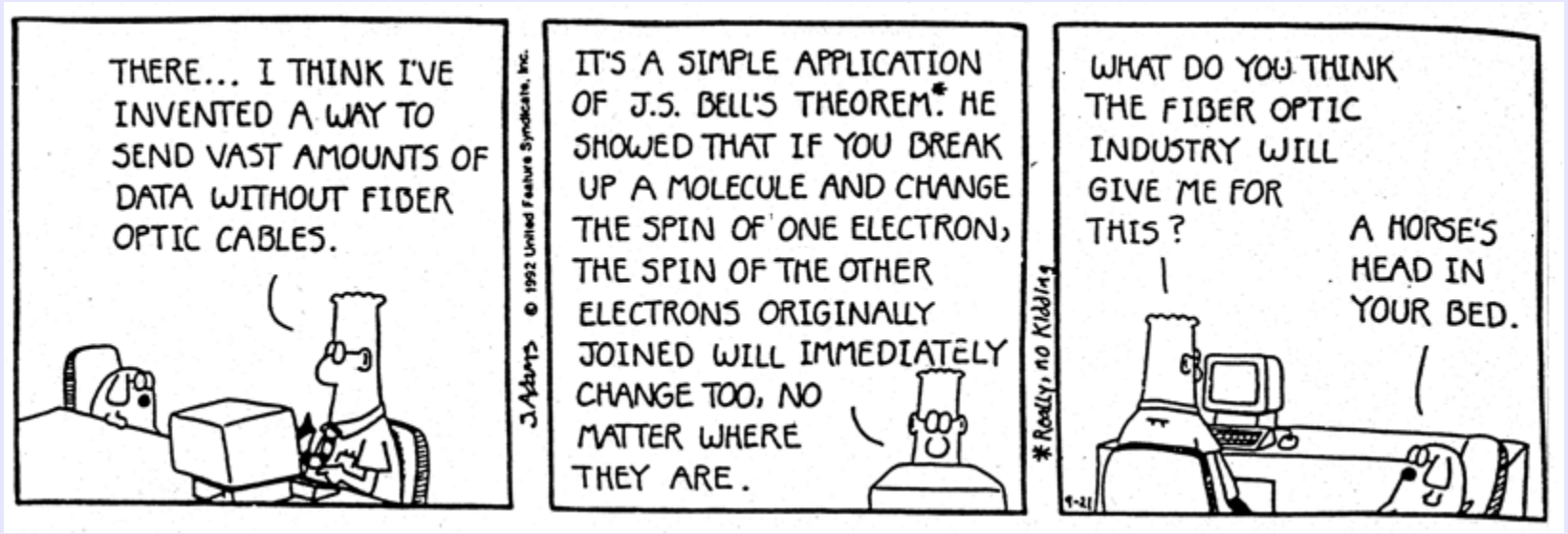
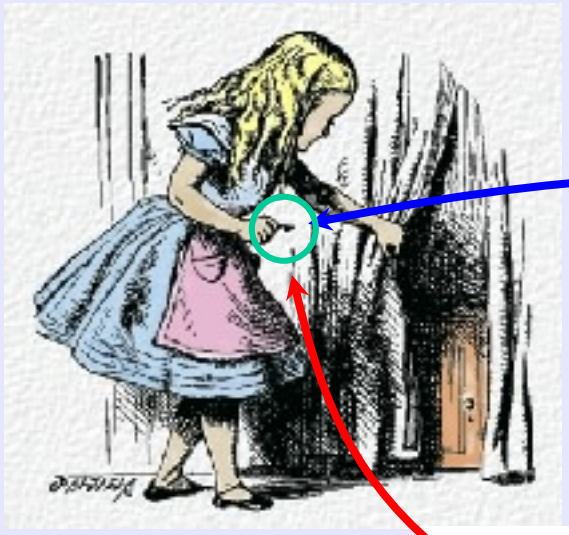
Quantum Cryptography



Quantum Cryptography

ALICE



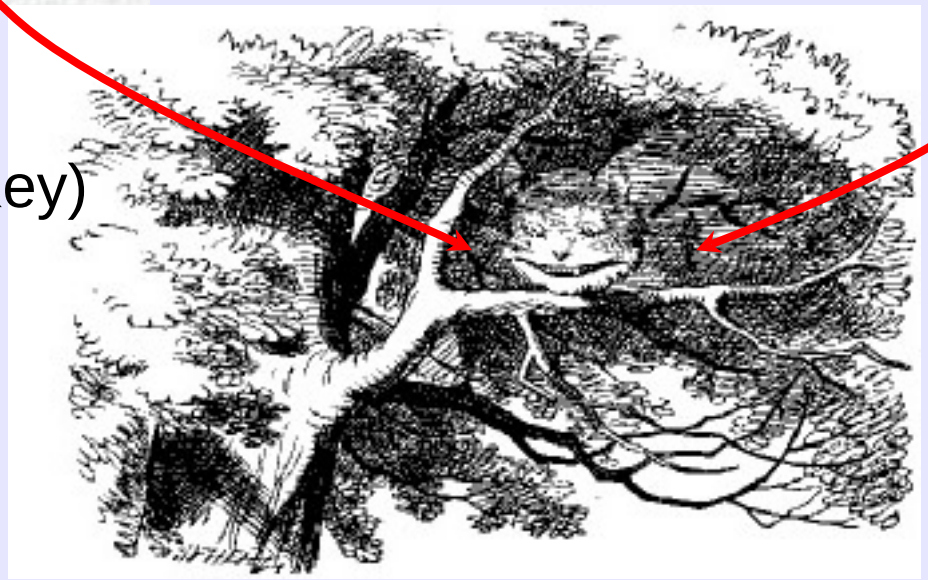
KEY:
…01000101001110100 1…

Cipher:
…0110010110100010…

BOB

XOR(Message,Key)

Cipher



XOR(Cipher,Key)

Message

EVE

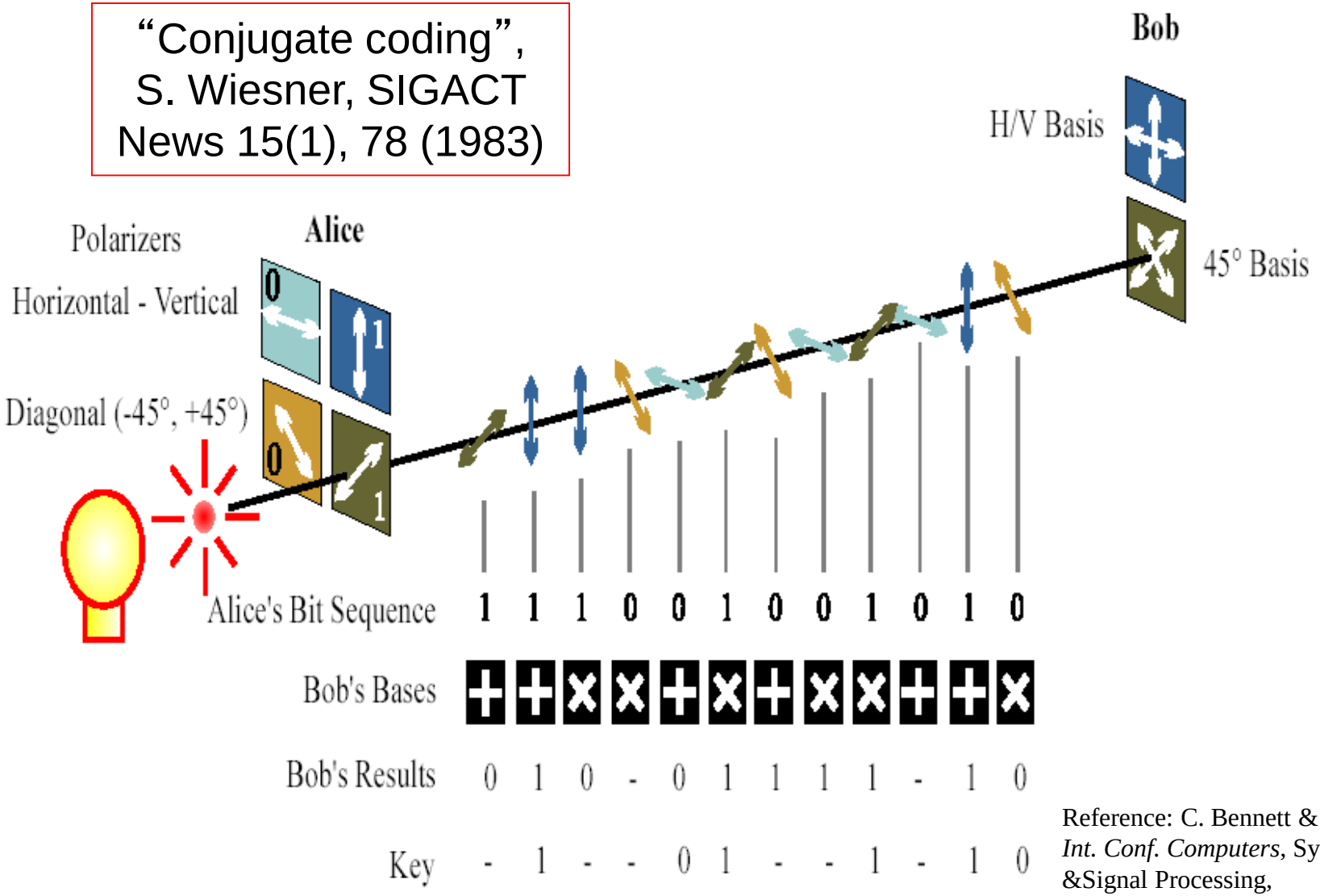
Quantum Cryptography

BB84 Protocol

Aaron VanDevender (vandvndr@uiuc.edu)

Polarization-encoded QKD: the BB84 protocol

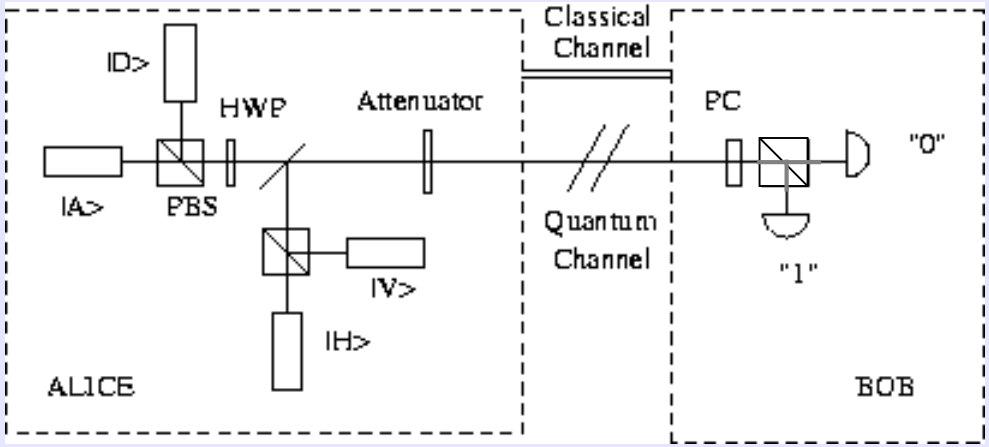
"Conjugate coding", S. Wiesner, SIGACT News 15(1), 78 (1983)



Reference: C. Bennett & G. Brassard *Int. Conf. Computers*, Systems &Signal Processing, Bangalore, India, 1984

Los Alamos NATIONAL LABORATORY

BB84 Protocol



Alice transmits a photon in one of **four** states.

Bob measures the photon in one of **two** bases.

Alice and Bob sift out the trials (50%)
where they used the same basis.

The sifted keys have “perfect” correlation.

An intrusive eavesdropper will induce errors up to 25%.

Six-state Protocol: Alice uses 3 bases (6 states).

Eavesdropper-induced BER → 33%

What about Eavesdropping?

• Eve cannot "tap" the line → photons that don't make it to Bob are not part of the key

• Eve cannot "clone" the photon → forbidden by basic quantum mechanics

• Measurements by Eve necessarily have a chance (25-33%) to disturb the quantum state

→ Alice and Bob can detect errors in the key!

If the bit error rate is too high, they simply discard the key. No message is ever compromised.

Otherwise they implement classical error correction, then 'privacy amplification' to distill a secret key.

