21 Years of Quantum Key Distribution

Richard Hughes

Physics Division

Los Alamos National Laboratory

- **retrospective on QKD**
- **going farther, faster with stronger security**
- **prospects for QKD in all-optical networks**
- **caveats:**
  - weak laser QKD
  - in optical fiber
  - somewhat LANL-centric

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

21 Years of Quantum Key Distribution

Richard Hughes
Physics Division
Los Alamos National Laboratory

ABSTRACT

I will review the history of and background to Quantum Key Distribution, starting from Bennett and Brassard's invention in 1984, and up to recent developments. I will describe some new results from QKD in dedicated ("dark") optical fiber using transition edge sensor (TES) photo-detectors, including new maximum transmission distance records and the implementation of a decoy-state protocol over 100km. I will conclude by describing some progress in making QKD compatible with all-optical fiber networks, including the co-existence of weak QKD signals with conventional optical data on the same fiber.

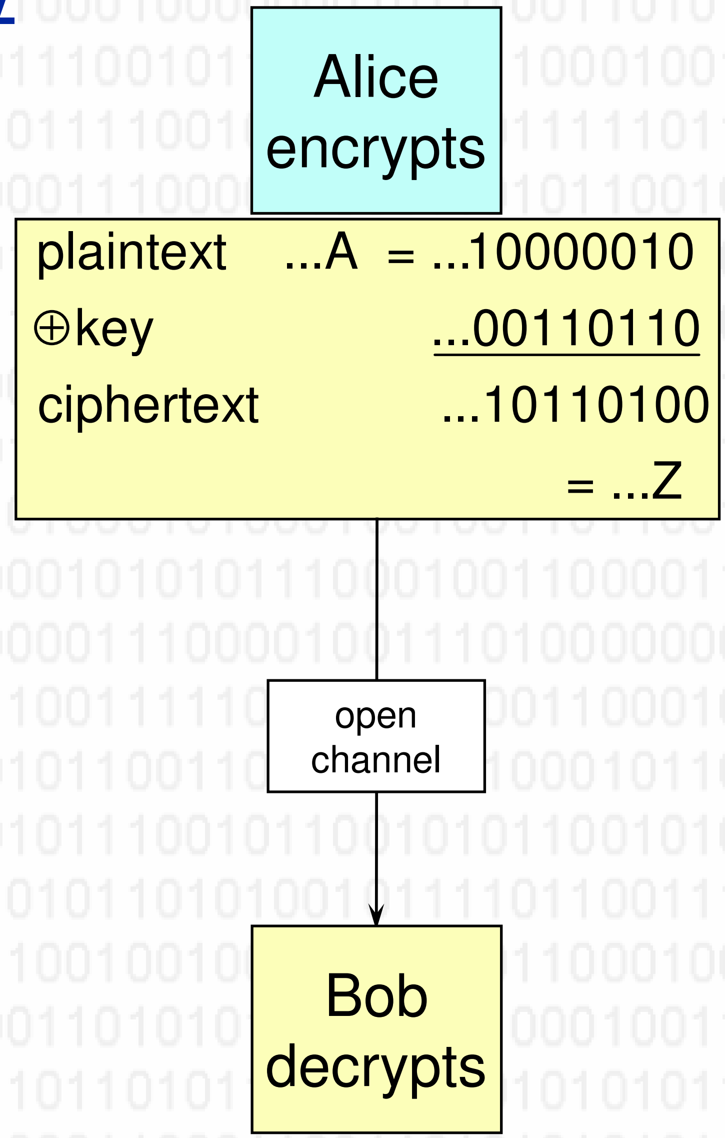
The power of shared, secret random bits (I): confidentiality

Communication Theory of Secrecy Systems*

By C. E. SHANNON

(1949)

- **confidentiality: the "one-time pad"**
  - **unconditionally secure against known ciphertext attacks**
  - but, subject to
    - manipulation,
    - chosen-plaintext attacks



Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

The power of shared, secret random bits (II): authentication

"On the Internet, nobody knows you're a dog."

New Hash Functions and Their Use in Authentication and Set Equality

MARK N. WEGMAN AND J. LAWRENCE CARTER

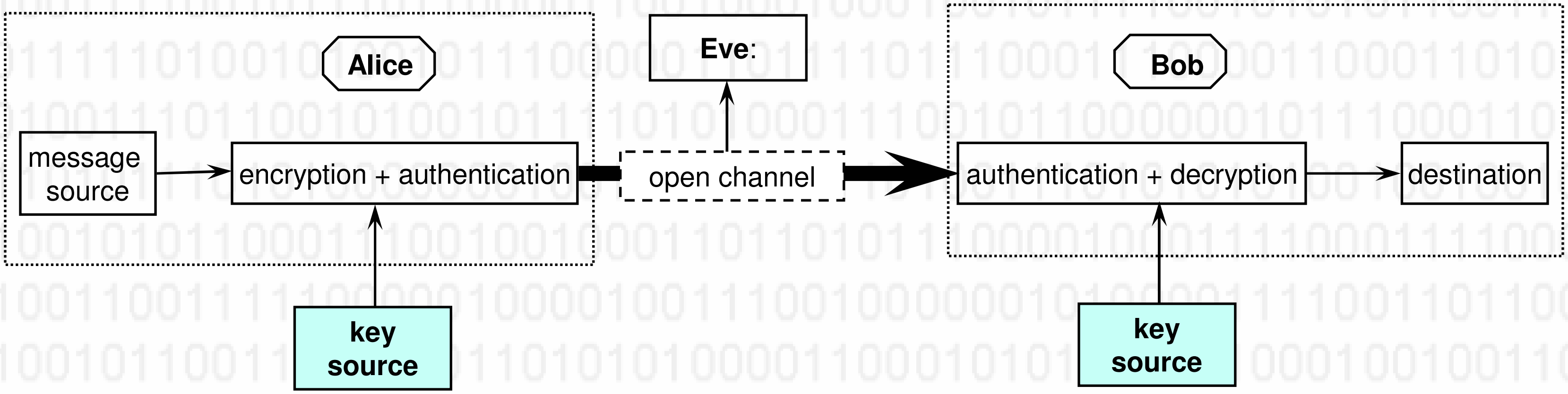
(1981)

- **authenticity: strongly univeral$_2$ hash functions**
  - not secret, but …
  - **unconditional security against impersonation and/or substitution**

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Los Alamos NATIONAL LABORATORY

The power of shared, secret random bits (III): the unconditionally secure channel



- **confidentiality + authenticity = secure channel**

- **<u>BUT</u> (pre-QKD): how to accomplish <u>unconditionally secure key distribution</u> ?**
  - courier ?
  - public key is “computationally secure”

- **QKD to the rescue ...**

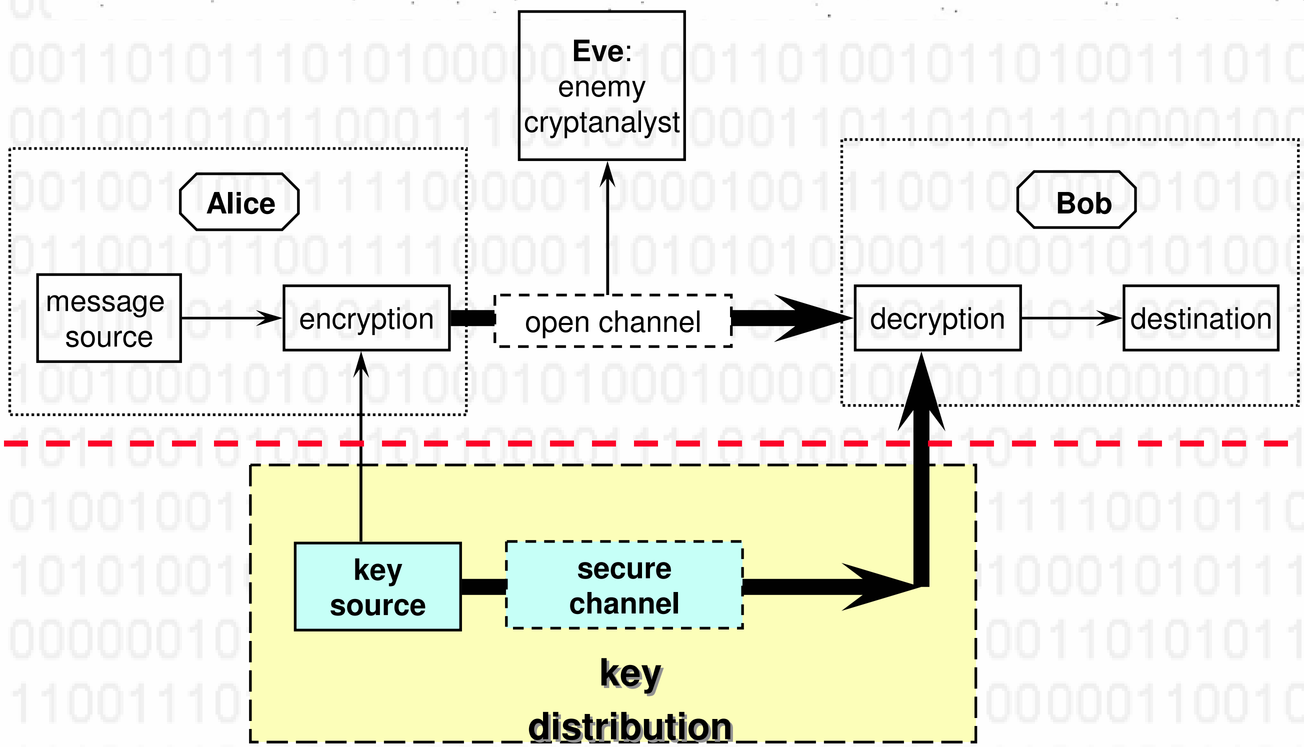
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Quantum Key Distribution was invented 21 years ago:

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

International Conference on Computers, Systems & Signal Processing Bangalore, India December 10-12, 1984



"When elementary quantum systems … are used to transmit digital information the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media."

- **on-demand key transfer by quantum communications: detectability and defeat of eavesdropping ensured by laws of physics & information theory**

Today: Spectacular basic research results in QKD

implementations of entangled photon QKD

Free-Space distribution of entanglement and single photons over 144 km

PRL 94, 150501 (2005)

Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 km: Towards Satellite-Based Global Quantum Communication

Cheng-Zhi Peng,[1,2] Tao Yang,[1] Xiao-Hui Bao,[1] Jun Zhang,[1] Xian-Min Jin,[1] Fa-Yong Feng,[1] Bin Yang,[1] Jian Yang,[1]

Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fiber

rsity of Science and

ermany

Differential phase shift quantum key distribution experiment over 105 km fibre

H Takesue[1,3], E Diamanti[2,3], T Honjo[1], C Langrock[2], M M Fejer[2], K Inoue[1] and Y Yamamoto[1,2]

[1] NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato

iiversity, 450 Via Palou, Stanford,

ering

implementations of new QKD protocols in fiber

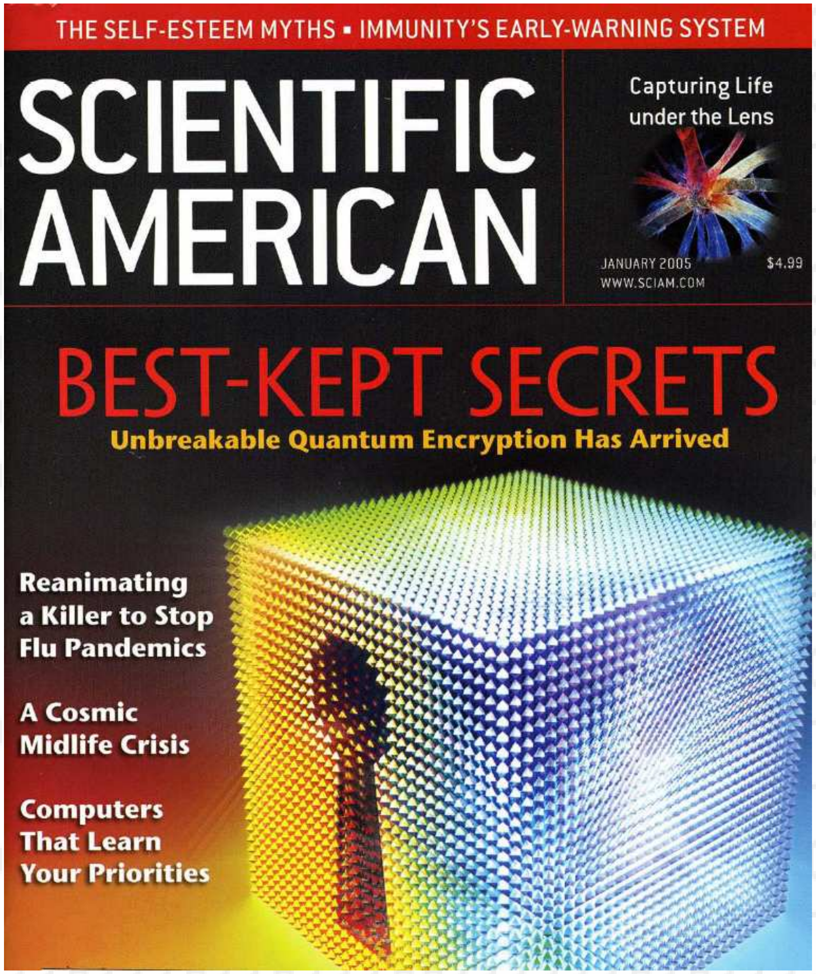
The Universal Composable Security of Quantum Key Distribution

Michael Ben-Or[1,4,5], Michal Horodecki[2,5], Debbie W. Leung[3,4,5], Dominic Mayers[3,4], and Jonathan Oppenheim[1,5,6]

new security proofs

Today: dark-fiber QKD is becoming commercially available ... in the US + Europe + Japan

first commercial (fiber) QKD systems: 2003



NEC extends quantum cryptography range and speed

System will go on sale in the second half of 2005

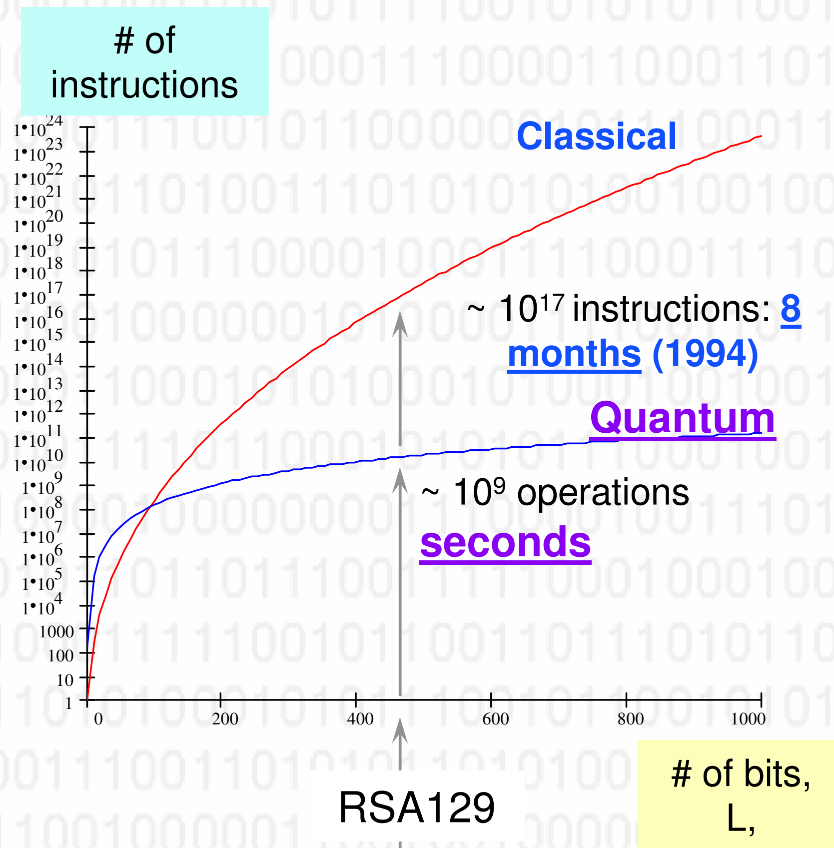
By Paul Kallender, IDG News Service

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Shor's Quantum Factoring Algorithm (1994):
Retroactive (In)security of Public Key Cryptography

Gartner Group Study: 2002
"Quantum Computers: The End of Public-Key Cryptography?"

"Although practical quantum computers are at least 10 years away, their potential will soon create distrust in current cryptographic methods. By 2006, new encryption methods will be needed for high-risk/high-value transactions."



3490529510		3276913299		1143816257578888676 6
8476509491		3266709549		9235779976146612010 2
4784961990	×	9619881908	=	1829672124236256256 1
3898133417		3446141317		8429357069352457338 9
7646384933		7642967992		7830597123563958705 0
8784399082		9425397982		5898907514759929002 6
0577		88533		879543541

Figure 1. Prime factors of the 129-digit number known as RSA-129.

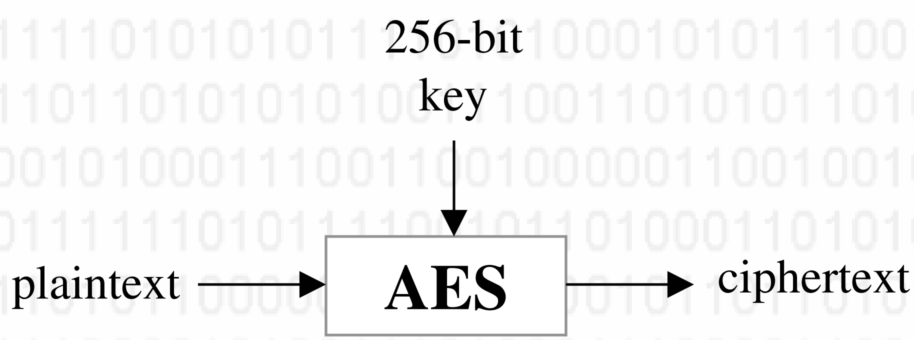
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Los Alamos NATIONAL LABORATORY

Practical security: private key for confidentiality / public key for key transfer

"if it's unconditionally secure, it probably isn't" (R. Anderson)

- **Alice and Bob use private key cryptography for encryption**
  - e.g. NIST's Advanced Encryption Standard, AES
  - must share a secret key, e.g., 256-bit key
- **Alice and Bob use "public key" cryptography to securely distribute their private keys**
  - e.g. RSA
  - security based on perceived difficulty of certain hard mathematical problems
    - factoring
- **a faith-based technology**



Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Skepticism

- "MagiQ Technologies is now selling an actual product that uses single photons to exchange keys over fiber optic lines. … I don't have any hope for this sort of product. I don't have any hope for the commercialization of quantum cryptography in general; I don't believe it solves any security problem that needs solving. I don't believe that it's worth paying for, and I can't imagine anyone but a few technophiles buying and deploying it. … it's not that quantum cryptography might be insecure; it's that we don't need cryptography to be any more secure.

