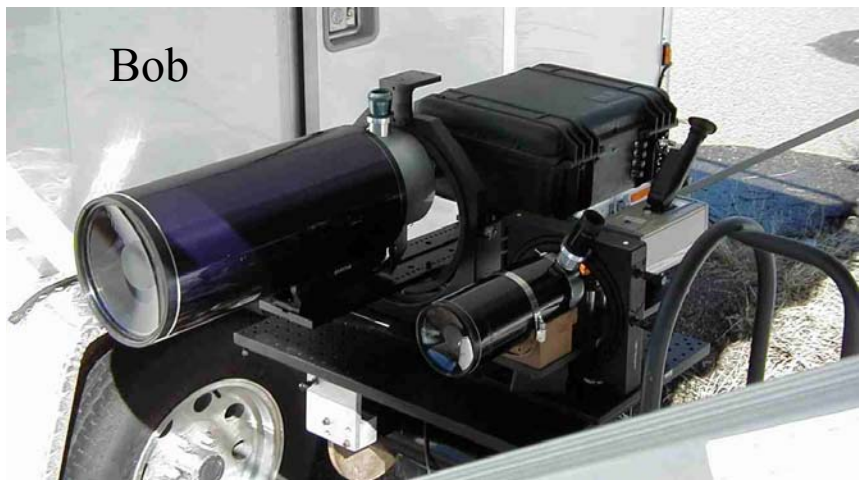
Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

QKD System Requirements Dictate Desired Detector Specifications

- Spatial filtering
  - Prefer size independent detector performance—many different applications
  - Want uniform QE across detector face
- Spectral filtering
  - Wavelength selectivity not now an intrinsic part of detectors
  - Would enable higher level of integration and possible co-existence with laser comm
- Time-domain filtering
  - Time resolution of ≤10ps
  - Pulse-pair resolution of ≤100ps (high rep rate, low deadtime)
  - Gateable
- High QE

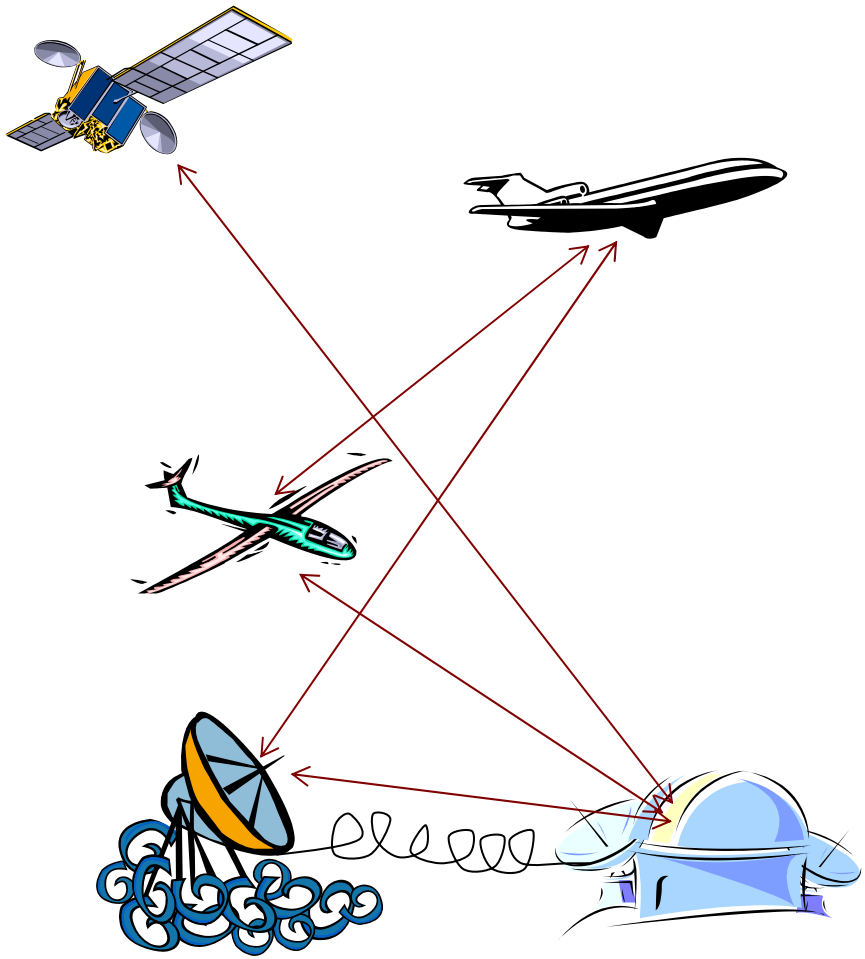
Alice



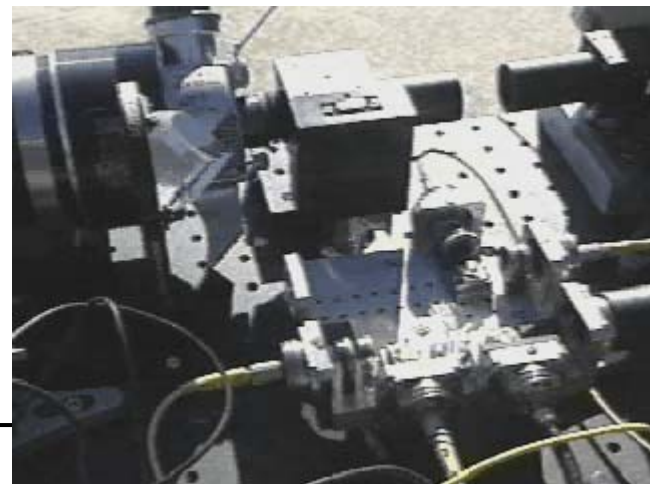


Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

Other Desired Detector Properties



- Security
  - –Multiple photon detection
- Low noise
  - –No dark counts or background
  - –No afterpulsing
- Convenience properties
  - –Polarization selectability
  - –No cryogens required
  - –Portability
  - –Radiation hardened
  - –Flyable
  - –Cheap

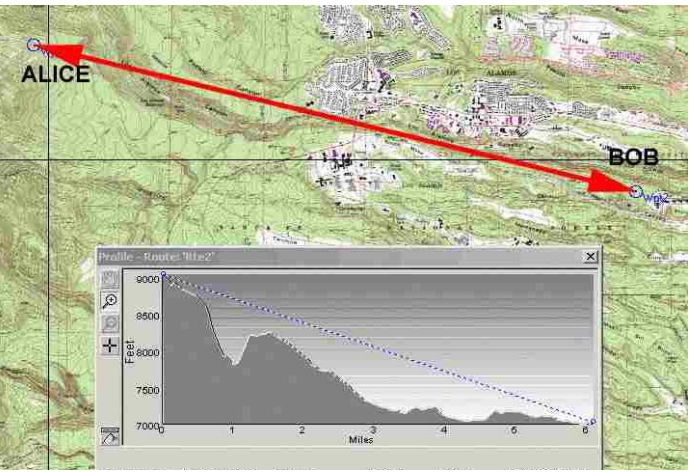


Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

Free-space Quantum Key Distribution

Richard Hughes, Jane Nordholt, Derek Derkacs and Charles Peterson

Pajarito Mountain Ski Area



From Pajarito Mtn., Los Alamos, NM to TA53, Los Alamos National Laboratory

Sample of key material at 10-km range (day)

one-airmass path: comparable optics to satellite-to-ground

A: 01110001 01111010 00100001 01100100 10100110
B: 01110001 01111010 00100001 01100100 10100110

A: 11100010 00111101 10011111 10000111 11001111
B: 11100010 00111101 10011111 10000111 11001111

R&D 100

- Key transferred by 772-nm single-photon communications
- 1-mhz sending rate; ~600-hz key rate
- Day: 45,576 secret bits/hour ; night: 113,273 secret bits/45 mins