QKD complete protocol

randomization
Alice generates a secret random bit sequence

"conjugate coding"
Quantum transmissions from Alice to Bob

time-stamping

sifting
reveal time slots + bases

reconciliation
error correction

bounding
Eve's information

privacy amplification
extract **secret bits**

authentication
of public messages

key confirmation

final, secret key

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

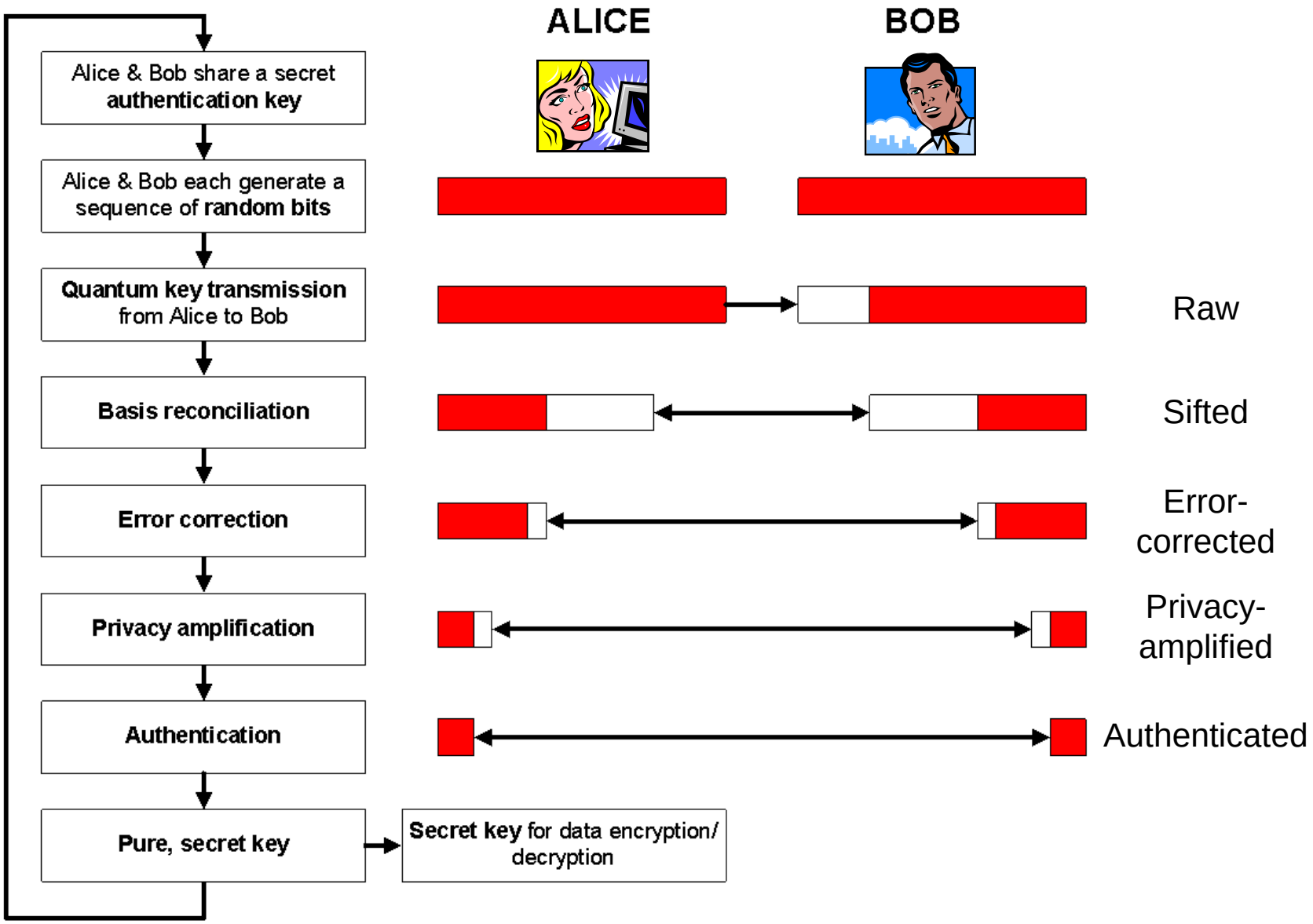
cryptography

Quantum cryptography

= Quantum key distribution

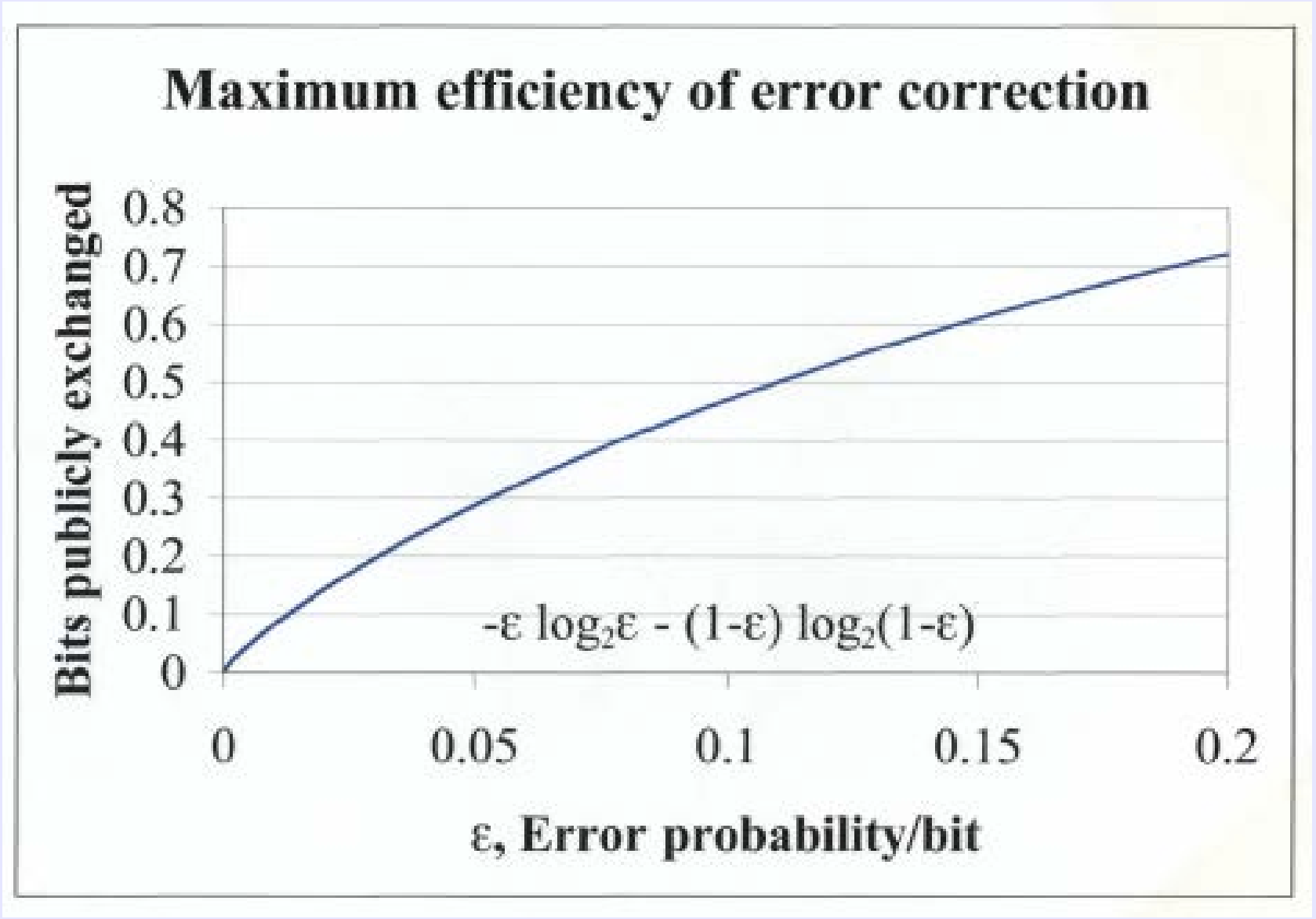
= Quantum secret growing

From Sifted Bits to a Secret Key: Privacy Amplification



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

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



Moral of the story: Keep BER low!