- B. Schneier, Cryptogram Dec 15, 2003:
- http://www.schneier.com/crypto-gram-0312.html#6

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

QKD is evolving along dual tracks

unconditional security

classical information
secrecy & authentication
PROVIDED shared, secret keys exist

practical security

strong cryptography
supported by
key management

heritage

influx

QKD today

new security paradigm

capability enhancement ?

quantum information
unconditionally secure key distribution

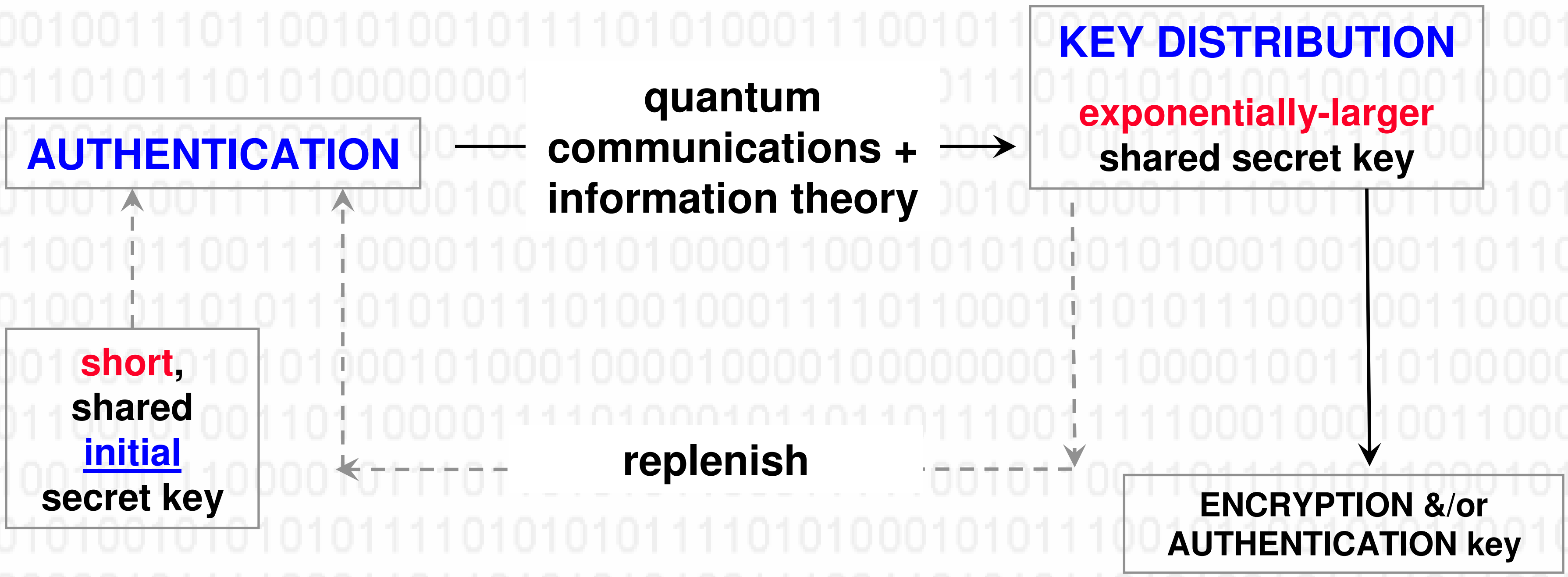
stronger, more flexible key management

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

c. f. C. Shannon (1949)

First core ingredient and foundation of QKD: authentication

- QKD bootstraps unconditionally secure, self-sustaining key distribution from (short-term) one-time authentication of public messages



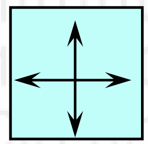
- can only be attacked with "today's technology"
- immune to future quantum computers
- detectability and defeat of eavesdropping

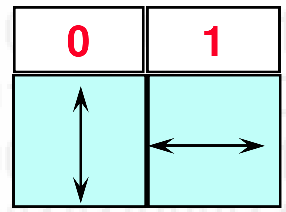
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Second core ingredient of QKD: "Conjugate coding"

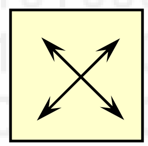
S. Wiesner, SIGACT News 15(1), 78 (1983)

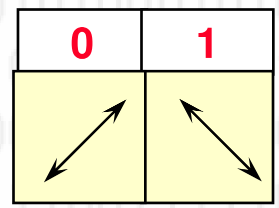
- a bit of information can be encoded in orthogonal polarization states of single photons, in different bases:
- e.g. in the rectilinear basis





- in the diagonal (45°) basis ("conjugate")





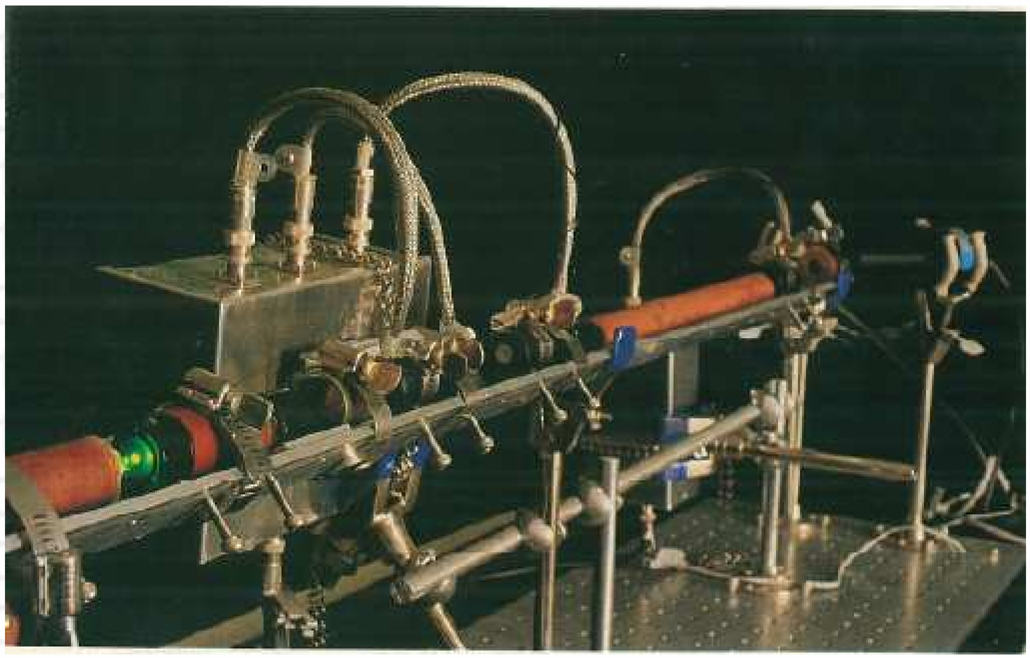
- the bit can be faithfully decoded if the encoding basis is known
- if the wrong decoding basis is used, the outcome is random

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

The BBBSS91 experiment

Experimental Quantum Cryptography

Charles H. Bennett — *IBM Research* *
François Bessette † — *Université de Montréal* ‡
Gilles Brassard § — *Université de Montréal* ‡
Louis Salvail — *Université de Montréal* ‡
John Smolin ¶ — *UCLA* **



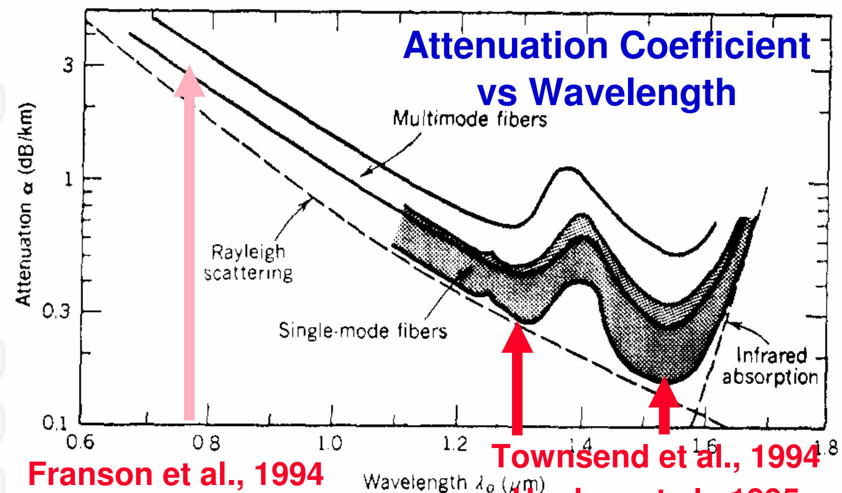
- **32-cm free-space transmission**
- **“unconditionally secure … provided Eve is deaf” (G. Brassard)**

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

1993-1996: the birth of long-distance QKD in optical fiber

QKD over telecommunications fiber networks ?

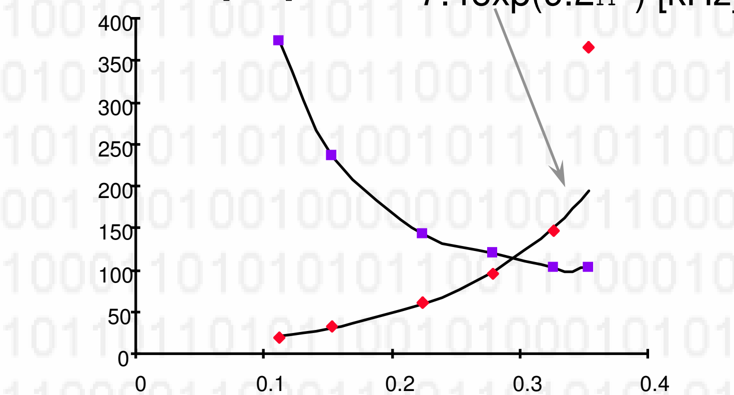
- **challenges:** single-photon detection at 1.3 μm, 1.55 μm



Photon counting with ns-gated InGaAs APDs

e.g. Morgan et al. (1997)

- cooled to 140 K
- low efficiency (< 20%), high noise (50 **k**Hz)
- **high noise rate offset by sub-ns time-resolution**



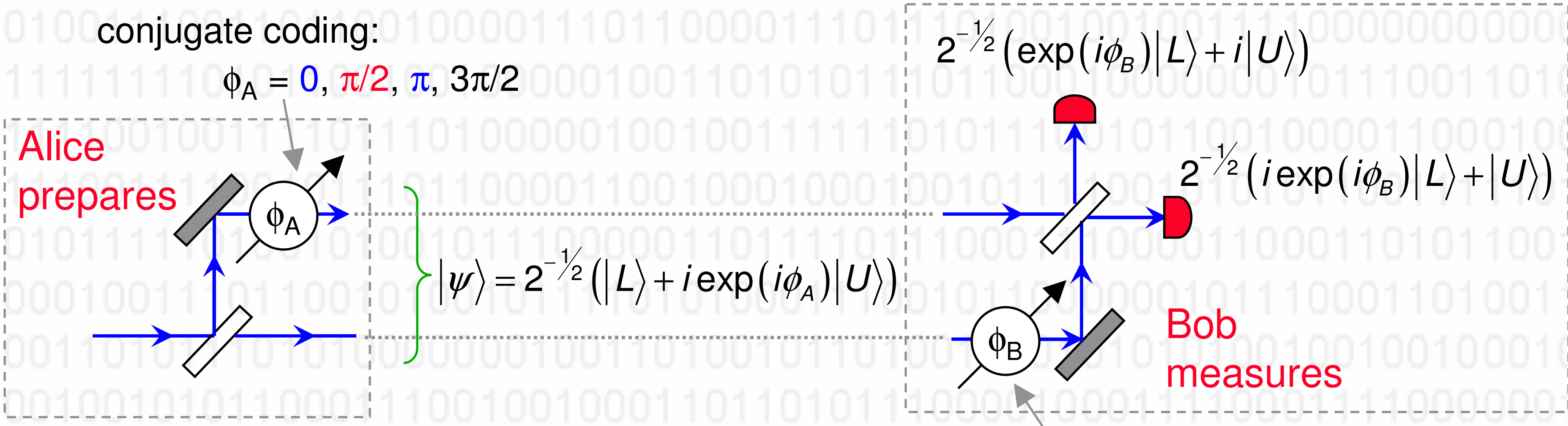
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Los Alamos
NATIONAL LABORATORY

Interferometric implementation of BB84 QKD in fiber

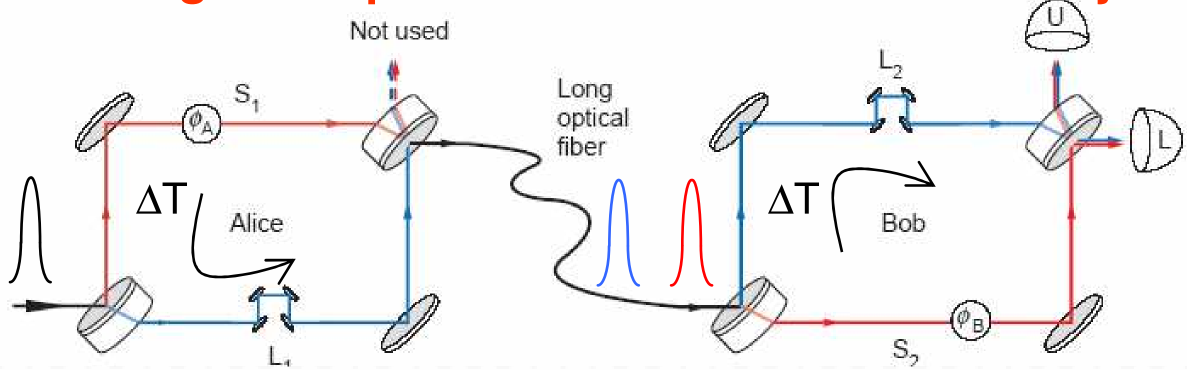
conjugate coding:

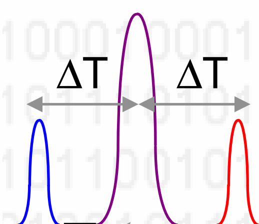
$\phi_A = 0, \pi/2, \pi, 3\pi/2$



basis selection: $\phi_B = 0, \pi/2$

Practical design multiplexes onto one fiber for stability:





C. Bennett (1992)

Sub-ns APD timing resolution allows discrimination of central (long-short + short-long) time bin for QKD

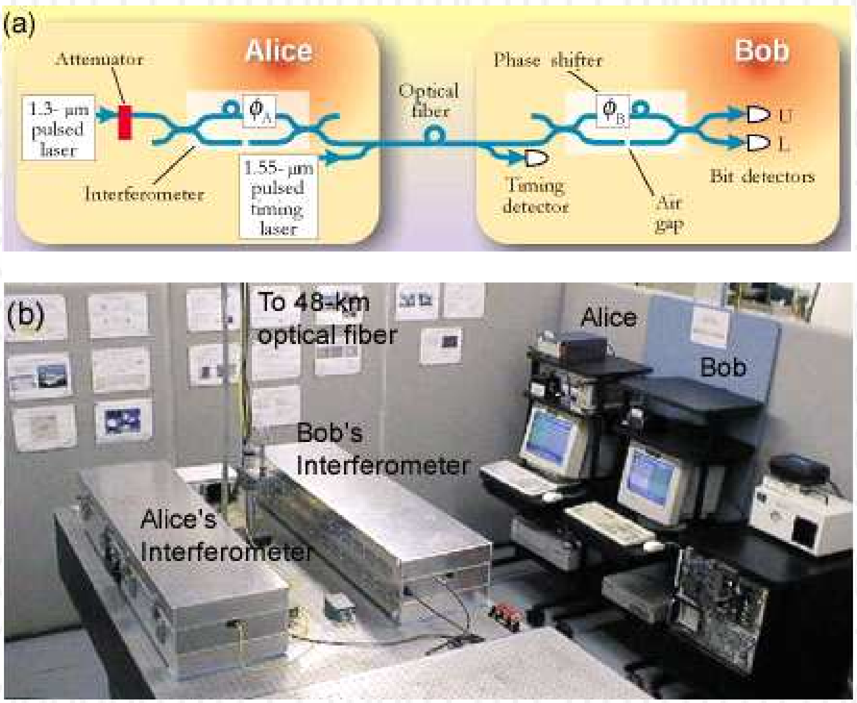
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

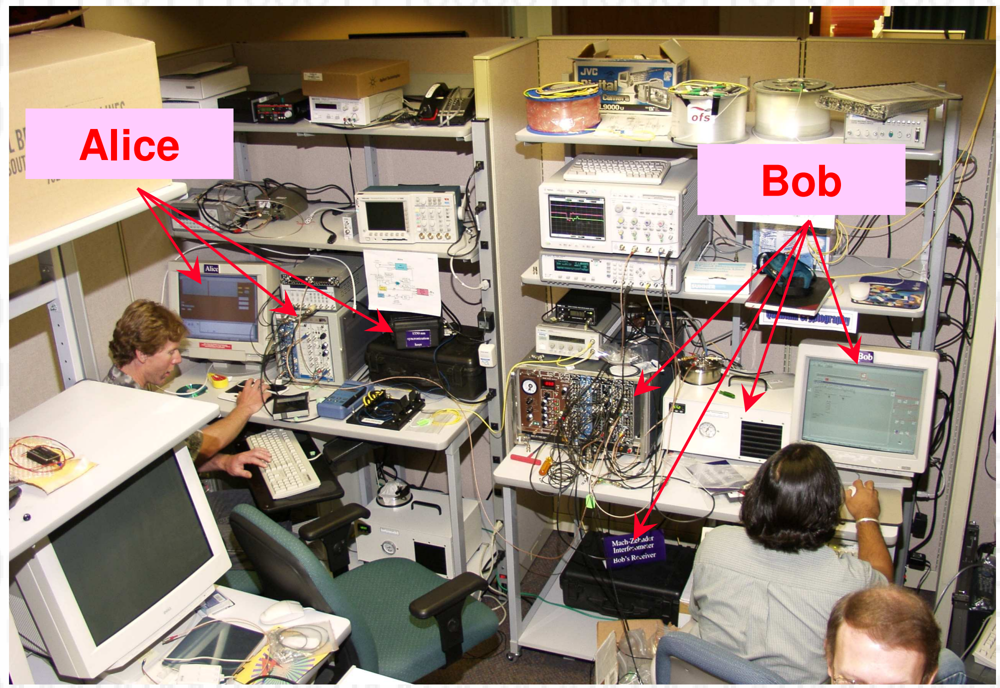
1st & 2nd generation LANL fiber QKD systems designed for dark fiber

Journal of Modern Optics 47, 533 (2000) – One Way QKD Systems

F1QKD (@ LANL > ‘95)

F2QKD (LANL > ‘96; MD > ‘02)





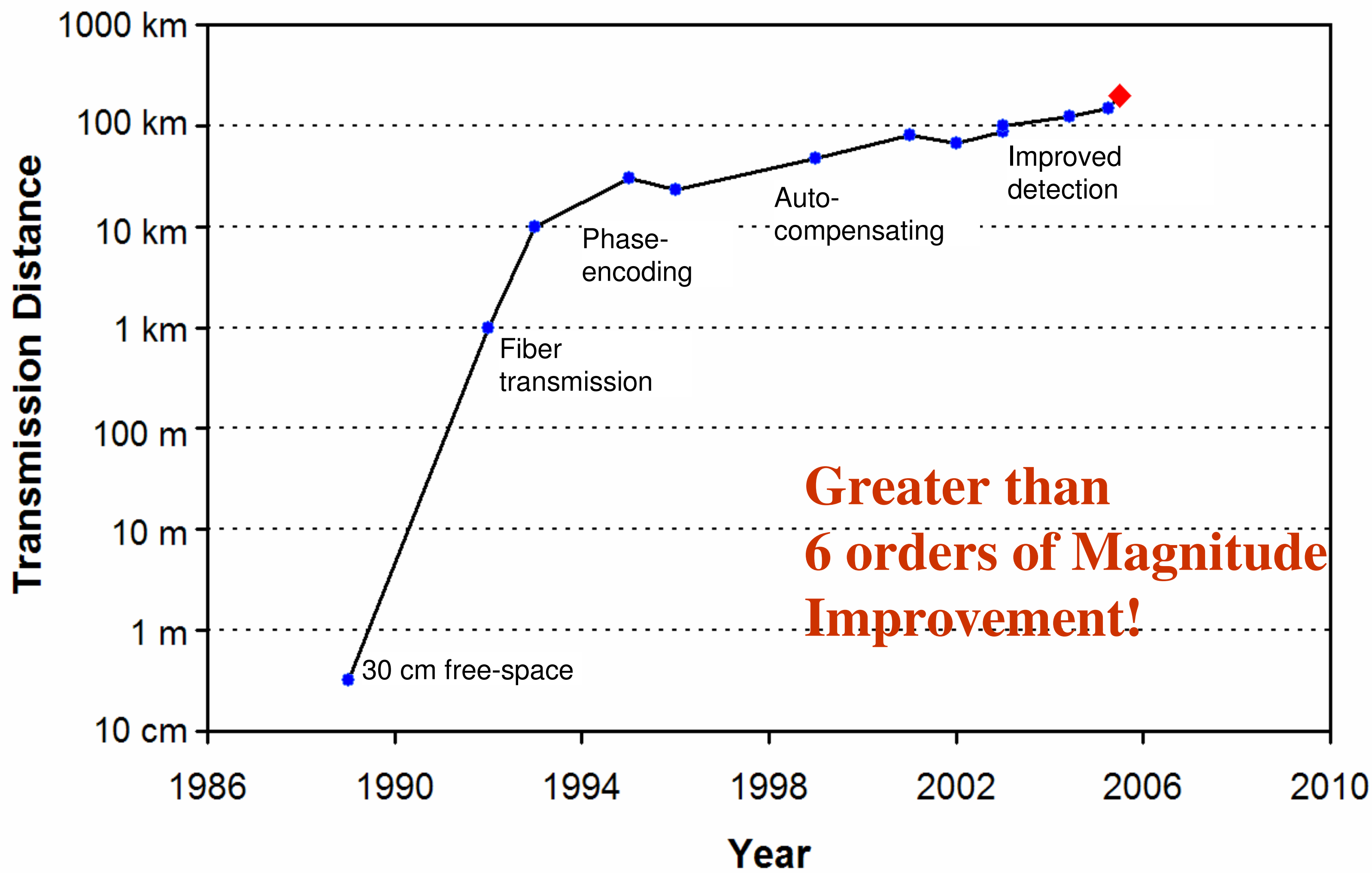
held distance records for multiple years, but not network- (or user-) friendly …