UAS

SNF

NNSA

Los Alamos

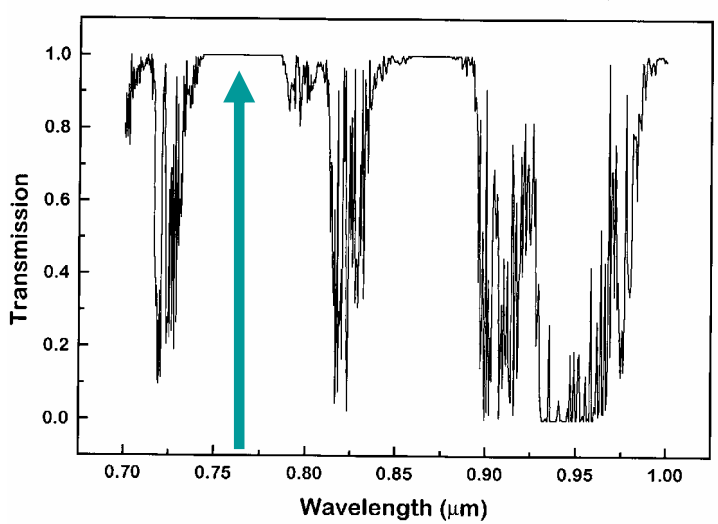
Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

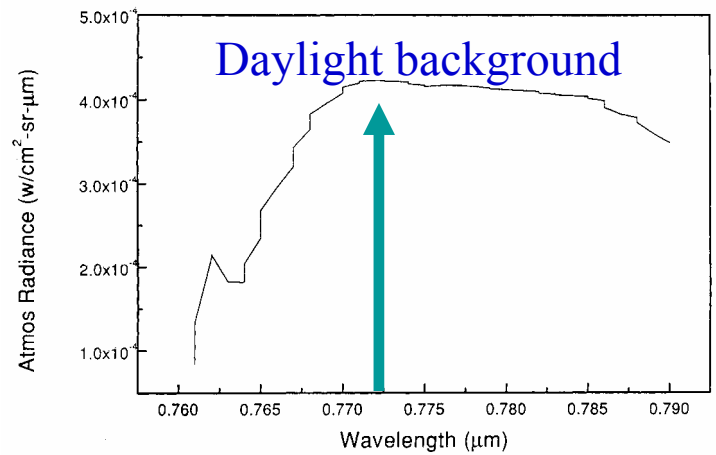
The Atmospheric QKD Quantum Channel

Low-loss Transmission Wavelength; High-efficiency Detectors

- Secrecy efficiency as a function of wavelength:
  - Proc SPIE 4635, 116 (2002)
- ~ 770 nm is optimal for QKD through the atmosphere
  - Single-photon detection with Si APDs
- Challenges
  - Background photons
  - Daylight radiance ~ 10^{13} photons s^{-1} cm^{-2} $Å^{-1}$ str^{-1}
    - ~ 10^{-7} photons $mode^{-1}$ ~40,000 modes
    - Temporal filtering: ~1 ns
    - Spectral filtering: 0.1 nm
    - Spatial filtering: 220-μrad FOV
  - Day/night ~ 10^6
  - Synchronization and timing
  - Atmospheric optics
    - Not birefringent; Intermittency: ~ 0.01-s

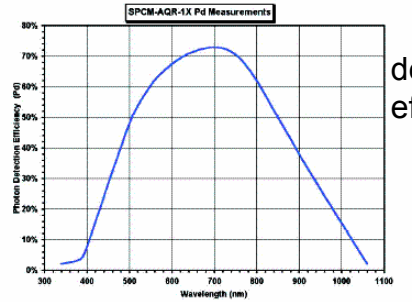
Atmospheric transmission vs. wavelength





Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

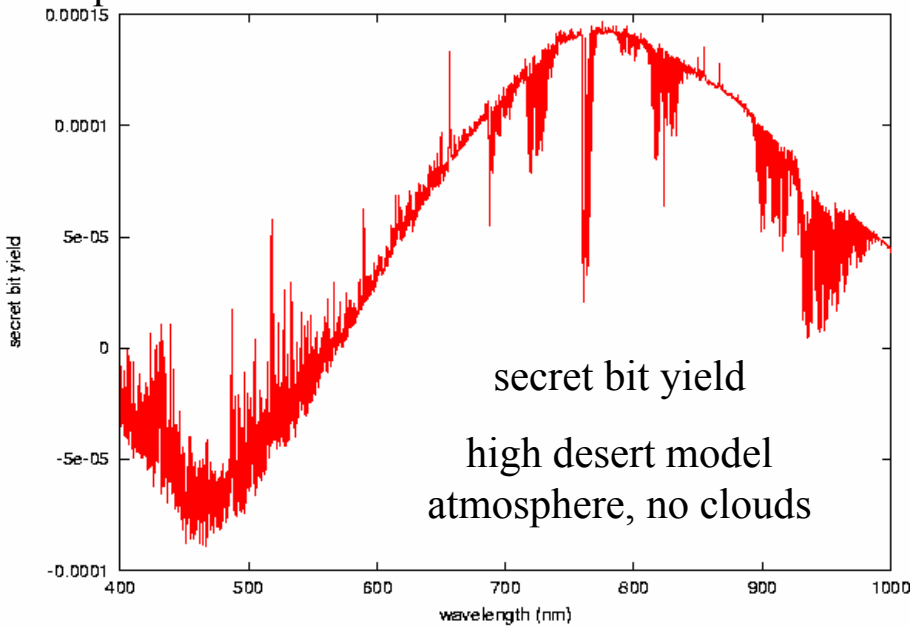
QKD Satellite Downlink in Daylight: Si APD Detectors