The BBBSS91 experiment

Experimental Quantum Cryptography

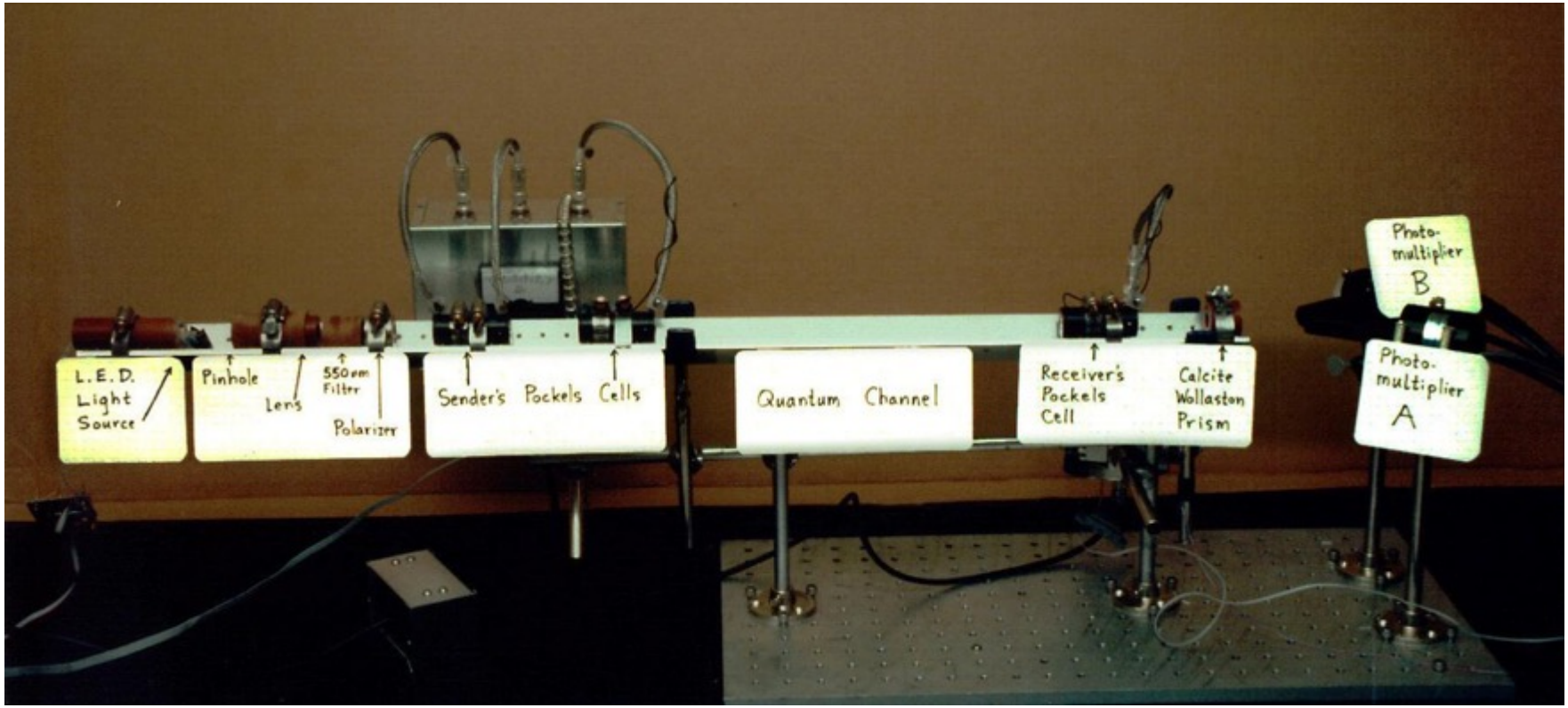
Charles H. Bennett
IBM Research *

François Bessette †
Université de Montréal ‡

Gilles Brassard §
Université de Montréal ‡

Louis Salvail

John Smolin ¶

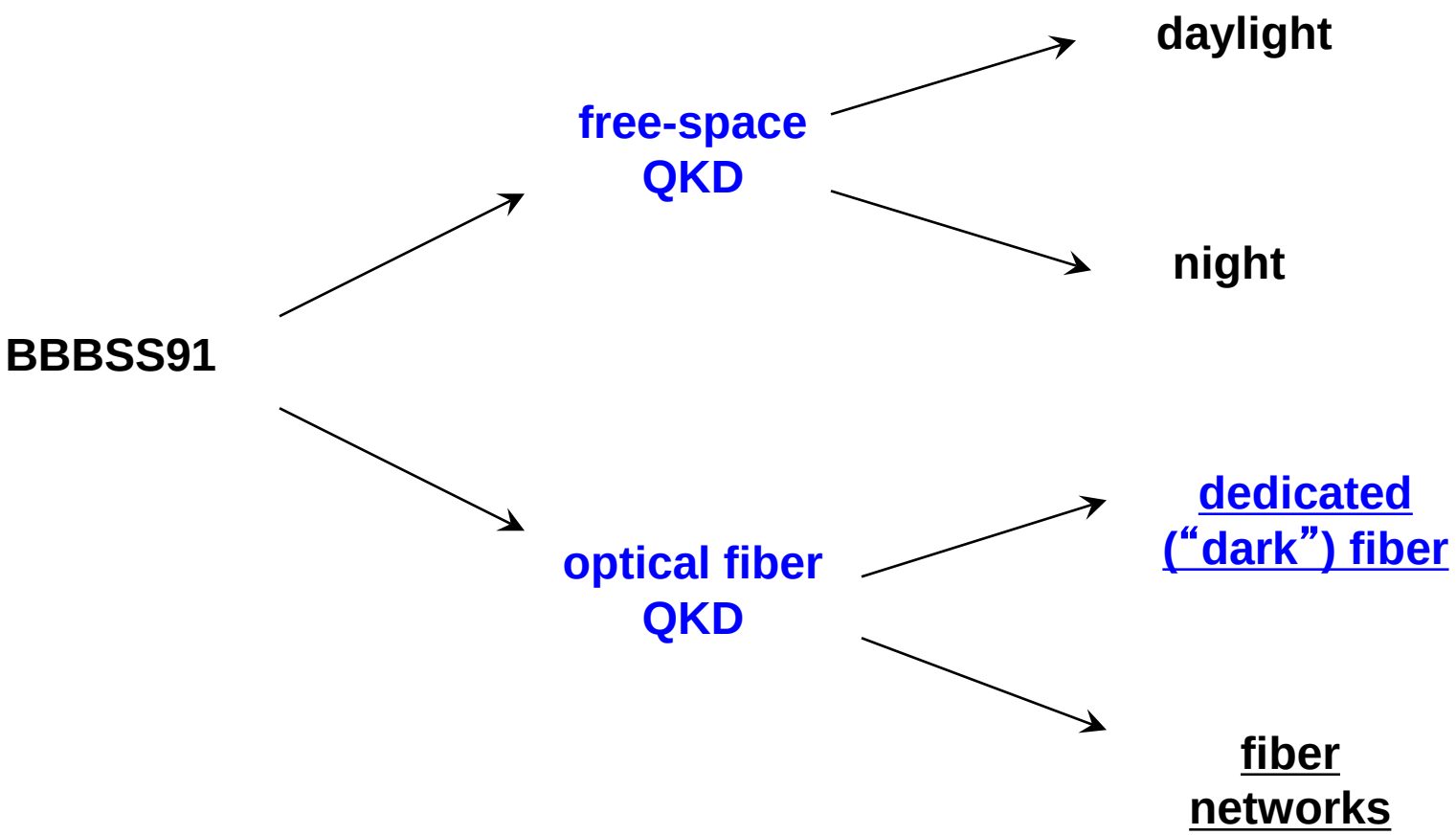


- **32-cm free-space transmission**
- **"unconditionally secure … provided Eve is deaf" (G. Brassard)**

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

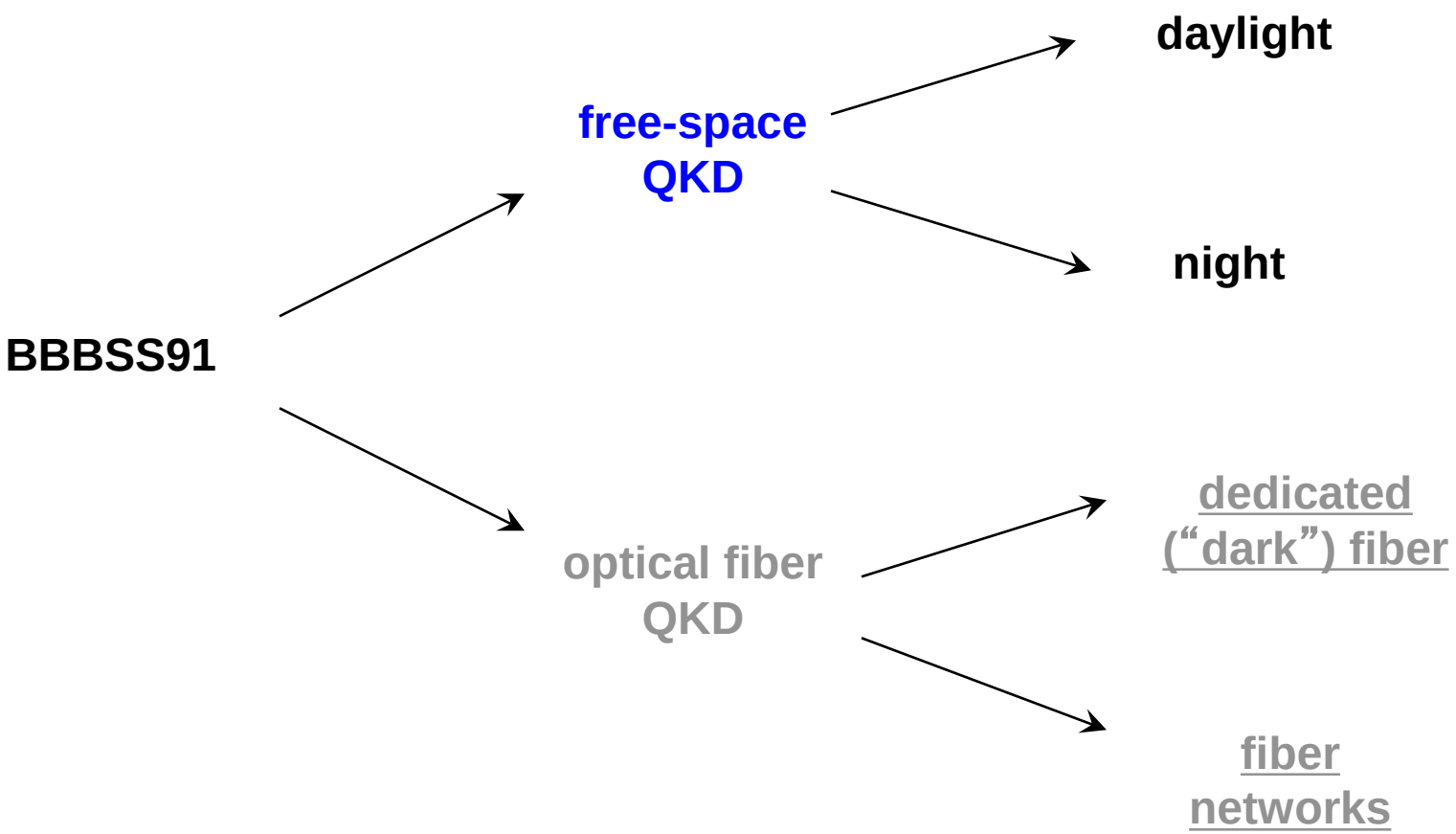
Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov

Evolution of QKD experiments



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

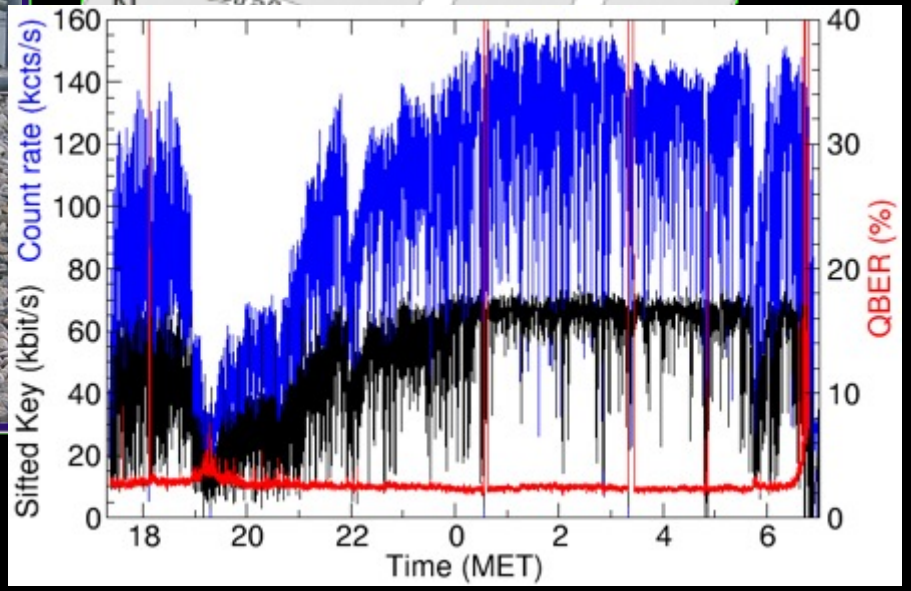
Evolution of QKD experiments



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

short distances

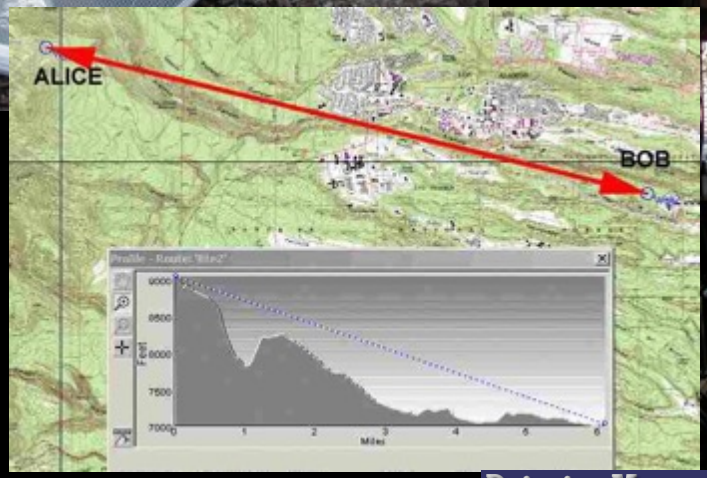
- down-town test range 500 m
- self aligning, synch on detected signals
- QBER 3.2%, 47 kbit/s sifted key
- ~20 kbit/s secure, corrected key all night

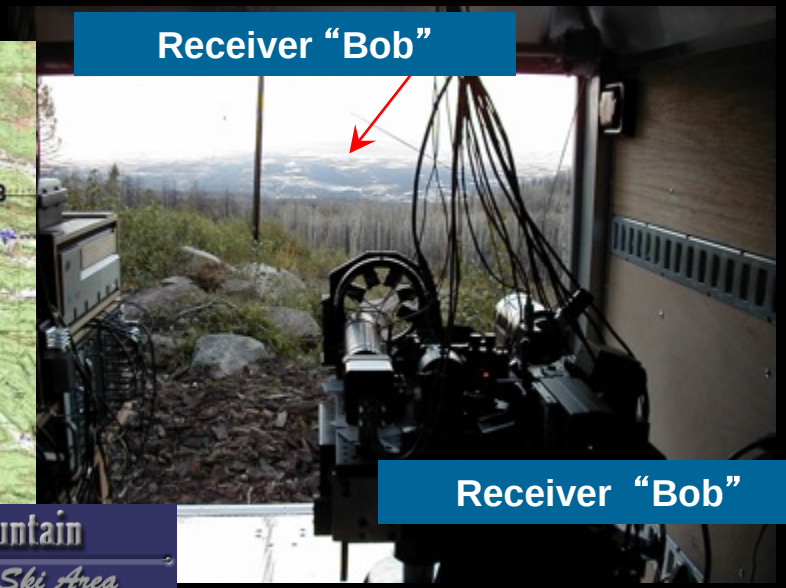


H. Weier et al. Fortschritte der Physik (2006)
J.C. Bienfang, Optics Express 12, 2011-2016 (2004)

Los Alamos free-space quantum cryptography

- 772-nm
- 1-MHz pulse rate; ~600-Hz key rate
- day: 45,576 secret bits;
- night: 113,273 secret bits



