LA-UR-04-8691

QUANTUM KEY DISTRIBUTION
THE SCIENCE OF SECRET COMMUNICATIONS

Richard J. Hughes
Physics Division
Los Alamos National Laboratory

ABSTRACT

Quantum key distribution (QKD) uses single photon communications to securely transfer cryptographic keys that are required for secure communications. I will describe the theory of QKD and its implementation in both optical fiber and free-space.

LA-UR-04-8691

Quantum key distribution
the science of secret communications

Richard Hughes
Physics Division
Los Alamos National Laboratory
505-667-3876; hughes@lanl.gov; http://quantum.lanl.gov

cryptographic key transfer by quantum (single-photon) communications:

- **overview of quantum information and cryptography**
- **the BB84 QKD protocol**
- **QKD in practice**
  - **in optical fiber**
  - **in free-space**

Quantum information ?

THEN

- **E. Schrödinger, Br. J. Philos. Sci. III, August 1952:**

"…**we never experiment with just one electron or atom** or (small) molecule. In thought experiments we sometimes assume that we do; this invariably entails ridiculous consequences. … In the first place it is fair to state that we are not experimenting with single particles, any more than we can raise Icthyosauria in the zoo."

and NOW

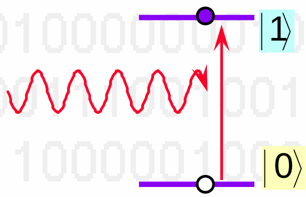
- **"… it seems that the laws of physics present no barrier to reducing the size of computers until bits are the size of atoms, and quantum behavior holds sway." R. P. Feynman (1985)**

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

Los Alamos
NATIONAL LABORATORY

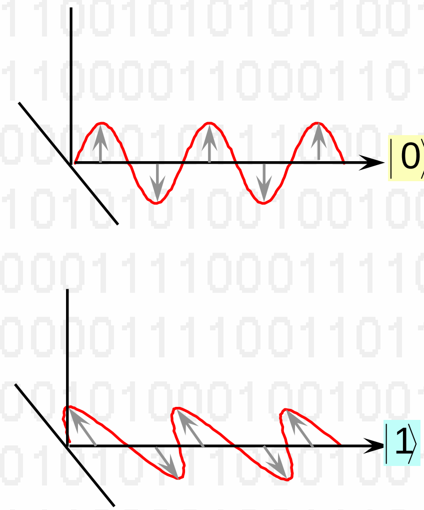
Quantum bits = “qubits”

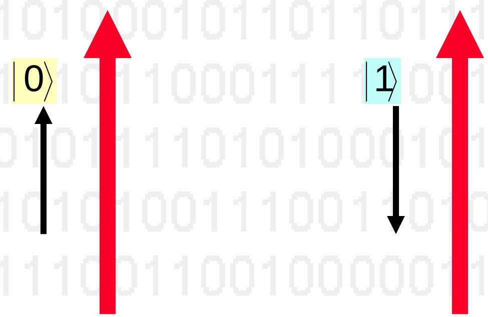
- **a single bit of information can be represented by a two-state quantum system**
  - a **“qubit”**



- **an atomic electron**

- **a polarized photon**





- **a spin in a magnetic field**

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

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)

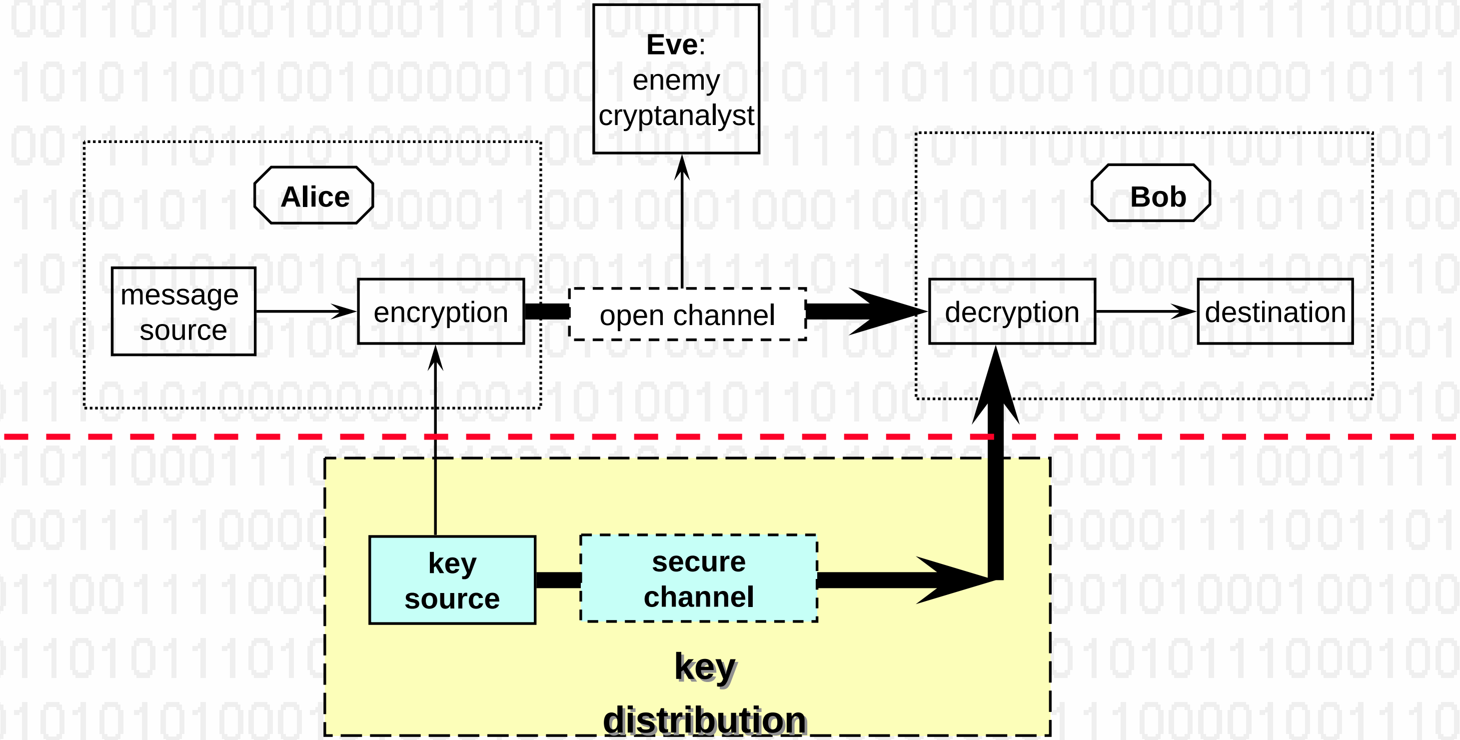
International Conference on Computers, Systems & Signal Processing Bangalore, India December 10-12, 1984

"When elementary quantum systems … are used to transmit digital information the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media." (1984)

first commercial (fiber) QKD systems: 2003

LA-UR-04-8691
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

(Quantum) Key Distribution



- **quantum key distribution = on-demand key transfer by quantum communications**
  - **detectability and defeat of eavesdropping ensured by laws of physics & information theory**
  - avoids latent vulnerability of public key broadcasts, and advent of quantum computers
    - passive monitoring ineffective
    - "today's quantum cryptography transmissions not vulnerable to tomorrow's technology"
  - reduces insider concerns: key material does not exist until transmission time
  - compatibility with optical communications/existing & planned infrastructures

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

Secrecy: the "one-time pad"

G. S. Vernam, Trans AIEE 45, 295 (1926)

- **key material is a (truly) random** bit **sequence**
  - XOR=⊕ = addition (mod 2) = binary addition without carry
- unconditionally secure
  - provided key is not reused
- key is as long as the message

Alice encrypts

plaintext	...A	= ...10000010
⊕key		...00110110
ciphertext		...10110100
		= ...Z

open channel

Bob decrypts

ciphertext	...10110100
⊕ key	...00110110
plaintext	...10000010

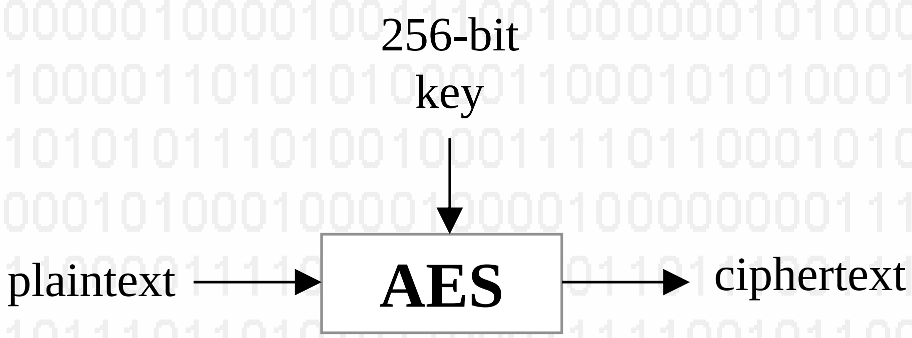
for surveys on confidentiality and authentication, see

"Contemporary Cryptology" G. J. Simmons ed., IEEE (1992)

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

Practical secrecy: symmetric key cryptography

- **“practical secrecy”: “very, very hard to break, and thoroughly analyzed”**
  - e.g. NIST’s Advanced Encryption Standard, AES



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

Quantum Key Distribution (QKD) is evolving along dual tracks:
Shannon (1949):“theoretical secrecy” & “practical secrecy”

theoretical secrecy

Bennett-Brassard 1984
authentication + quantum communications + information theory = QKD

heritage

new security paradigm

“unconditional security”

practical secrecy

computational security

influx

capability enhancement ?

future secure communications needs

QKD today

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

C. E. Shannon, Bell Syst Tech J 28, 656 (1949)

QKD (“1st and 2nd waves”)

FIRST QKD PROTOCOL
Bennett & Brassard (1984)