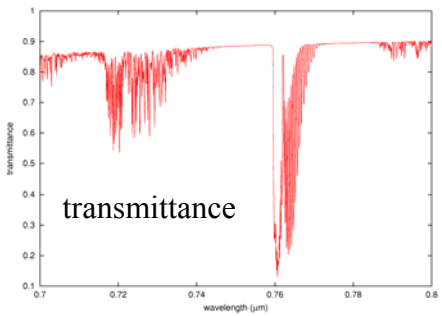


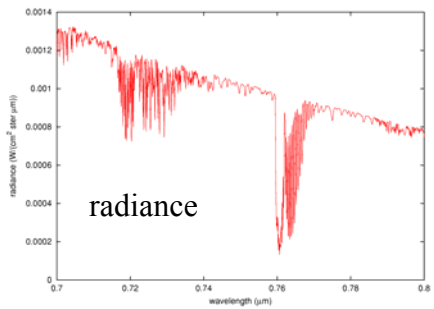
detection efficiency

Optimum wavelength ~ 770 nm

Optimum bit rate ~ 1 kHz at 10 MHz transmit rate







- 700-km altitude orbit
- Ground station at Los Alamos
  - 45° elevation, 180° azimuth
  - 50-cm receive aperture
  - 1% geometric capture
  - 40-μrad FOV, 0.1-nm filter, 1-ns coincidence window
- 0.5 photons per pulse
  - Protects against USD attack
    - Accessible loss = atmosphere
  - BBBSS privacy amplification

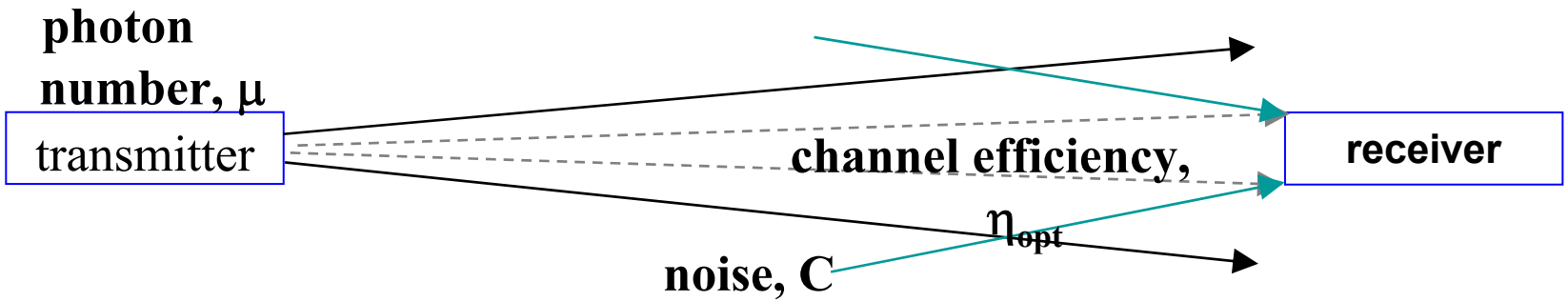
Nordholt, Jane E., Richard J. Hughes, George L. Morgan, Charles G. Peterson, Christopher C. Wipf, "Present and Future Free-Space Quantum Key Distribution," *Free-Space Laser Communication Technologies XIV*, G. Stephen Mecherle, Editor, Proceedings of SPIE Vol. 4635 (2002), pp 115-126 .

NASA

Los Alamos

Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

Scaling Laws for Secrecy Efficiency



- # sifted bits ~ $\mu\ \eta_{opt}$
- sifted BER, $\varepsilon \sim C/\ \mu\ \eta_{opt}$

secrecy efficiency = transmission & detection x protocol efficiency x error correction x privacy amplification

physics: introduce errors

physics

information theory: reveals side information

information theory: collision entropy – side information

secret bits per initial bit

$$R \approx 1-\mu-4\varepsilon\log_2 1.5+1.19\left[\varepsilon\log_2\varepsilon+(1-\varepsilon)\log_2(1-\varepsilon)\right]$$

- **Secret bits/sifted bit is a function of μ, η/c ONLY**
- **Can scale to other ranges/wavelengths/instrumental conditions**