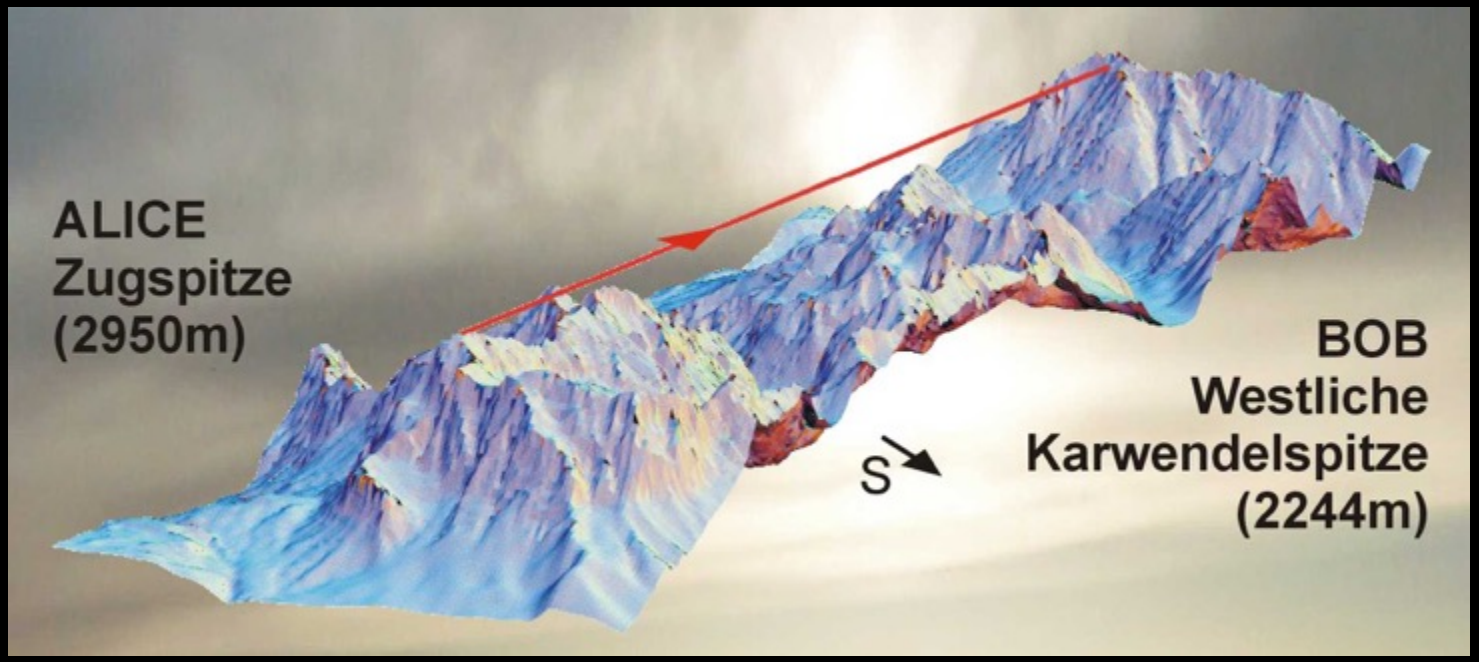


Pajarito Mountain
Ski Area

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

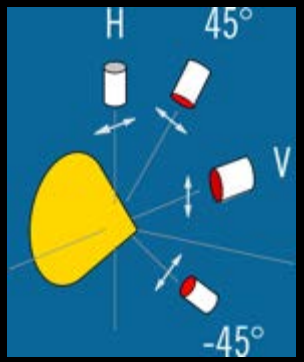
R.J. Hughes, J.E. Nordholt, D. Derkacs,Ch.G. Peterson, *New Journal of Physics* **4**, 43 (2002)

Secure key exchange over 23.4 km



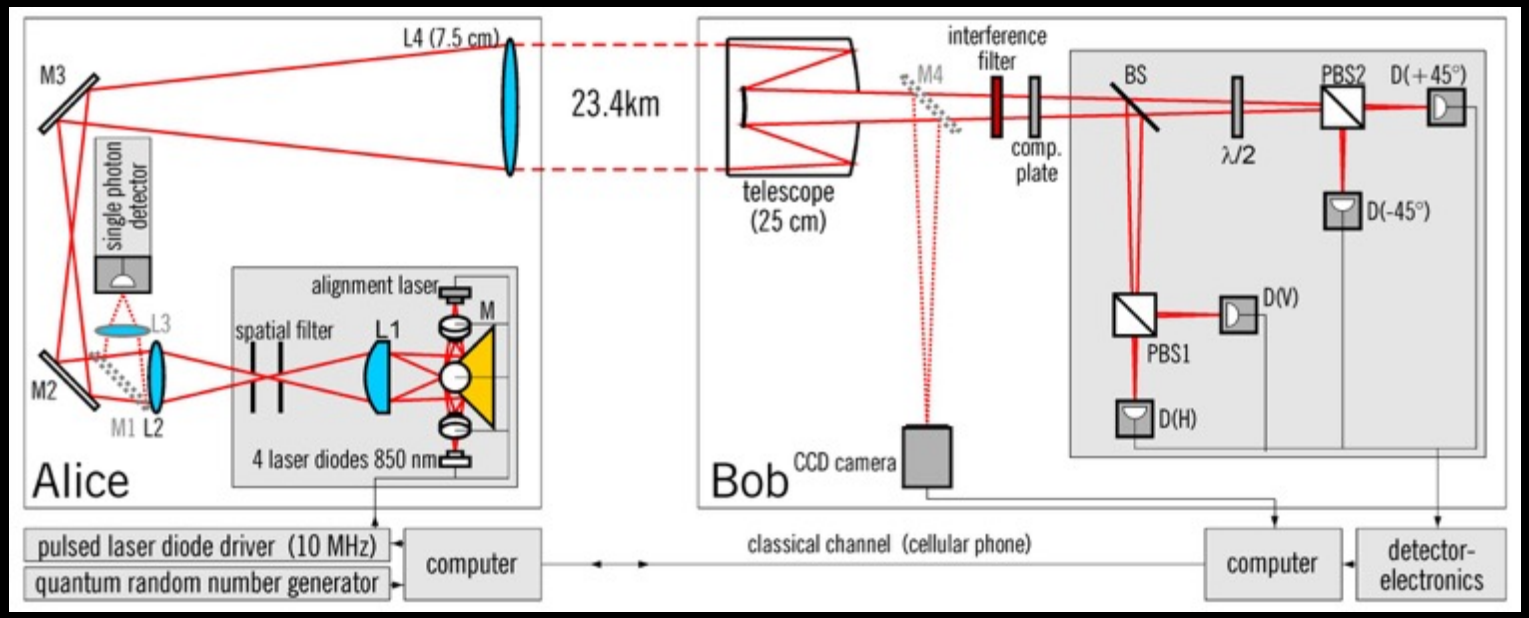
new design: reliable, efficient, stable

<n>	0.096
loss	30 dB
bit rate	1365 s^{-1}
QBER	2.7%



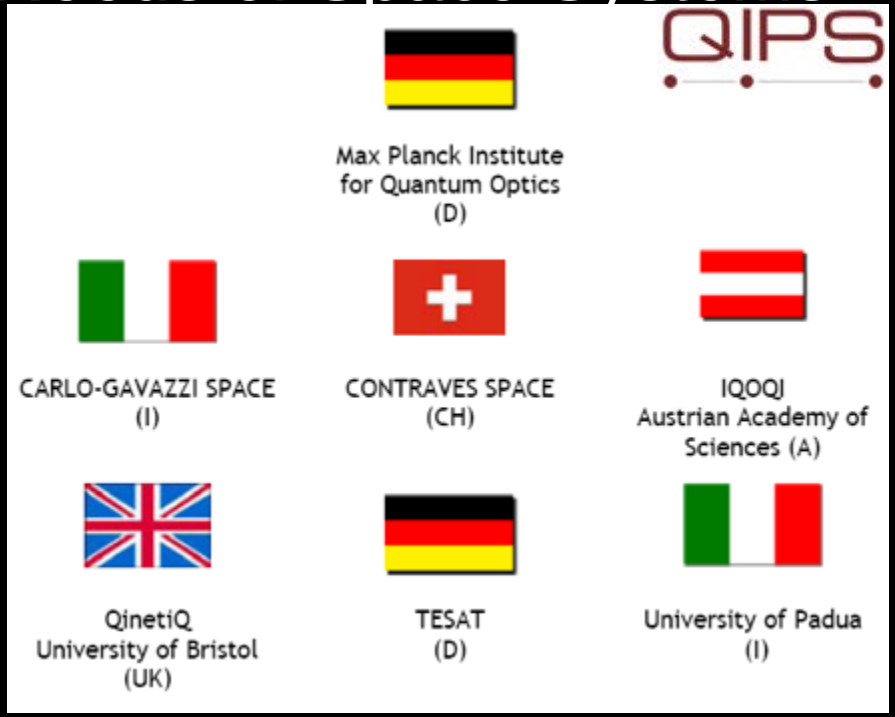
Ch. Kurtsiefer et al., Nature **419**,450 (2002)

The Zugspitz experiment 23.4 km

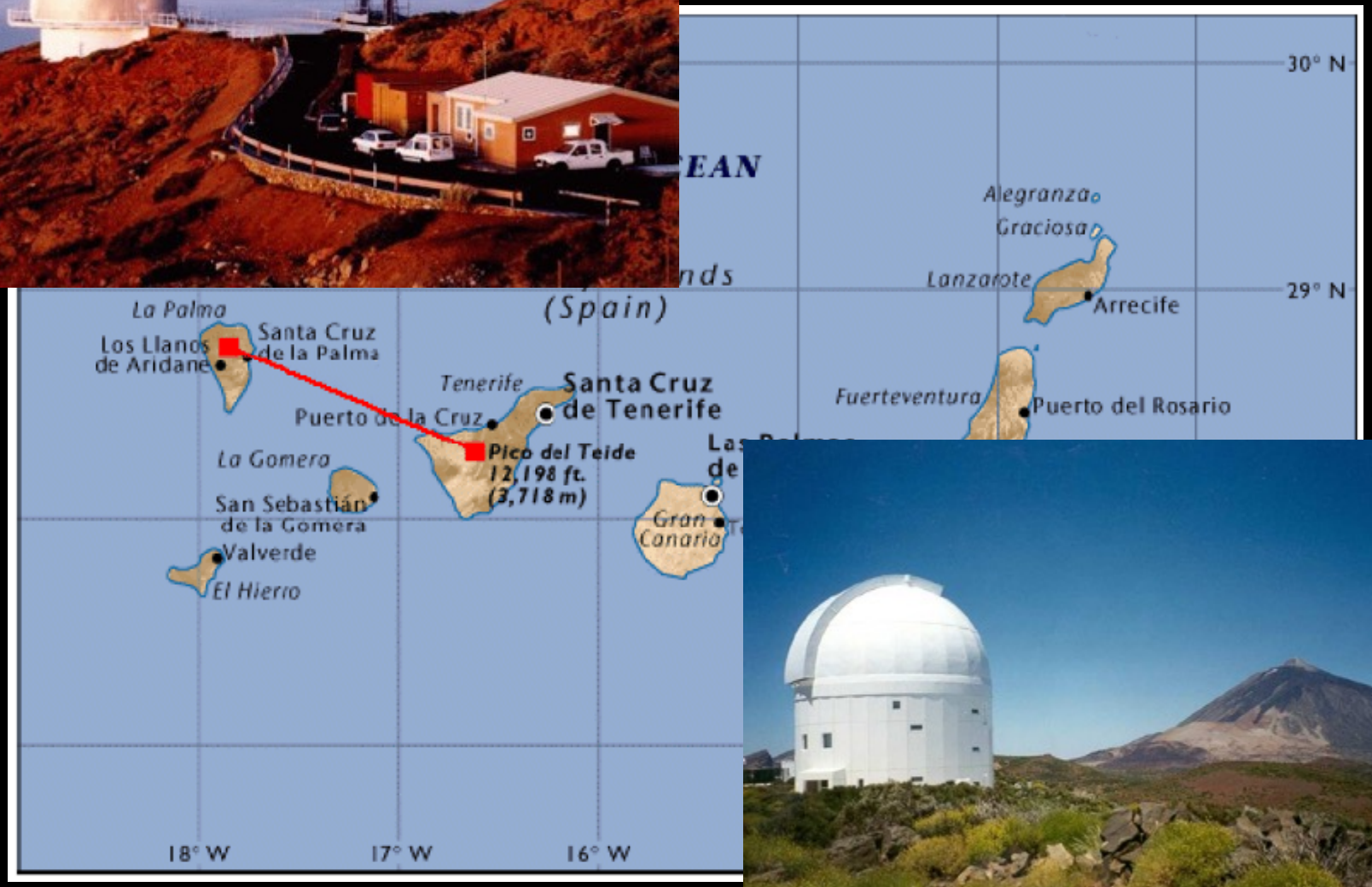


The 144 km link

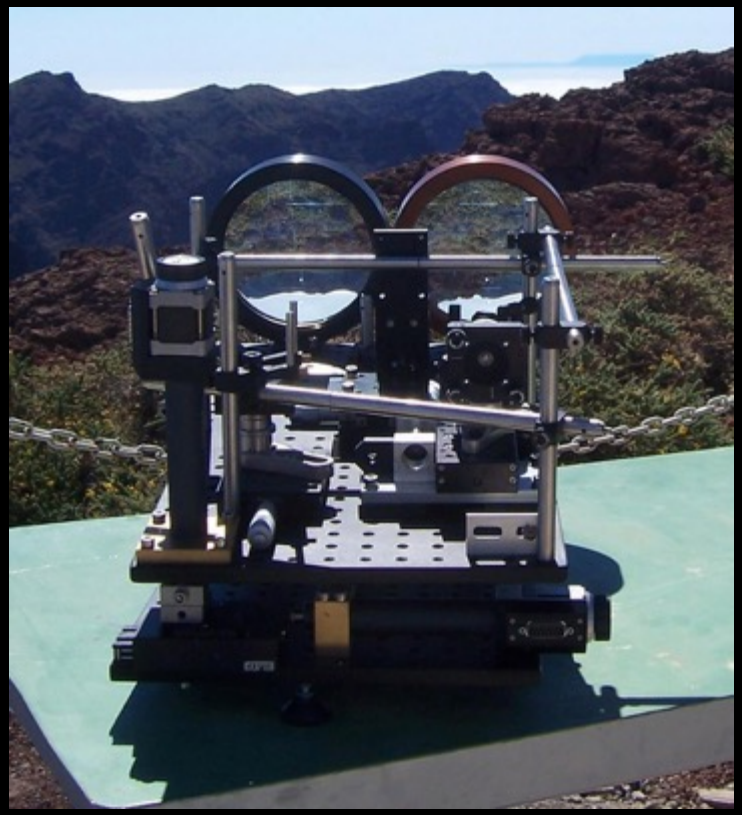
- ESA-project QIPS for Experimental Evaluation of Quantum Communications in the Framework of the Current Needs of Space Systems