FIRST QKD EXPERIMENT
Bennett et al.(1991)

QKD FIBER EXPERIMENTS
Rarity, Townsend et al. (UK, > 1994)
Franson et al. (APL, 1994)
Gisin et al. (Geneva, > 1995)
Hughes et al. (LANL > 1995)
Bethune et al. (IBM > 1999)
Karlsson et al. (Stockholm > 2000)
Polzik et al. (Denmark > 2001)

FREE-SPACE EXPERIMENTS
Franson et al. (1996)
Hughes et al. (LANL > 1996)
Rarity et al. (UK > 2000)

ENTANGLED-PHOTON QKD
Ekert (1991)
Gisin et al. (Geneva, > 2000)
Zeilinger et al. (Austria, 2000)
Kwiat et al. (LANL, UIUC > 2000)

“SINGLE-PHOTON” QKD
Yamamoto et al. (2002)
Grangier et al. (2002)

CONTINUOUS VARIABLE QKD
Grangier et al. (2002)
…

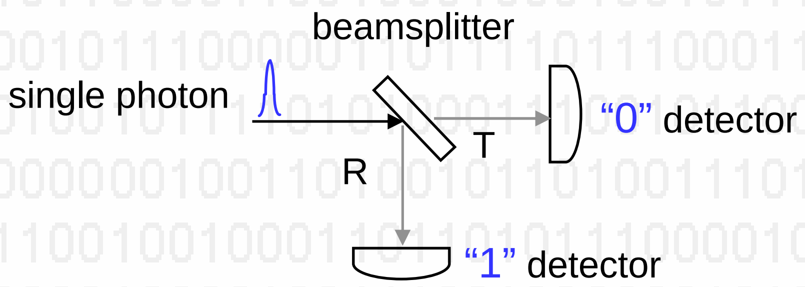
2nd wave

“THIRD WAVE”
non-QKD protocols

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

Quantum mechanics of ideal single photons & detectors

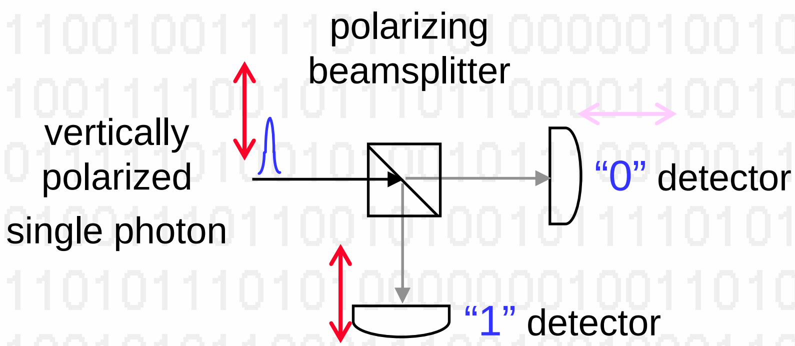
- a single photon cannot be split



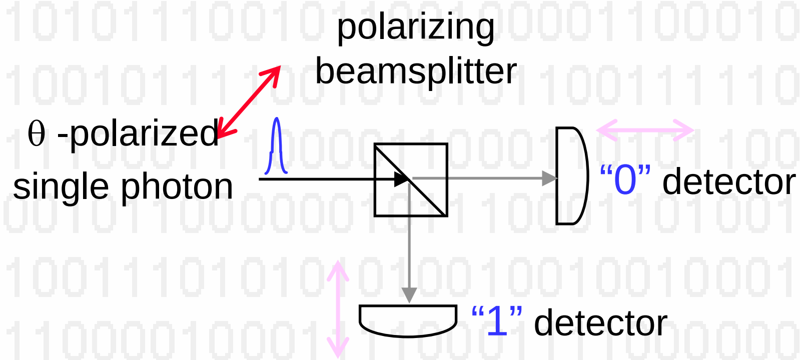
- **EITHER detector "0" fires OR detector "1" fires**
  - not both
- **we cannot predict, even in principle, which detector will fire**
  - irreducible randomness of quantum physics

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

Quantum mechanics & (linearly) polarized single photons



- **detector "0" <u>never</u> fires**
- **detector "1" <u>always</u> fires**



- **detector "0" fires with prob = $\cos^2\theta$**
- **OR, "1" fires with prob = $\sin^2\theta$**
  - <u>not both</u>
  - <u>we cannot predict which one</u>

implications

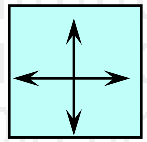
- **<u>orthogonal</u> polarization can be distinguished**
- **non-orthogonal** polarizations cannot be faithfully distinguished
- after **measurement** a photon has no "memory" of its prior polarization
- **[non-orthogonal** polarizations cannot be faithfully copied ("no cloning")]

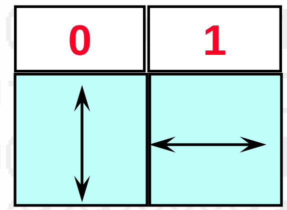
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

“Conjugate coding”

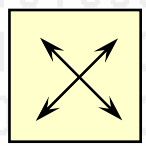
S. Wiesner, SIGACT News 15(1), 78 (1983)

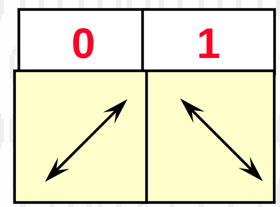
- **a bit of information can be encoded in <u>orthogonal</u> polarization states of single photons, in different bases:**
- **e.g. in the rectilinear basis**





- **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 <u>random</u>**

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

The core ingredients of the BB84 QKD protocol (I)

- **Alice has two sources of random bits**
  - long-term secret data bits
  - independent, short-term secret encoding bits

- **Bob has an independent source of short-term secret random decoding bits**

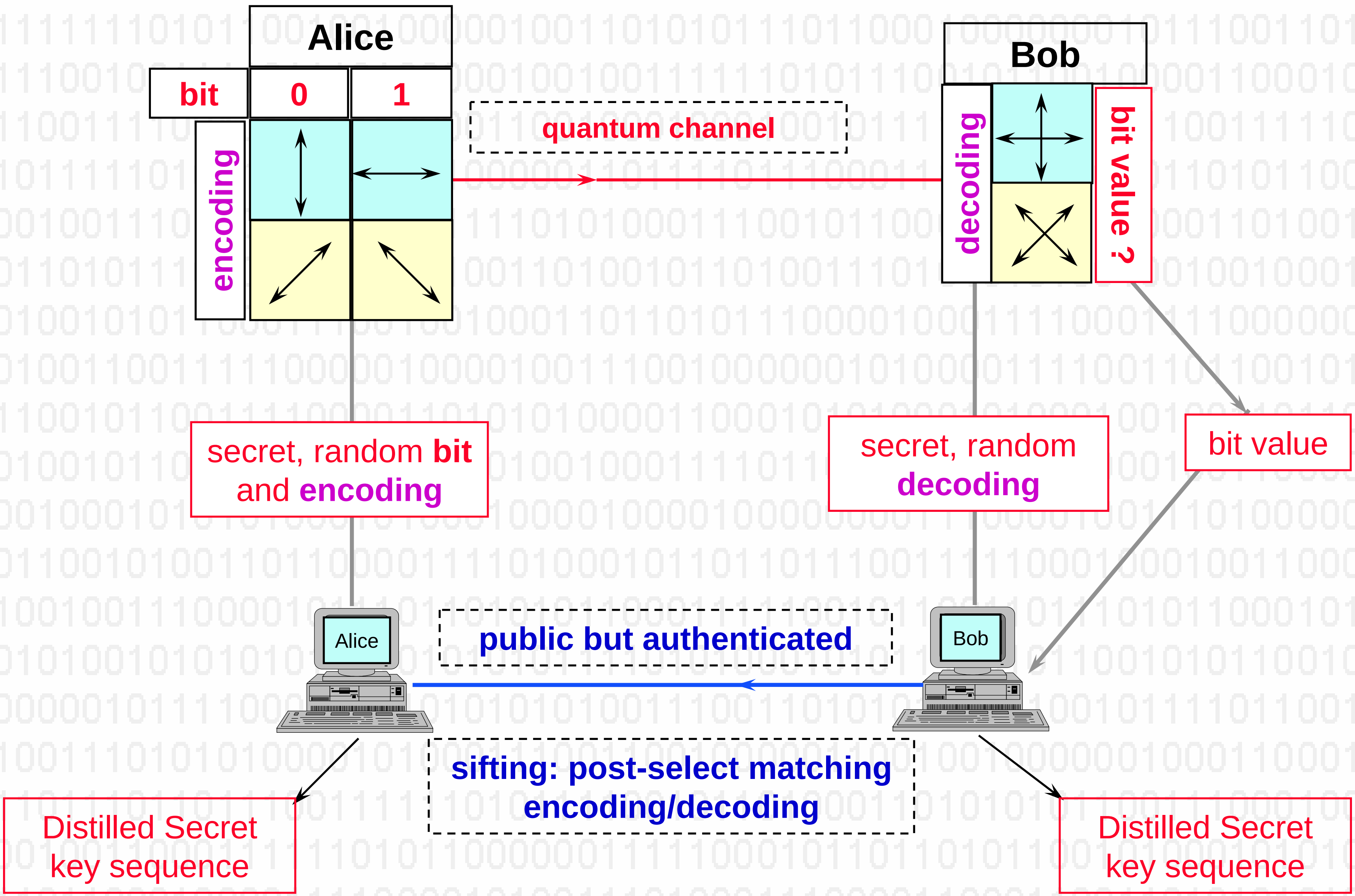
- **they have a quantum channel**
  - allows the faithful transmission of polarized single photons

- **they have a means to perform conjugate encoding and decoding**
  - ideal single photon sources and detectors

- **they have an authenticated, but non-secret, conventional public channel**
  - they know they are communicating with each other, and not an impersonator ("Eve")
  - they know that Eve has not substituted her own messages

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

Core ingredients of the BB84 (QKD) Protocol (II)



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

An example of BB84

Alice data bit	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**1**
Alice basis	+	+	×	+	×	×	×	+
A→B quantum	↔	↕	⤢	↕	⤡	⤡	⤢	↔
Bob basis	+	×	×	×	+	+	×	+
Bob detects	1	0/1	0	0/1	0/1	0/1	0	1
B→A public	R	D	D	D	R	R	D	R
A→B public	Yes	No	Yes	No	No	No	Yes	Yes
sift	**1**		**0**				**0**	**1**

- **Alice and Bob now share 4 random ("sifted") bits**

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

Points to note

From Alice and Bob's perspective:

- **on average the protocol is 50% efficient**
- **Alice and Bob cannot predict which bits they will share**
  - sifted key is a random sequence of random bits
- **only photons that arrive can enter the sifted key**
  - photon loss reduces the key rate
- **in practice other photons may enter the quantum channel**
  - source of errors ?