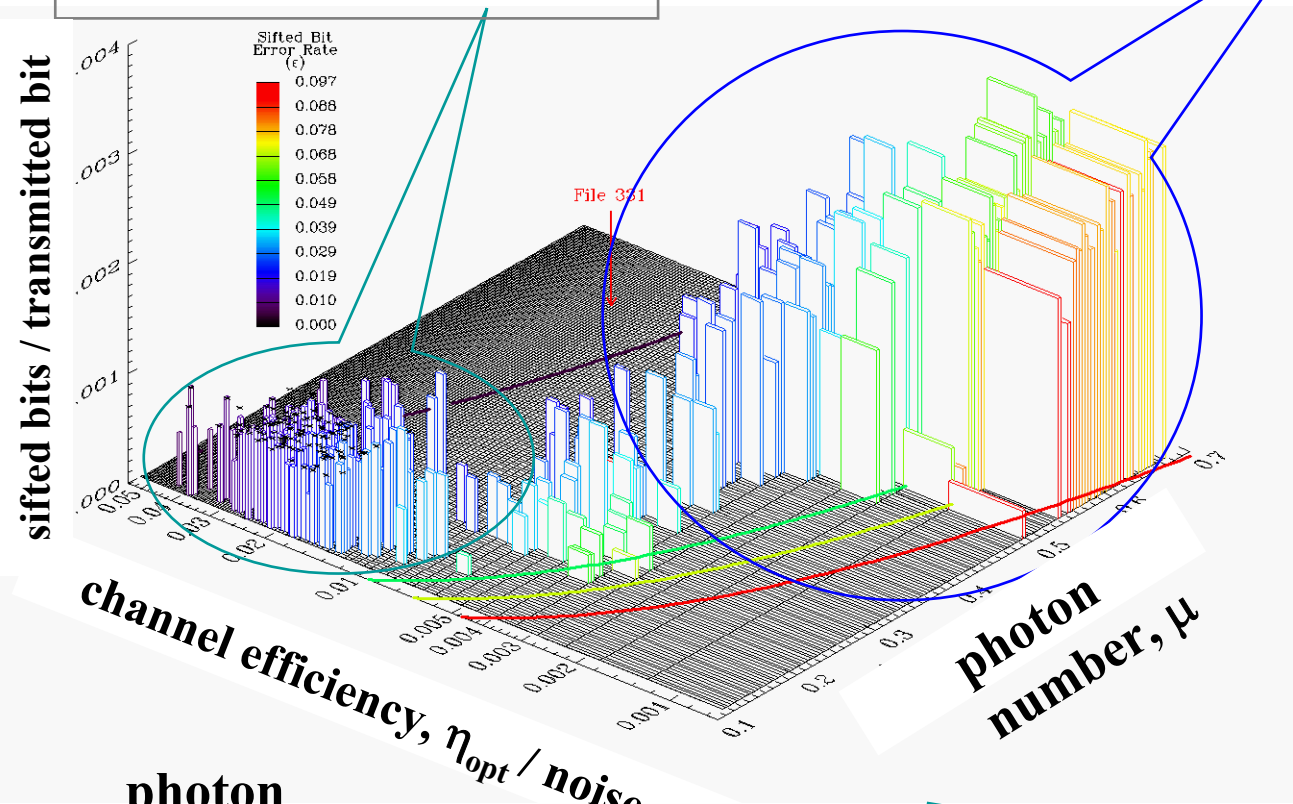
NNSA Los Alamos

Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

10-km Sifted Key Data: 4 October, 2001

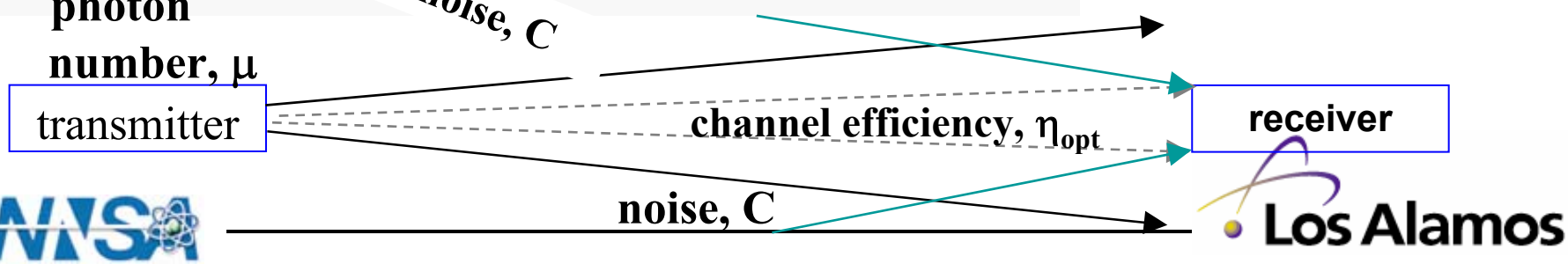
night: 18:45 to 19:29 MST
- 192,925 sifted bits
- noise, C ~ 1-2 s^{-1}
  - detector dark counts

daylight: 17:42 to 18:44 MST
- 394,004 sifted bits
- noise, C < 50 s^{-1}
  - background
    ~ 2 mW cm^{-2} μm^{-1} str^{-1}



Hughes, Richard J; Nordholt, Jane E; Derkacs, Derek; Peterson, Charles G, "Practical Free-Space Quantum Key Distribution Over 10 Km In Daylight And At Night", *New Journal of Physics*, Volume: 4, Issue: 1 July 01, 2002, pp. 43-43, URL: stacks.iop.org/1367-2630/4/43 .

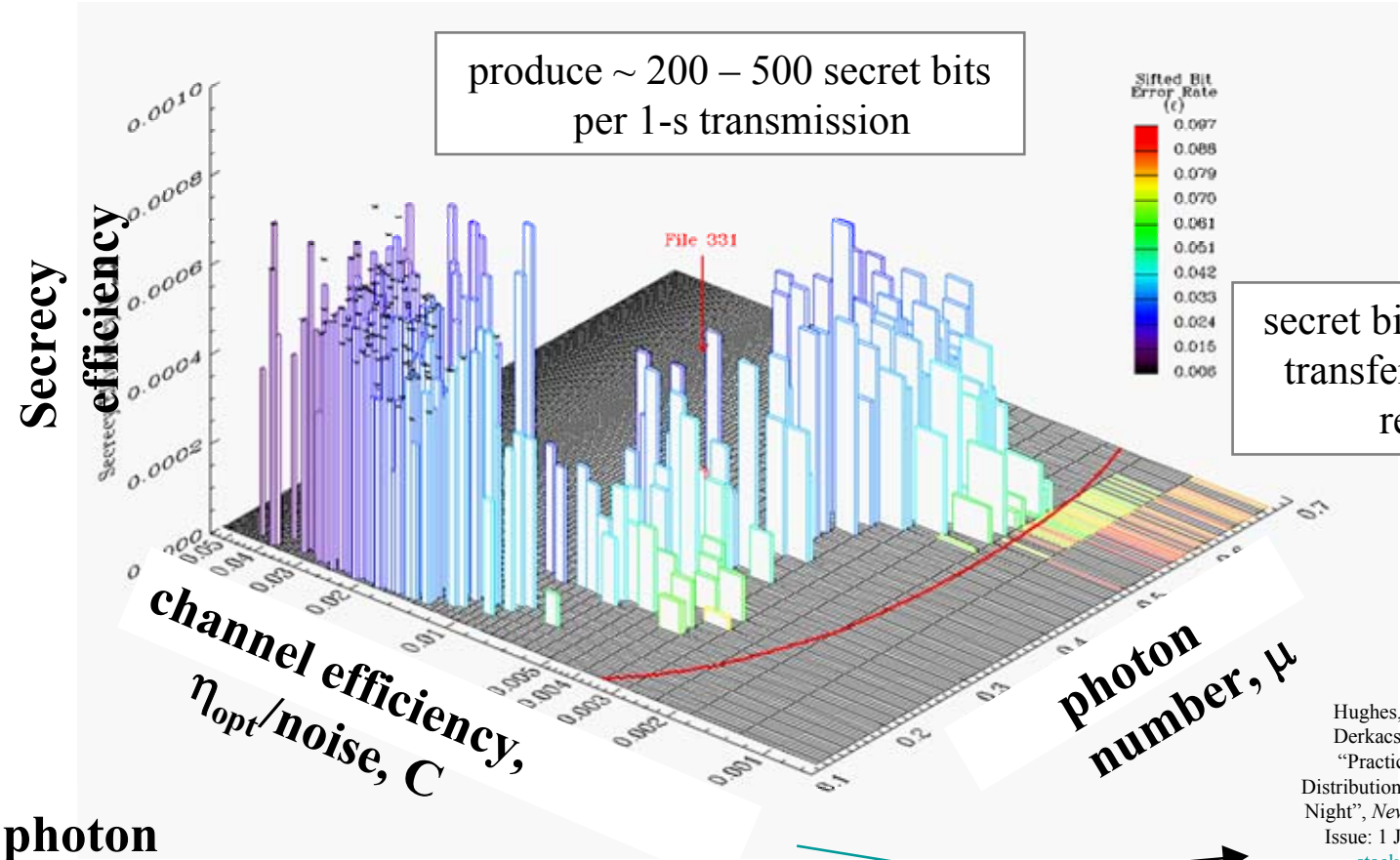
- # sifted bits ~ μ η_{opt}
- sifted BER, ε ~ C/ μ η_{opt}



Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

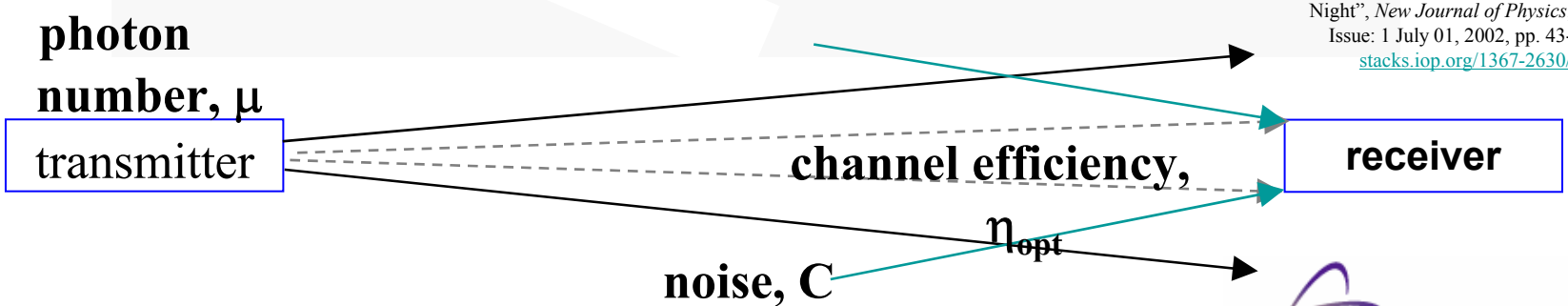
10-km Secrecy Efficiency: 4 October, 2001 (Secret Bits Per Transmitted Bit)

produce ~ 200 – 500 secret bits per 1-s transmission



secret bits cannot be transferred in some regimes

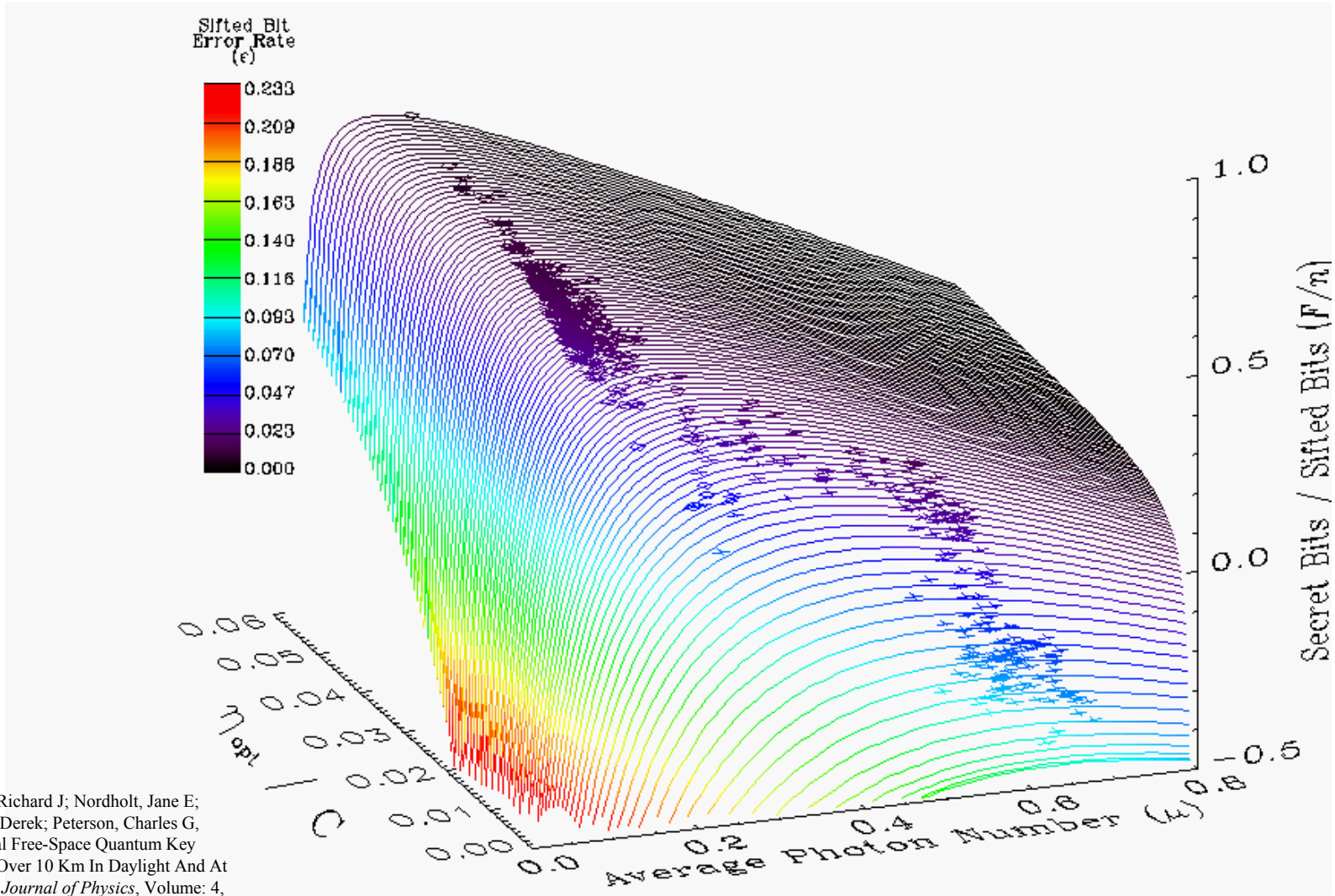
Hughes, Richard J; Nordholt, Jane E; Derkacs, Derek; Peterson, Charles G, "Practical Free-Space Quantum Key Distribution Over 10 Km In Daylight And At Night", *New Journal of Physics*, Volume: 4, Issue: 1 July 01, 2002, pp. 43-43, URL: stacks.iop.org/1367-2630/4/43 .



max ground-to-ground range (this system): 30 km (day); 45 km (night)

Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

Background Count Rate, C, Critical to Bit Yield



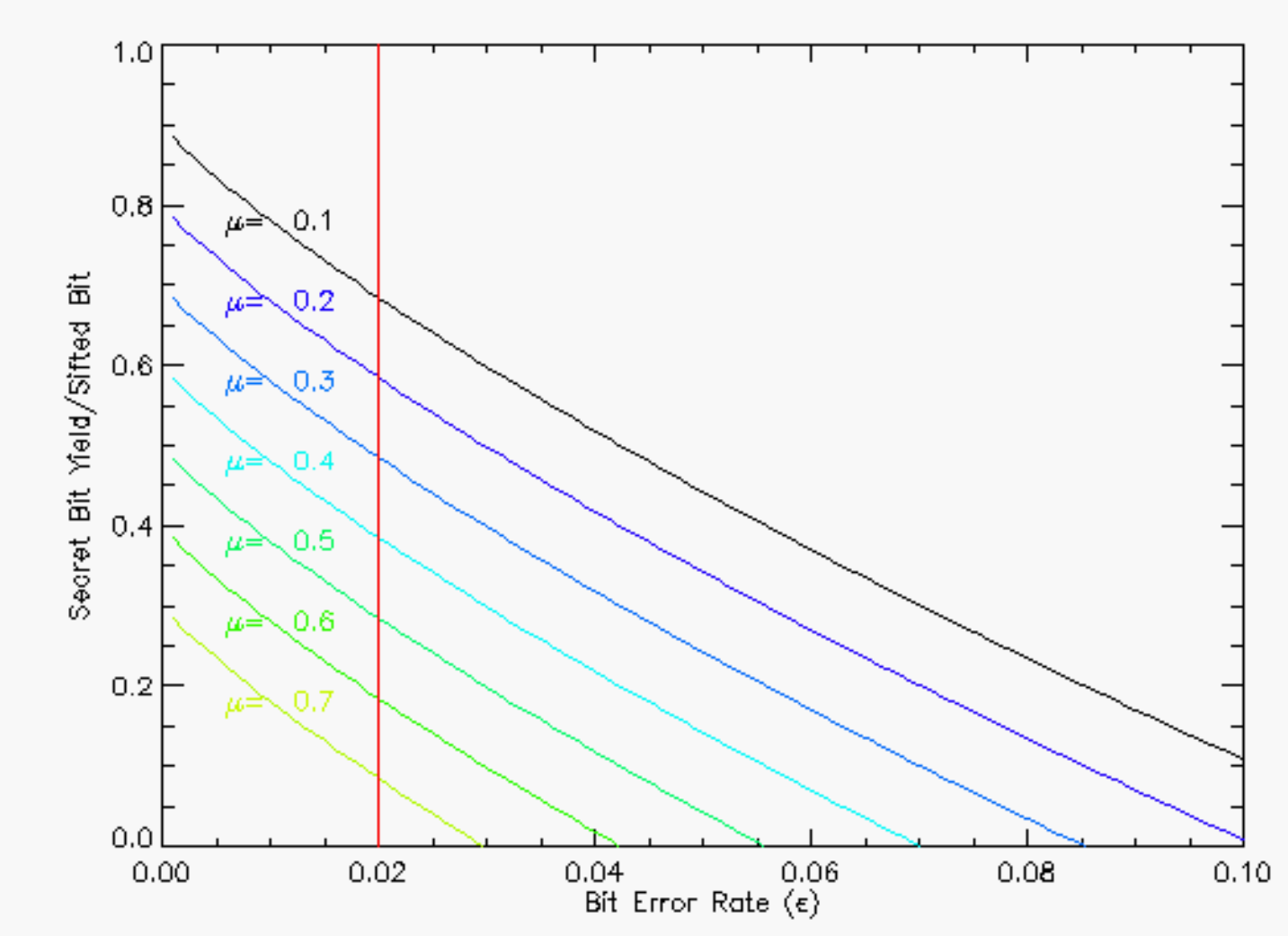
Hughes, Richard J; Nordholt, Jane E; Derkacs, Derek; Peterson, Charles G, "Practical Free-Space Quantum Key Distribution Over 10 Km In Daylight And At Night", *New Journal of Physics*, Volume: 4, Issue: 1 July 01, 2002, pp. 43-43, URL: stacks.iop.org/1367-2630/4/43 .

NNSA

Los Alamos

Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

Error Rate Is Proportional to Dark-Count Rate



Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

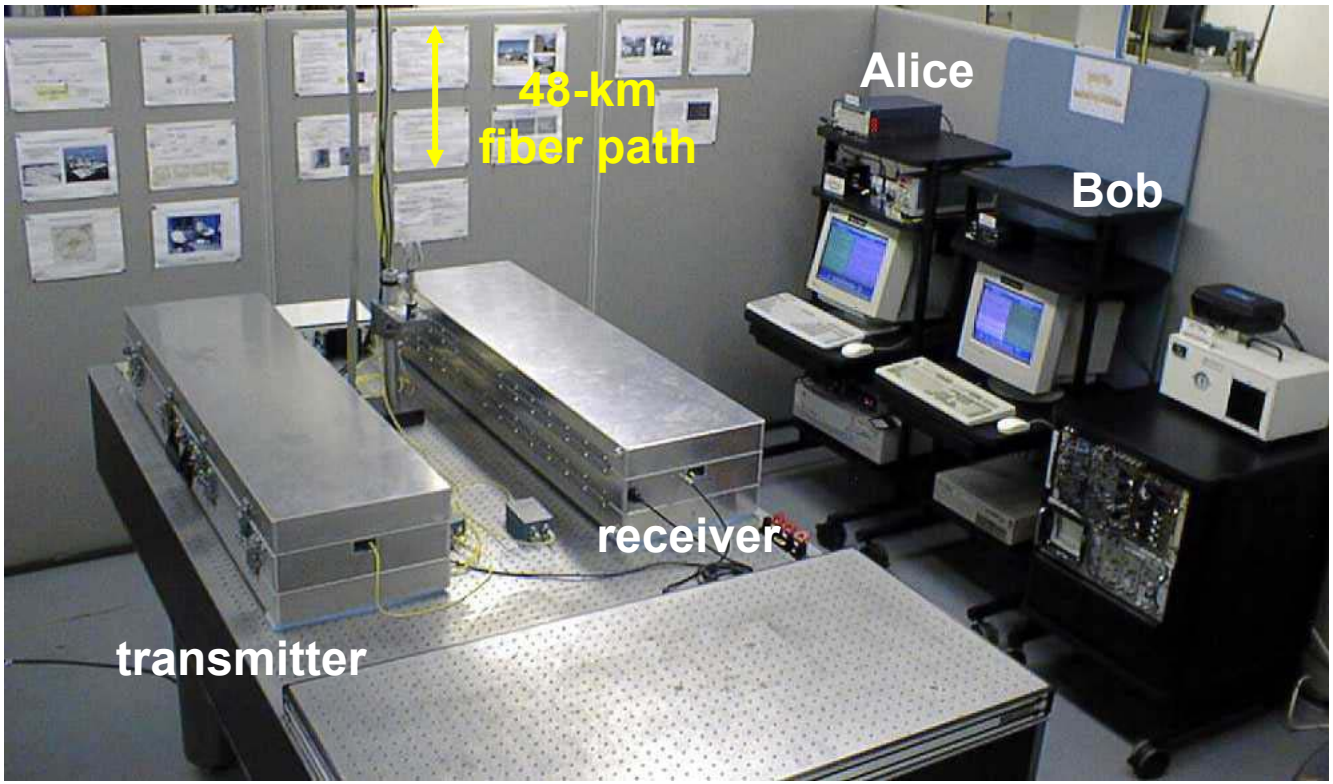
Single-photon Light Sources and Detectors

- Significantly higher secret bit yields possible with "single-photon" light sources
- But, for daylight operation need:
  - (1>) intensity > 0.2
  - Bandwidth ~ 0.1 nm
  - Time ~ 1 ns

- Improved single-photon detectors will increase the bit rate, range and security of QKD
- In optical fiber at telecom wavelengths (1,310 and 1,550 nm), present day detectors are the range-limiting element

Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

Los Alamos 48-km Optical Fiber Quantum Key Distribution Experiment

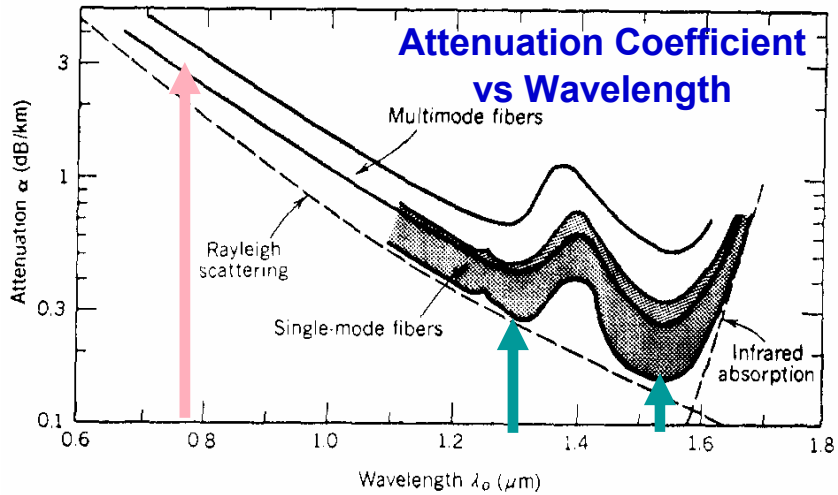


Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

The QKD Quantum Channel

Low-loss Transmission Medium; High-efficiency Detectors

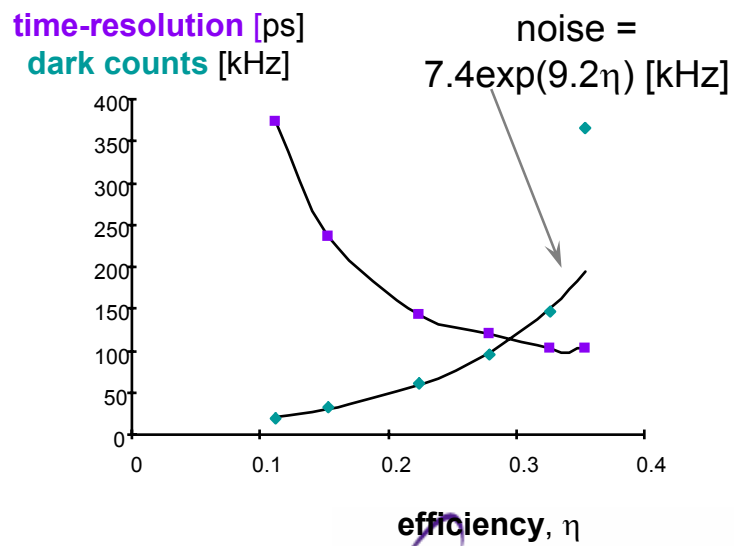
- **Optical fiber**
  - QKD over telecommunications fiber networks ?
  - **Challenges:** single-photon detection at 1.3 μm, (1.55 μm)



- (Ge), InGaAs APDs
  - Rarity et al., Cova et al., Gisin et al., Morgan et al.

E.G. InGaAs APDs (Fujitsu)

- Cooled to 140 K
- Detection efficiency, time-resolution and noise **increase** with over-voltage
- 20% efficiency, 50 **k**Hz noise
- **High noise rate can be offset by sub-ns time-resolution**

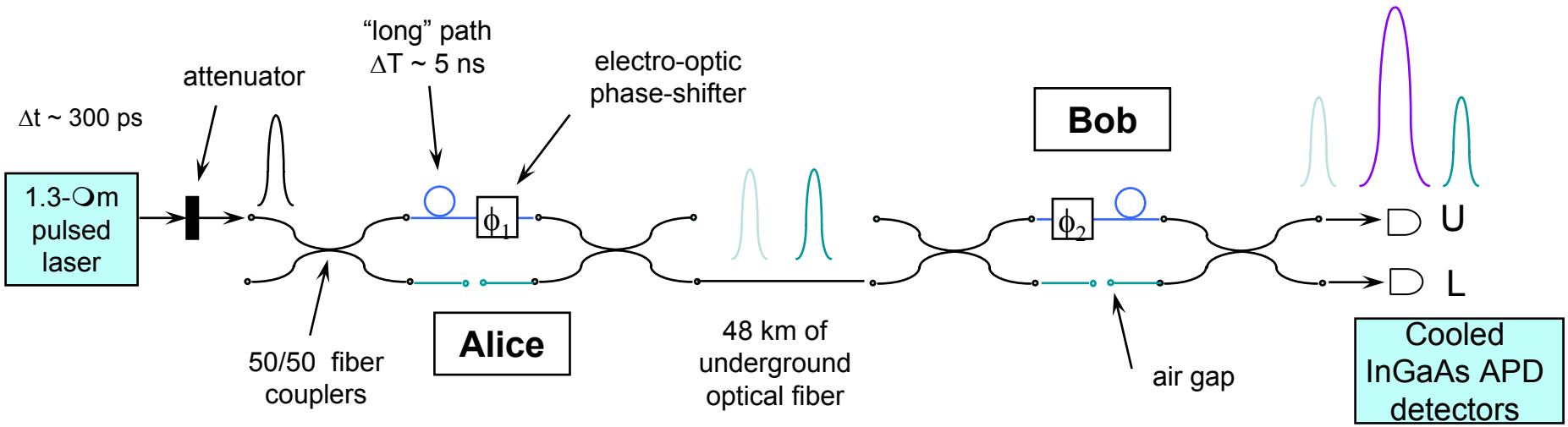


NNSA

Los Alamos

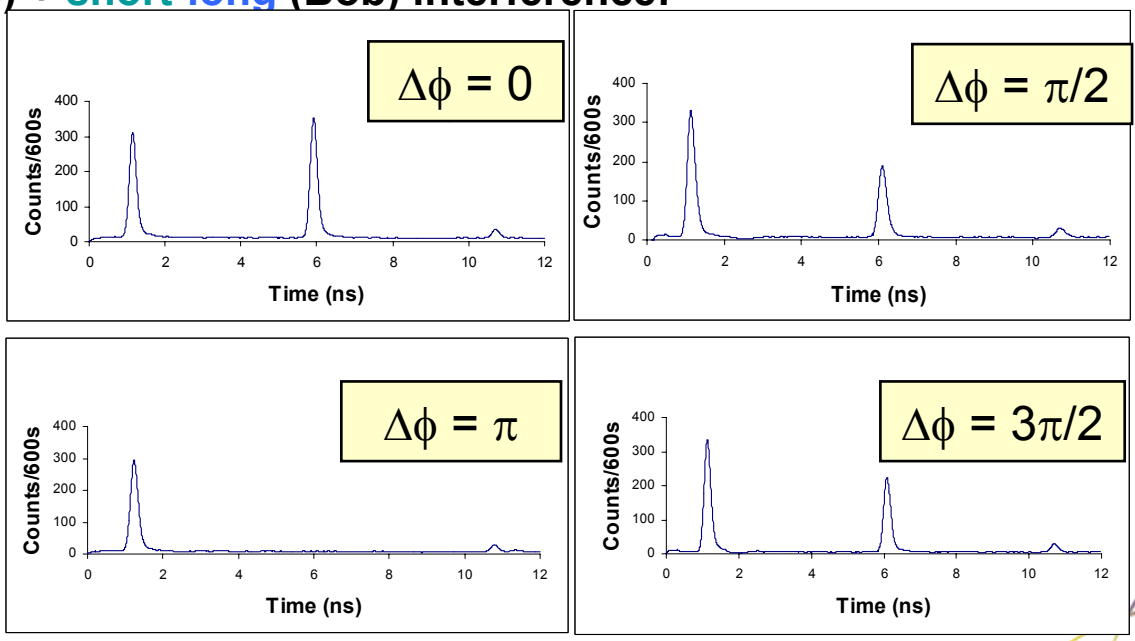
Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