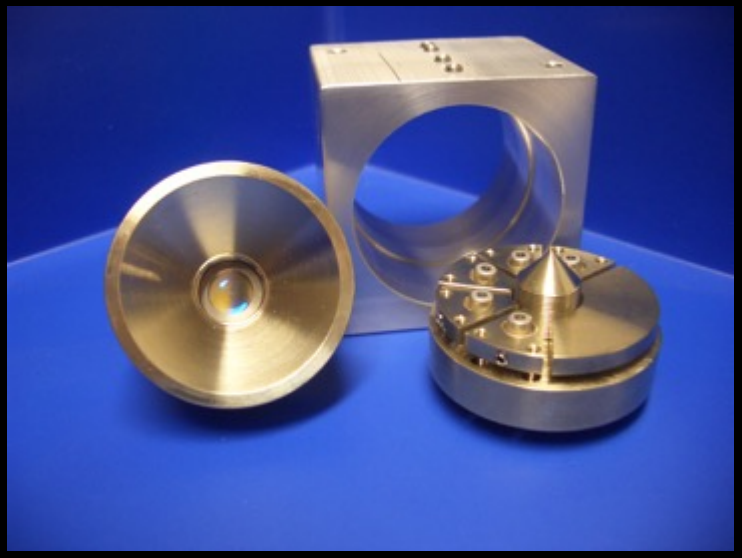


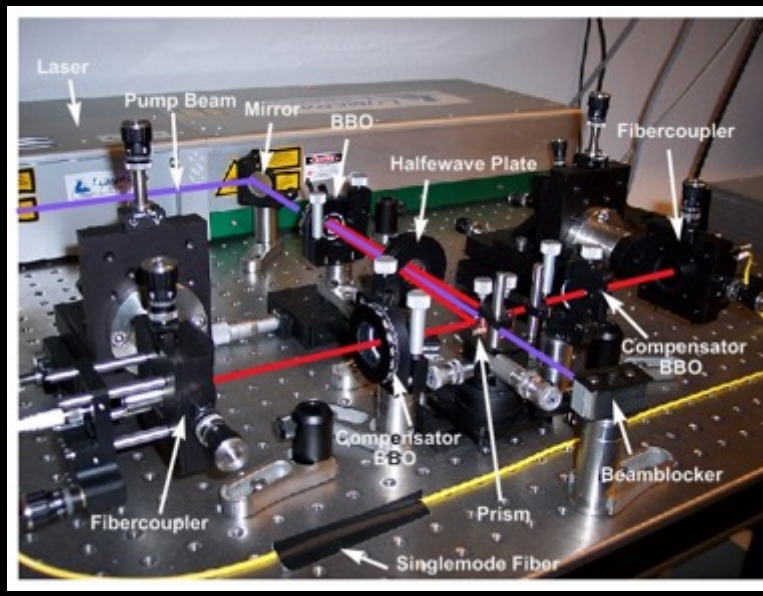
ma and Tenerife



sender



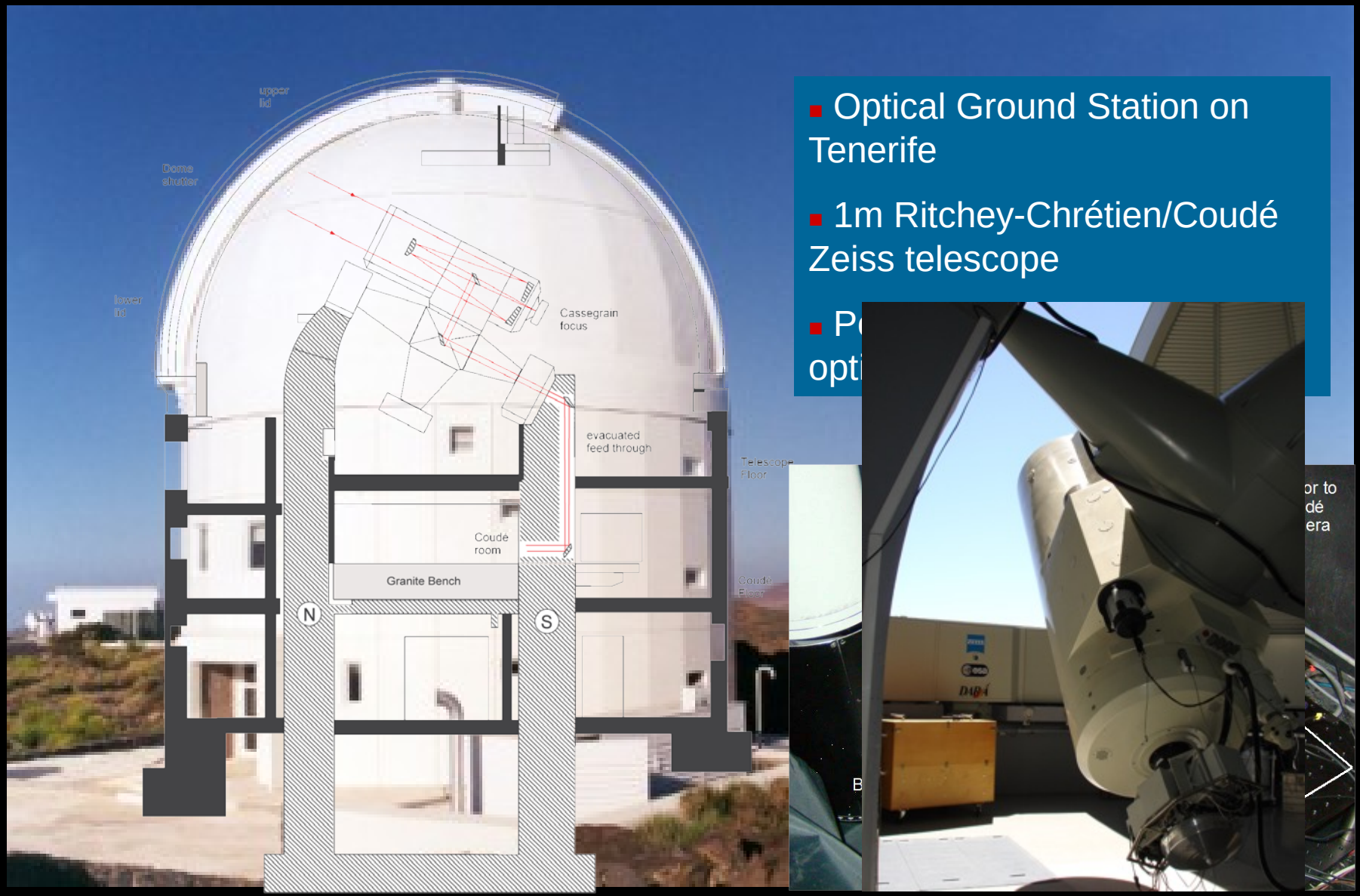




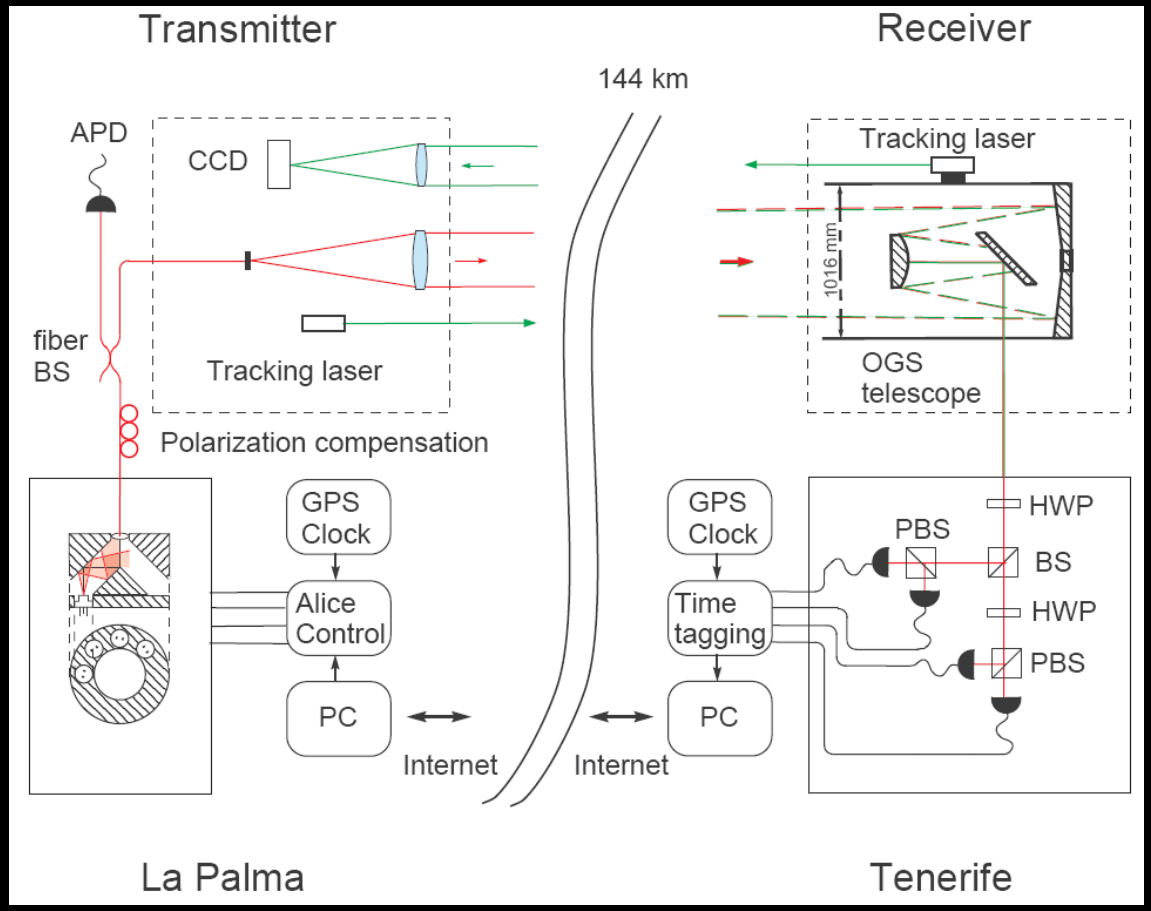
- attenuated pulse 4 LD, conical mirrors
- SPDC: Nd:Vanadate 355nm, 250 MHz, 3W: 145000 coincidences locally (M.Lindenthal et al.)

receiver

- Optical Ground Station on Tenerife
- 1m Ritchey-Chrétien/Coudé Zeiss telescope
- P
opti



attenuated pulses



how to avoid/detect photon number splitting attack?