From Eve's perspective

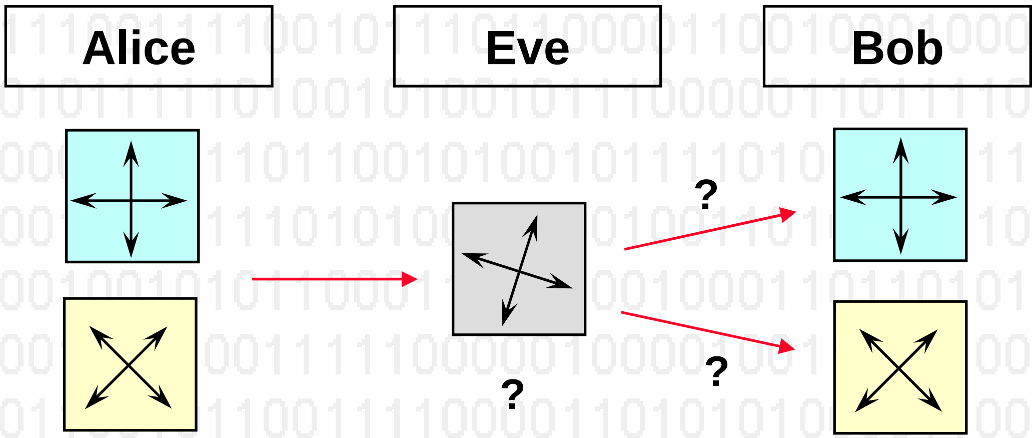
- **cannot passively monitor the quantum channel: a photon cannot be split**
  - no possibility of storing information for future analysis
- **public channel conveys no information about the (secret) data bits**
- **cannot perform a man-in-the-middle attack**
  - public channel is authenticated
- **use quantum physics methods to distinguish the quantum channel states?**

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

(Intercept-resend) eavesdropping on QKD ?

C. H. Bennett et al., J. Crypto 5, 3 (1992)

- **Eve inserts a polarizer at angle θ ?**



e.g. Alice sends “V”, Eve tests “θ”
- P(Eve correct) = $\cos^2\theta$
  - sends Bob θ
- P(Eve wrong) = $\sin^2\theta$
  - sends Bob (90°–θ)

- e.g: Eve tests randomly in the rectilinear and diagonal bases: on average
  - learns 50% of Alice’s bits
  - has 50% bit error rate (BER) on the rest
- once she learns the basis information

- **impacts:**
  - **Eve can only gain <u>partial</u> information**
    - **deterministic or probabilistic**
  - **necessarily causes a disturbance**
    - **Bob has a 25% BER if Eve tests every bit**

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

Bisective search interactive error correction: "BINARY[1]"

Alice

1 1 0 1 1 0 0 0 1 0 1 1

A → B : ⊕ = 1

1 1 0 1 1 0 | 0 0 1 0 1 1

A → B : ⊕ = 1

1 1 0 | 1 1 0

⊕ = 0

1 1 | 0

⊕ = 0

1 | 1

⊕ = 1

1

Bob

1 1 0 1 0 0 0 0 1 0 1 1

⊕ = 0

1 1 0 1 0 0 | 0 0 1 0 1 1

⊕ = 1

1 1 0 | 1 0 0

⊕ = 1

1 0 | 0

⊕ = 1

1 | 0

⊕ = 0

X → 1

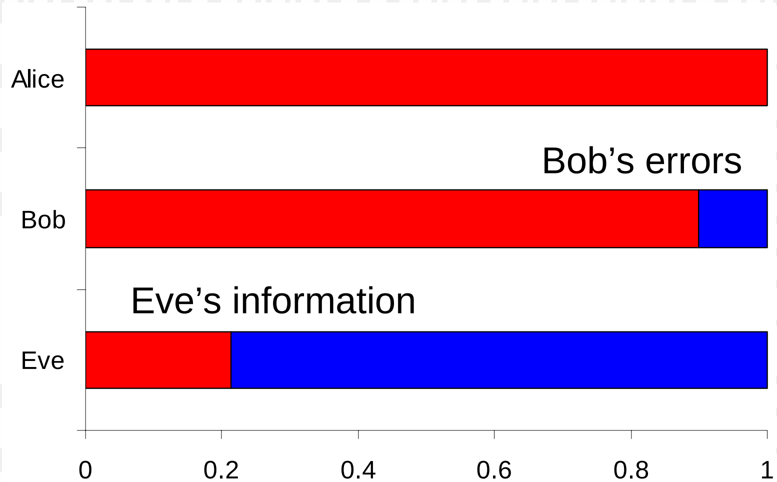
[1] C. H. Bennett et al. J. Crypto 5, 3 (1992)

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

Los Alamos
NATIONAL LABORATORY

Eavesdropping on QKD can be detected and defeated

- **Eve may only obtain partial information by testing Alice's photons**
- **and at the price of introducing errors into Bob's key:**



- **Alice and Bob can upper bound Eve's information after error correction**

- **using "privacy amplification" Alice and Bob 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**

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

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

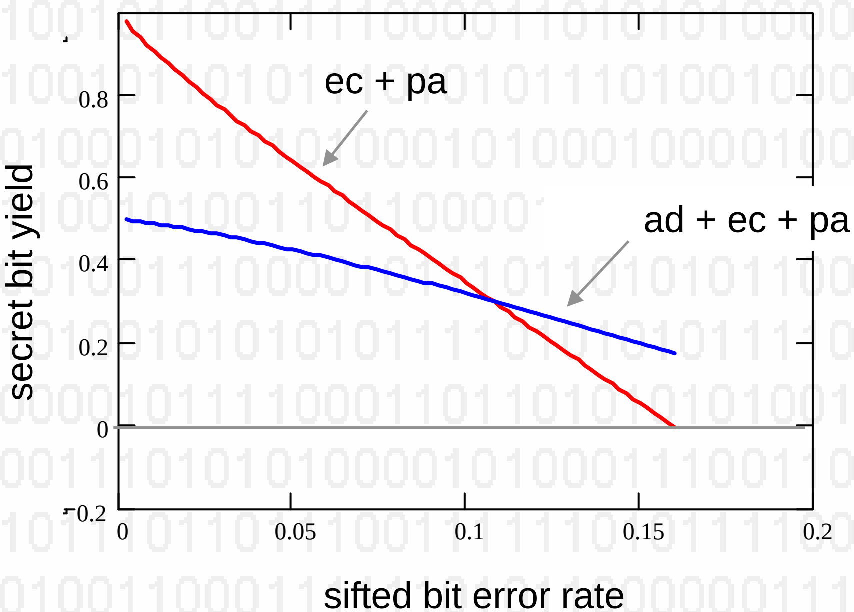
Los Alamos
NATIONAL LABORATORY

QKD link equation: an interplay between quantum physics and information theory

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

- secrecy efficiency: secret bits per initial bit
- transmission & detection: **physics** introduce errors
- protocol efficiency: **physics**
- error correction: **information theory** reveals side information
- privacy amplification: **information theory**

final secrecy efficiency



security attributes
either: <u>defeat</u> eavesdropping (up to a point)
or: <u>failsafe</u> (eavesdropping becomes DoS)
NB. tolerant of high quantum BERs

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

LA-UR-04-8691

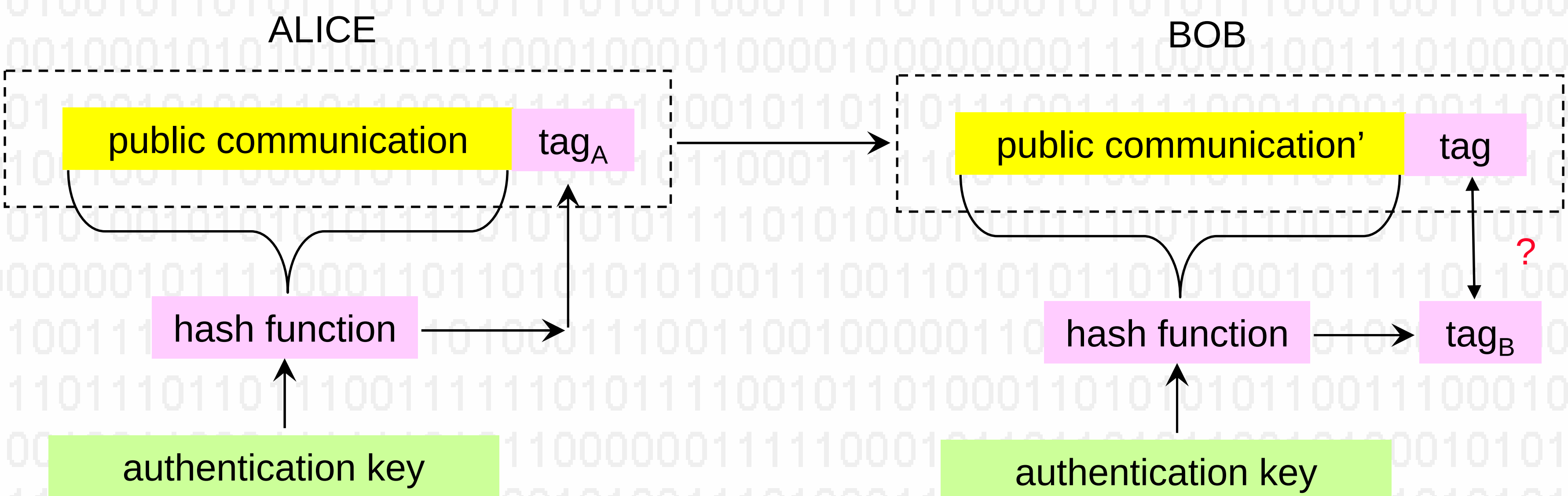
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Los Alamos NATIONAL LABORATORY