- **“set-up and frequent tuning by physicist, reconfiguration by re-wiring”**
  - fixed wavelength, static distance, low-background, low clock rates, out-of-band bright synch pulses, laboratory electronics, refrigerator for detectors

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Progress in QKD Fiber Transmission

(fiber pt-to-pt systems except 1st demo in free-space)

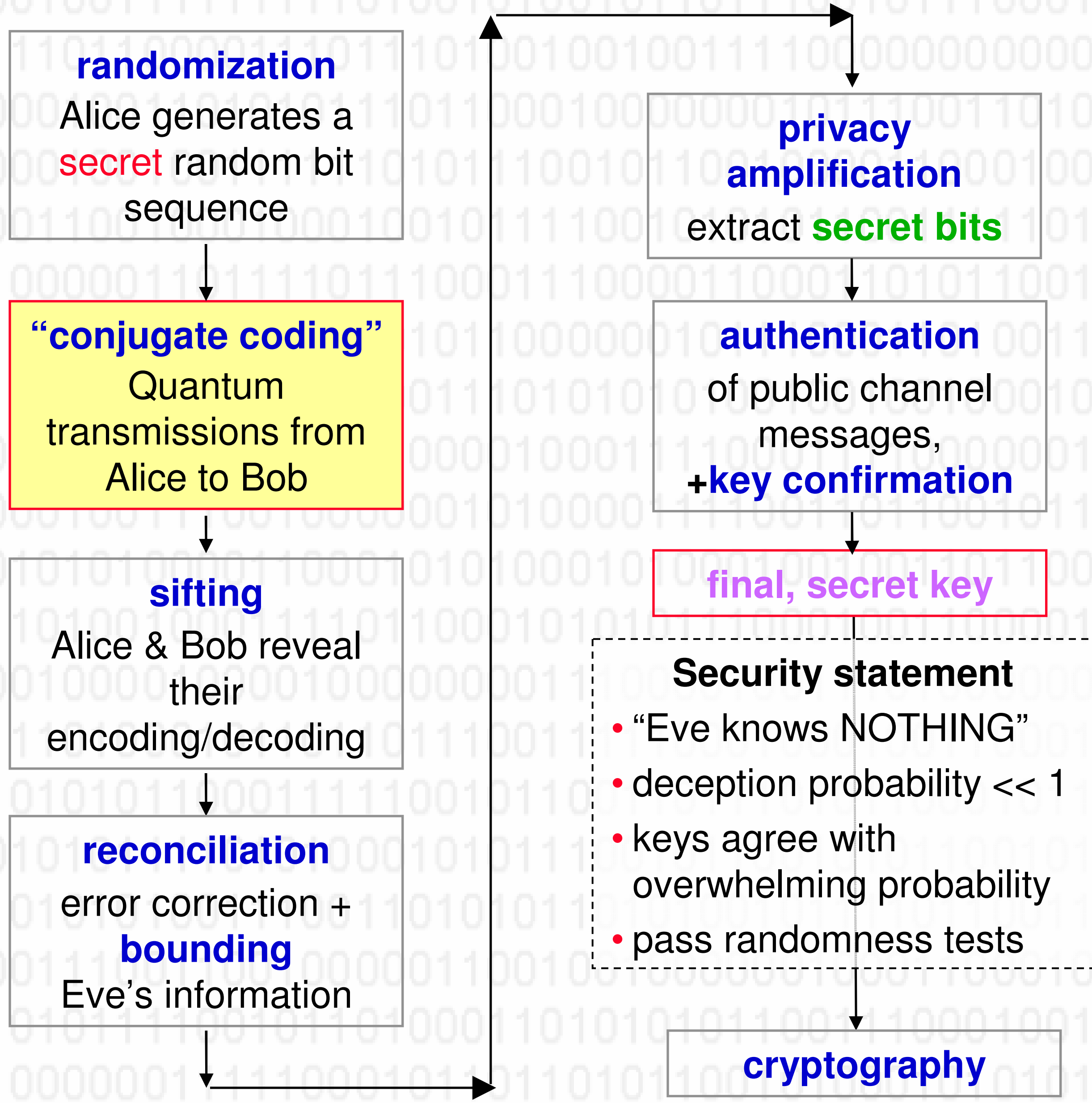


Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Los Alamos NATIONAL LABORATORY

INGREDIENTS of a FULL QKD PROTOCOL

- cryptographic quality random bits
- quantum comm.
- sifting
- error correction
- bound on information leakage
- privacy amplification
- authentication
- key confirmation
- security statement
- randomness tests
- standards



see e.g. N. Lutkenhaus, Phys Rev A59, 3301 (1999)

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Third core ingredient of QKD: "privacy amplification"

C. H. Bennett et al., IEEE Trans Inf Th. 41, 1915 (1995)

- **quantum physics provides Alice and Bob with an upper bound on Eve's partial information from sifted BER**
- **with "privacy amplification" they can produce a shorter, secret key:**
- e.g. Alice and Bob have 6 bits:

a, b, c, d, e, f

- they KNOW Eve knows 3 bits, but not which three
  - they can extract 2 SECRET bits:

a⊕b⊕c⊕d and **c⊕d⊕e⊕f**

- **privacy amplified bits are unknown to Eve:**
  - can be used for cryptography

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

The QKD link equation: secret bits per second

$$R_{\text{secret}} = R_{\text{clock}} \times P_{\text{sift}}(\mu,\eta) \times P_{\text{sift}\to\text{secret}}(\mu,\varepsilon)$$

figure of merit

secret bits/second

$$\approx \frac{1-\exp(-\mu\eta)}{2}$$

probability a transmitted bit is sifted

weak laser signals, $\mu < 1$: mean photon number / signal

$\eta \ll 1$: transmission/detection efficiency

ε= sifted BER

$$\approx 1-\mu-4\varepsilon\log_2 1.5+1.16\left[\varepsilon\log_2\varepsilon+(1-\varepsilon)\log_2(1-\varepsilon)\right]$$

multi-photon signals

eavesdropping on single-photon signals

"cost" of encrypting error correction

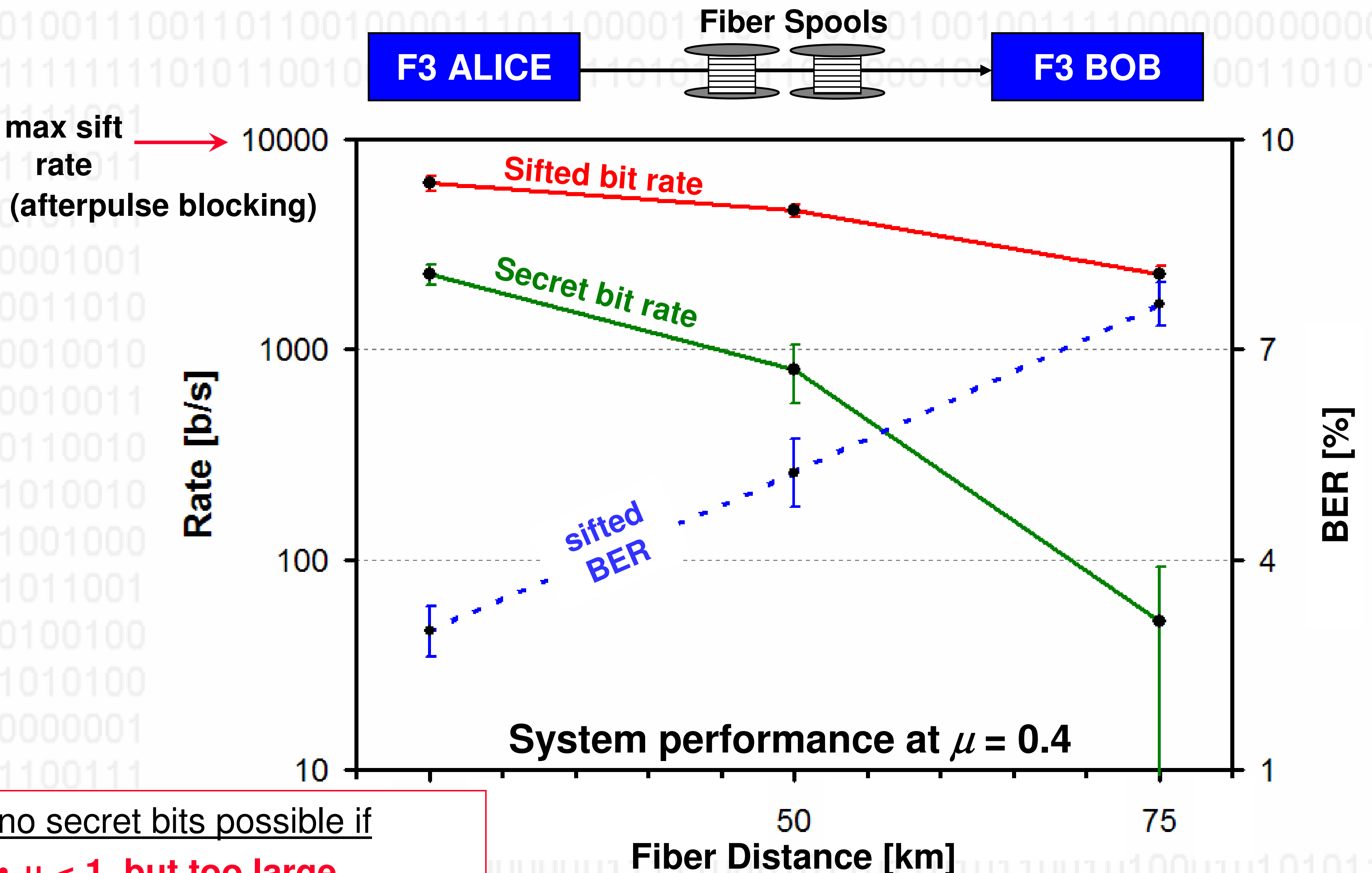
Bennett et al. (J. Crypto. '91) "BBBSS91" privacy amplification factor baseline

- **random deletion (beamsplitter) channel**
- **all multi-photon bits entering sifted key deemed known to Eve**
- **all bit errors attributed to intercept/resend by Eve on single photon signals**

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Los Alamos NATIONAL LABORATORY

The limits to optical fiber QKD with InGaAs APDs: e.g. LANL F3QKD



<u>no secret bits possible if</u>

- μ < 1, but too large
- SNR too small
  - <u>range limit</u>

Secret bit rate depends on detector properties

"Its all about signal-to-noise" (J. Nordholt)

Secrecy efficiency	=	Transmission & detection	x	Protocol efficiency	x	Error correction	x	Privacy amplification

- Levels of error correction and privacy amplification driven by bit error rate, which depends on probability of real count vs dark count
  - High efficiency
  - Low dark count rate
- Signal to noise ratio also limits the ultimate range of a system (~100 km for InGaAs APDs in a BB84 fiber QKD system). Above this range, no secret bits can be exchanged, regardless of clock rate.
- Transition-edge sensor photodetectors
  - 89% system detection efficiency at 1550 nm
    - D. Rosenberg et al. APL 88, 021108 (2006)
  - No intrinsic dark counts

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Can we achieve longer ranges, at higher rates with stronger security in optical fiber QKD ?

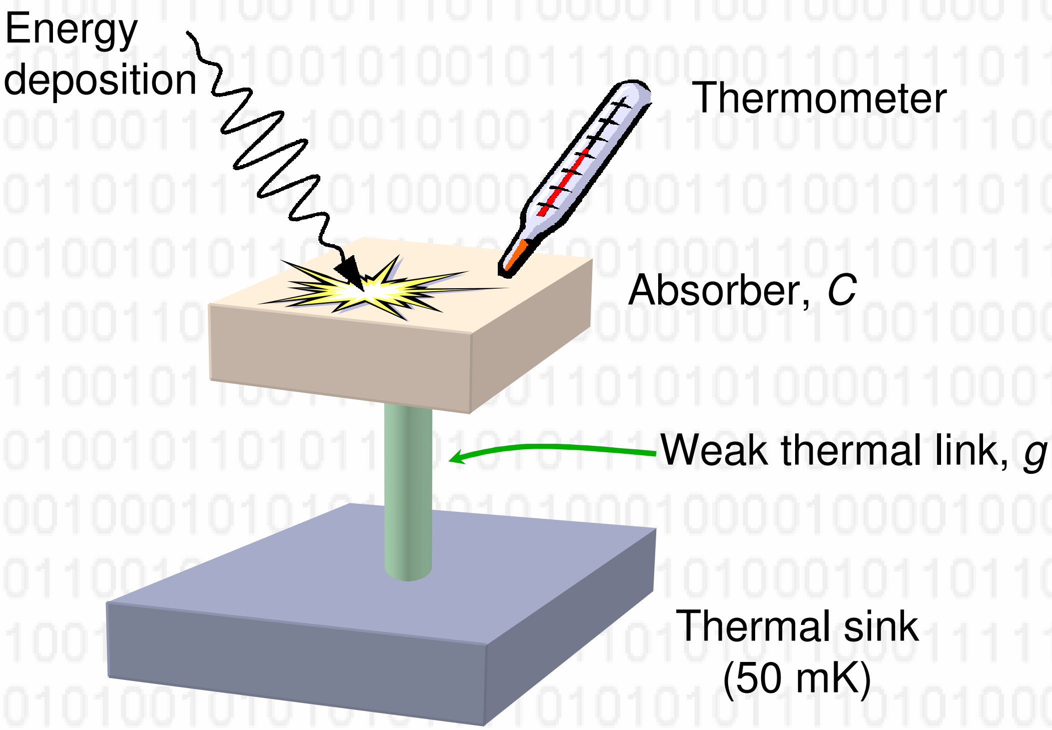
(J. Nordholt et al., LANL + S. Nam et al., NIST-Boulder)

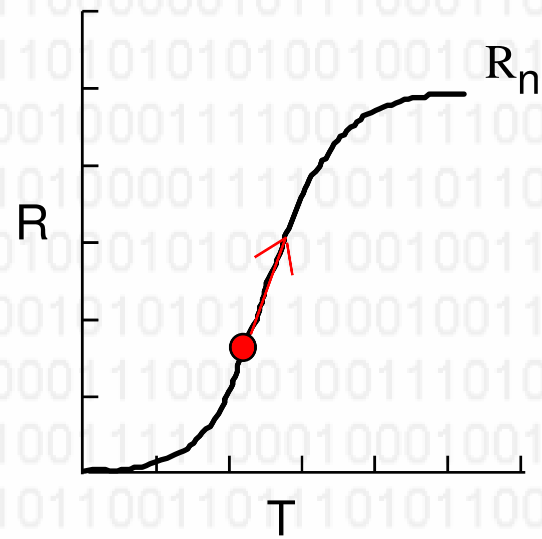
Goal: explore limits to the ultimate range, secret bit rate, and security of fiber QKD by using high-efficiency, noise-free transition-edge sensors.

- **Dark counts in detectors place limits on range and secret bit rate**
- **TES have high efficiency at telecom wavelengths and no dark counts**
  - Longer range
  - Higher secret bit rates
- **Integration of TESs in a fiber QKD system**
  - Rosenberg et al, Applied Physics Letters, 88, 021108 (2006)
- **Four new distance records**
  - Bennett et al privacy amplification (BBBSS91) over 148km at $\mu = 0.1$
  - BBBSS91 security over 185km at $\mu = 0.5$
  - PNS-security over 68km
  - Decoy-state protocol over 107km

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Transition Edge Sensor (TES) Technology
(Sae Woo Nam et al., NIST-Boulder)





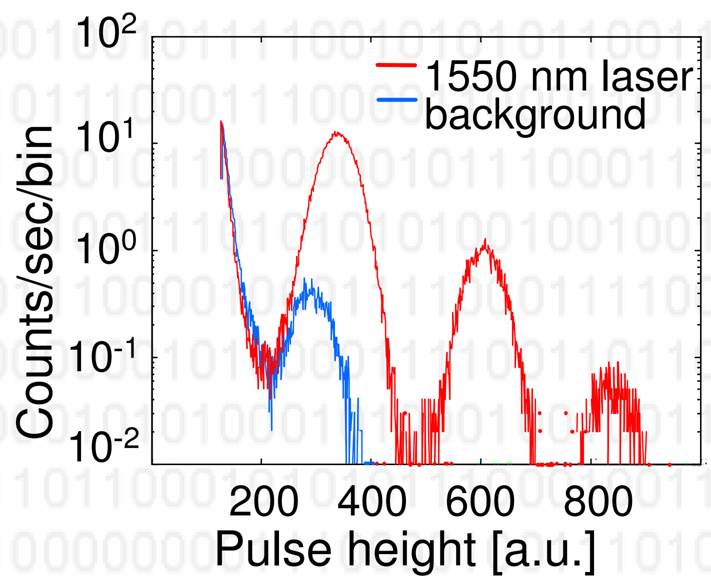
Calorimetric detection of UV/optical/IR photons:

- Photon(s) absorbed by a heat capacity *C* connected to a thermal sink by a weak thermal link *g*.
- Temperature of the absorber is monitored by an ultra-sensitive thermometer (superconducting-to-normal transition).
- Temperatures are ~100 mK to ensure low noise and high sensitivity.

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

TES background count rate

Photons from blackbody radiation from room temperature objects propagate down the optical fiber, creating a background count rate.



Ideal solution: In-line fiber filter or coating that only allows 1550 nm photons through

Crude filtering method: coil a section of cold fiber- long wavelengths preferentially discarded, but some 1550 nm photons are also lost.