What about Eve…

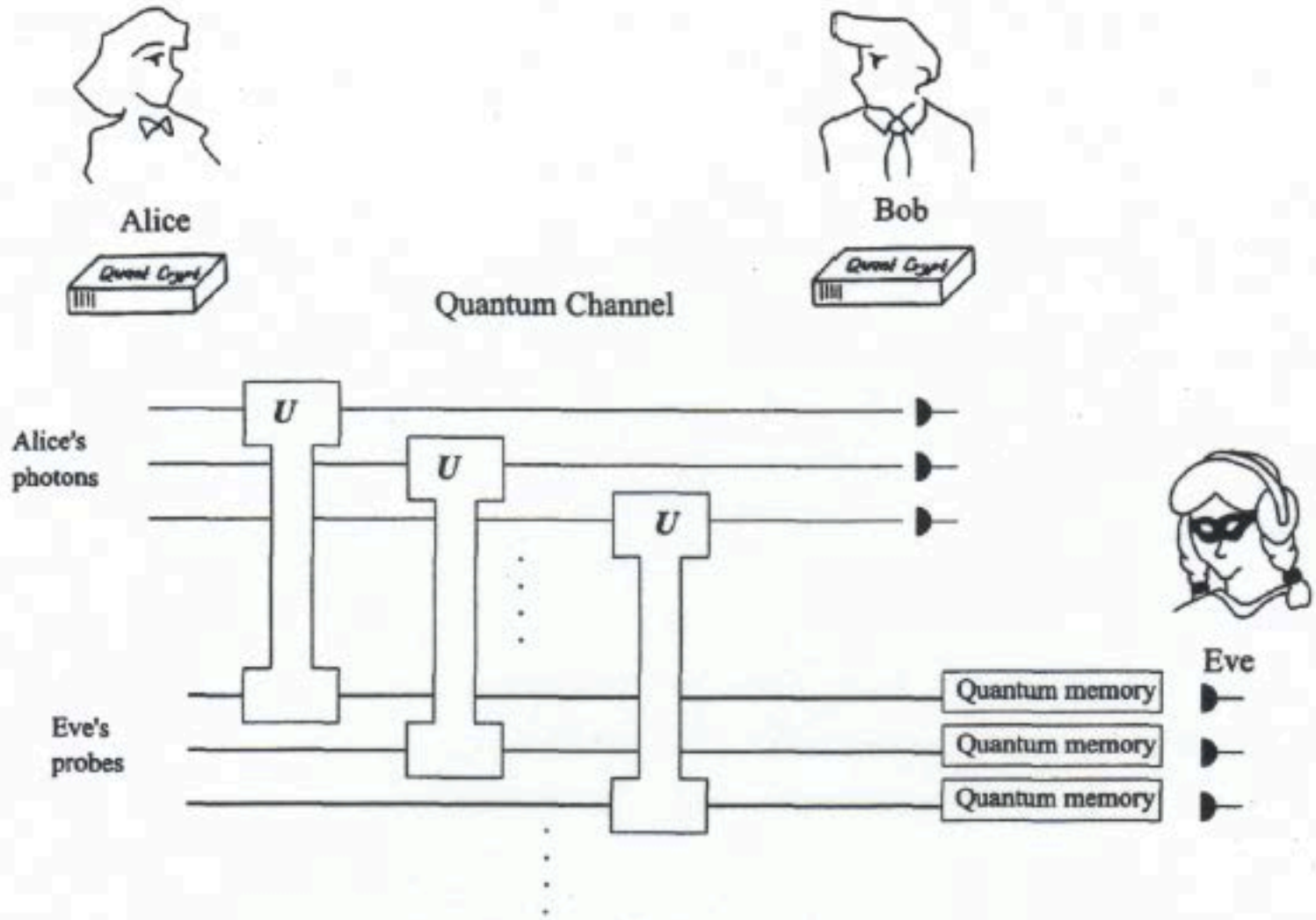


Fig. 2.8. Incoherent attacks: each photon is entangled independently to a 2-qubit probe. The probes are stored in a quantum memory until measurement bases are announced. Then each probe is measured independently.

Current conclusions

Preskill showed that BB84 is secure whenever the error rate (commonly called quantum bit error rate, QBER) is less than 11 percent. Allowing two-way classical communications between Alice and Bob, Gottesman and Lo [15] have shown that BB84 is secure whenever the QBER is less than 18.9 percent. Subsequently, Chau [16] extended the secure region up to 20.0 percent. An upper bound on the tolerable QBER is also known: BB84 is known to be insecure when observed correlations contain no quantum correlations anymore [17], which happens when the average QBER is above 25 percent. [18] A major open question is the following: What is the threshold value of QBER above which BB84 is insecure? Is there really a gap between the 20% and the 25%?

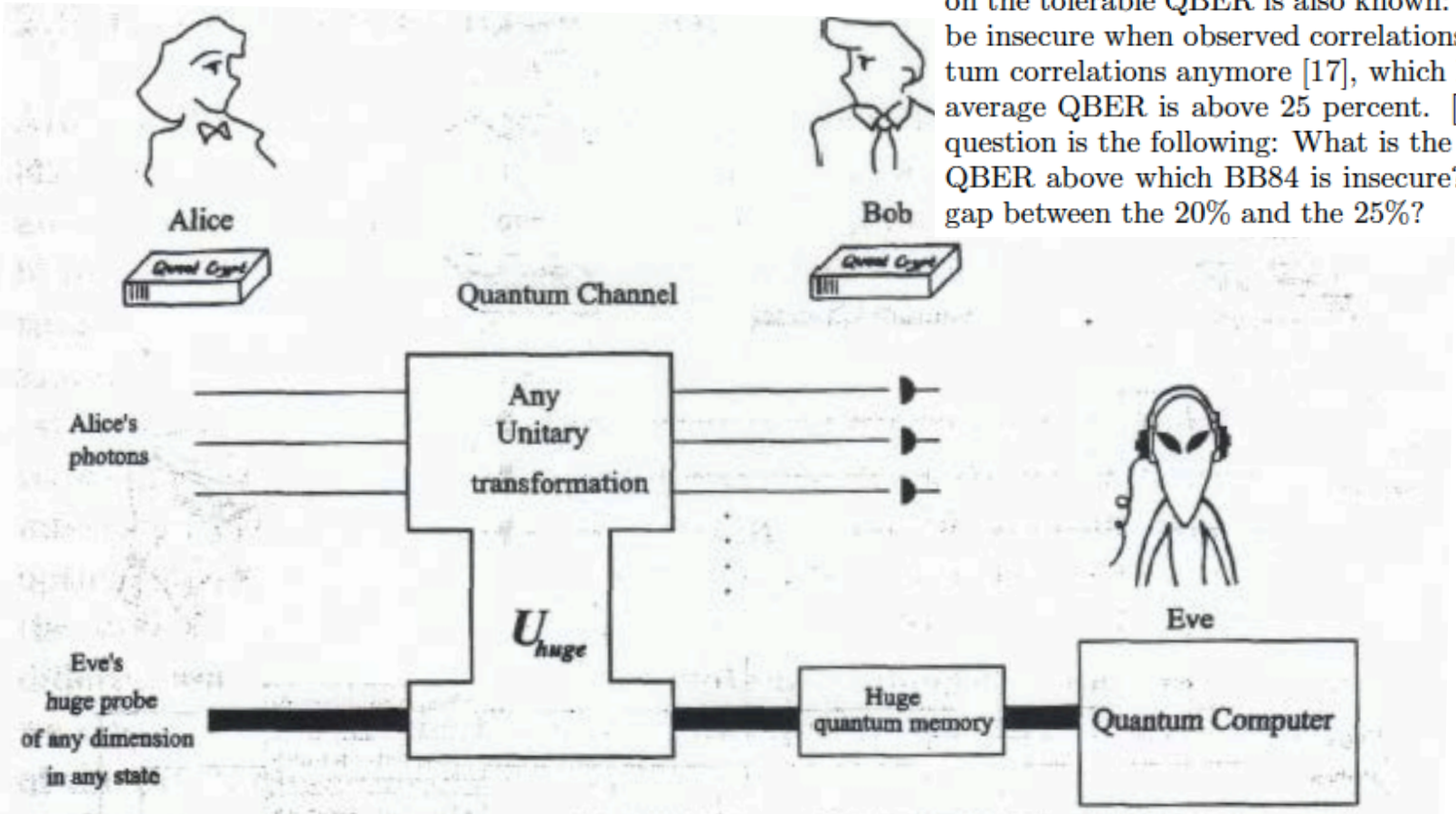


Fig. 2.9. Coherent attacks: Eve is allowed to use a probe of any dimension in any initial state and to entangle it with every photon sent by Alice in any unitary manner. This probe is stored until bases are announced.

Eavesdropping 102

Depending on the number of photons sent by Alice, there are different optimal eavesdropping strategies:

- 1 photon: intercept-measure-resend → changes $|\psi\rangle$

  intercept-entangle to her QC-resend

  → changes $|\psi\rangle$ (now ρ)

PROBLEMS?

Eavesdropping 102

Depending on the number of photons sent by Alice, there are different optimal eavesdropping strategies:

- 1 photon: intercept-measure-resend → changes $|\psi\rangle$

  intercept-entangle to her QC-resend

  → changes $|\psi\rangle$ (now ρ)

  PROBLEM: Assumes there's no 'leakage' to some other DOF.

  PROBLEM: There aren't any ideal single-photon sources yet…

  •2 photon: Eve can strip off and store one (PNS = 'photon number splitting') until she hears the classical discussion between Alice and Bob → how to measure her stored photon

- 3 photon: Eve can sometimes completely determine the state (e.g., {H,D,A} → "H", {H,V,D} → "D"). She can then send the correct state on to Bob.

"Decoy-State QKD"

Eve can stay undetected if channel loss too high:

- Eve blocks all pulses that have <2 photons
- She stores one, and uses lossless teleportation to deliver the expected state to the receiver (and waits to hear the basis info)
- Susceptible to this attack unless $\lceil < T/2$ → must use dim pulses

BUT…

- Alice uses pulses with different $\lceil_i$ (e.g., 0, 0.3, 0.6)
- Bob evaluates statistics of detected pulses
- Able to have secure QKD with brighter pulses

→ longer distance

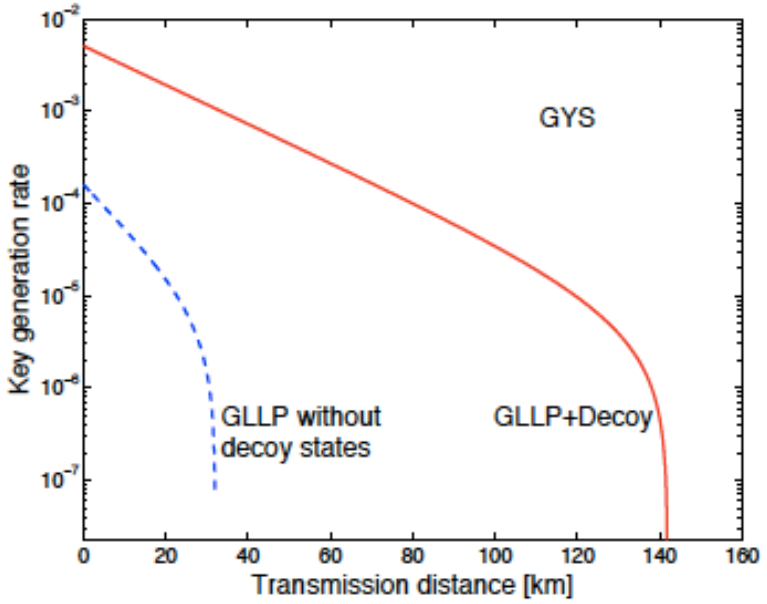


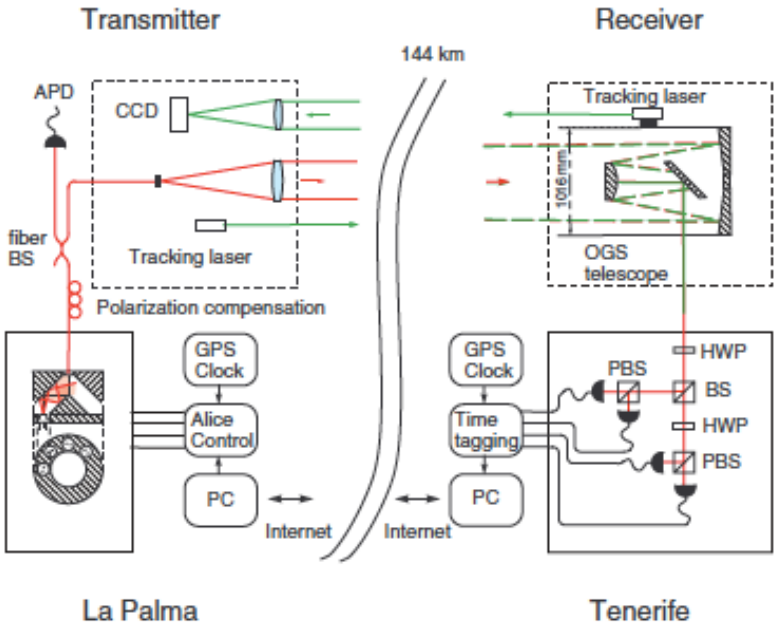
FIG. 3: Key rates for the experimental set-up in [26] using the GLLP results [21] with and without the

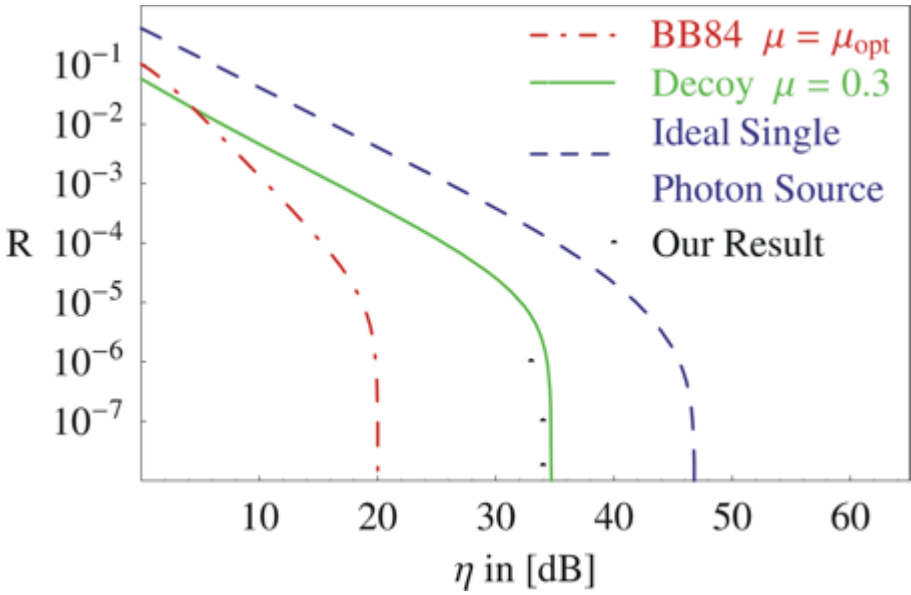
W.-Y. Hwang, PRL 91, 057901 (2003).
H.-K. Lo, X. Ma, and K. Chen, PRL 94, 230504 (2005).

Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km

Tobias Schmitt-Manderbach,[1,2,*] Henning Weier,[2] Martin Fürst,[2] Rupert Ursin,[3] Felix Tiefenbacher,[4,3] Thomas Scheidl,[4,3] Josep Perdigues,[5] Zoran Sodnik,[5] Christian Kurtsiefer,[6] John G. Rarity,[7] Anton Zeilinger,[4,3] and Harald Weinfurter[1,2]

We report on the experimental implementation of a Bennett-Brassard 1984 (BB84) protocol type quantum key distribution over a 144 km free-space link using weak coherent laser pulses. Optimization of the link transmission was achieved with bidirectional active telescope tracking, and the security was ensured by employing decoy-state analysis. This enabled us to distribute a secure key at a rate of 12.8 bit/s at an attenuation of about 35 dB. Utilizing a simple transmitter setup and an optical ground station capable of tracking a spacecraft in low earth orbit, this outdoor experiment demonstrates the feasibility of global key distribution via satellites.



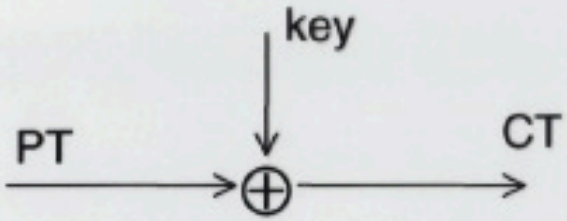


Note added.—A new Alice module now enabled, for 10 MHz pulse rate, a secure key rate of 42 bit/s.

How to use key material ?

The dream

- **use key material in one-time pad**
  - unconditionally secure encryption
  - requires as much key as plaintext
  - **impractical for most purposes**



Richard J. Hughes
Neutron Science & Technology, P-23
(505) 667-3876
hughes@lanl.gov
http://p23.lanl.gov/Quantum/quantum.html

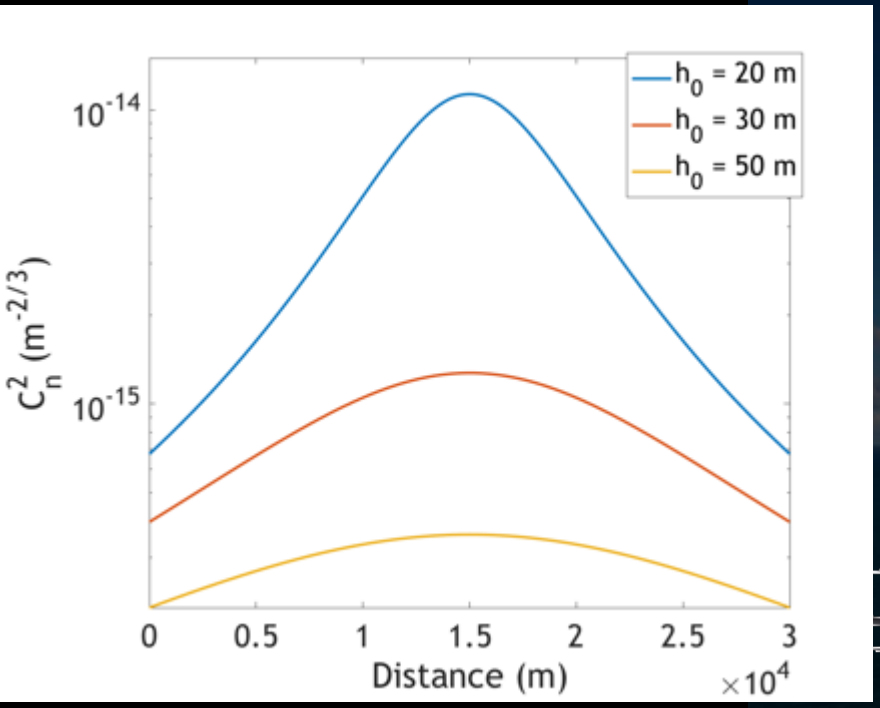
QKD for the Navy

Comprehensive, basic science investigation of free-space QKD strategies that can automatically adjust for optimal performance in the highly variable environment encountered over the sea deck and can operate at secure rates above 100 Mb/s.

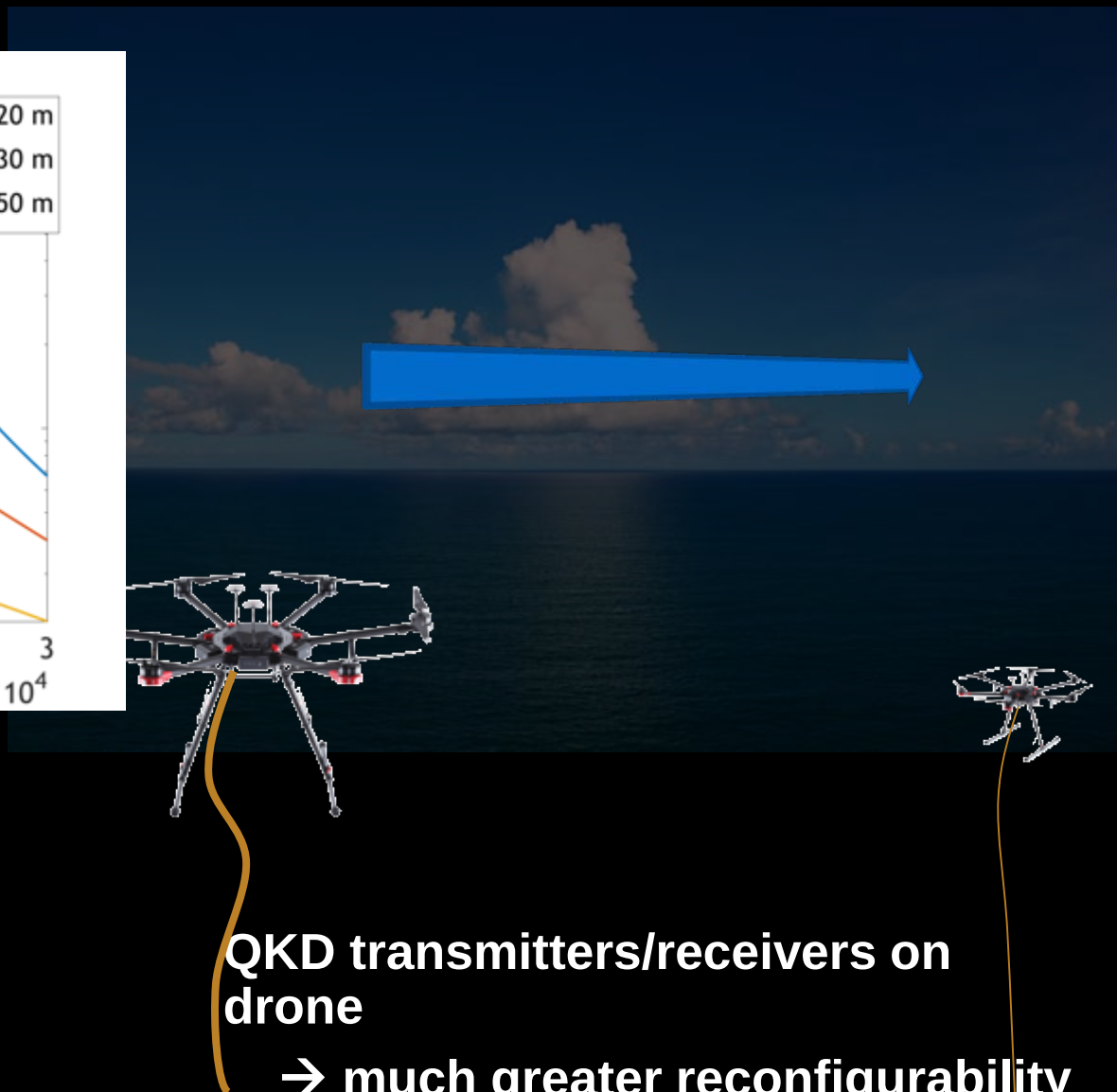
Problems – ???

UIUC, OSU, Duke,
Boston U., U. Arizona

Motivation



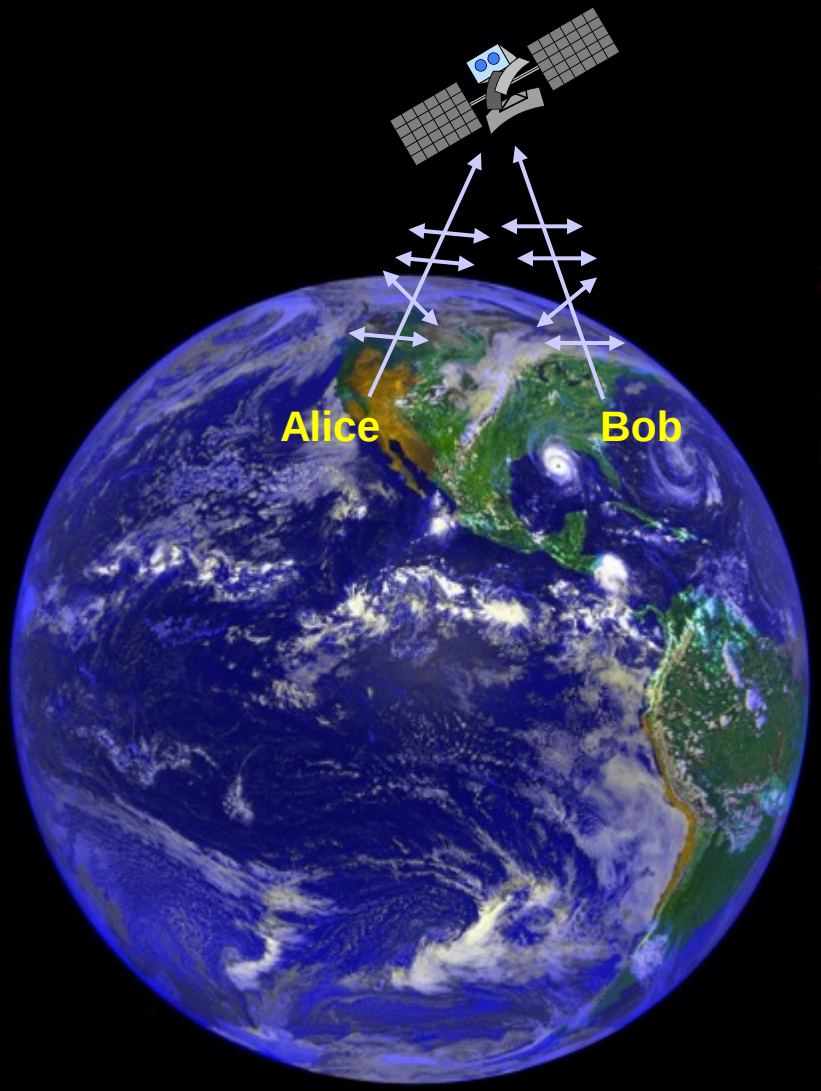
Turbulence strength scales favorably with height, especially over long distances due to earth curvature.