Unconditionally-secure Wegman-Carter authentication

M. Wegman and J. Carter, J. Comp Sys Sci 22, 265 (1981)

- **protection against “man-in-the-middle” ?**
  - Alice must know she is talking with Bob, and vice-versa
    - impersonation by Eve ?
  - authentication of public channel communications
    - substitution by Eve ?
  - Alice and Bob share a short (short-term) secret authentication key
    - compute a keyed hash; apply as authentication tag to messages
    - “cost” is small: logarithmic in # bits authenticated



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

NECESSARY INGREDIENTS of QKD

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

randomization
Alice generates a secret random bit sequence

↓

"conjugate coding"
Quantum transmissions from Alice to Bob

↓

sifting
Alice & Bob reveal their encoding/decoding

↓

reconciliation
error correction
+**estimatation**
Eve's information

→

privacy amplification
extract **secret bits**

↓

authentication
of public channel messages,
+**key confirmation**

↓

final, secret key

Security statement
- keys agree with overwhelming probability
- pass randomness tests
- Eve knows << 1 bit
- deception probability << 1

↓

cryptography

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

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

What does QKD offer ?

- "from one-time authentication to self-sustaining key distribution"
  - drastically narrows an adversary's scope & window of opportunity:
    - must break initial authentication in real-time and attempt an invasive "man-in-the-middle" attack ?

AUTHENTICATION → quantum communications + information theory → **KEY DISTRIBUTION**: exponentially-larger shared secret key

KEY DISTRIBUTION → **ENCRYPTION &/or AUTHENTICATION key**

short, shared initial secret key → **AUTHENTICATION**

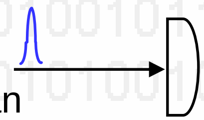
KEY DISTRIBUTION → replenish → **AUTHENTICATION**

- can only be attacked with "today's technology"
- immune to future quantum computers
- reduced insider threat ("passwords for chocolate")
- detectability and defeat of eavesdropping

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

Practical light sources, quantum channel & photon detectors

"single photon"
=
weak Poissonian



detector efficiency = η

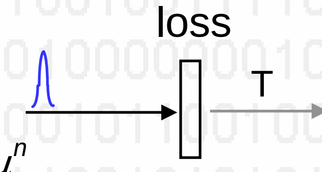
$$P(n) = \frac{e^{-\mu}\mu^n}{n!}$$

$$\langle n \rangle = \mu < 1$$

$$P_D = \left(1 - e^{-\mu\eta}\right)$$

sometimes send > 1 photon: security ?

sometimes don't detect it



$$P(n) = \frac{e^{-\mu}\mu^n}{n!}$$

$$P(n) = \frac{e^{-T\mu}(T\mu)^n}{n!}$$

$$\langle n \rangle = T\mu$$

"loss" = random partitioning

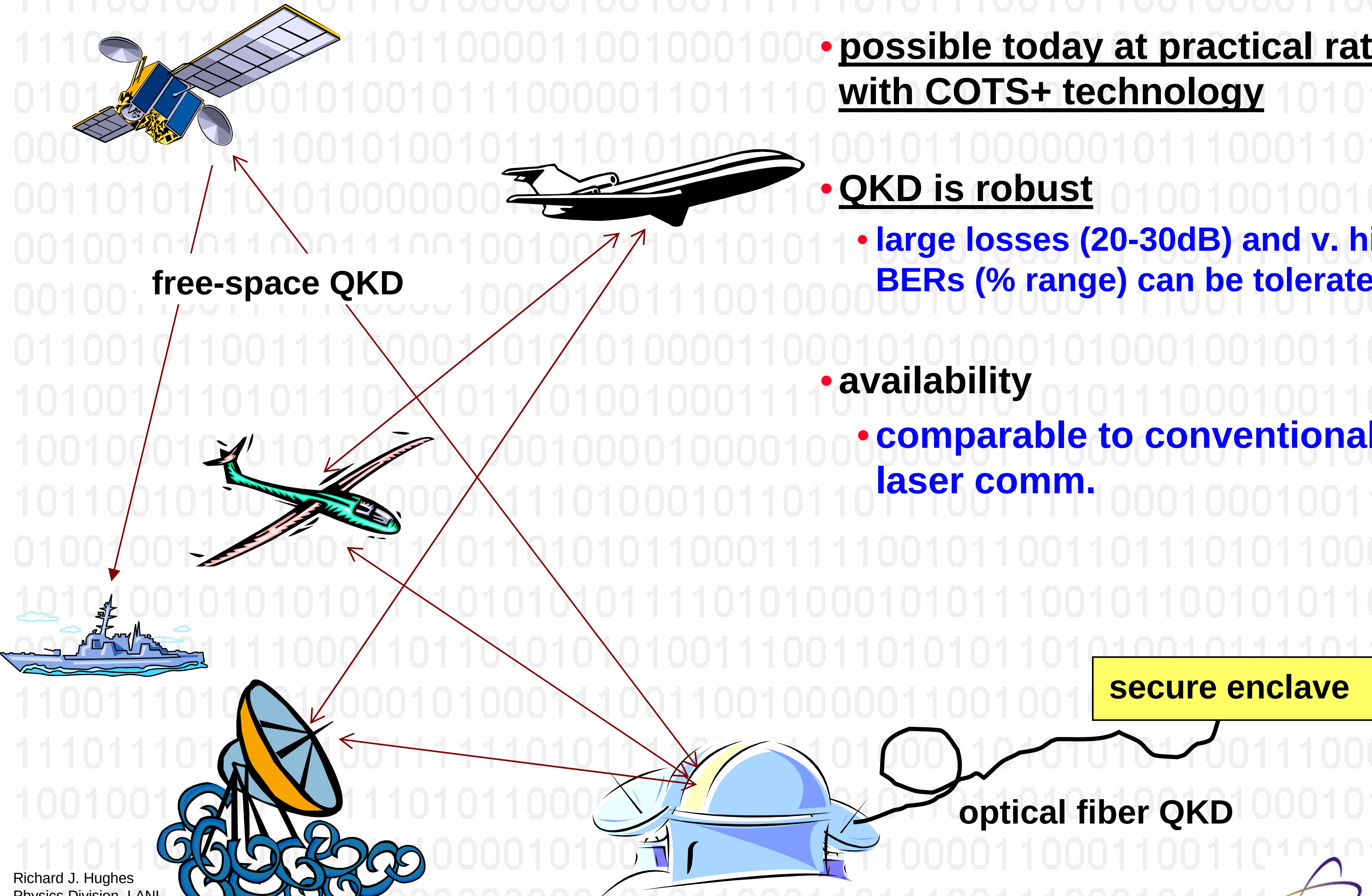
- no-photon fraction and loss make it harder for Alice and Bob
- multi-photon fraction & noise introduce new opportunities for Eve
- revised privacy amplification
- secret bit rate ?

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

Line-of-sight ("free-space") QKD would be especially useful

R. J. Hughes and J. E. Nordholt, Physics World, May 1999, 31.

- **possible today at practical rates with COTS+ technology**
- **QKD is robust**
  - **large losses (20-30dB) and v. high BERs (% range) can be tolerated**
- **availability**
  - **comparable to conventional laser comm.**



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

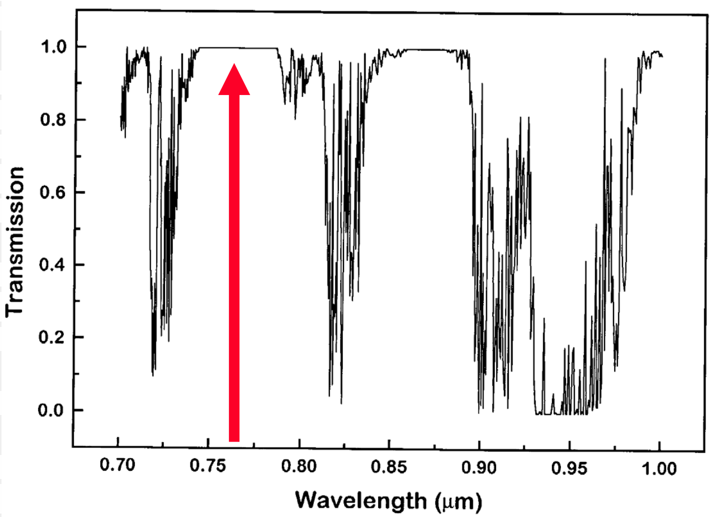
The atmospheric QKD quantum channel

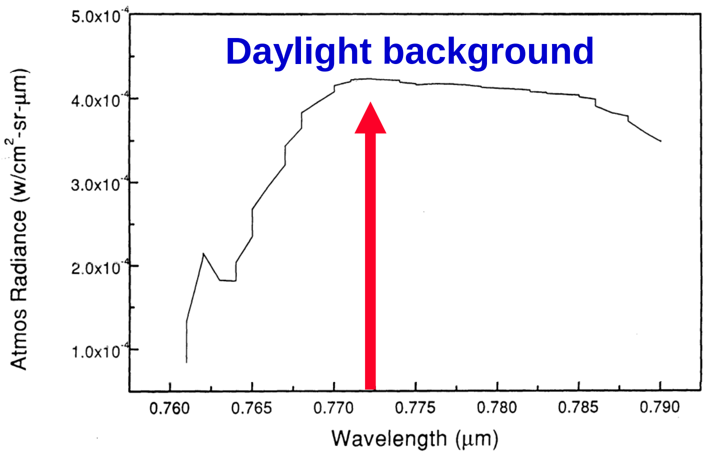
low-loss transmission wavelength; high-efficiency detectors