89% system efficiency
400 counts/sec background

⇨

65% system efficiency
10 counts/sec background

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Comparison Between InGaAs and TES Detectors

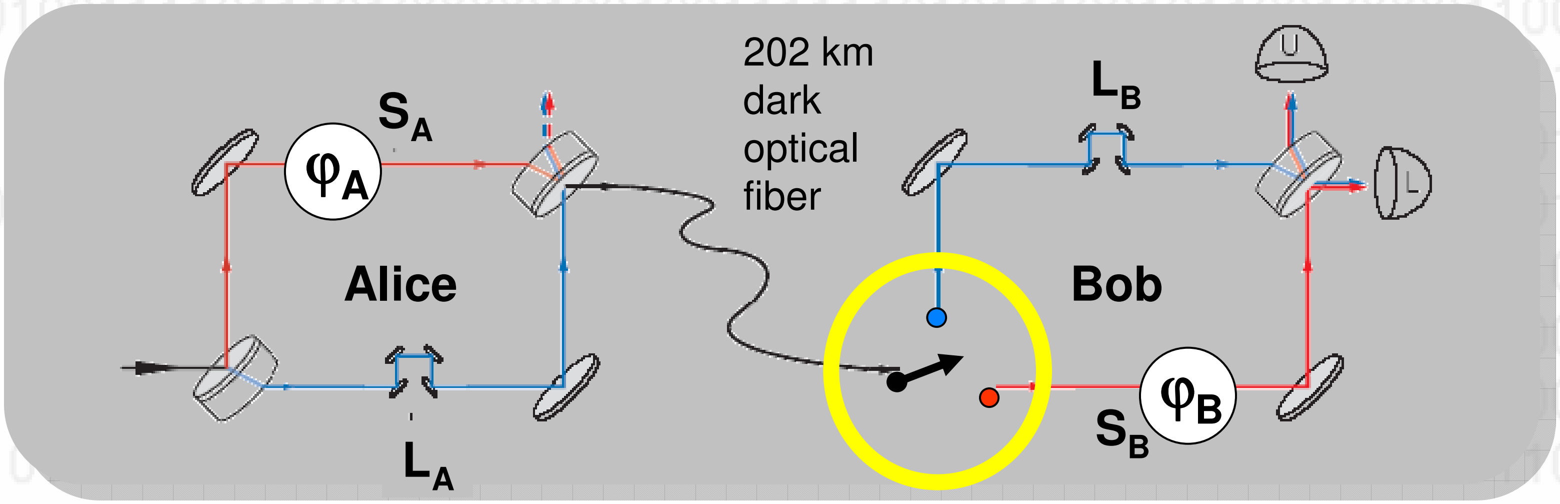
		Ratio of dark count rate to detection efficiency
InGaAs APDs (Princeton Lightwave)		
Detection efficiency	13 %	
Timing resolution	0.12 ns	
Dark counts (ungated)	15 kcps	$1.2 * 10^{-4}$
Dark counts per 1 ns gate	$1.5x10^{-5}$	
Dead time	20-50 μs	
Transition-edge sensors		
Detection efficiency	65 %	
Timing resolution	80 ns	
Background count (ungated)	10 cps	
Background per 200 ns window	$2x10^{-6}$	$3.1 * 10^{-6}$
Dead time	4 μs	

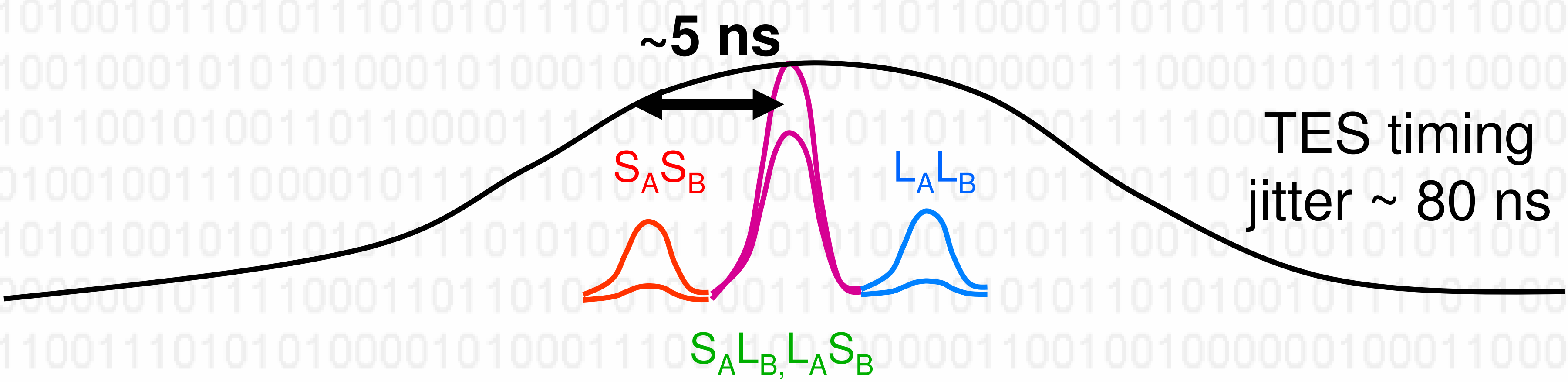
and, higher sift rate possible at lower clock rate ⇒ more secret b.p.s

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Integration of TESs into fiber QKD system

Laboratory version of F3



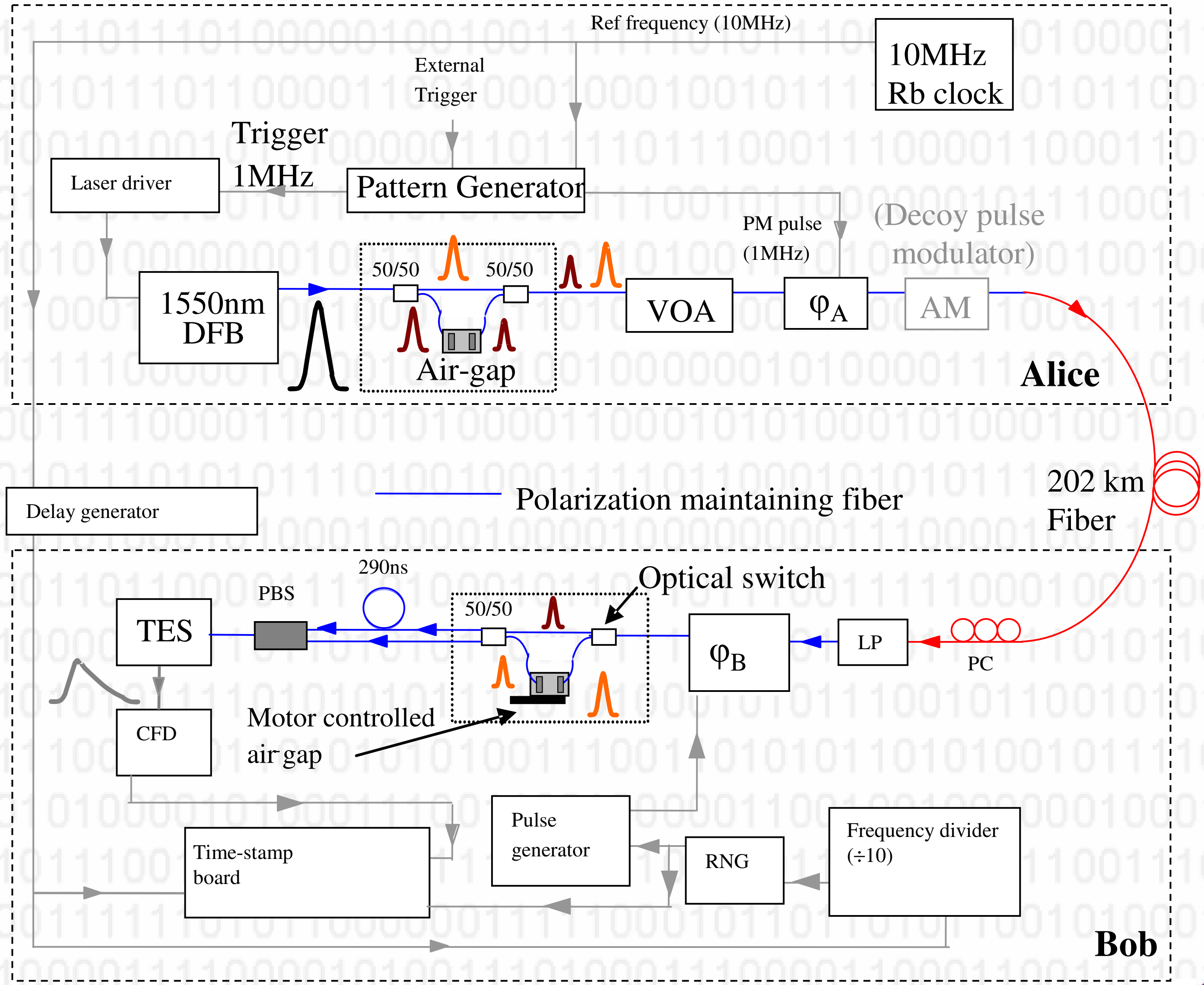


Switch is set to route all S_A (L_A) photons from Alice to L_B (S_B)

* Hiskett et al, to be submitted (LA-UR-06-3211)

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

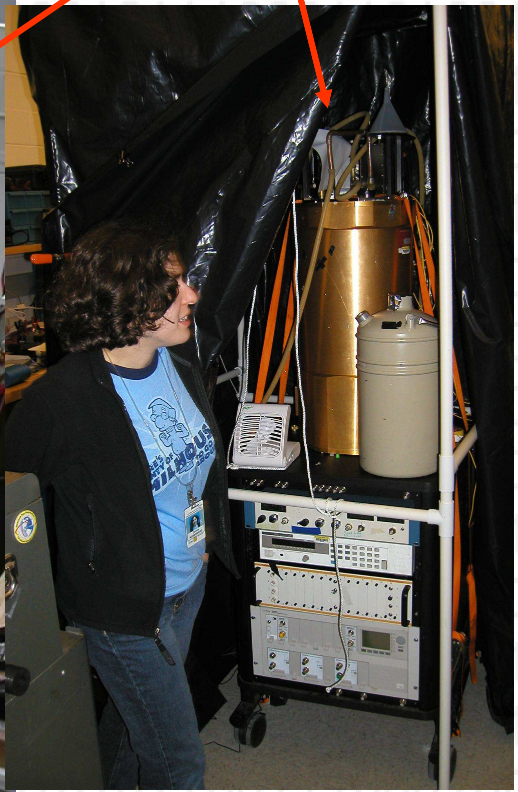
TES QKD



Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

TES QKD set up

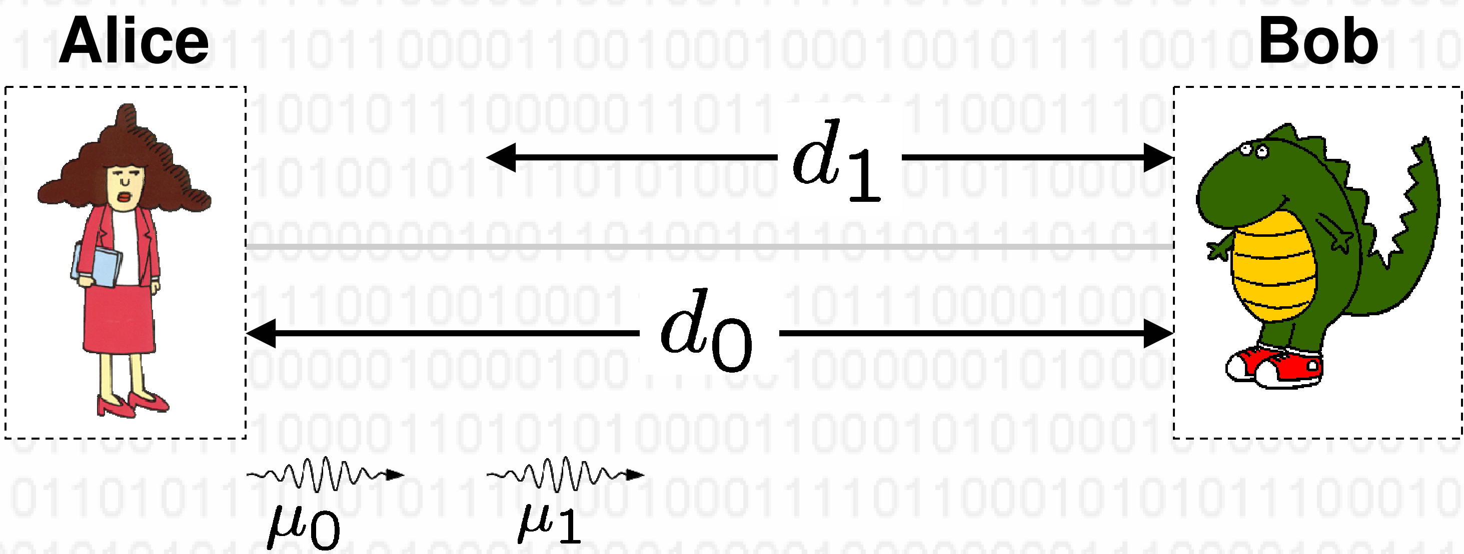
TES dewar



Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Transmission over 202 km

Can redefine Alice to include some of the fiber link



$$\mu_1 = \mu_0 10^{-\frac{\alpha}{10}(d_0 - d_1)}$$

$$d_1 = d_0 + \frac{10}{\alpha} \log_{10}\left(\frac{\mu_1}{\mu_0}\right)$$

α = loss per unit length of fiber = 0.2 dB/km

Translates values of μ_0 over 202 km to effective distance at μ_1

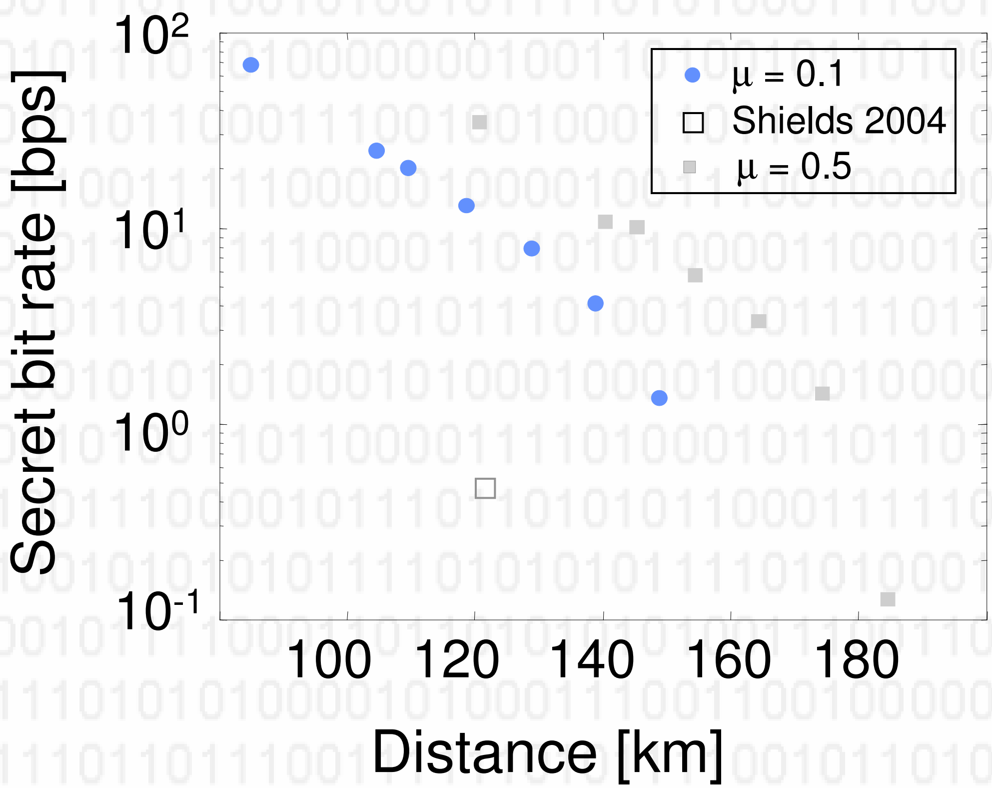
Acknowledgement: fiber loaned by Joe Dempsey of Corning

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Secret bit rate

Implemented BB84 protocol with a weak coherent laser source in F3 laboratory system clocked at 1 MHz

- CASCADE error correction
- BBBSS91 privacy amplification



Transmission at μ=0.1 over **148 km***, a new record.

Previous record: Shields APL 2004 μ=0.1 over **122 km**.

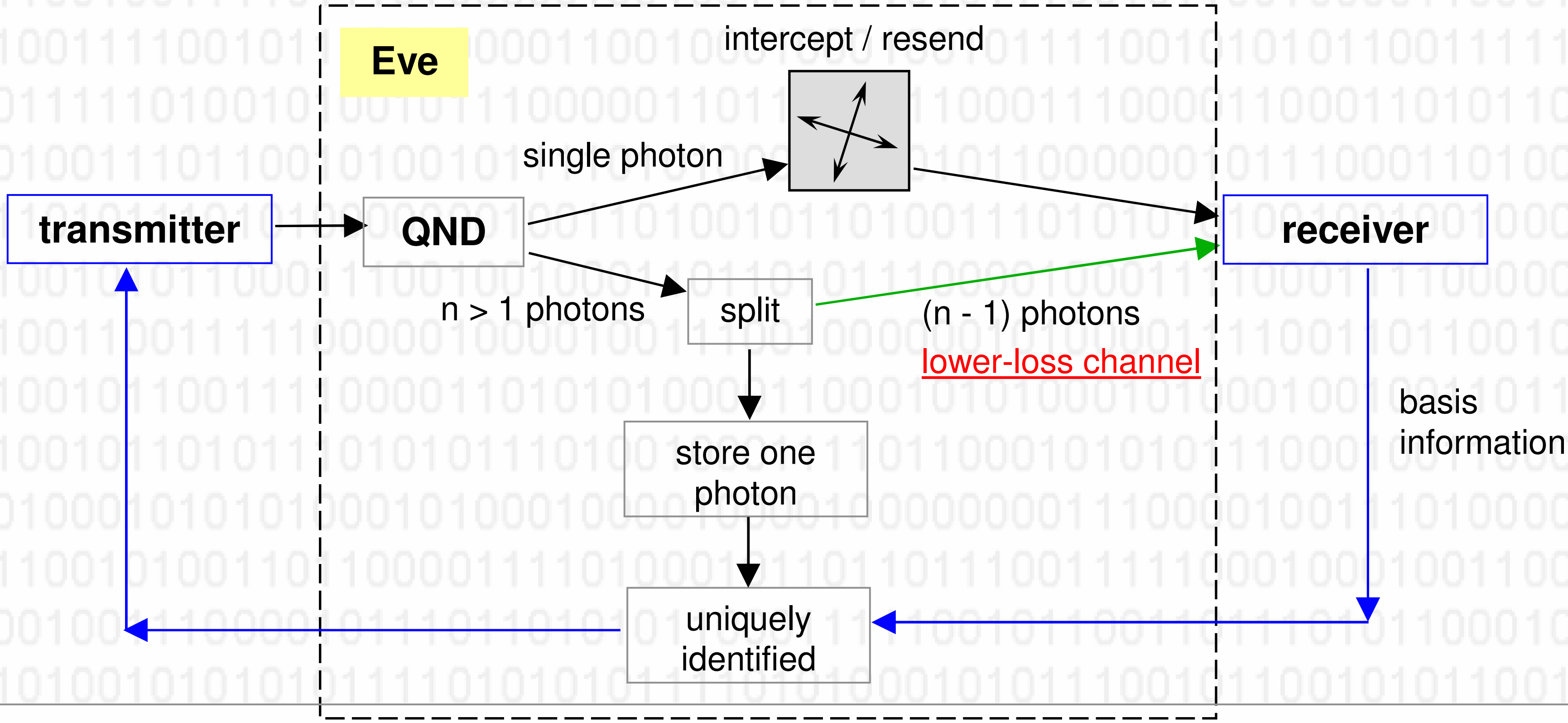
Transmission at μ=0.5 over **185 km***, a new record.