QKD Using Single-photon Interference



long-short (Alice) + short-long (Bob) interference:

- "U" detector
- η ~ 11%
- μ ~ 0.63
- 98.99±1.24% visibility
- 100kHz sending rate
- 22.9 dB loss



NNSA

Los Alamos

Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

(Dark) Fiber QKD Secrecy Efficiency at 10km: Dependence on Detection Efficiency and Dark Noise

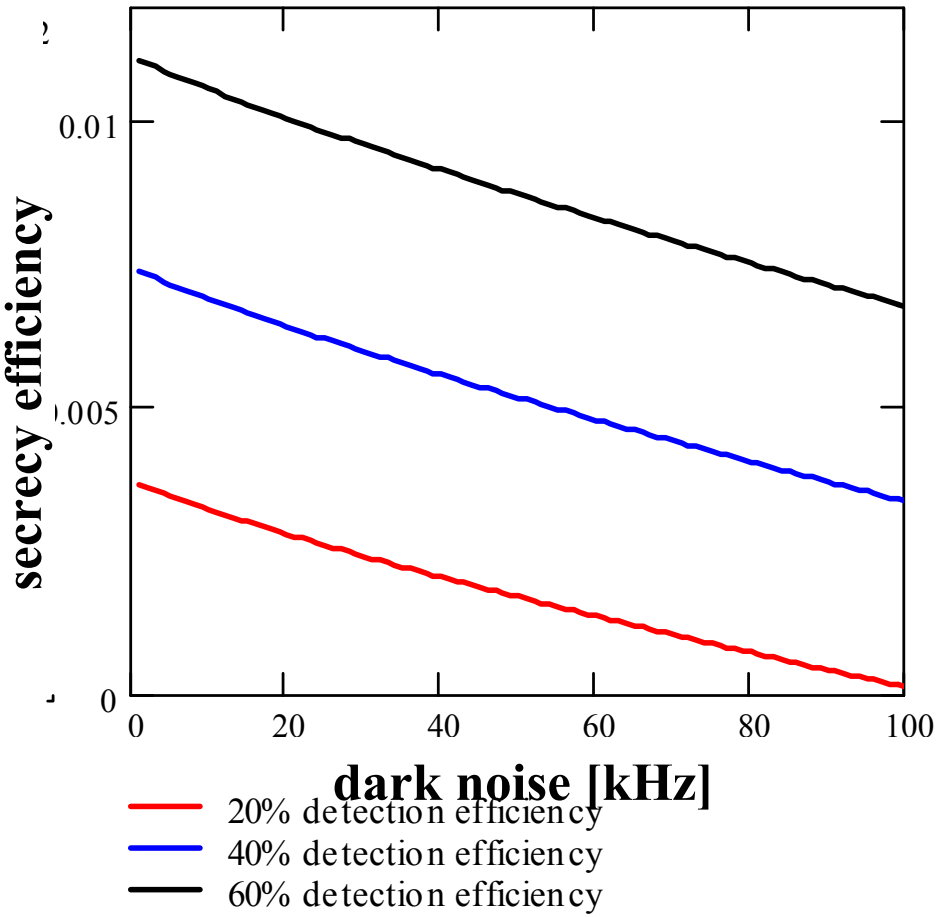
Assumptions:

- Photon number, $\mu = 0.5$
- 30% receiver optical efficiency
- Bisective-search error correction
- BBBSS91 privacy amplification
- 3db fiber attenuation

Caveats:

- X (clock rate) to get secret bits s^{-1}

x100 reduction in dark noise ~ x2 increase in detection efficiency



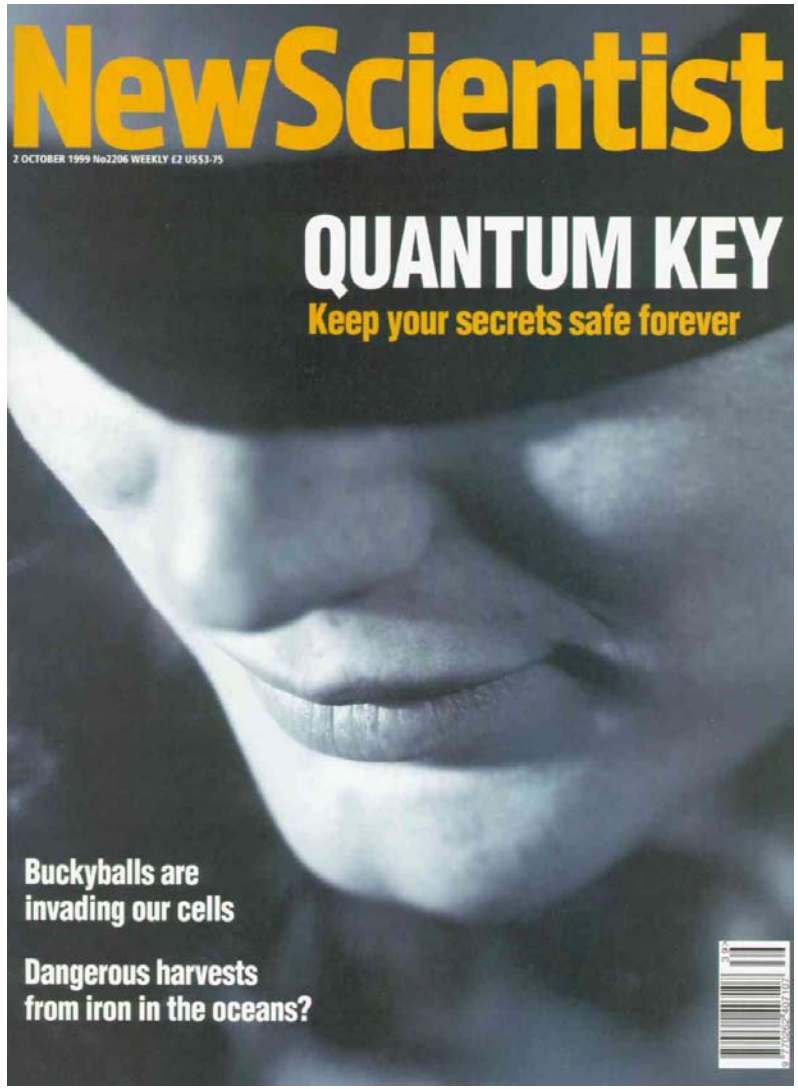
NNSA

Los Alamos

Jane E. Nordholt
Physics Division, LANL
(505) 667-3897
JNordholt@LANL.gov

Summary and Conclusions

- QKD secrecy, transmission rate, and distance can all be improved with improvements in single photon detectors
- Single photon detectors are often the limiting factor in QKD systems
- New detectors will make QKD a more viable technology than it already is



NNSA

Los Alamos