QKD transmitters/receivers on drone

→ **much greater reconfigurability**

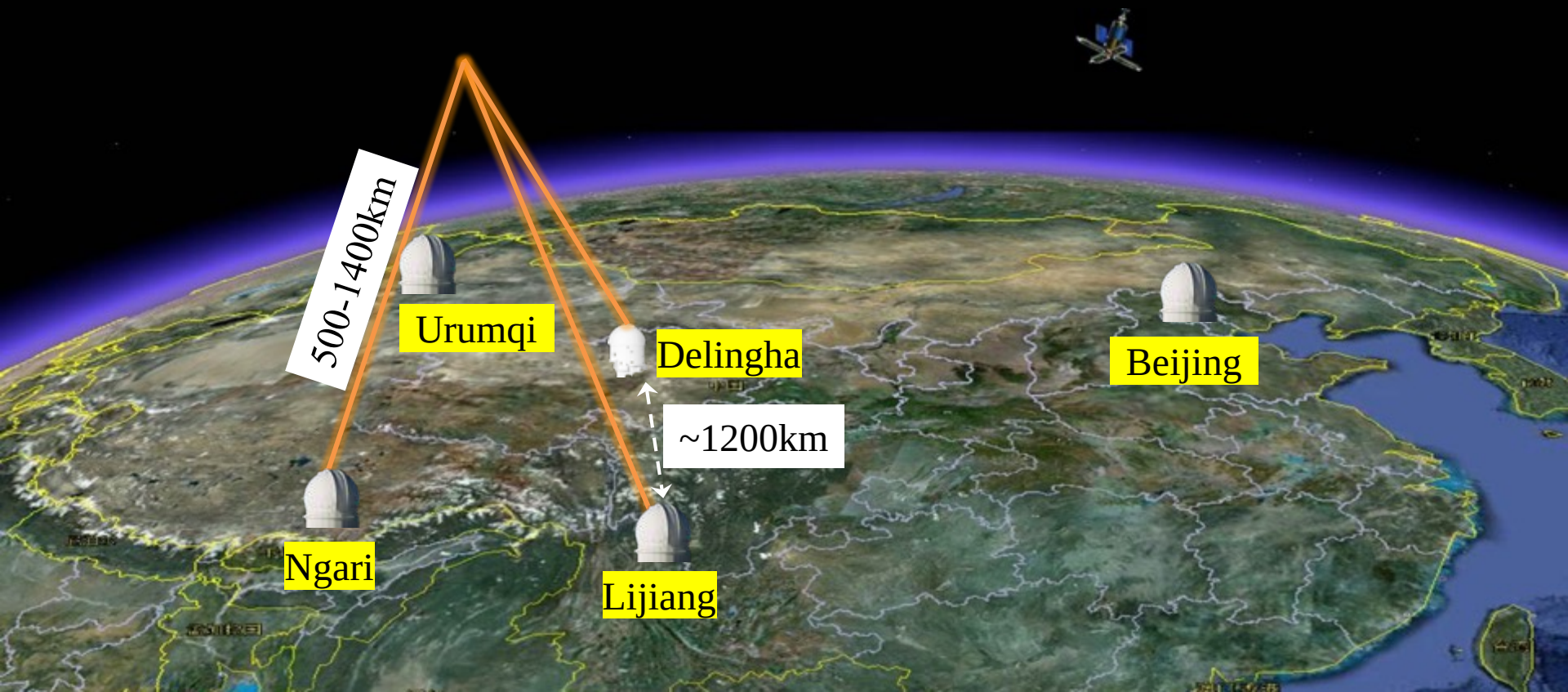
Satellite QKD for Long-Distance Key Generation



- Alice and Bob generate quantum keys K_A and K_B with satellite
- satellite tells Bob which bits need to be flipped, so that $K_B = K_A$
- Alice and Bob use K_A for encrypted communications
- Assumption that you trust the satellite. Unless you use entanglement, in which case the security can be constantly verified

Quantum Science Satellite “Micius”

- Launched on 16 Aug. 2016
- High-rate QKD between satellite and ground [Nature 549, 43 (2017]
- Quantum entanglement distribution from satellite, test of quantum nonlocality under strict Einstein's locality condition [Science 356, 1140 (2017)]
- Quantum teleportation between ground and satellite [Nature 549, 70 (2017)]



PHYSICAL REVIEW LETTERS **120,** 030501 (2018)

Satellite-Relayed Intercontinental Quantum Network

Sheng-Kai Liao,[1,2] Wen-Qi Cai,[1,2] Johannes Handsteiner,[3,4] Bo Liu,[4,5] Juan Yin,[1,2] Liang Zhang,[2,6] Dominik Rauch,[3,4] Matthias Fink,[4] Ji-Gang Ren,[1,2] Wei-Yue Liu,[1,2] Yang Li,[1,2] Qi Shen,[1,2] Yuan Cao,[1,2] Feng-Zhi Li,[1,2] Jian-Feng Wang,[7] Yong-Mei Huang,[8] Lei Deng,[9] Tao Xi,[10] Lu Ma,[11] Tai Hu,[12] Li Li,[1,2] Nai-Le Liu,[1,2] Franz Koidl,[13] Peiyuan Wang,[13] Yu-Ao Chen,[1,2] Xiang-Bin Wang,[2] Michael Steindorfer,[13] Georg Kirchner,[13] Chao-Yang Lu,[1,2] Rong Shu,[2,6] Rupert Ursin,[3,4] Thomas Scheidl,[3,4] Cheng-Zhi Peng,[1,2] Jian-Yu Wang,[2,6] Anton Zeilinger,[3,4] and Jian-Wei Pan[1,2]

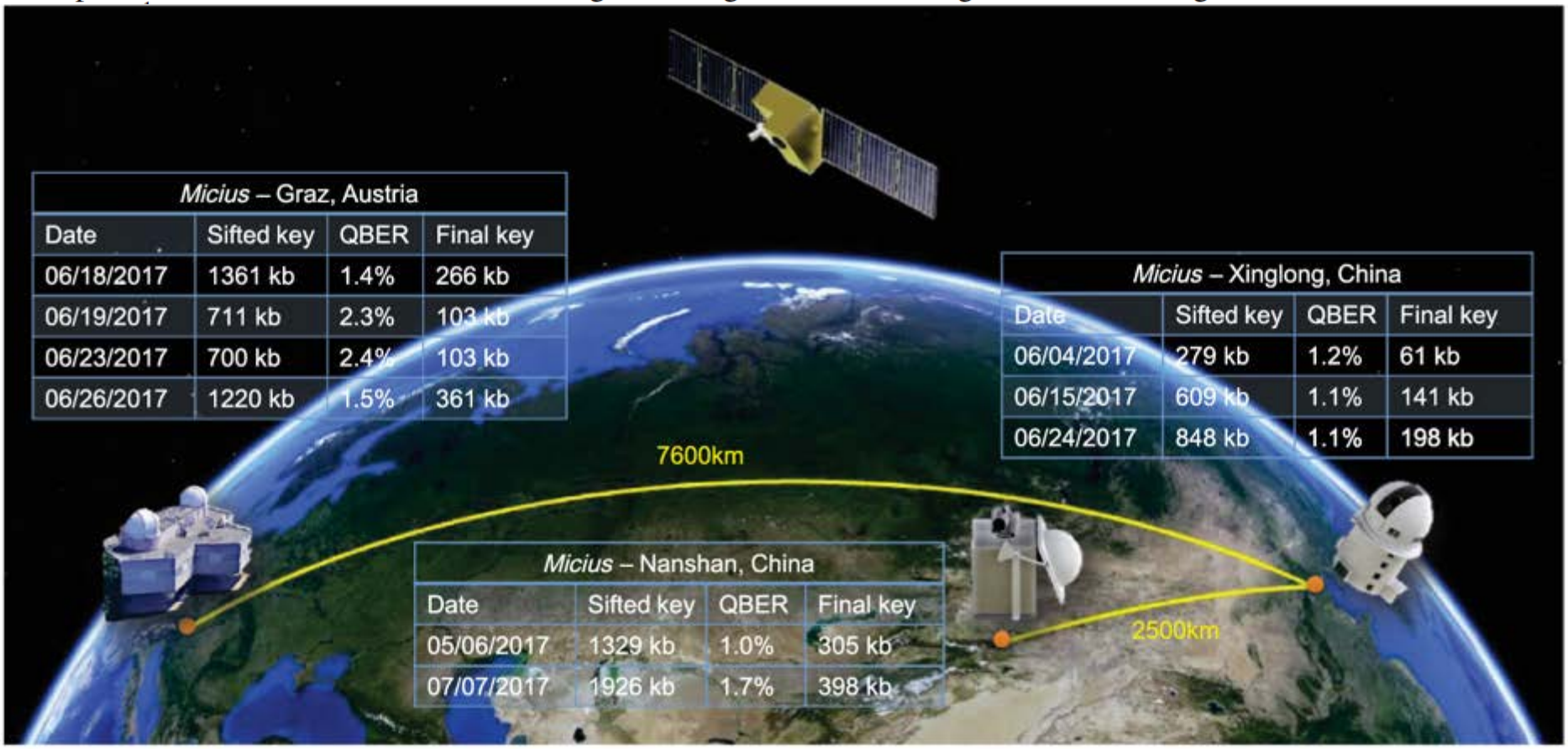
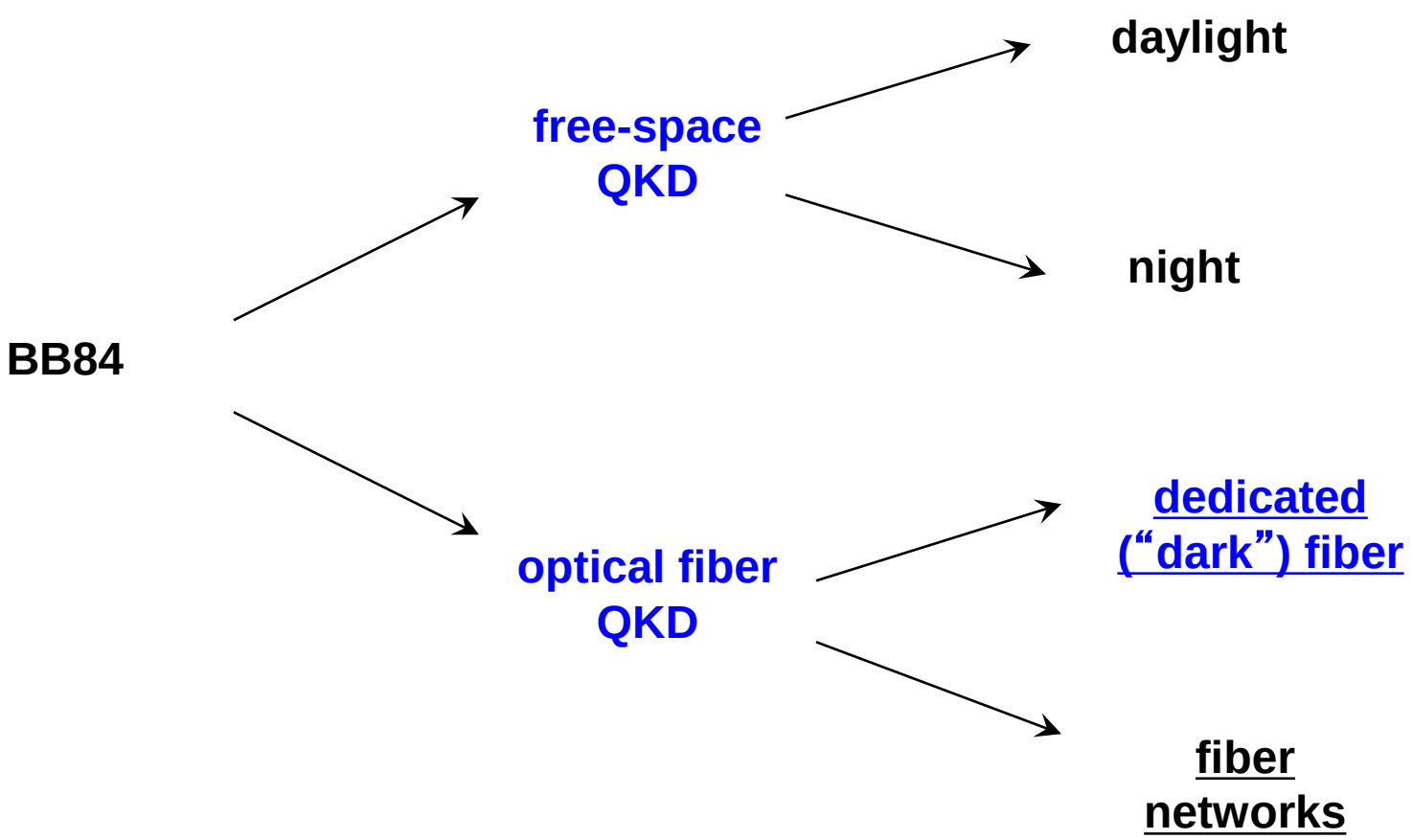


FIG. 1. Illustration of the three cooperating ground stations (Graz, Nanshan, and Xinglong). Listed are all paths used for key generation and the corresponding final key length.

In this work, QKD is performed in a downlink scenario—from the satellite to the ground. One of the payloads in the satellite is a space-qualified QKD transmitter [12], which uses weak coherent laser pulses to implement a decoy-state Bennett-Brassard 1984 (BB84) protocol that is immune to the photon-number-splitting attack [13,14]. Eight tunable fiber lasers, emitting light pulses with a wavelength of ~850 nm at a repetition rate of 100 MHz, are used to generate the signal, decoy, and vacuum states. After being collected into single-mode fibers and collimated, the laser pulses enter a BB84-encoding module. It consists of a half-wave plate (HWP), two polarizing beam splitters (PBSs), and one nonpolarizing beam splitter (BS). The photons emitted and sent to the ground station are randomly prepared in one of the four polarization states: horizontal, vertical, linear 45°, and linear −45°. In the three ground stations, corresponding BB84-decoding setups are used, consisting of a BS, a HWP, two PBSs and four single-photon detectors [15].

A photography of a quantum-secure intercontinental video conference held between Chinese Academy of Sciences and Austrian Academy of Sciences on 29 September, providing a real-world demonstration of quantum communication. Credit: Chinese Academy of Sciences

Evolution of QKD experiments



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