* P. Hiskett et al, quant-ph/0607177

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Photon Number Splitting: BBBSS91 security is conditional on a random deletion channel

N. Lutkenhaus (2000); G. Brassard et al. (2000).



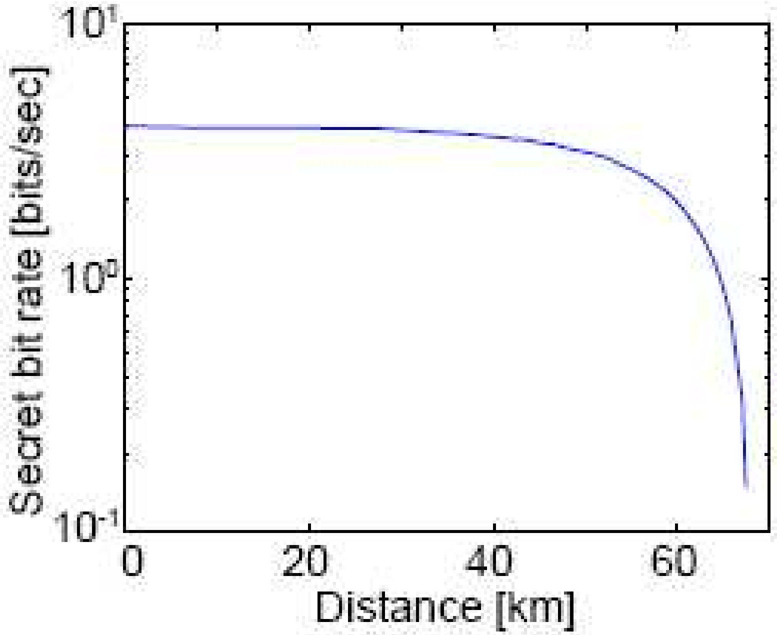
- **conventional security: need multi-photon emission < single-photon arrival**
  - **upper bound on photon number in terms of accessible loss: $\mu^2/2 < \eta\mu$**
  - **adversely impacts key rate ~ η^2, and range**
- **new solution: "decoy states" to characterize single-photon transmittance of channel**

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

PNS-secure transmission

Transmission at low μ (short distance) ensures that some of the signals at Bob originated from single photons

- "Modified CASCADE" error correction (Sugimoto and Yamazaki, IEICE Trans. Fundamentals, 2000)
- GLLP privacy amplification assuming all multi-photons at Alice are tagged (Gottesman, Lo, Lutkenhaus, and Preskill, QIC 2004)



Assuming that Bob's losses are accessible to Eve, we find that the secret bit rate goes to zero at **67 km** (μ = 0.004)

Previous record: Shields Electronic Letters 2004 **50.6 km**

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Decoy state protocols protect against channel replacement

Hwang (2003), Lo, Ma, Chen (2004), Harrington et al. (2005)

- **"how many single-photon signals enter the sifted key ?"**

- **decoy state protocols dramatically increase the range, security and secret bit rate of weak laser QKD**
  - randomly choose the signal strength, μ, from a set of values
  - after signals are received by Bob, Alice reveals the strength values

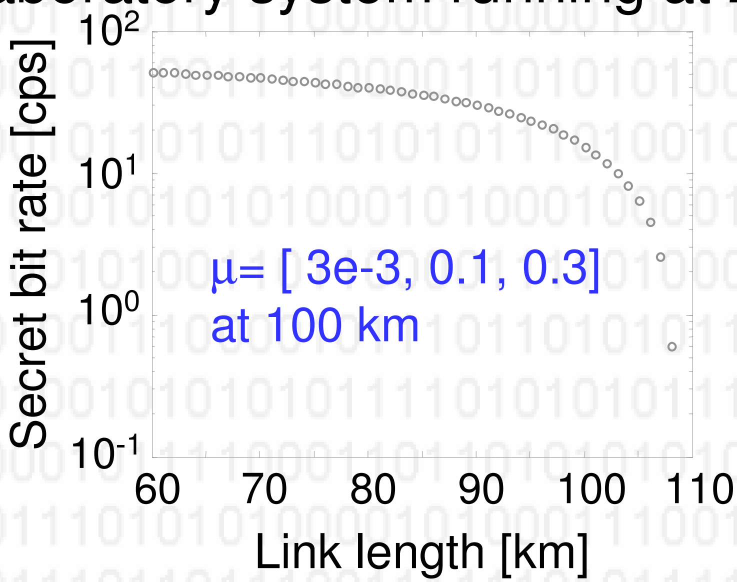
- **intuition: e.g. a three-level decoy state protocol**
  - μ_0 ~ 1 provides most of the secret bits
  - μ_1 ~ 0.1, most non-empty signals are single-photon signals
    - allows single-photon channel transmittance to be bounded
  - μ_2 ~ 0, allows channel noise to be bounded
  - when Eve sees a single-photon she cannot discriminate between a μ_0 and μ_1 signal

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Decoy state QKD with TESs

Recently developed finite statistics decoy state protocol places confidence levels on single photon transmittance and enables PNS-secure key creation at much higher mean photon numbers (μ~1): J. W. Harrington et al., quant-ph/0503002

Implemented decoy state protocol using 3 power levels in F3 laboratory system running at 2.5 MHz



Creation of PNS-secure key over 107 km of optical fiber*, an increase of 80% over previous highest reported distance of 60 km (see H.-K. Lo quant-ph/0601168)

*D. Rosenberg et al, quant-ph/0607186
(see also Peng et al., quant-ph/0607129: 75km)

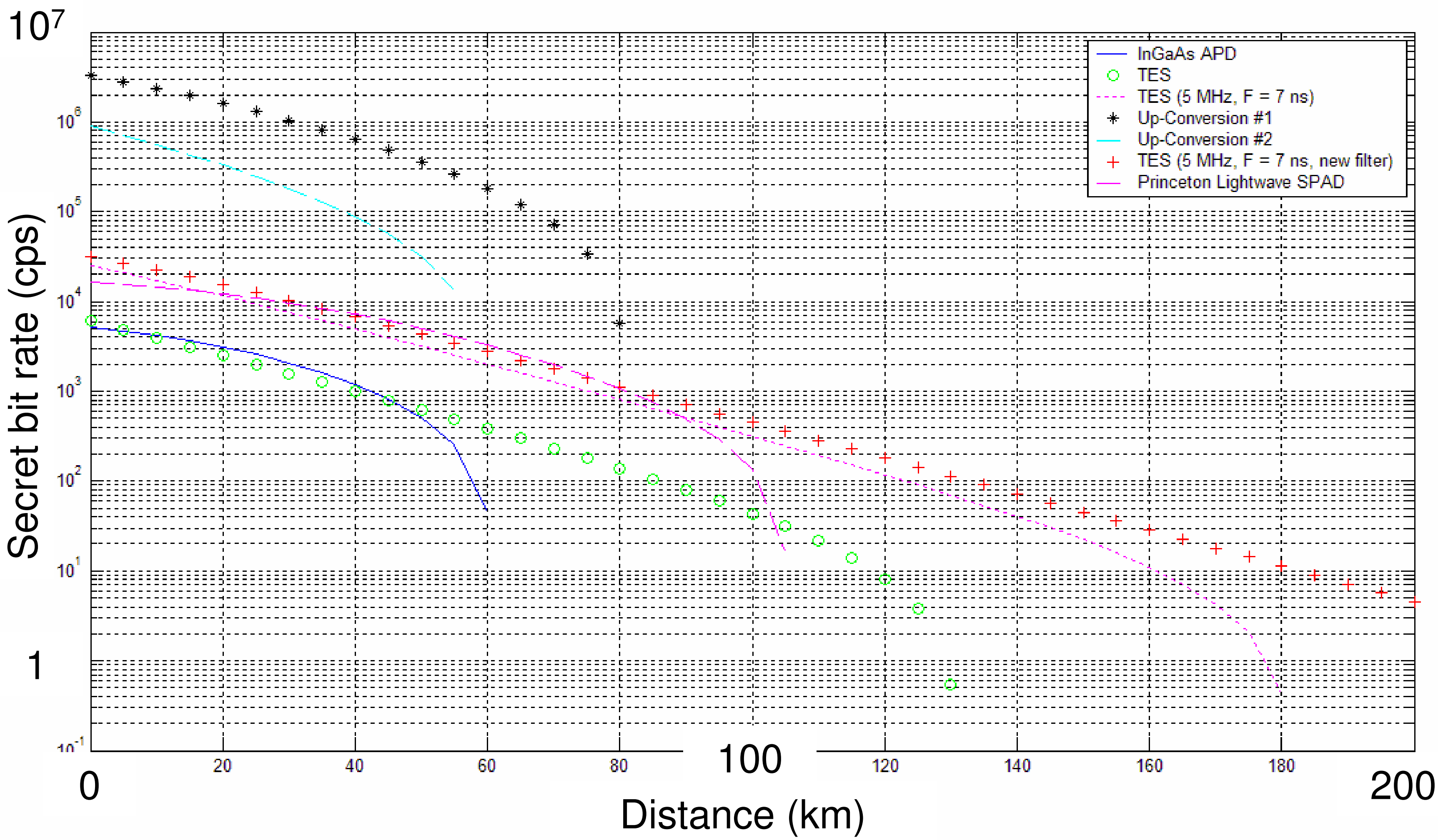
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

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

Los Alamos NATIONAL LABORATORY

QKD range: comparison of InGaAs, TES and up-conversion detectors at 1550nm

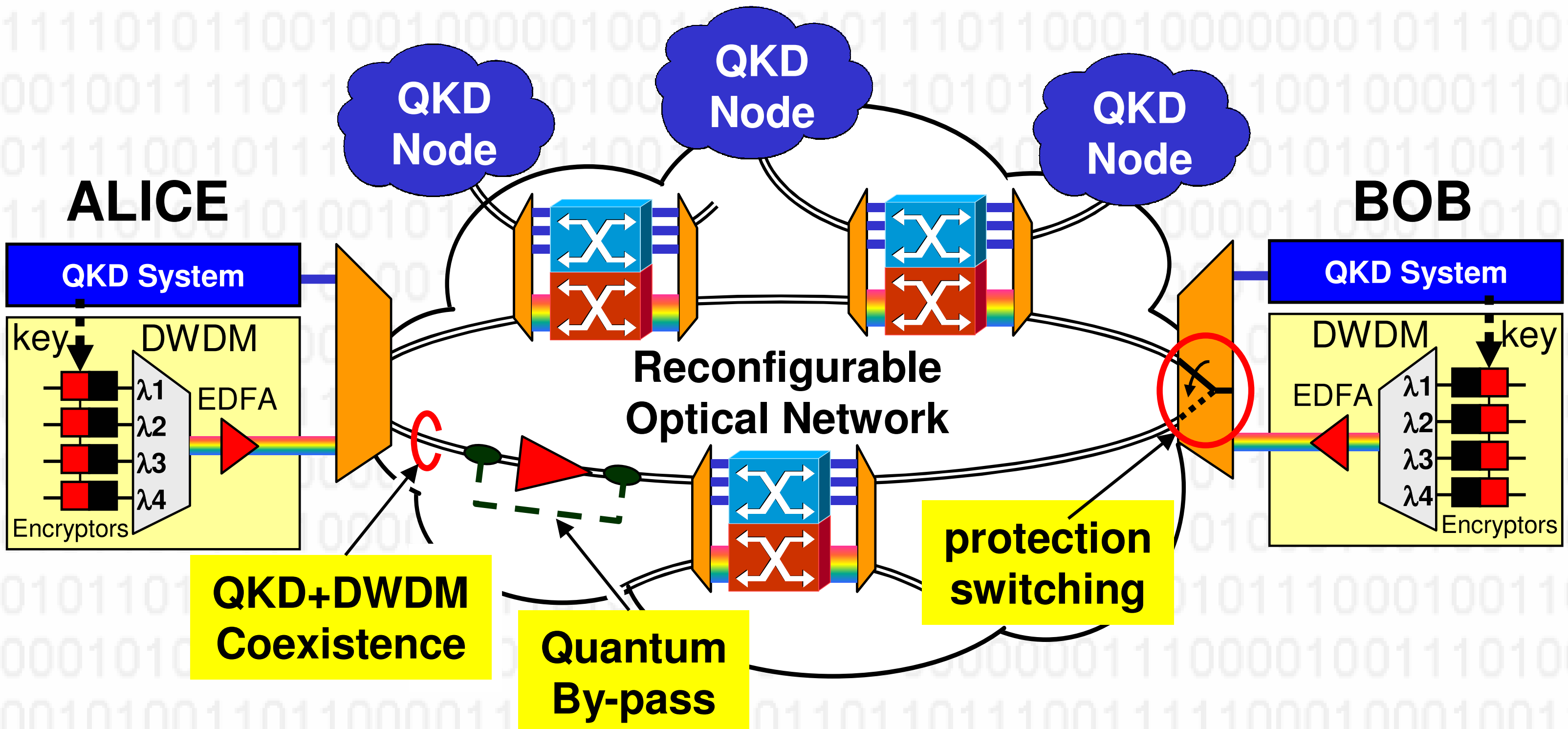
(D. J. McCracken, unpublished)



- GLLP privacy amplification … beamsplitter channel, no decoy states
- SSPDs ?

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

The Vision: Securing Networks with QKD



- **QKD and encrypted data λs share a common physical fiber path**
  - Efficient use of today's existing fiber infrastructure
- **Optical switches route quantum & data λs on different spectral bands**
  - "Quantum by-pass" paths for amplifiers and legacy electronic systems
- **Network provides multi-party key distribution, reconfigurable optical paths, and protection switching**

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Requirements for QKD in all-optical fiber networks

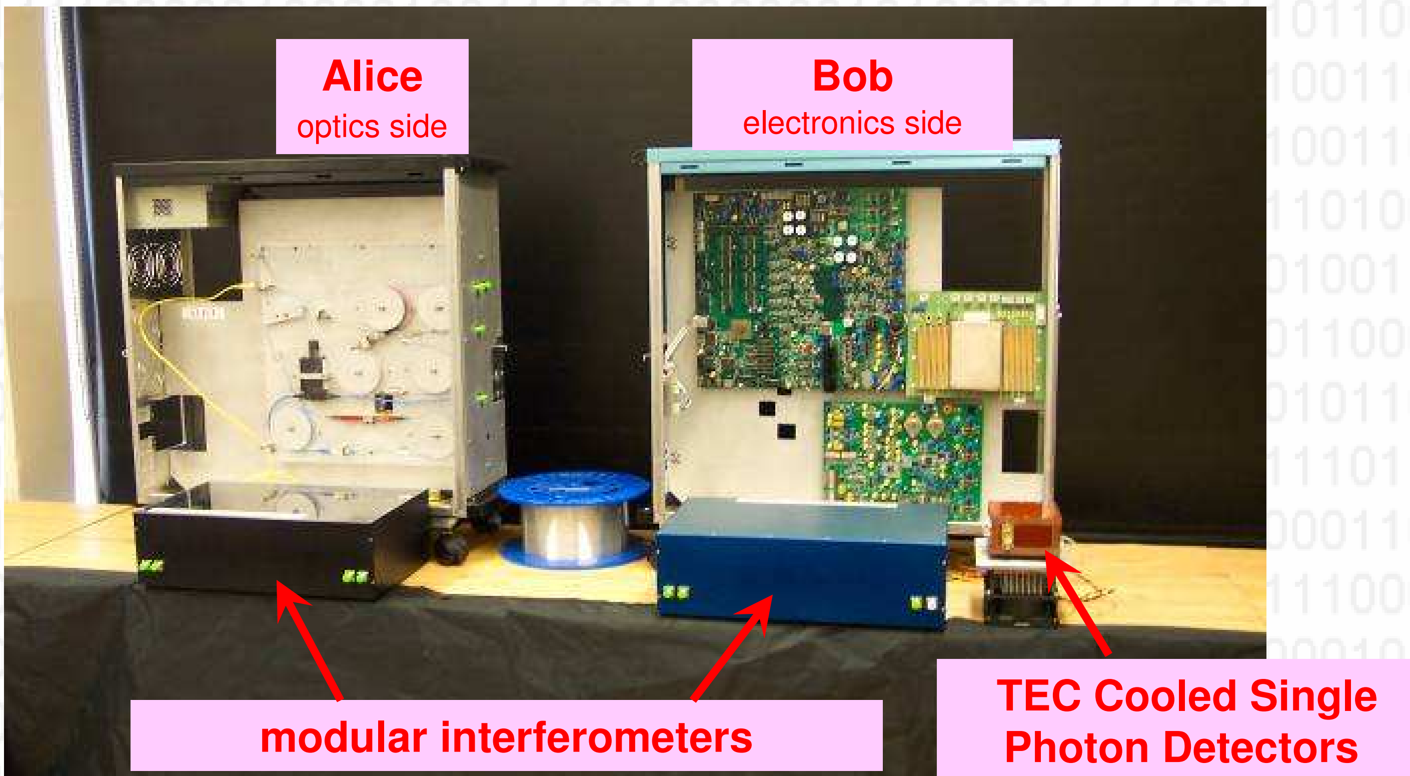
Requirement	F1/F2 limitation	F3 solution
"Ease of use", availability & stability	Physicist required	Engineered, automated, stable system
Multi-wavelength, multi-protocol flexibility	Fixed wavelength	Novel modular design
Network- and QKD-friendly synchronization	Out-of-band bright pulses	Syntonized Rb oscillators
Accommodate path length & polarization changes	Static path length	Auto-synchronization and tuning
Background tolerant	Dark fiber	Epitaxx InGaAs APDs
Clock rates < 10 MHz	Clock rates < 100 kHz	"After-pulse blocking"
Complete protocol, self-sustaining operation	–	Includes all classical elements + authentication

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Third Generation LANL Fiber QKD System: F3QKD

(R. J. Hughes et al., Proc SPIE 5893, 1 (2005))

- **Complicated test equipment not required**
  - control, data acquisition and protocol layer interfaces to “QKD package” via USB interface
  - all reconfiguration driven by software
  - automated setup and tuning
- **modular electronic/optical QKD package**



Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Los Alamos
NATIONAL LABORATORY

F3a: complete protocol suite

QKD package

monolithic randomizers

randomization
Alice generates a secret random bit sequence

"conjugate coding"
Quantum transmissions from Alice to Bob

time-stamping

software

sifting
reveal time slots + bases

CASCADE or MYCADE

reconciliation
error correction

"BBBSS91"

bounding
Eve's information

privacy amplification
extract **secret bits**

software

random matrix or Toeplitz hash

authentication
of public messages

key confirmation

cryptographic CRC hash

final, secret key

Security statement

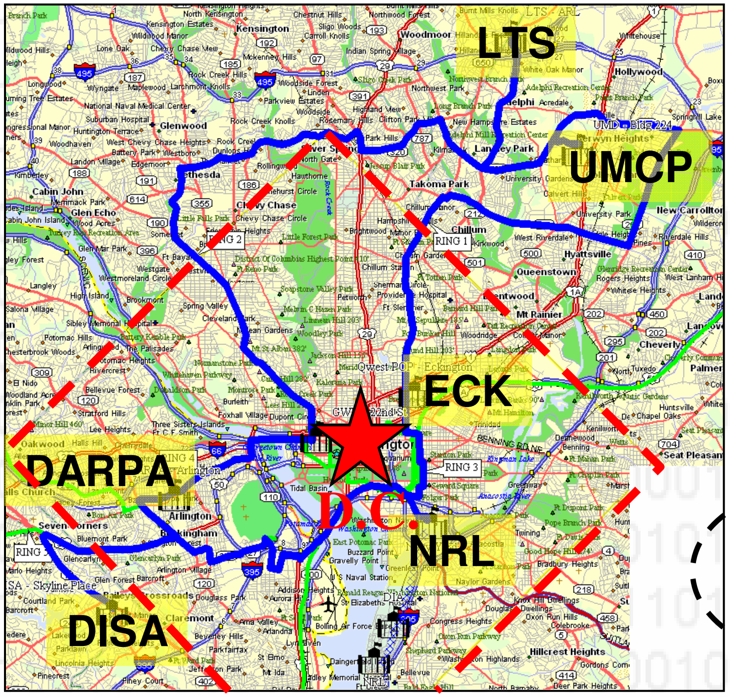
- "Eve knows NOTHING"
- deception probability << 1
- keys agree with overwhelming probability
- pass randomness tests