J. E. Nordholt et al., Proc SPIE 4635, 116 (2002)

- **secrecy efficiency as a function of wavelength:**
  - ~ 780 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} $Å^{-1}$ sr^{-1}
    - ~ 10^{-7} photons $mode^{-1}$
    - 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





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

Free-space quantum key distribution

R. J. Hughes et al., New Journal of Physics (www.njp.org) 4, 43.1-43.14 **(2002)**

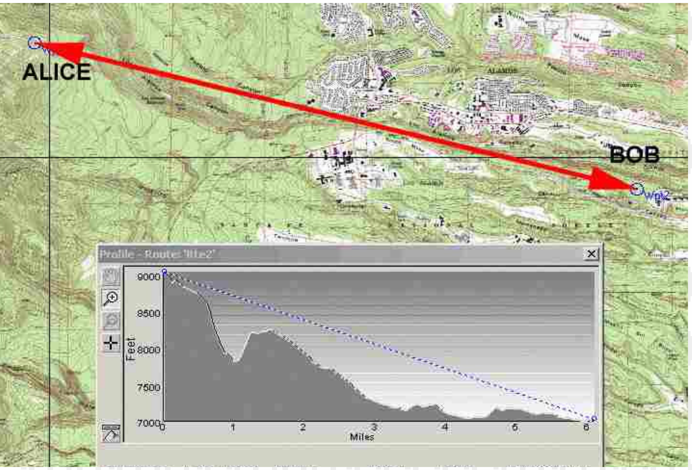
Sample of key material at 10-km range (day)

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

- 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

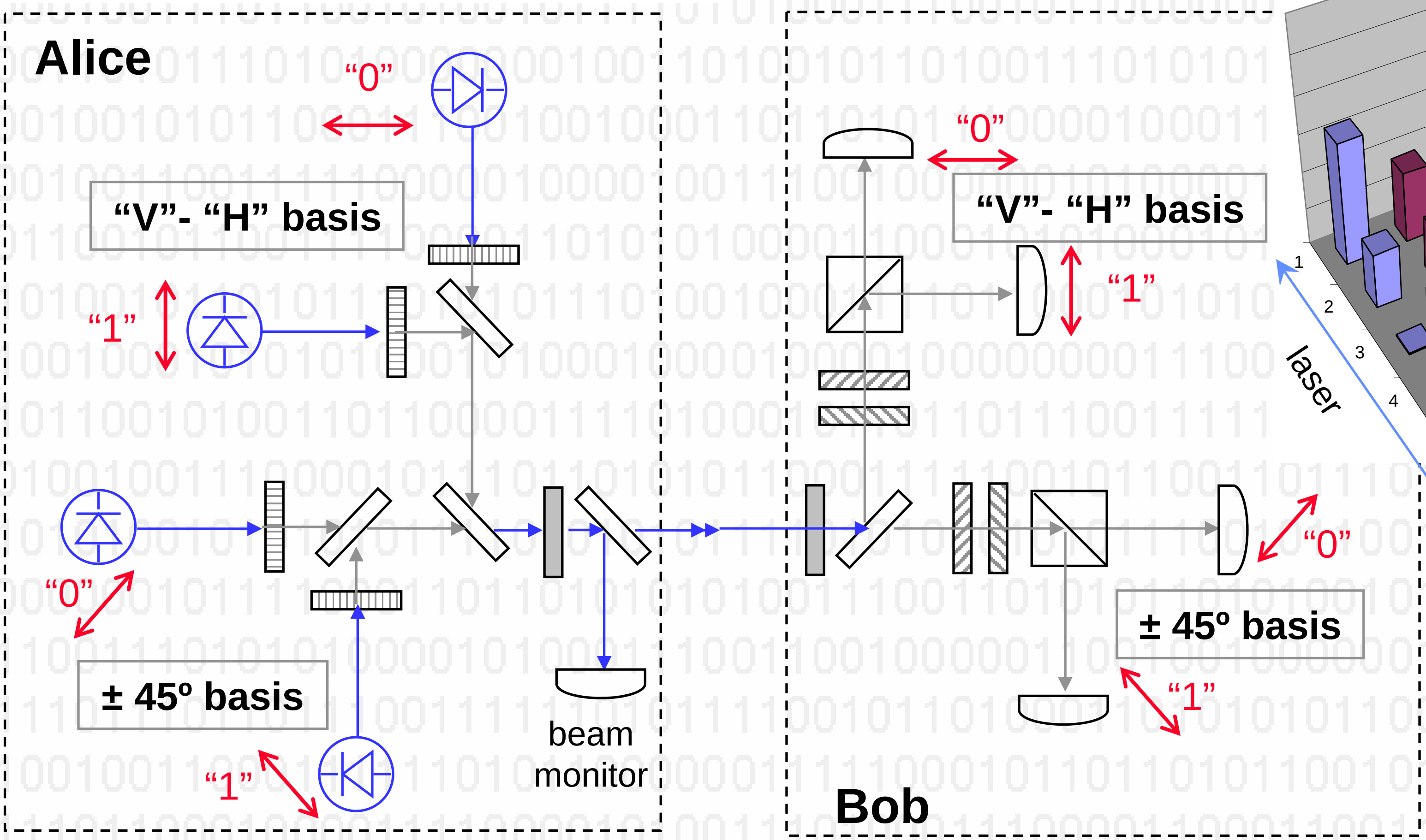


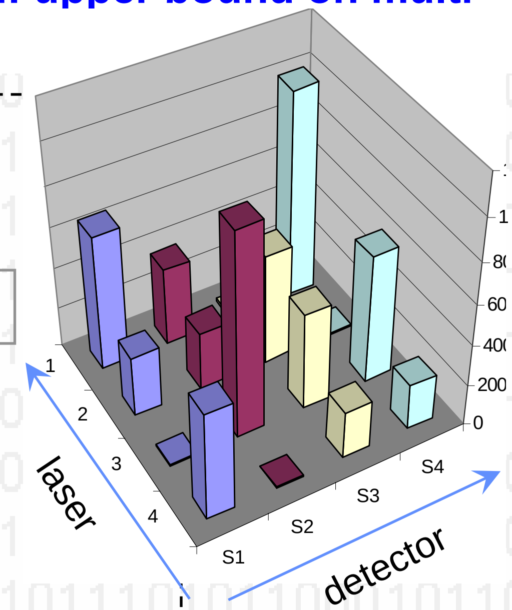
From Pajarito Mtn., Los Alamos, NM to TA53, Los Alamos National Laboratory

Receiver "Bob"

BB84 subsystem

- monolithic randomizer chip
  - **2-MHz clock rate → 1-MHz signal rate**
- **BB84 photons: attenuated 772-nm lasers**
  - 1-s quantum transmissions
- single-photon detectors: cooled Si APDs
  - passive quench; η~61%; dead time ~ 1 μs
- **quantum random number generation**
- **multi-detector system: upper bound on multi-photon pulses**



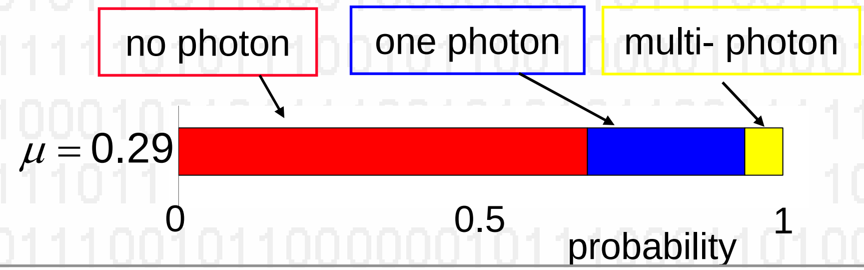


Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

From sifted bits to secret bits
e.g. in daylight from 18:40:26 - 18:40:27 MDT 4 October, 2001

In 1 s, from 10^6 transmitted bits with **photon number μ = 0.29** Alice and Bob produce **651 (partially secret) sifted bits** with **21 errors** (BER, ε = 3.2%):

00000110011000100100000101101000011001110010001111100010
00111100101100100110000101001100110001010110110110111110
00101010011111001111110111111011110110111100001010010001
00101011000011011000010110000100101110010100111001010011
11101110011000011100010000110111011100011100010100100010
01100011001011001111011111111000001111011011001100011100
10110100110100110100111010100010101100000101000111011011
11001110110111101001111100110010101101001110001110010101
00101000001101111001001000100111110111100100110100111100
11110011011000100010101110110010111111100000111111010110
11110100000111100110010110111010110111100011110101110010
000110000101011100101101100101101100



BBBSS91 privacy amplification[1]

Eve's entropy >

651 bits

-171 bits (multi-photon)

- 40 bits (intercept-resend)

-155 bits (side information: error correction)

- 2 bits (side information: bias)

- 20 bits ("safety factor")

= 264 bits (secret)

Alice's and Bob's 264-bit final secret key:

(produced as parities of random subsets)

101111000101010010001110110010010100000101010000
001111111011011010110101001101100001111011011111
000100101100010001100010001101110110110110011 1
100000111111010010110000100010010100111111011111
100101011111010111010001000010000000111101011010
011001100010110011101000101111 1000

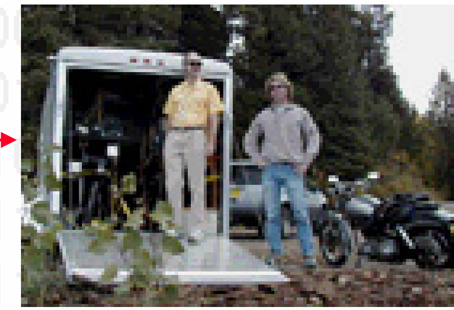
Eve's expected information < 10^{-6} bits

[1] C. H. Bennett et al. J. Crypto 5, 3 (1992)

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

One-time pad encryption of an image using final key (error correction, privacy amplification & check)

Encrypted Image



Alice encrypts

by adding a word of her key to each pixel

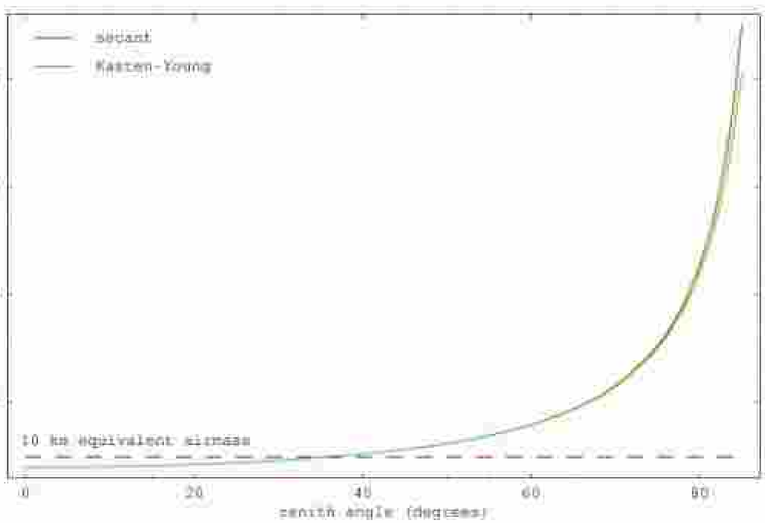
Bob decrypts

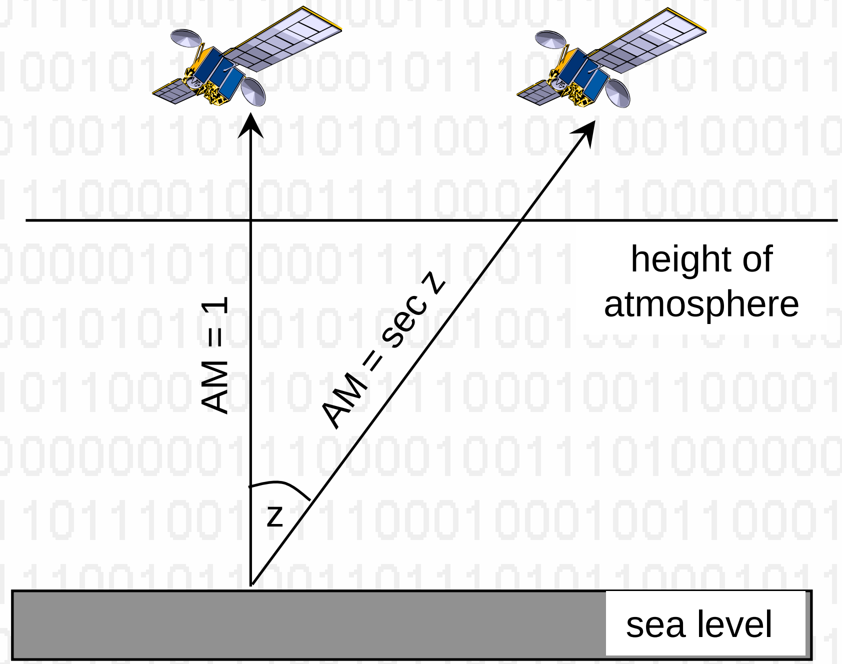
by subtracting a word of his key from each pixel

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

Atmospheric optics of 10-km path

- **10-km path has** **extinction** **(1 AM),** **background** **and** **capture efficiency** **comparable to a path to space**
  - "airmass": a measure of atmospheric extinction (and "seeing")
  - zenith path from Los Alamos has ~ 0.8 AM

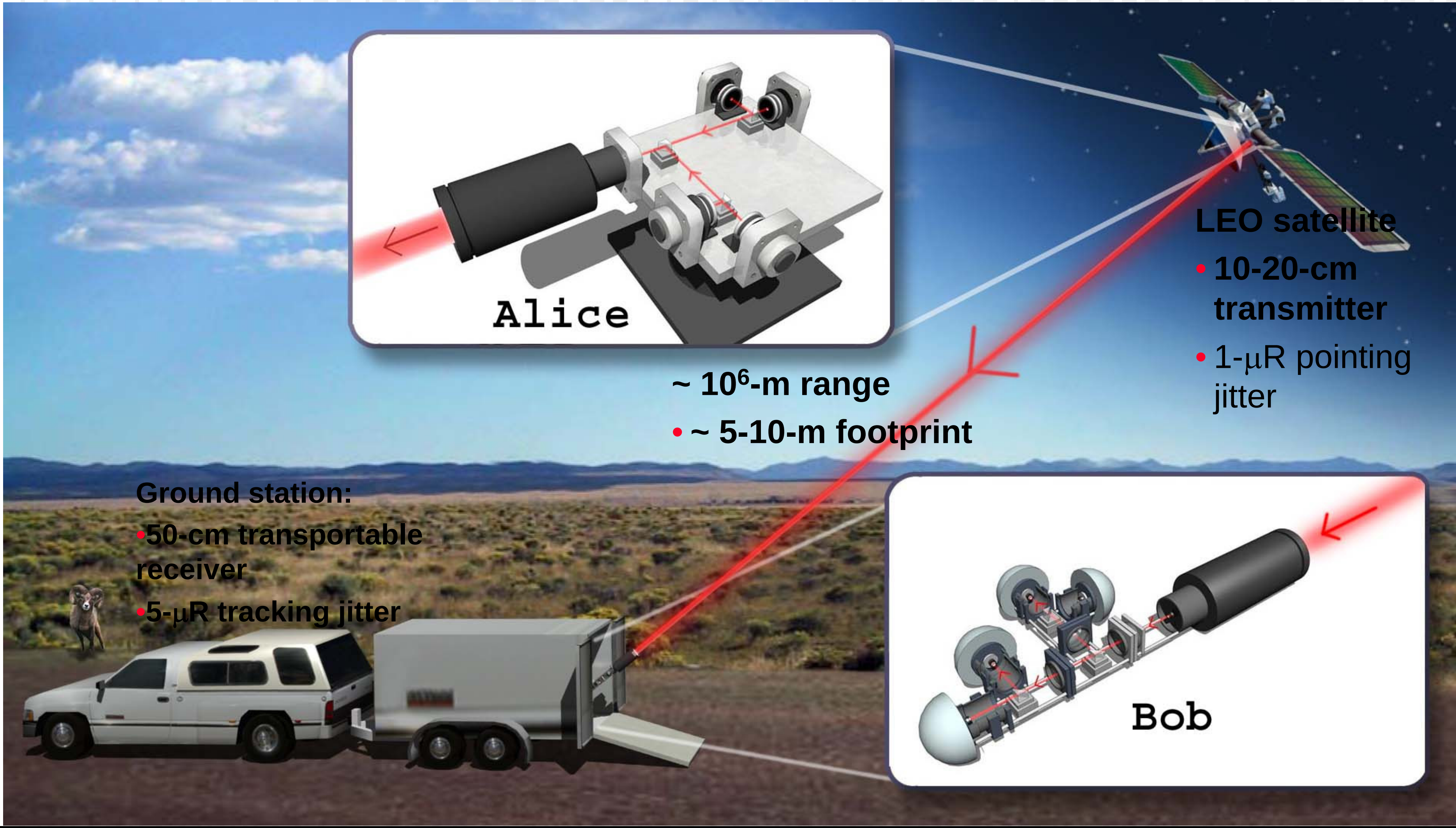




Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

QKD with LEO Satellites Possible with Small Terminals

J. E. Nordholt et al., Proc SPIE 4635, 116 (2002)



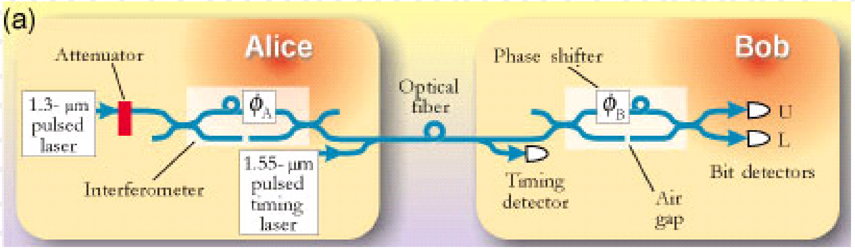
availability: rates ~ "100s secret keys/contact minute/notional day" feasible

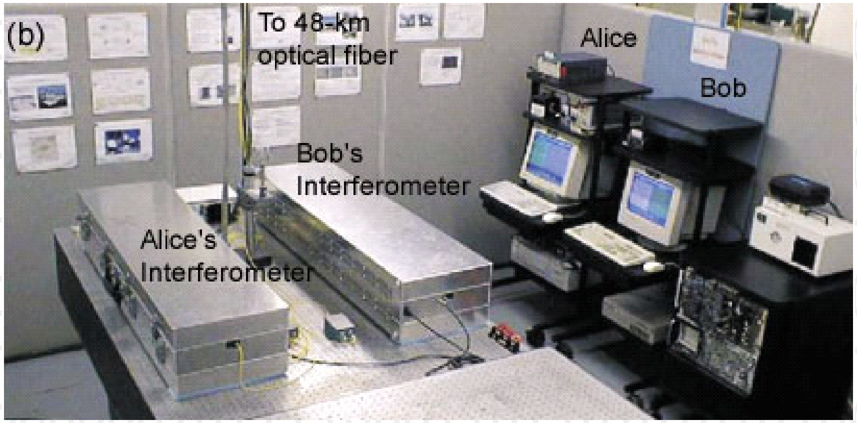
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

QKD in optical fiber: e.g. previous LANL QKD systems designed for dark fiber

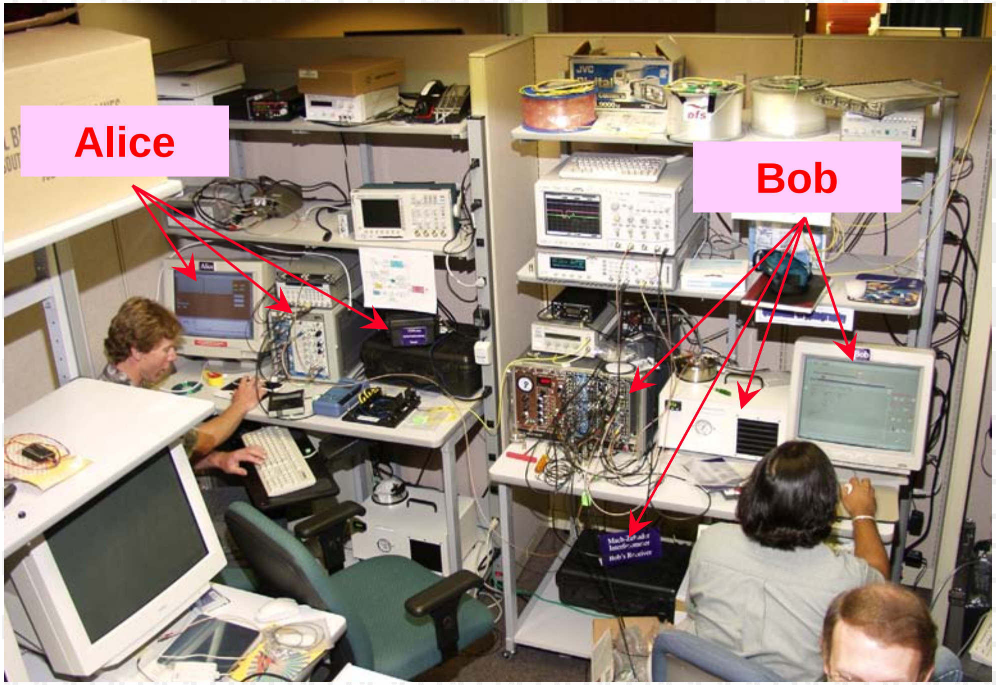
R. J. Hughes et al., LNCS 1109, 329 (1996)

F1QKD (@ LANL > ‘95)





F2QKD (@ FtMeade > ‘97; LTS > ‘02)



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

- **the challenge for fiber-based QKD: “co-existence” in an active optical network … LANL next-generation system: “Fiber III”**

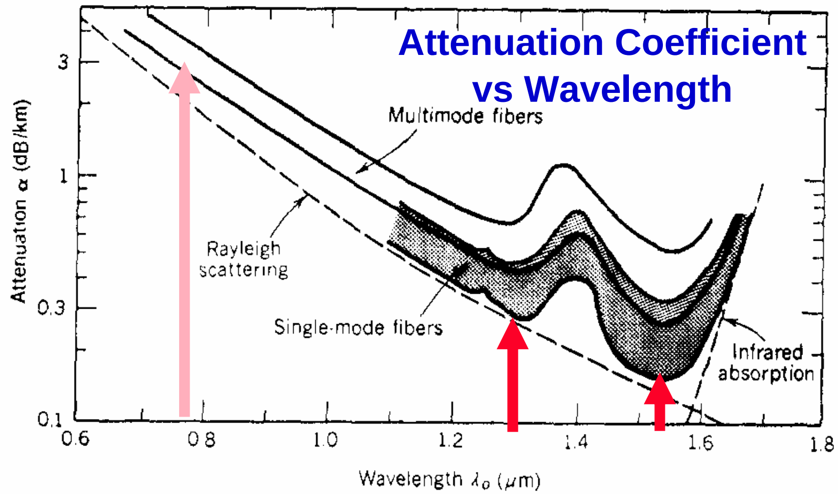
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Los Alamos NATIONAL LABORATORY

The QKD Quantum Channel

low-loss transmission medium; high-efficiency detectors

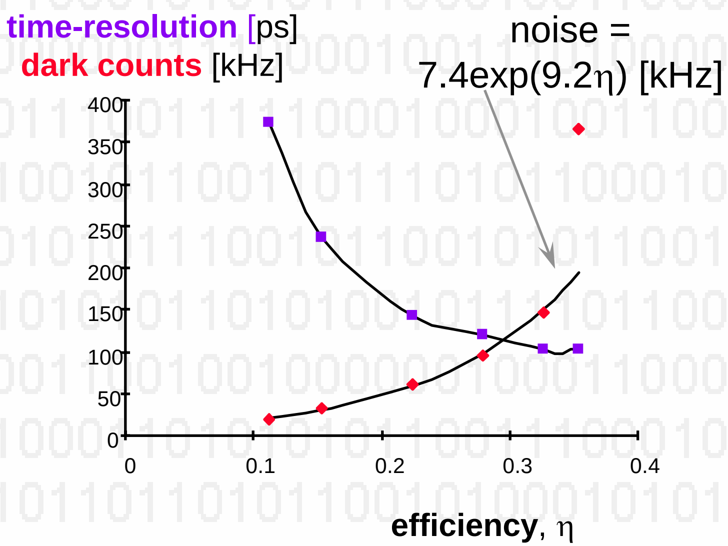
- **optical fiber**
  - QKD over telecommunications fiber networks ?
  - **challenges:** single-photon detection at 1.3 μm, (1.55 μm)



- (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**

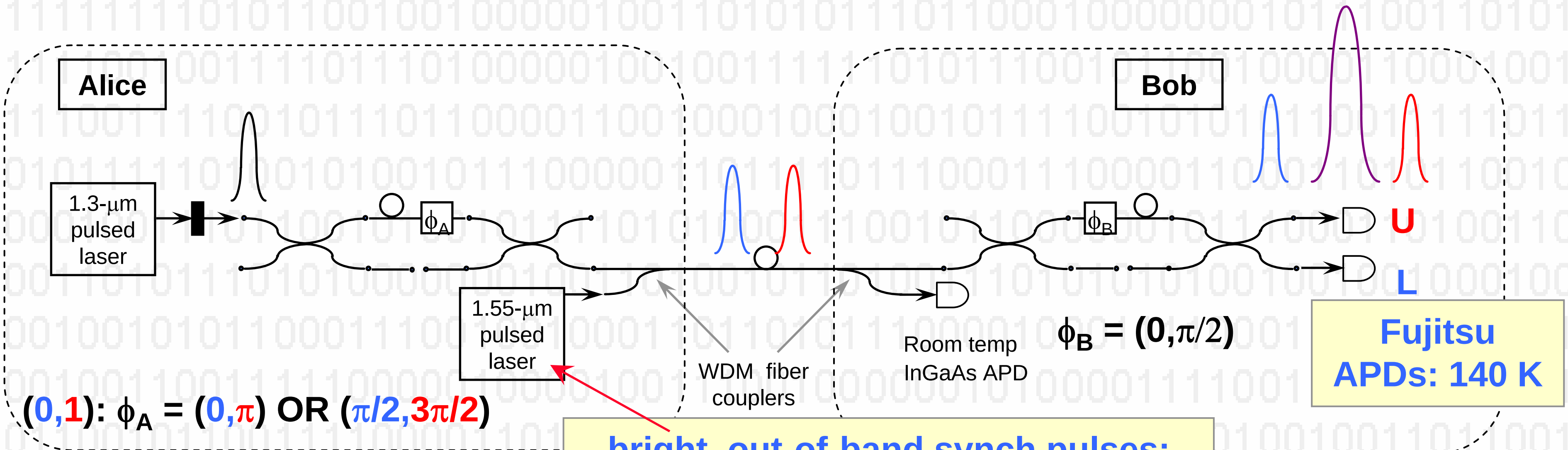


Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Los Alamos NATIONAL LABORATORY

F1QKD: BB84 using (multiplexed) single-photon interference

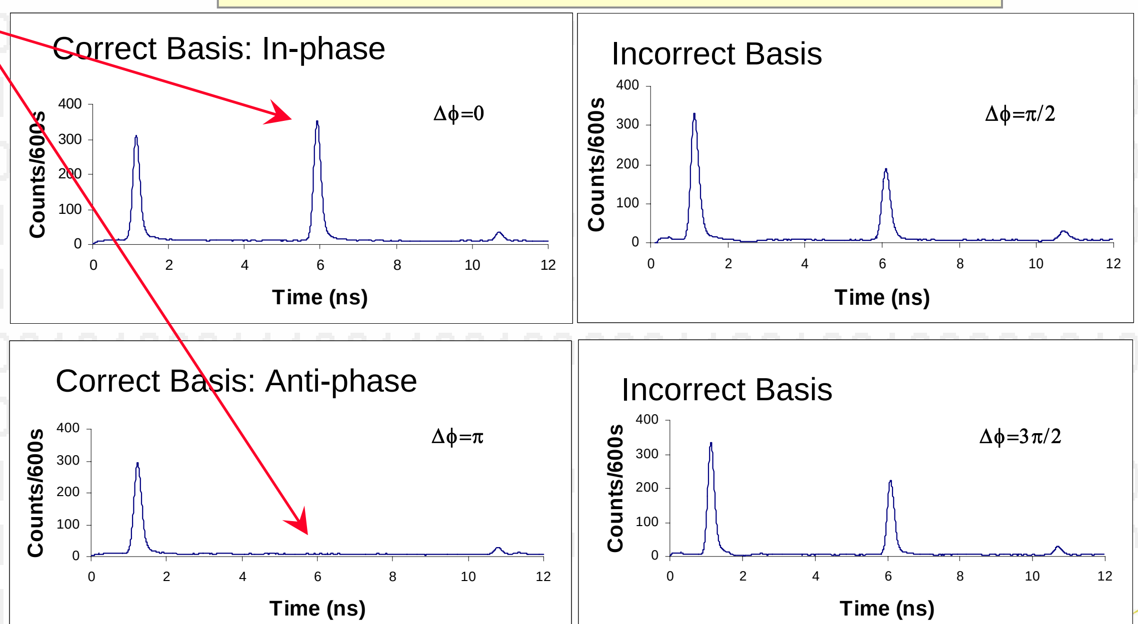
R. J. Hughes et al., J. Mod. Opt. 47, 533 (2000)



Fujitsu APDs: 140 K

bright, out-of-band synch pulses: network and APD hostile

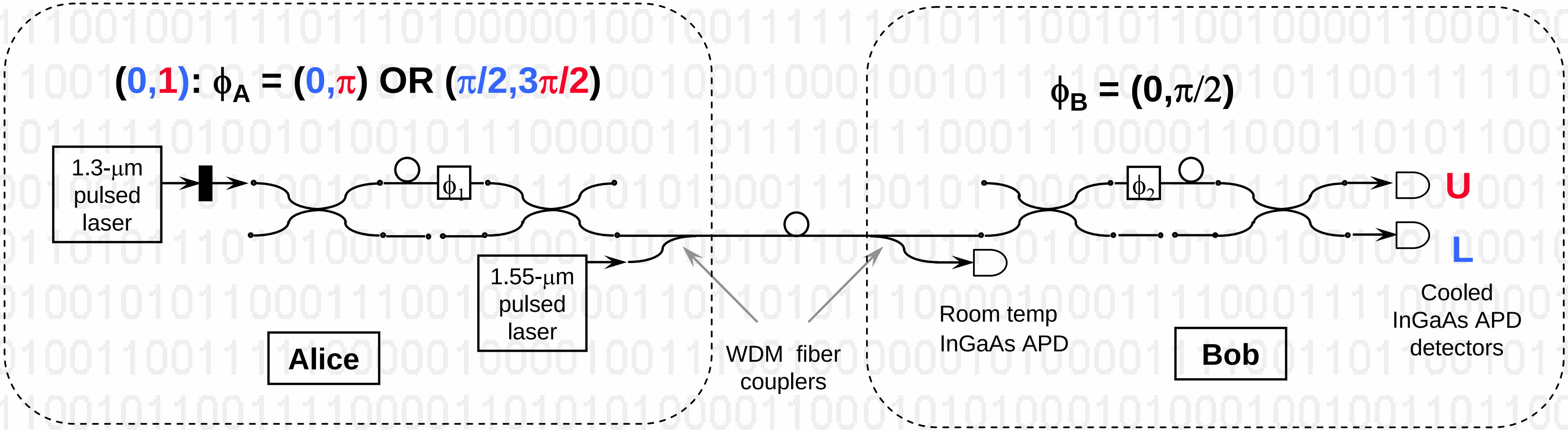
long-short + short-long interference:



e.g. LANL 48-km dark-fiber path
- 98.99±1.24% visibility
- 22.9 dB loss

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

BB84 key generation



Sample of 48-km BB84 key bits

A 00001001 01111111 10000111 10000000 01110001 10011110 00110101 10000111

B 00001101 01111111 00000011 10000000 00110000 10011110 00110101 10000111

A 00010000 00001000 10100010 00000011 00100101 00000000 00110011 01100010

B 00000000 00101000 10100010 00000111 00100101 00000000 00110011 01100010

- BER ~ 9.3 %; key rate ~ 20 Hz (2x B92)

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

Los Alamos
NATIONAL LABORATORY

Requirements for QKD in AONs

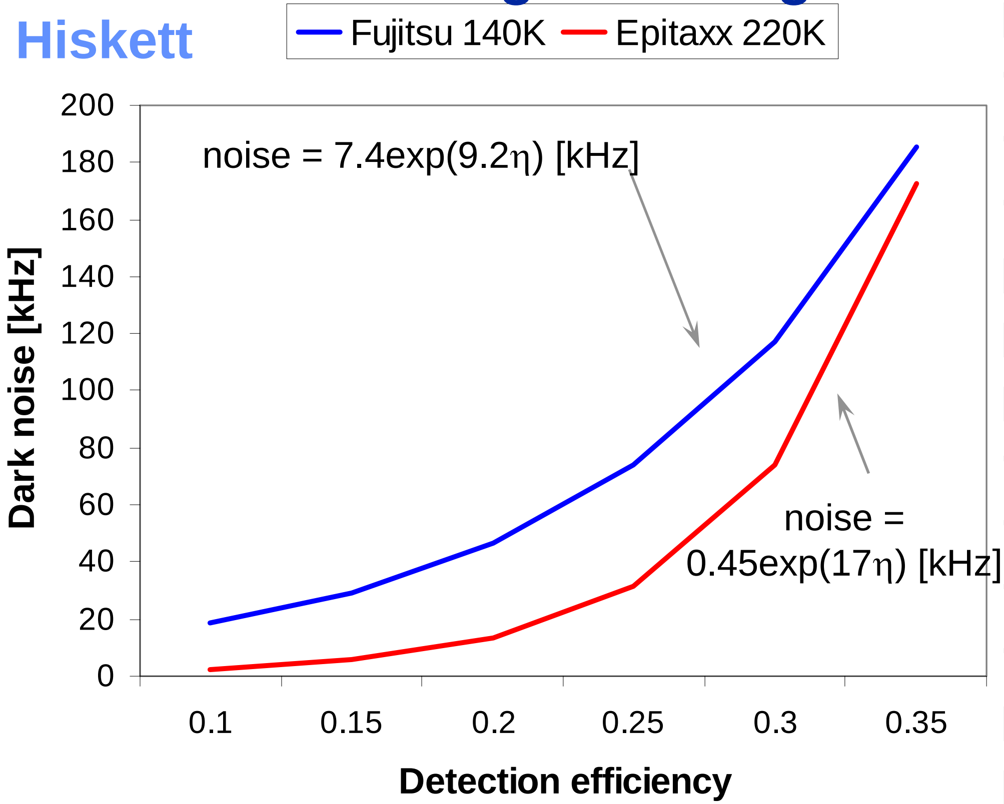
Requirement	F1/F2 limitation	F3QKD solution
"Ease of use": focus on network, not physics	Physicist required	Engineered, automated, stable system
Multi-wavelength capable: co-existence	Fixed wavelength	Novel modular design
Network-friendly synchronization	Out-of-band bright pulses	Syntonized Rb oscillators
Accommodate path length changes	Static path length	Auto-synchronization and tuning
Background tolerant	Dark fiber	Epitaxx APDs
Clock rates < 10 MHz	Clock rates < 100 kHz	After-pulse blocking APD gates ~ 600ps
Complete protocol	_	Includes all classical elements + authentication

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

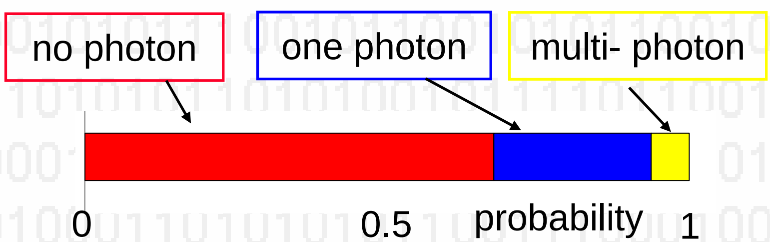
F3QKD Epitaxx APDs: "ease-of-use" + tolerate higher backgrounds

P. Hiskett

- **F1/F2QKD: Fujitsu InGaAs APDs required refrigerator to reach 140K**
- **Epitaxx APDs: lower dark noise for same efficiency at higher temperatures**
  - accessible with TE cooling
- **e.g. η ~ 20%, dark noise**
  - Fujitsu (140K) ~ 47 kHz
  - Epitaxx (220K) ~ 13 kHz
- **in dark fiber**
  - greater max range: 32dB loss vs 24dB
  - higher yield at given range: e.g. @20dB
    - 1.9×10^{-4} secret bits/trans bit (Epitaxx)
    - 0.8×10^{-4} secret bits/trans bit (Fujitsu)



BBBSS91 privacy amplification



Eve identifies all multi-photon signals, errors due to intercept/resend on single-photon signals

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

The ARDA QIS&T Roadmaps: http//qist.lanl.gov

QIS&T

- **today: a healthy endeavor spanning the range from basic science to emerging technology**
  - potentially offering unprecedented new information assurance capabilities
- **where would we like to be in 10 years?**
- **what will it take to get there ?**
  scientific, technological, infrastructure, skills (people), targeted $, … developments ?
- **(how) will the present array of approaches help us get there ?**

a Research Roadmap:

apply some gentle direction

describe state-of-play and likely progress

identify opportunities and gaps + places where strategic investments would be beneficial

an aid to the research community and a descriptive tool for program management

a living document

LA-UR-04-4085

A Quantum Information Science and Technology Roadmap

Part 2: Quantum Cryptography

Report of the Quantum Cryptography Technology Experts Panel

"When elementary quantum systems…are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media."
Charles H. Bennett and Gilles Brassard (1984)

Disclaimer:
The opinions expressed in this document are those of the Technology Experts Panel members and are subject to change. They should not to be taken to indicate in any way an official position of U.S. Government sponsors of this research.

July 19, 2004
Version 1.0

ARDA

This document is available electronically at: http://qist.lanl.gov

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

Los Alamos NATIONAL LABORATORY

Summary

QKD is evolving from fundamental physics towards a "quantum information assurance" era

- a new tool for secure communications, enhancing conventional key management, to meet future needs
- a physical layer technology
  - co-existence with conventional optical communications ?

- **Satellite-to-ground QKD**
  - no showstoppers
- **QKD in all-optical fiber networks**

Further reading:

J. E. Nordholt & R. J. Hughes,
Los Alamos Science **27,** 68 (2002)
http://www.lanl.gov/science/

"Information, Science and Technology in a Quantum World"

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