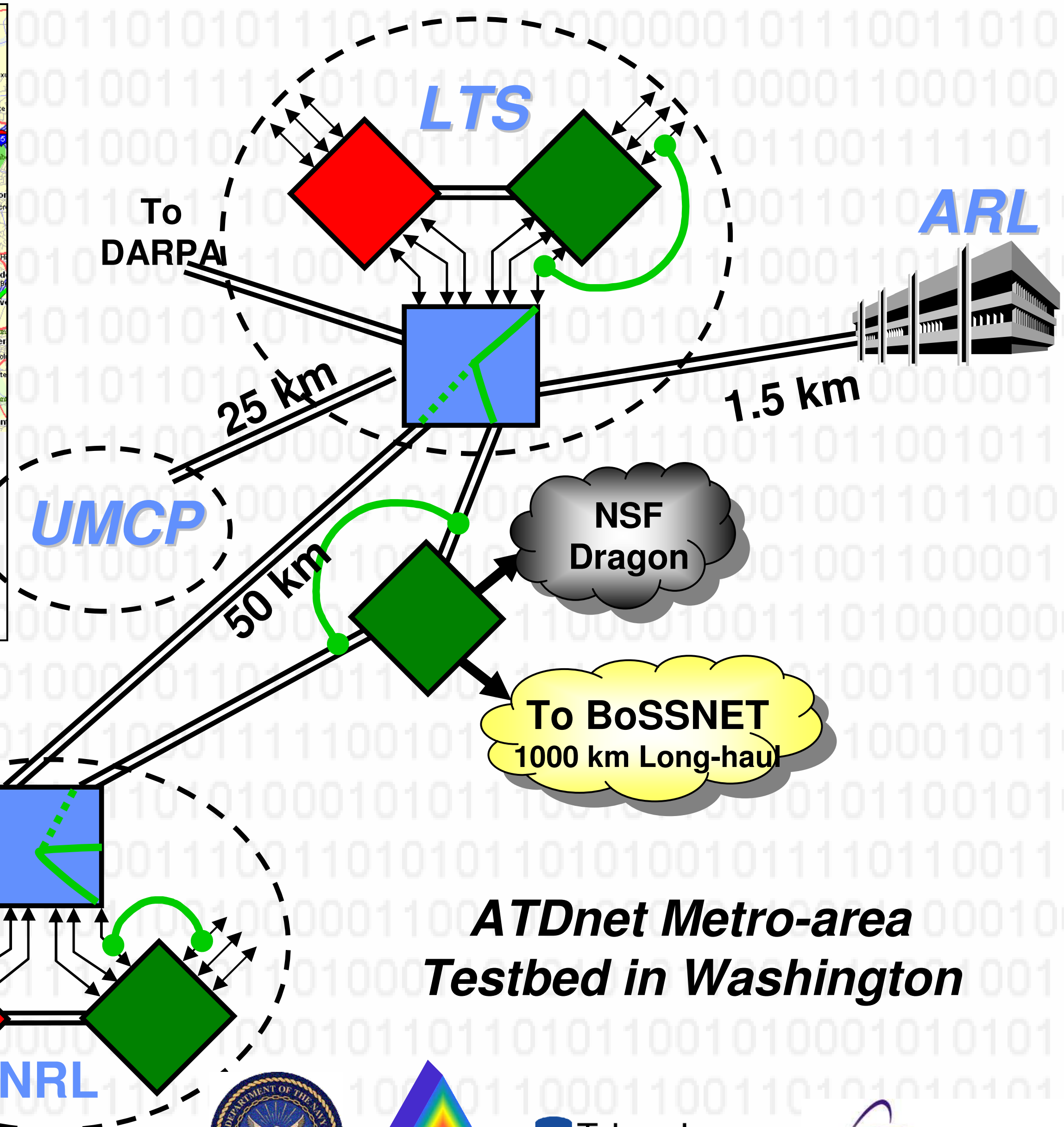
FIPS 140-2

cryptography

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

ATDNet Optical Networking Environment



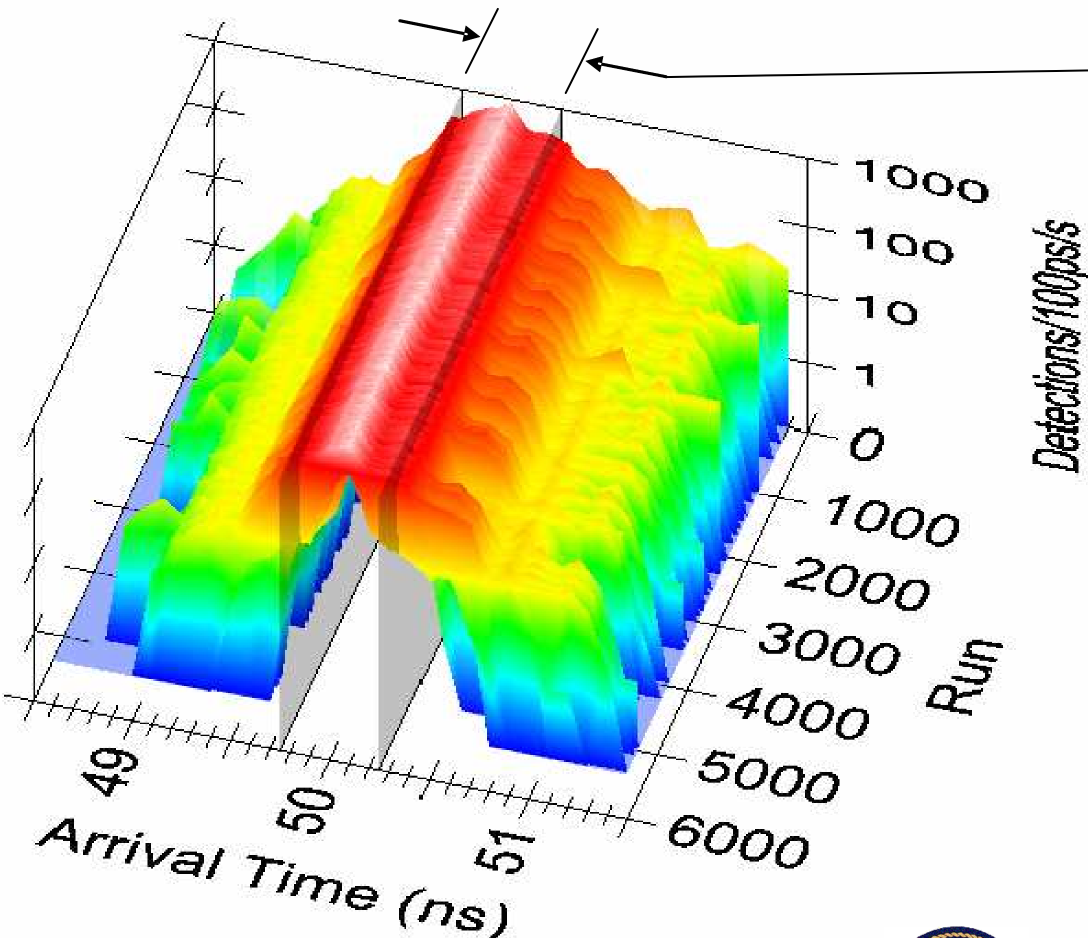


ATDnet Metro-area Testbed in Washington

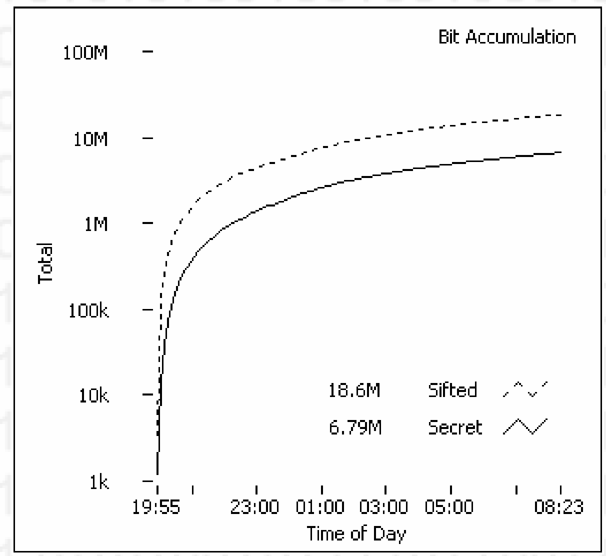
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

F3 is capable of continuous, unattended, <u>self-sustaining</u> operation over installed fiber

e.g. 12 hours of data over 25-km College Park loop



Events <u>selected from 0.5ns</u> <u>window</u> yield <u>6.8M secret bits</u>



μ = 0.2
BER = 4.9%
Sifted bit rate: 3.5 kHz
<u>Secret bit rate: 1.3 kHz</u>

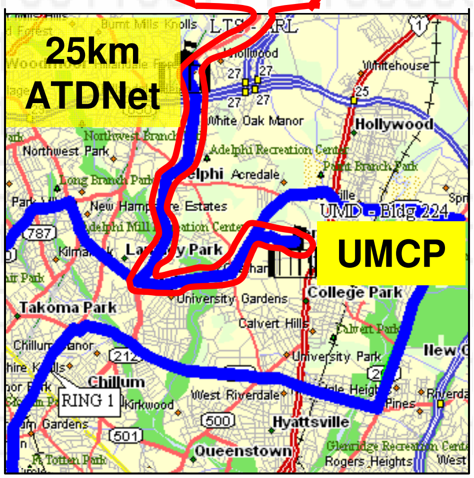
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

LTS
Telcordia Technologies
Los Alamos NATIONAL LABORATORY

4-Day F3QKD Performance over ATDNet

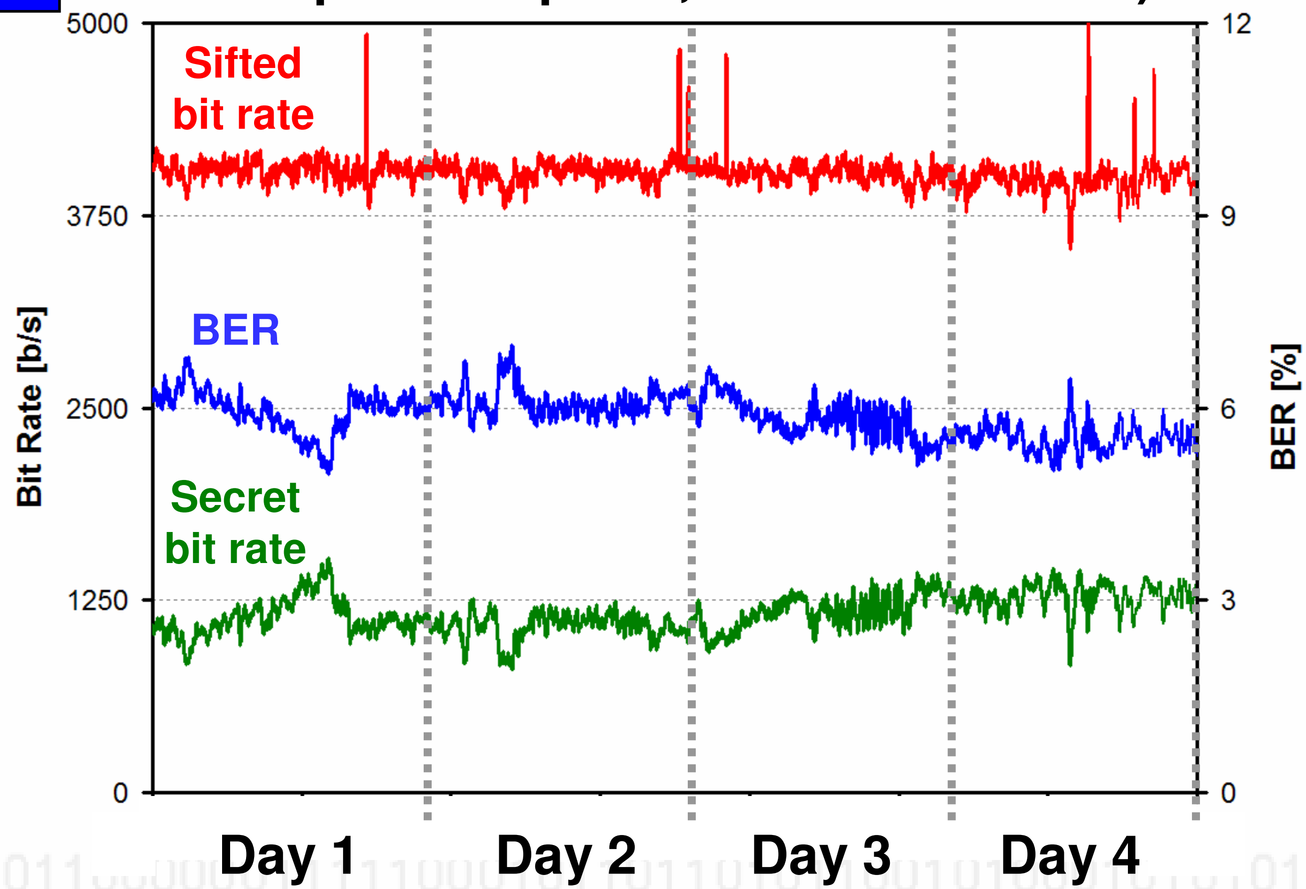
F3 ALICE

F3 BOB



25 km ATDNet Round Trip

(Unattended, fully automated operation, 0.2 photons/pulse, 38.4M secret bits)

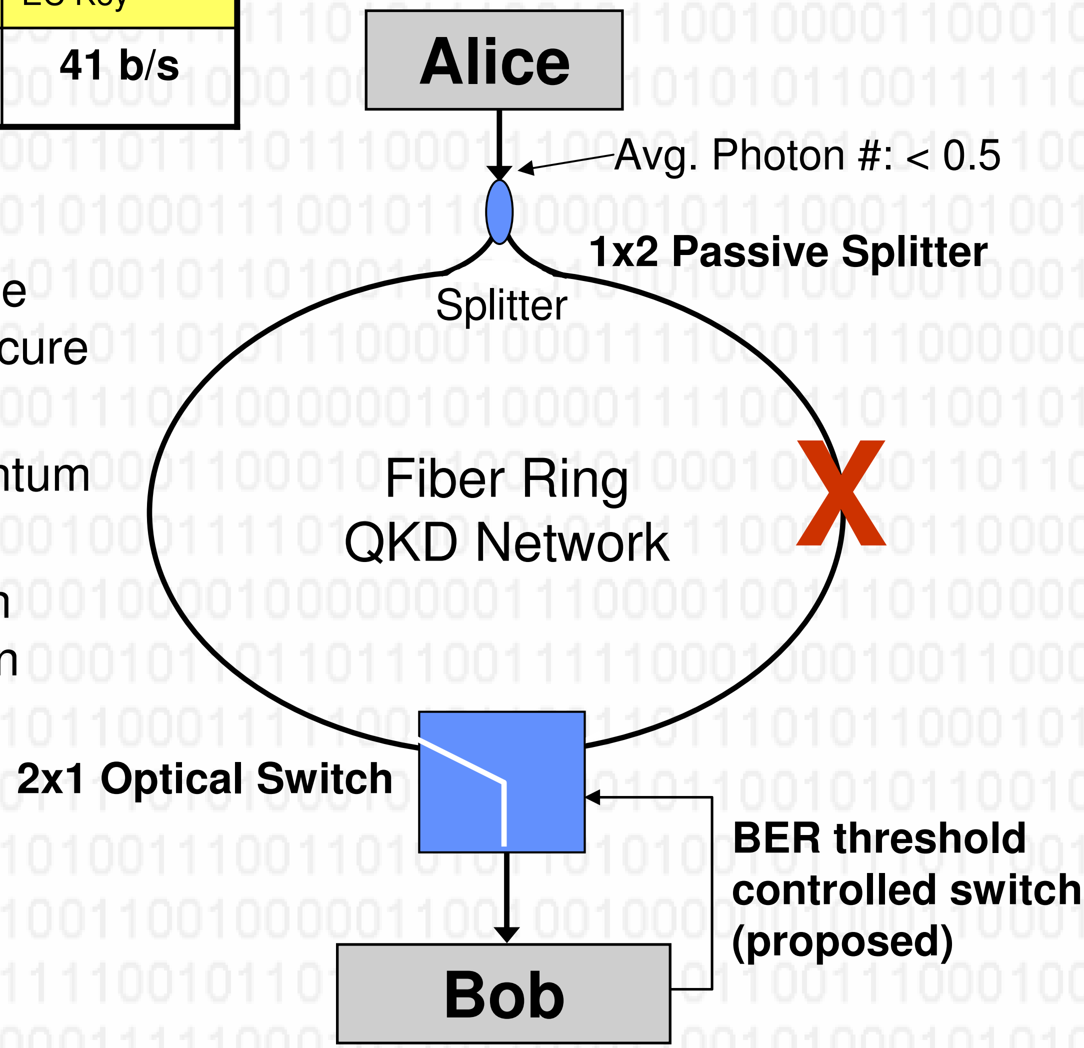


Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Ring Network for QKD Protection Switching

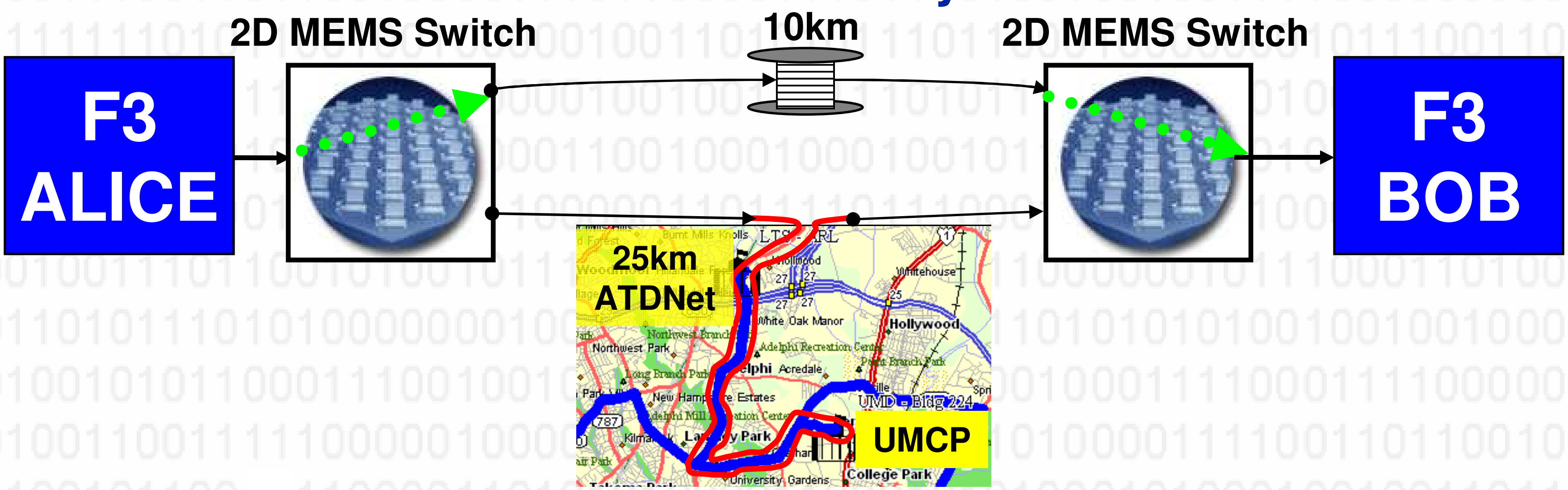
Path Loss	BER	Raw Rate	EC Key
4.7 dB	< 10%	105 b/s	41 b/s

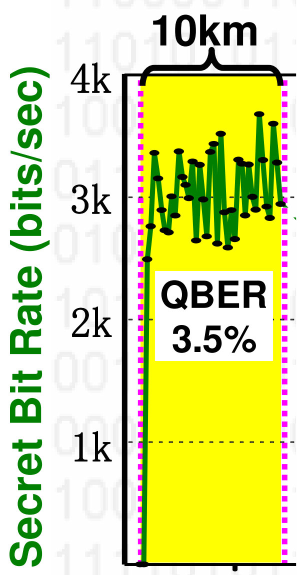
- If Eve drives QBER higher on one path, protection switch allows secure use of redundant path
- Ring architecture enhances quantum channel availability
- Similar optical network protection architecture found in metropolitan areas



Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

First Automated QKD Resynchronization

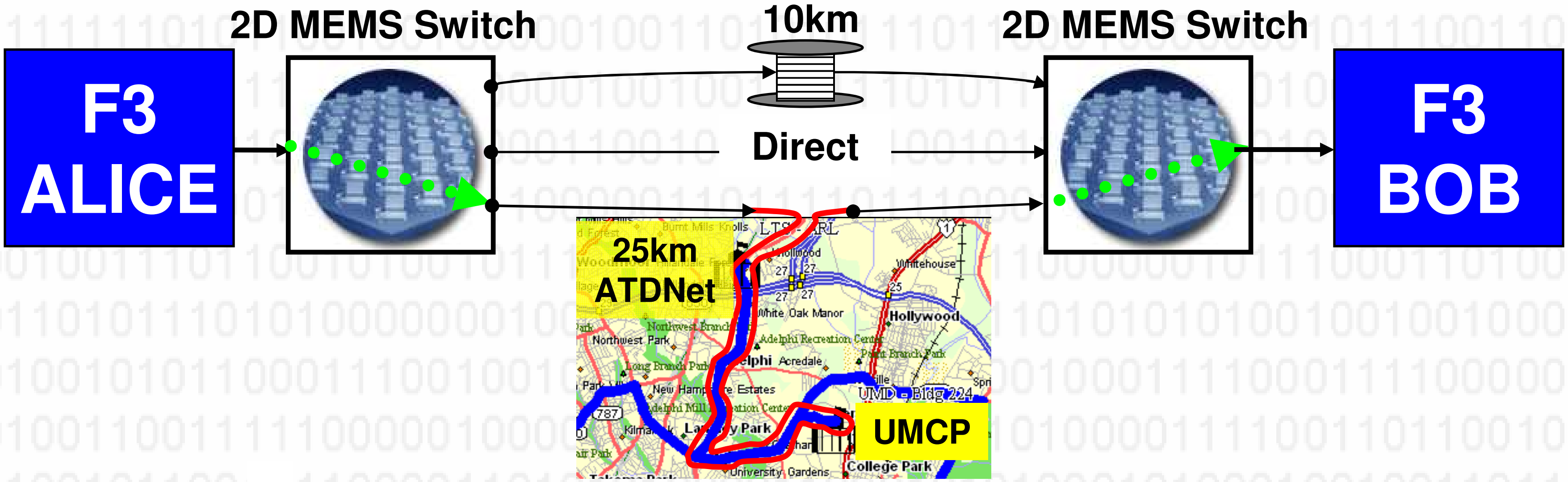


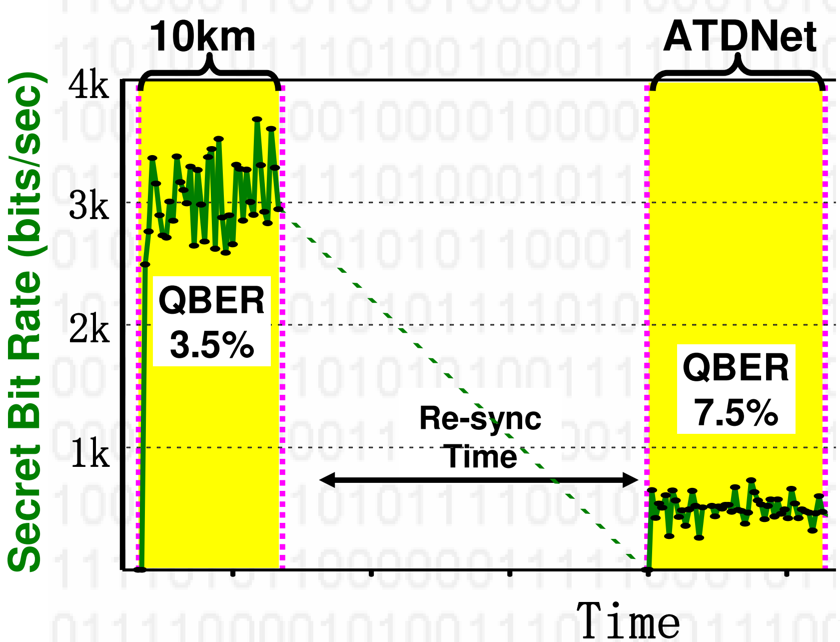


R. Runser, et. al., OFC 2006 (Invited)

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

First Automated QKD Resynchronization

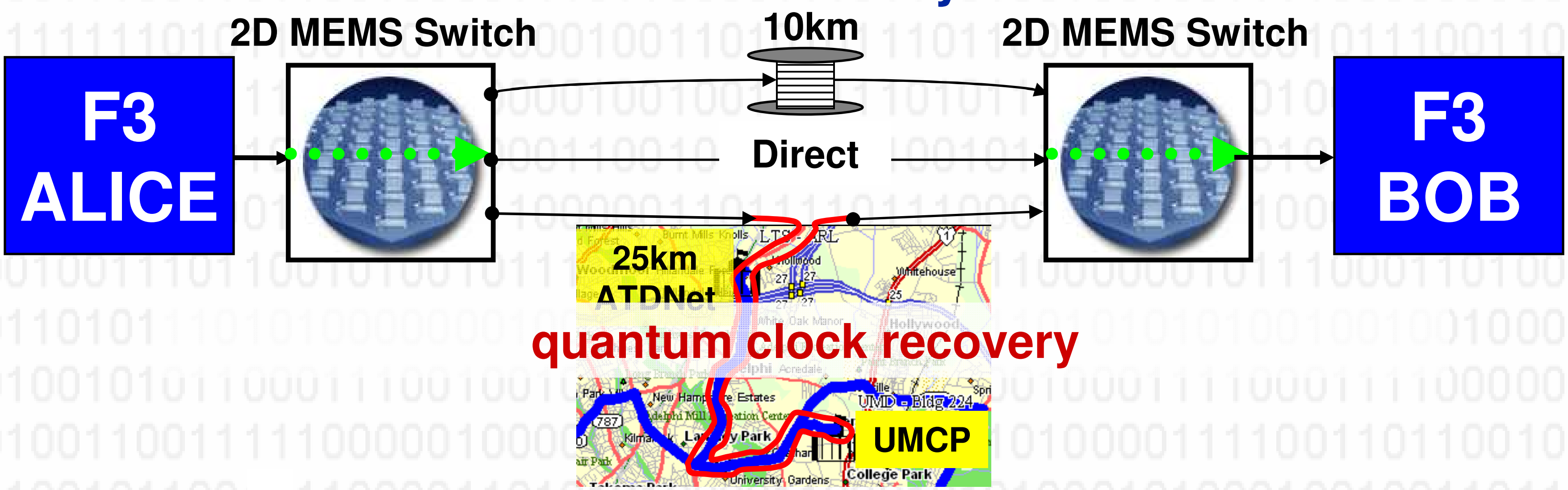


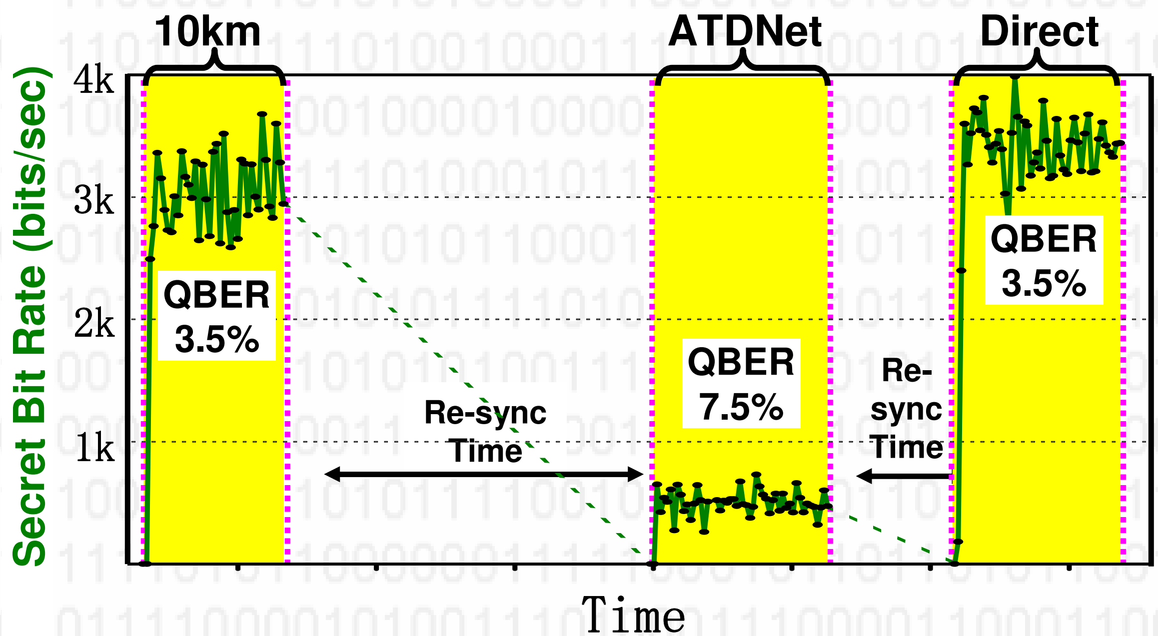


Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Telcordia Technologies
Los Alamos NATIONAL LABORATORY

First Automated QKD Resynchronization





Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

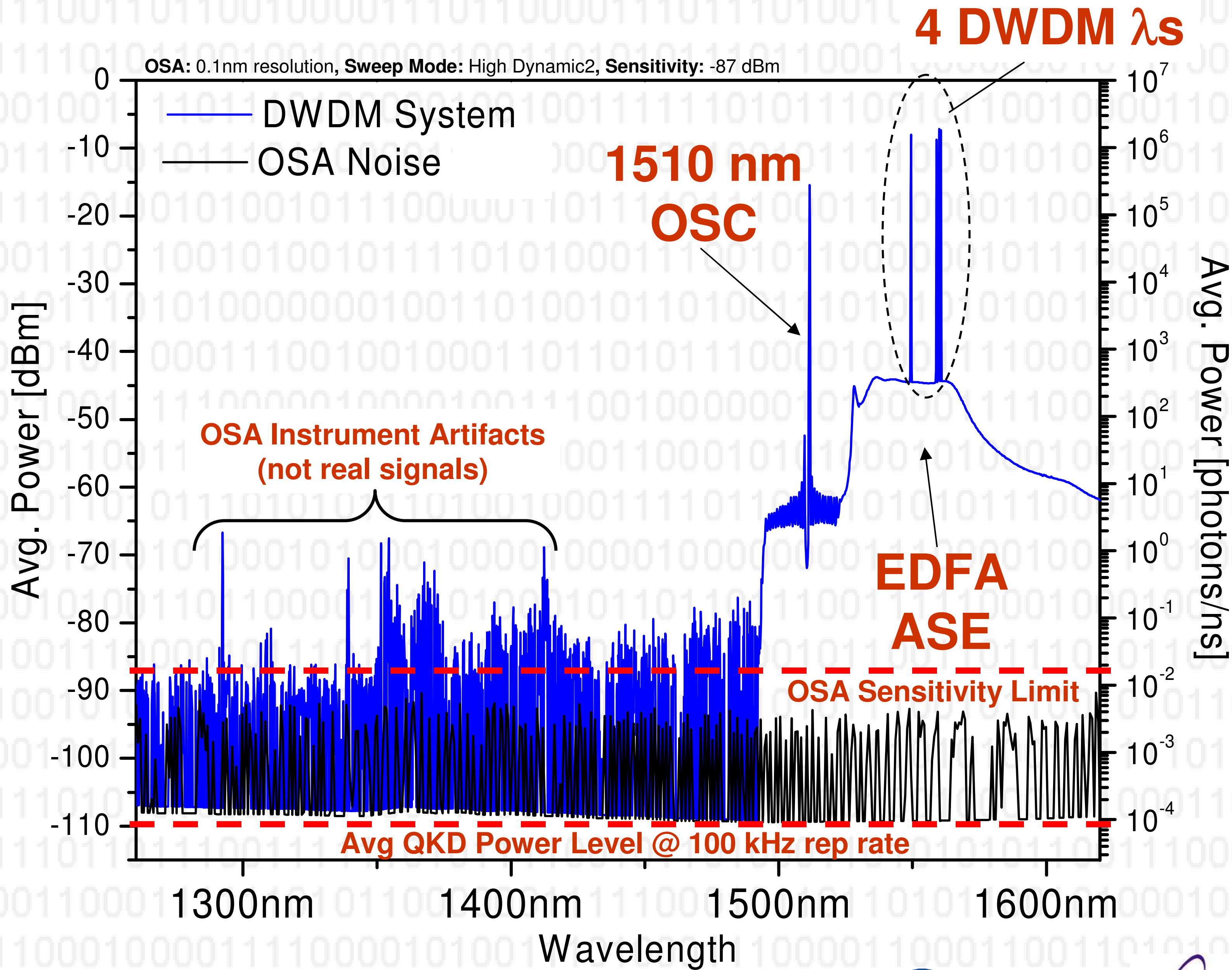
QKD Coexistence with classical channels

T.E. Chapuran, et al., *Proc. SPIE* ***5815, 164*** (2005)

- Coexistence: **An architecture where the quantum channel shares a common optical path with one or more classical optical channels**
  - Does not waste expensive infrastructure on low data rate channel
- **Separating classical and quantum channels is a challenge!**
  - Single photon detectors integrate energy over a very broad optical spectrum
  - **Classical and quantum signals differing in average power by 11 orders of magnitude!**
- **In-band quantum channel noise sources may include:**
  - Broadband ASE noise from optical amplifiers such as EDFAs
  - Broadband spontaneous emission noise from optical data channel lasers
  - Cross-talk from classical channels through components such as filters and optical switch fabrics
  - Nonlinear mixing and scattering processes among channels in common optical path

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Noise in DWDM Optical Systems

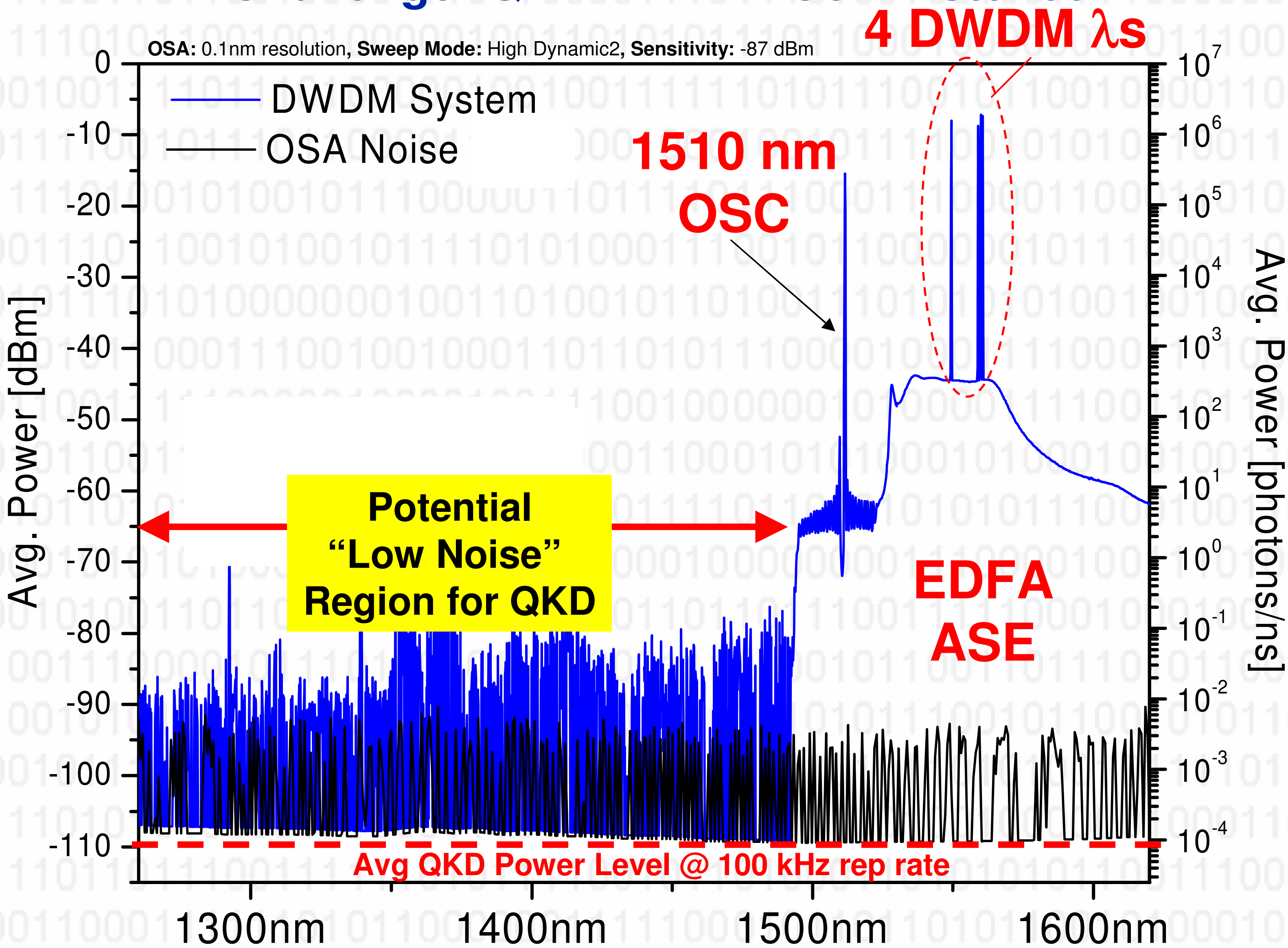


Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Telcordia Technologies

Los Alamos NATIONAL LABORATORY

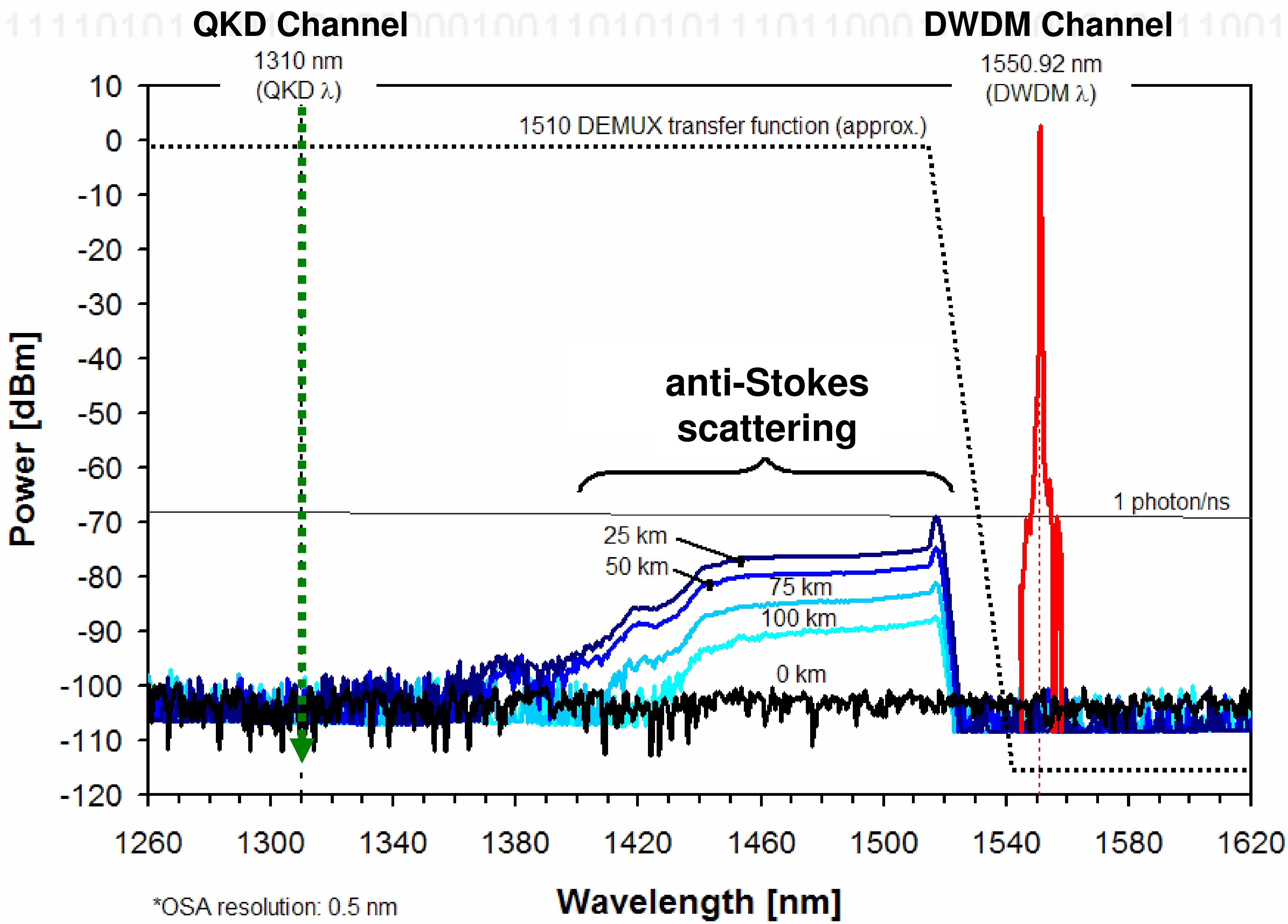
Challenge: QKD+DWDM Co-Existence



T.E. Chapuran, et al., *SPIE Defense and Security Symposium*, March 30, 2005.

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Anti-Stokes Noise Generated by Scattering in Fiber

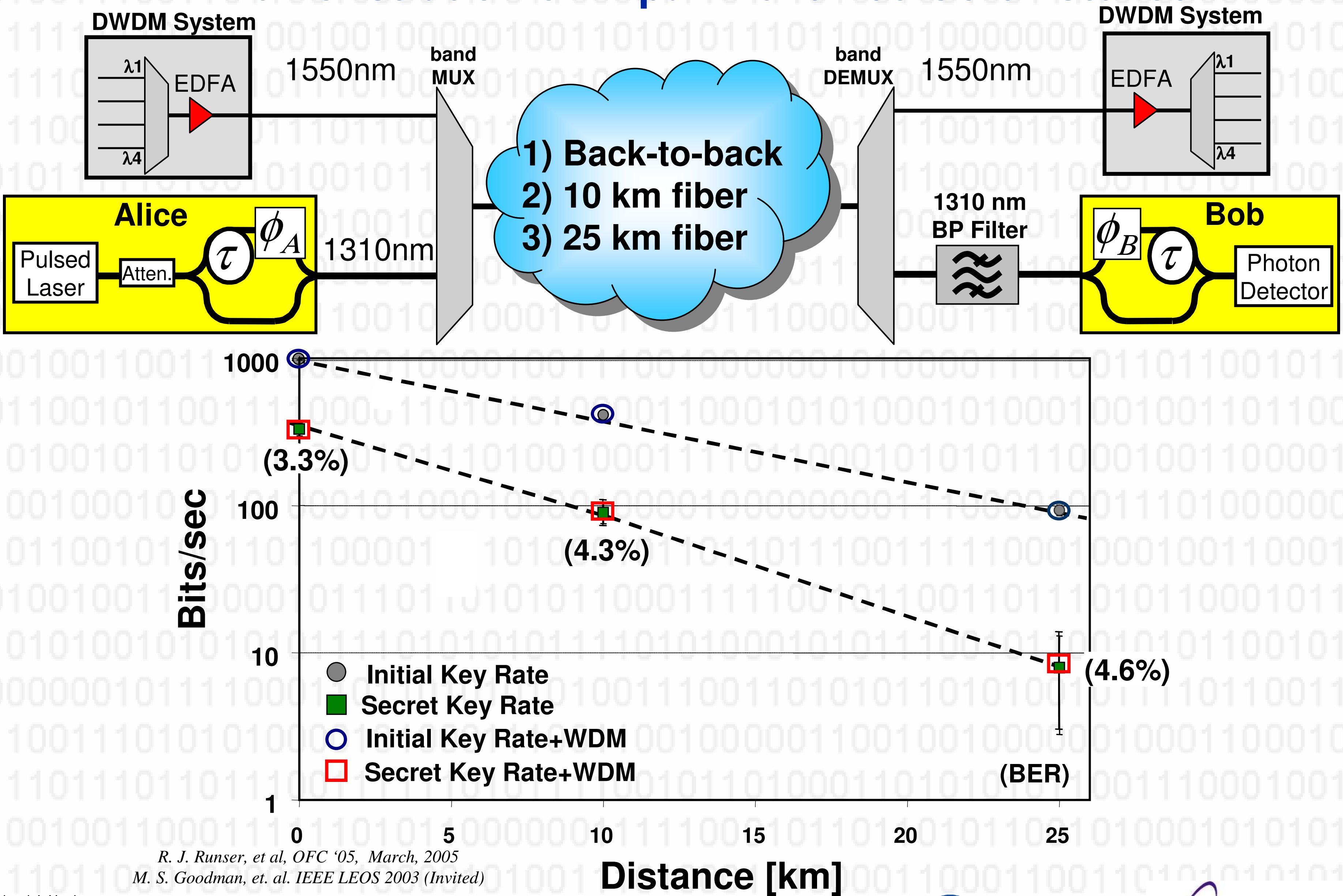


Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Telcordia Technologies

Los Alamos NATIONAL LABORATORY

Demonstration of Impairment-free Co-existence



R. J. Runser, et al, OFC '05, March, 2005
M. S. Goodman, et. al. IEEE LEOS 2003 (Invited)

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Summary and Conclusions

- **QKD has come of age: the first quantum information application**

- **QKD-optimized detectors and new protocols greatly extend the scope**
- **e.g. TES detectors enable longer distances/higher security for optical fiber QKD**
  - Future work
    - Use decoy state protocol with TESs to extend unconditionally secure transmission distance to greater than 150 km.
    - Detector development
      - Higher efficiency
      - Improved filtering of blackbody radiation
      - Faster devices (approaching MHz in the short term)

- **QKD in all-optical networks shows great promise**
  - engineered F3b system under development at 1310nm

- **outlook for QKD basic research is very bright**
- **outlook for commercial QKD … will anyone use it ?**

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Collaborators

Nick Dallmann, Jim Harrington, Phil Hiskett, RJH, Kevin McCabe, Jane Nordholt, Nick Olivas, Glen Peterson, Pat Rice, Danna Rosenberg
and
Kush Tyagi
Los Alamos National Laboratory

Sae Woo Nam, Aaron Miller and A. Lita
NIST-Boulder

Robert Runser, Paul Toliver, Tom Chapuran, Tom Banwell, Janet Jackel, Jeff Young, and
Matt Goodman
Telcordia Technologies

Scott McNown, Nnake Nweke, and
Dave Hardesty
Laboratory for Telecommunication Sciences

Linden Mercer and Hank Dardy
Naval Research Laboratory

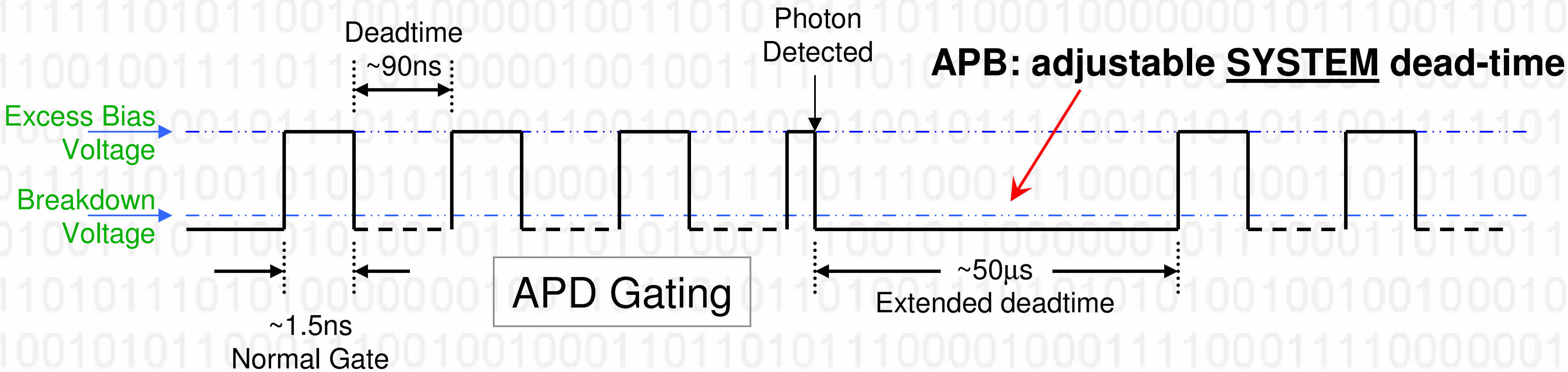
+ Jill McCracken

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

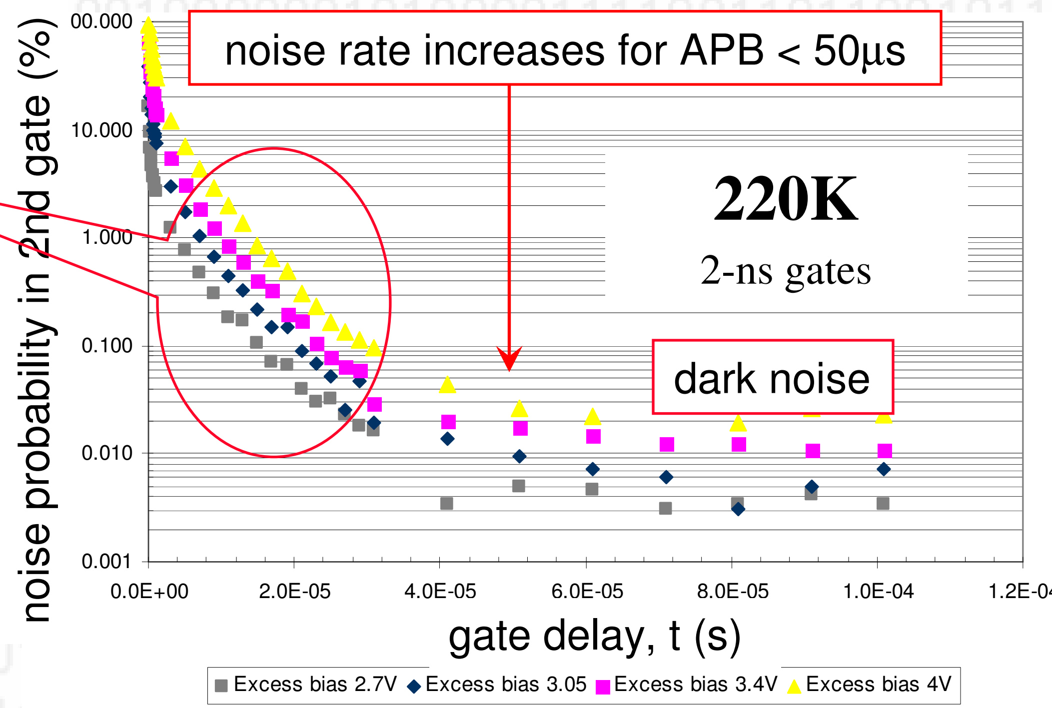
BACKUP SLIDES

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

F3a after-pulse blocking: high-clock rates w/o high noise



- **allows x50 clock rate from 20kHz to 10 MHz**
  - higher secret bit rate
- **BUT, max sift rate is 10 kbps for APB = 50 µs**

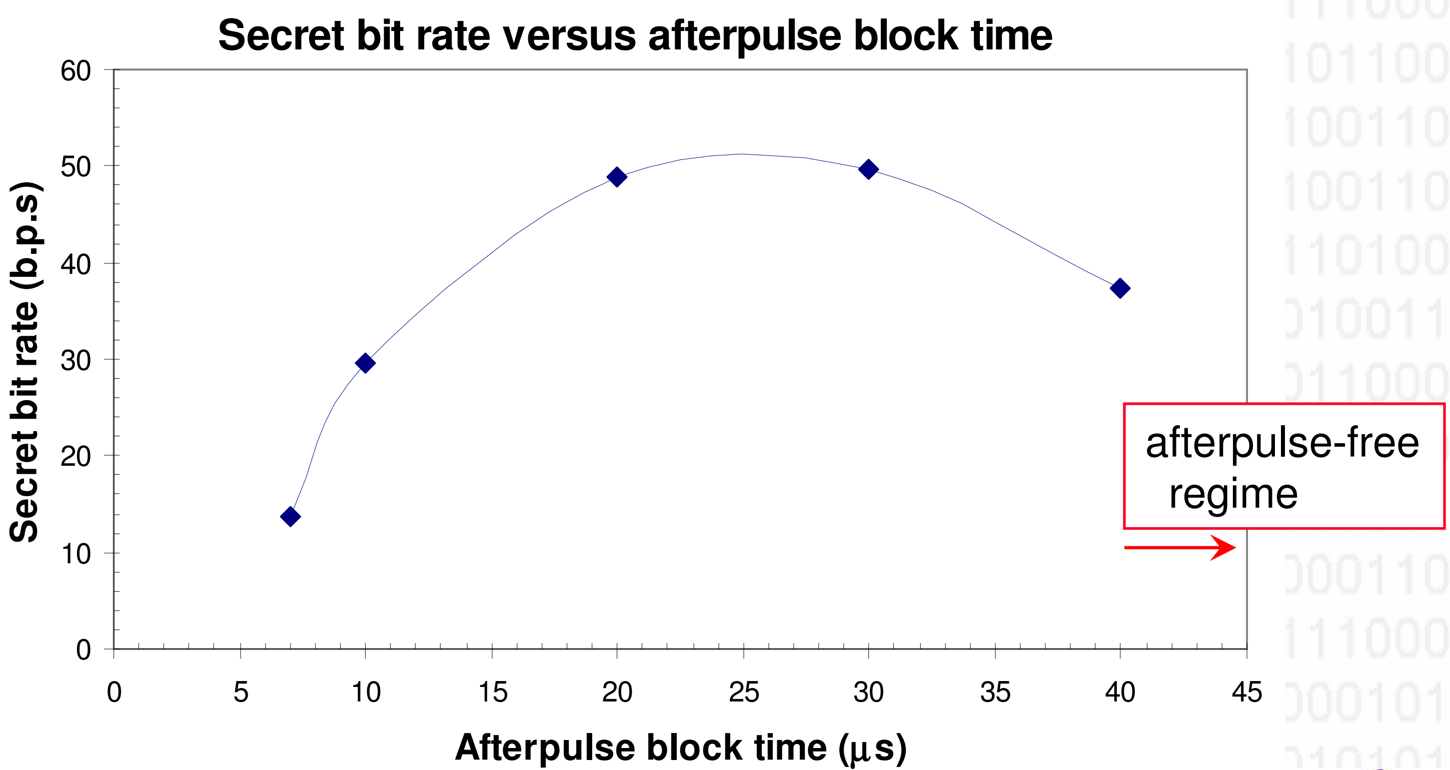


Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Los Alamos NATIONAL LABORATORY

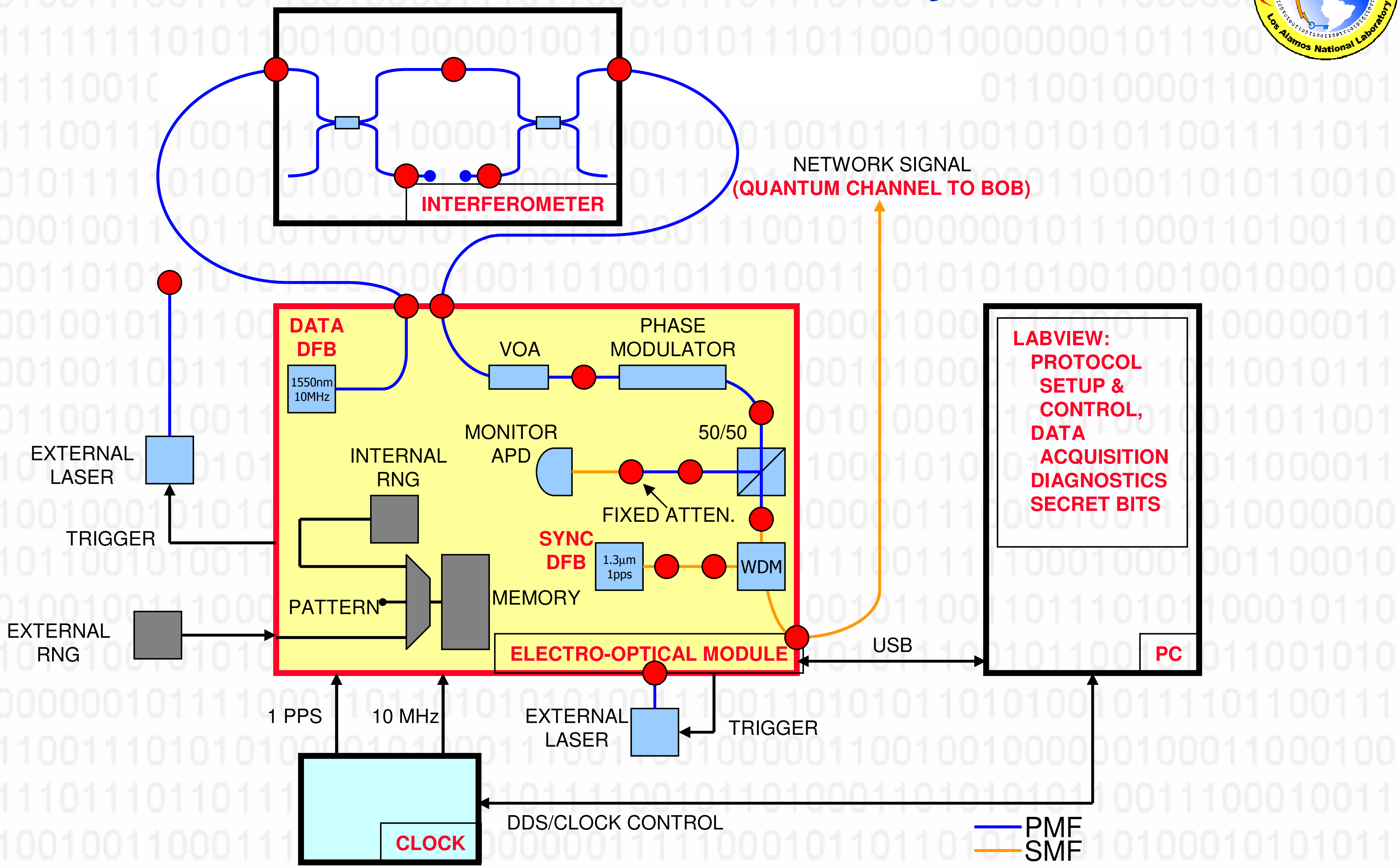
F3a: secret bit rate dependence on afterpulse blocking time 50km dark fiber; 1MHz clock; μ = 0.1

- **optimal secret bit yield is attained in regime with some afterpulsing**
  - reduced dead time results in more sifted bits at modest cost in BER … up to a point



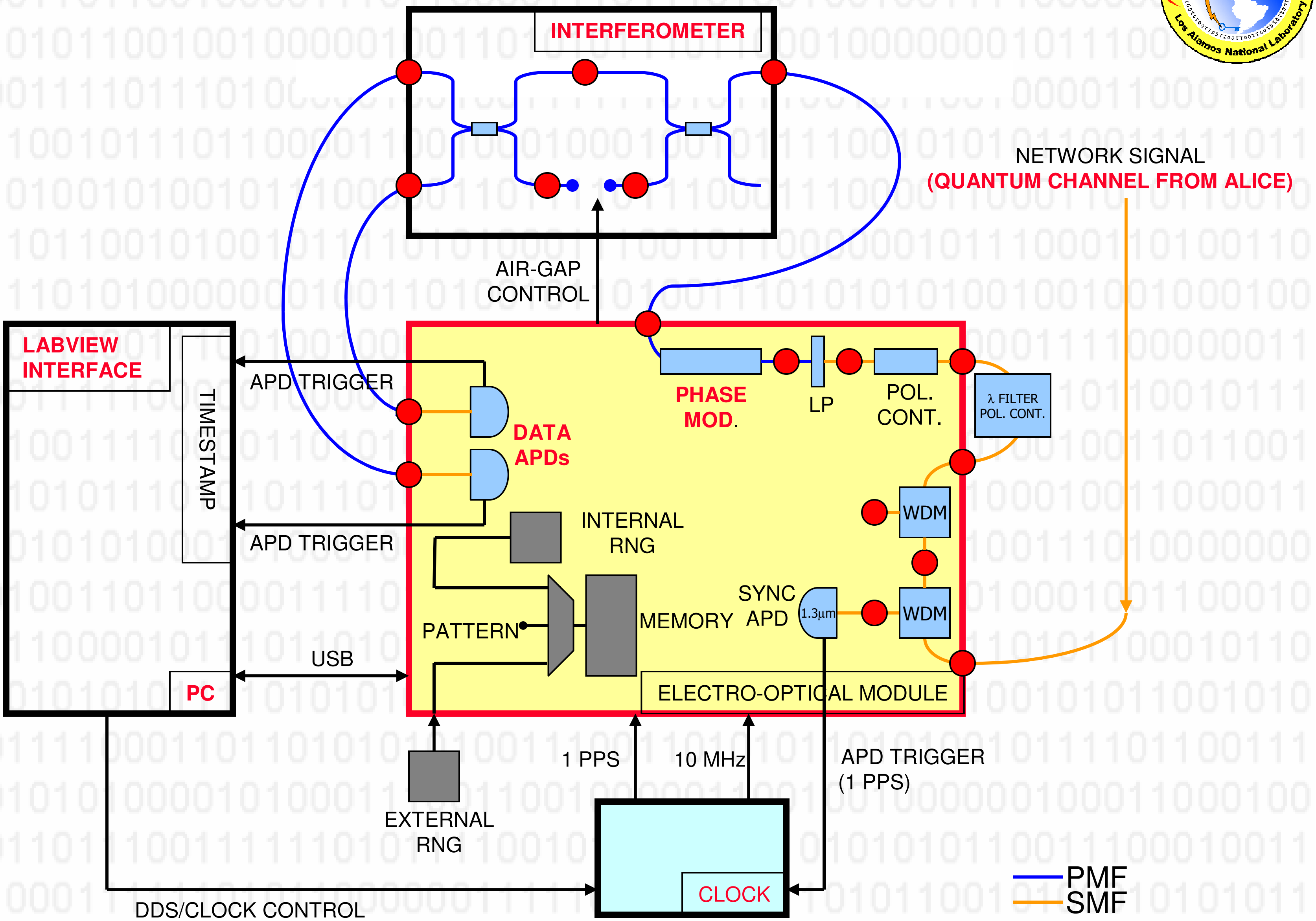
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

F3a "Alice": functional layout



Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

F3a Bob functional layout



Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov