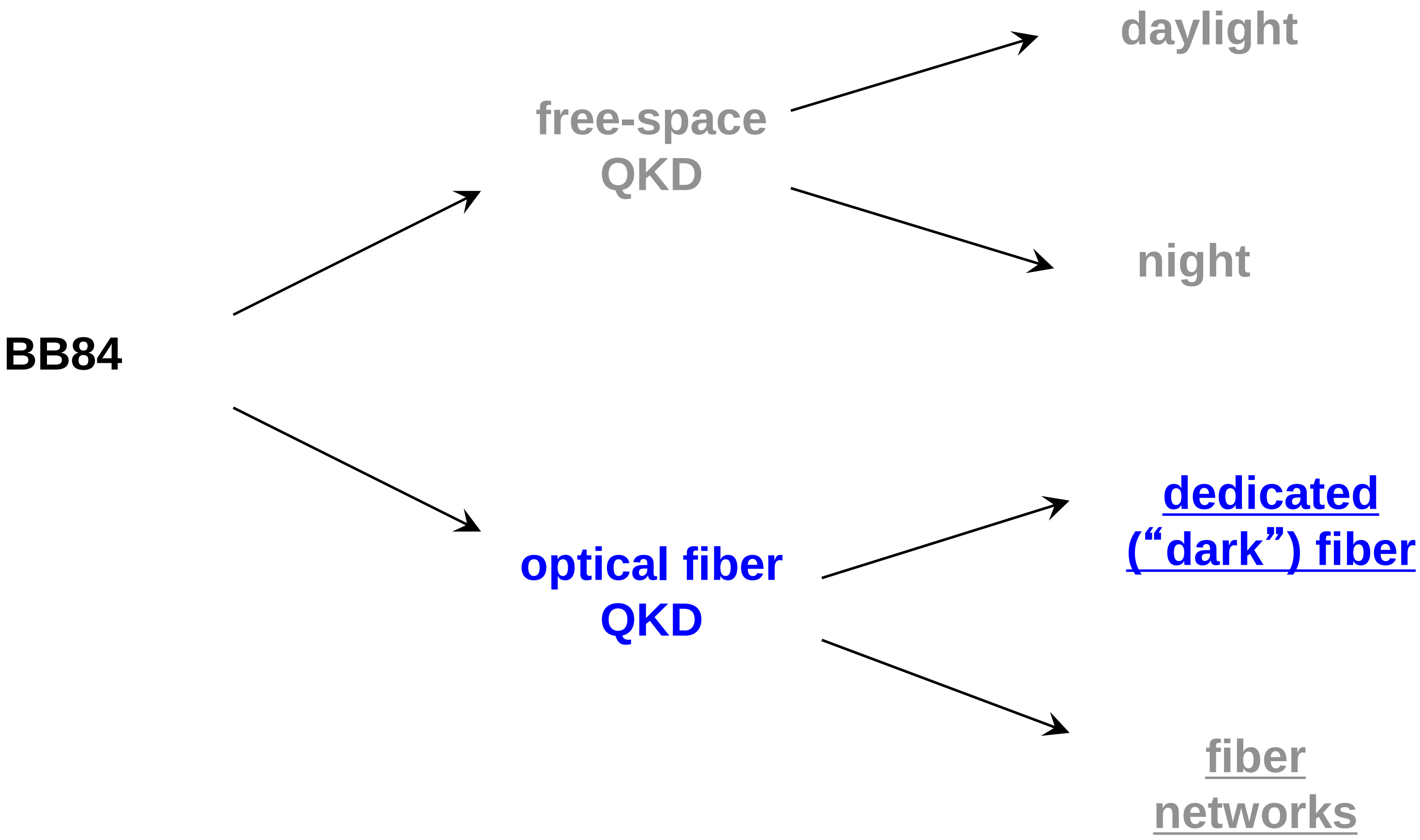
Evolution of QKD experiments



BB84

free-space QKD

daylight

night

optical fiber QKD

dedicated ("dark") fiber

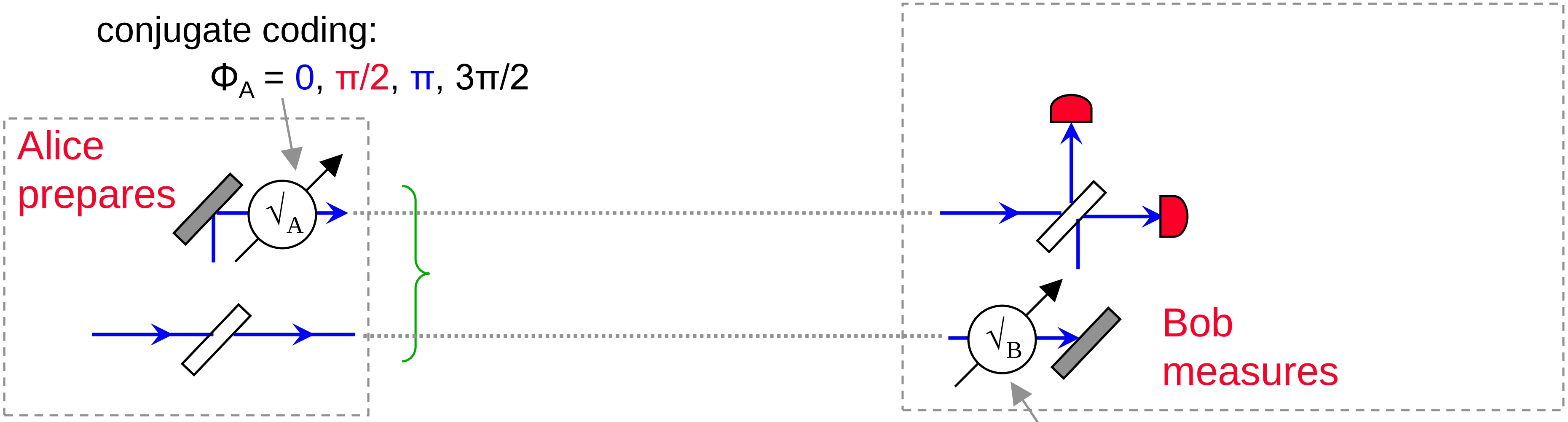
fiber networks

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

Interferometric implementation of BB84 QKD in fiber

conjugate coding:

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

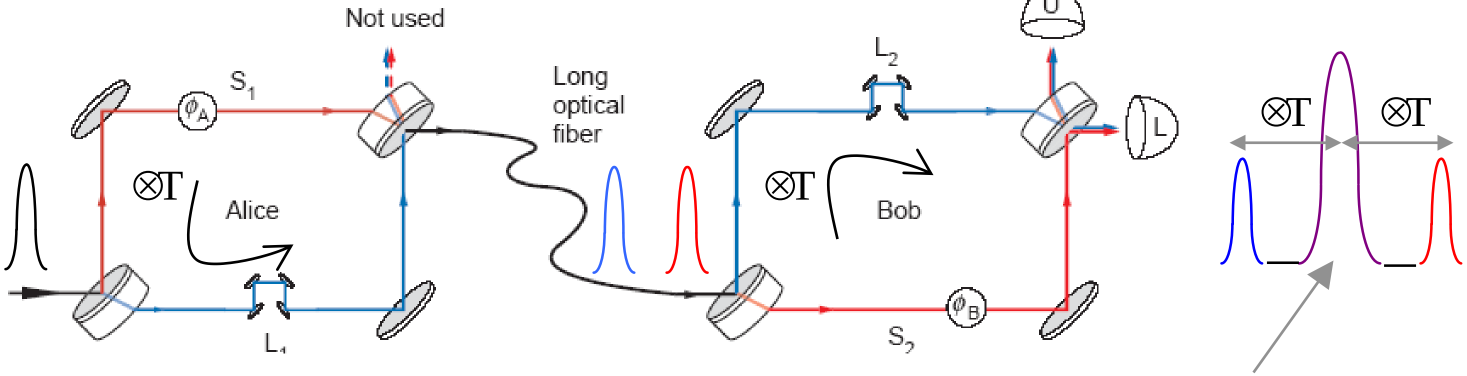


Alice prepares

Bob measures

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

Practical design multiplexes onto one fiber for stability:



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

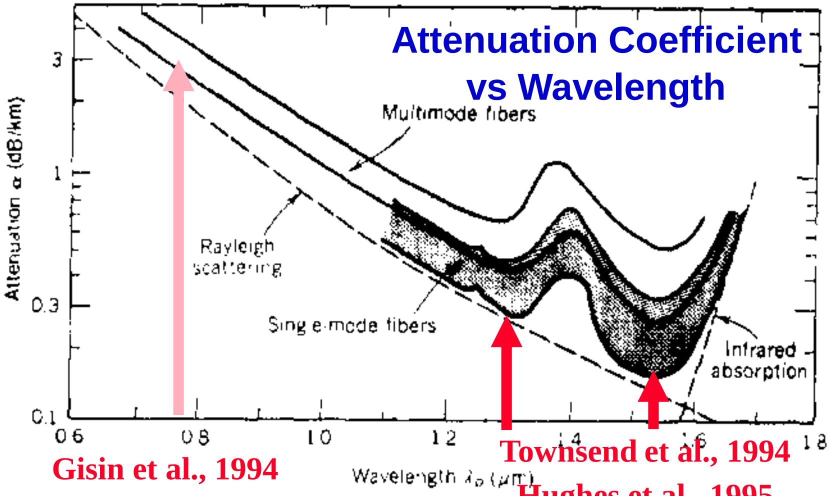
C. H. Bennett, Phys Rev Lett (1992)

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

InGaAs APDs

QKD over telecommunications fiber networks ?

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



Gisin et al., 1994

Franson et al., 1994

Townsend et al., 1994

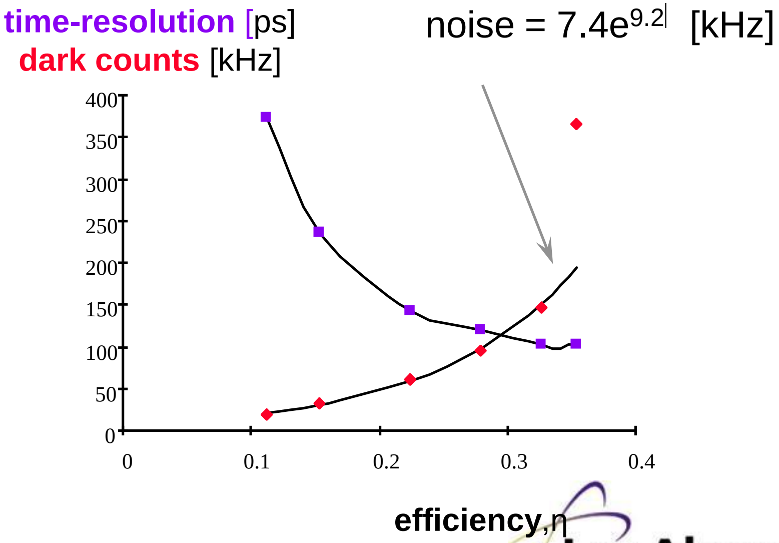
Hughes et al., 1995

Gisin et al. 1996

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

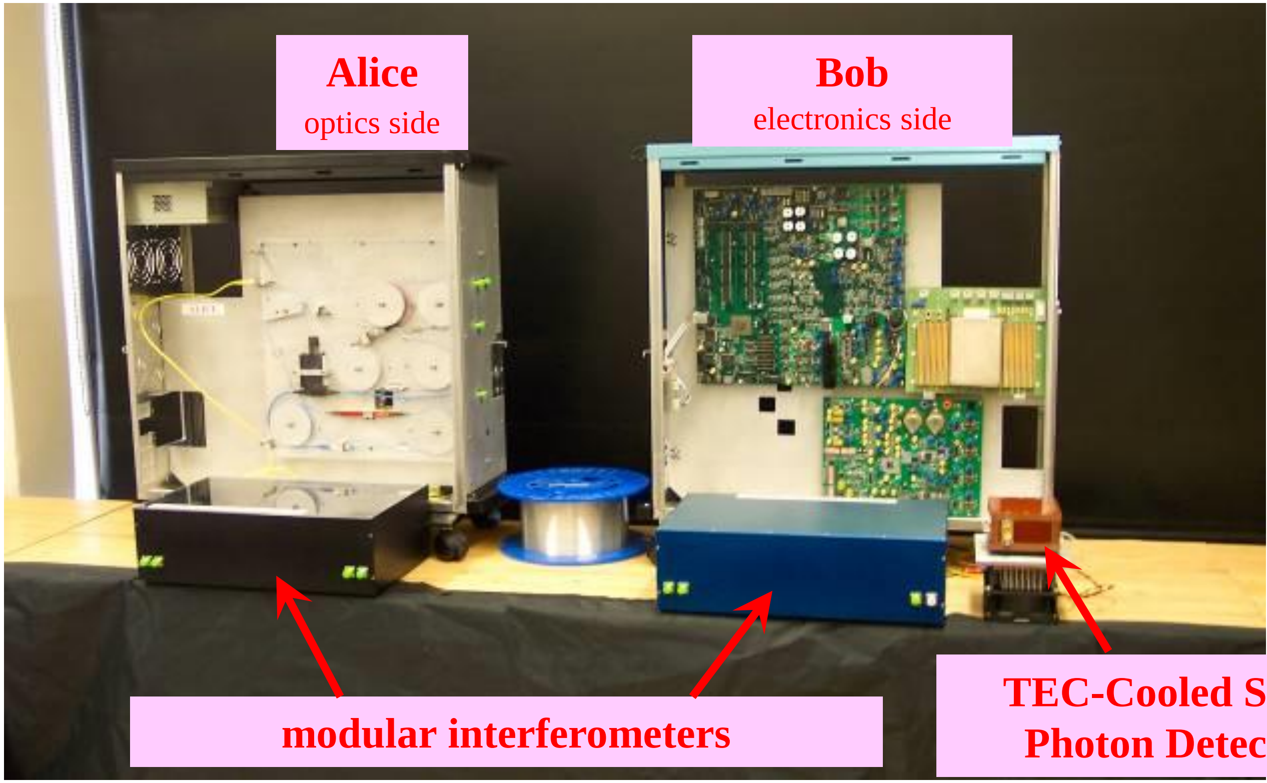
Optical fiber quantum key distribution

- Use phase/interferometers instead of polarization/polarizers
- >2 commercial companies (IDQuantique, MagiQ)
- Only a point-to-point protocol, and no optical→electrical

Third Generation LANL Fiber QKD System: F3QKD

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

- **designed to be "network friendly"**
- **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**



Alice
optics side

Bob
electronics side

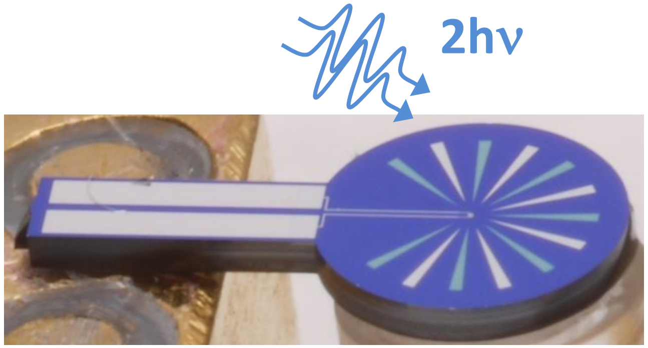
modular interferometers

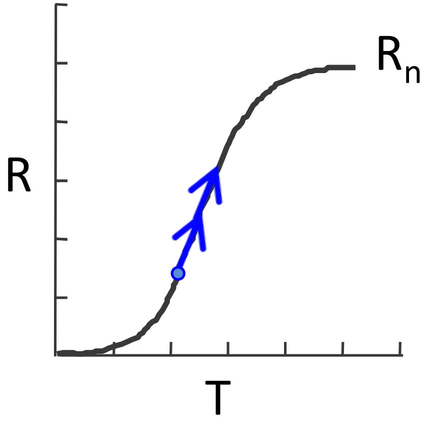
TEC-Cooled Single-Photon Detectors

Tungsten (W) Transition Edge Sensor (TES) Photon Number Resolving (PNR)

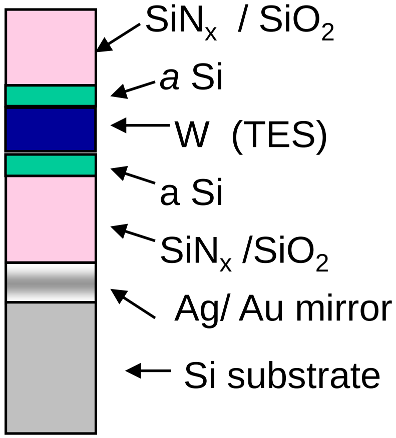
NIST
S. W. Nam
A. Lita
A. Miller
B. Calkins
T. Gerrits
K. Shalm

Calorimetric detection of UV/optical/IR photons

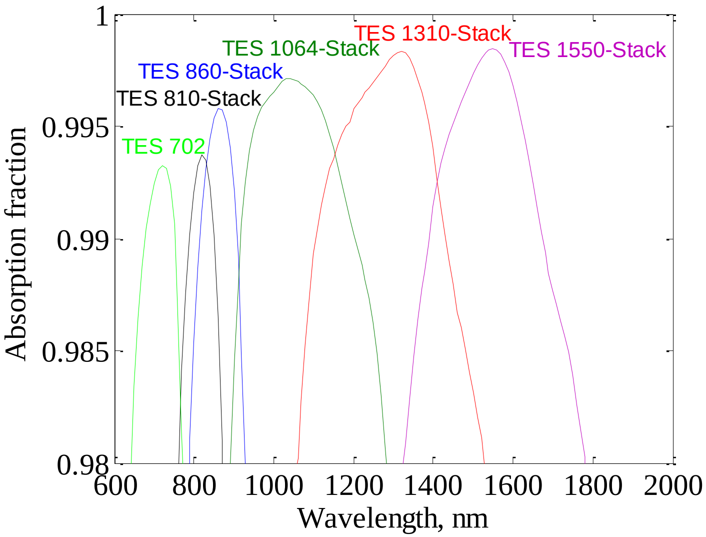


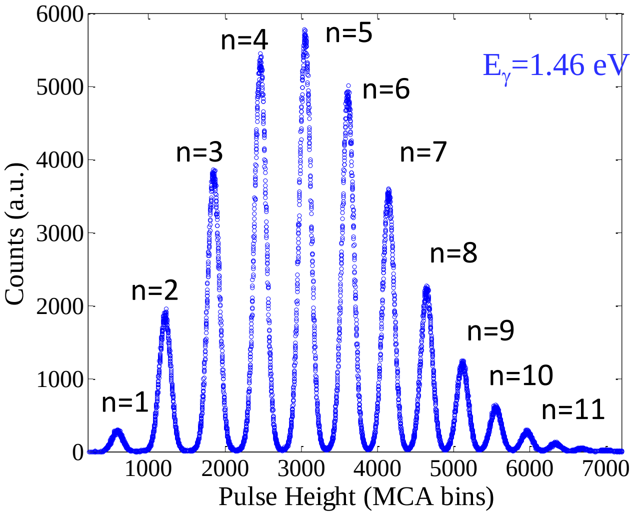


Optical stack



TES Simulated Absorption





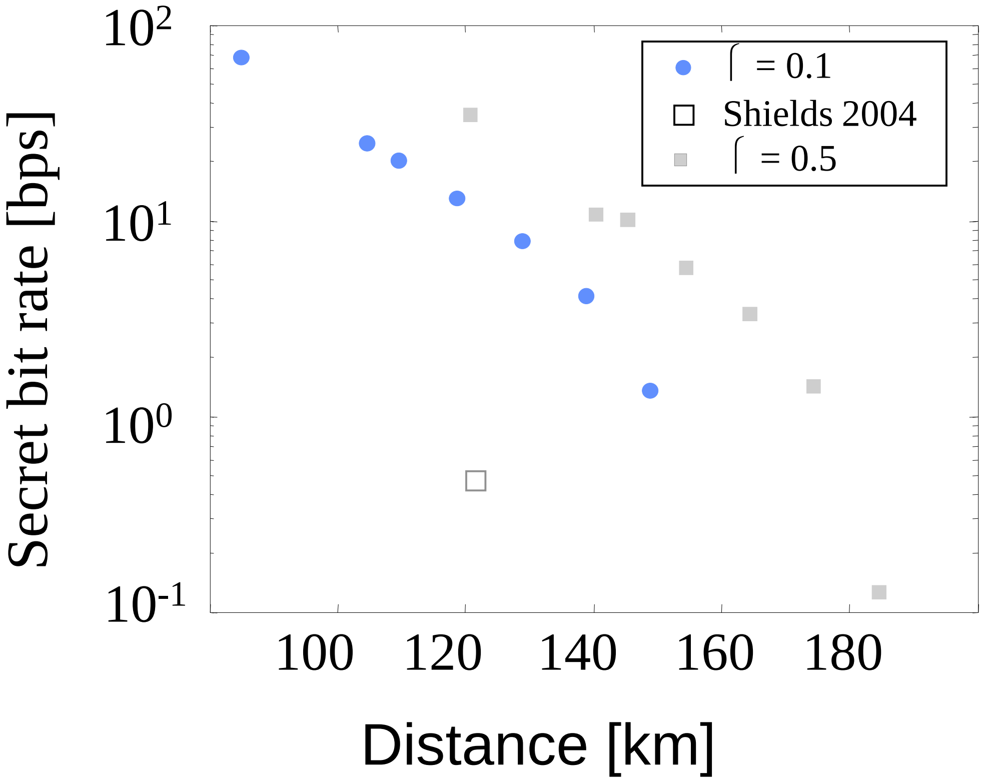
Fiber coupled self-aligned TES
< 1% coupling loss

A. E. Lita *et al.*, Opt. Exp. **16**, 3032 (2008)

Record-setting ranges and secret bit rates with TES QKD

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

- CASCADE error correction
- BBBSS91 privacy amplification



BBBSS91-security at ⌠=0.1 over **148 km*,** a new record.

x50 secret bit rate at **122 km** with ⌠=0.1 (previous record: Shields APL 2004)

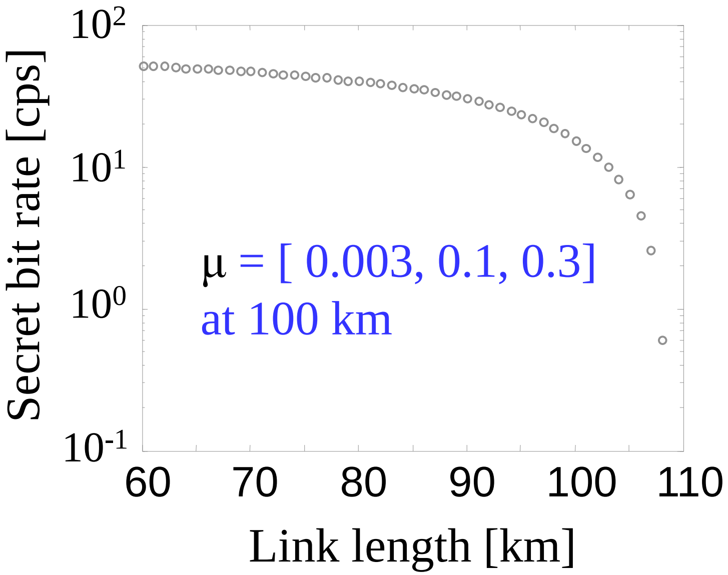
BBBSS91-secure transmission at ⌠=0.5 over **185 km*,** a new record. **(Assumes no PNS attack)**

* P. Hiskett et al, New J Phys 8, 193 (2006)

Decoy state QKD with TES detectors

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 signal levels in F3 laboratory system running at 2.5 MHz



μ = [0.003, 0.1, 0.3]
at 100 km

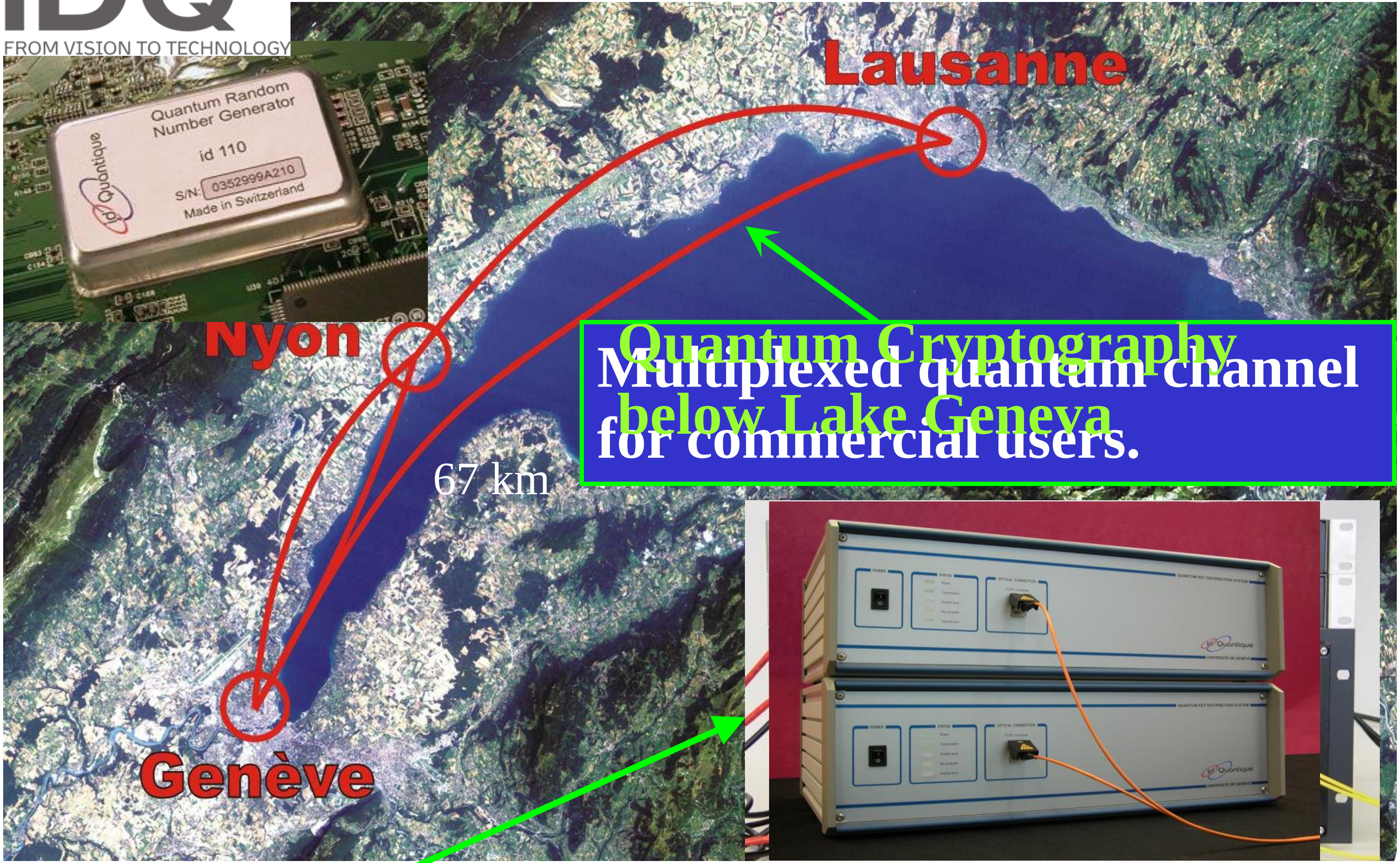
Creation of PNS-secure key over 107 km of optical fiber*, an increase of 80% over previous highest reported distance of 60 km

- (see H.-K. Lo quant-ph/0601168)

*D. Rosenberg et al, Phys Rev Lett 98, 010503 (2007)
(see also Peng et al., and Weinfurter et al., same issue)

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

Spin-off, University of Geneva 2001

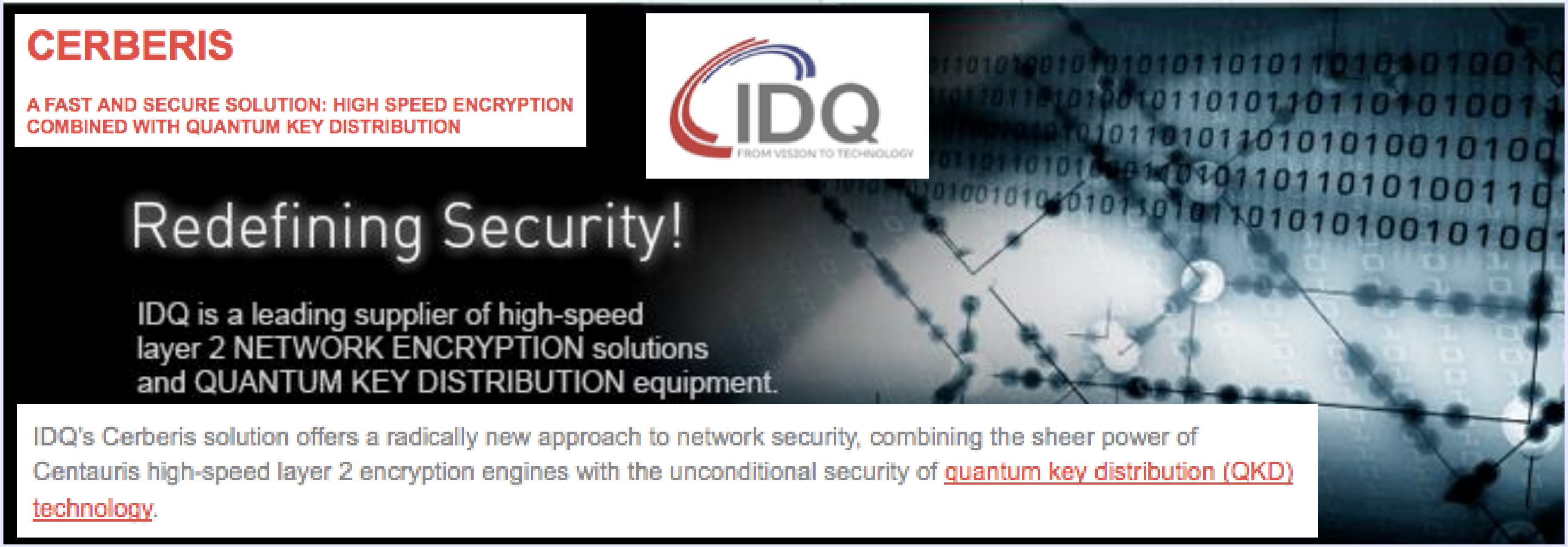


Quantum Cryptography below Lake Geneva

Multiplexed quantum channel for commercial users.

Used daily by some commercial customers

QKD Goes Commercial…



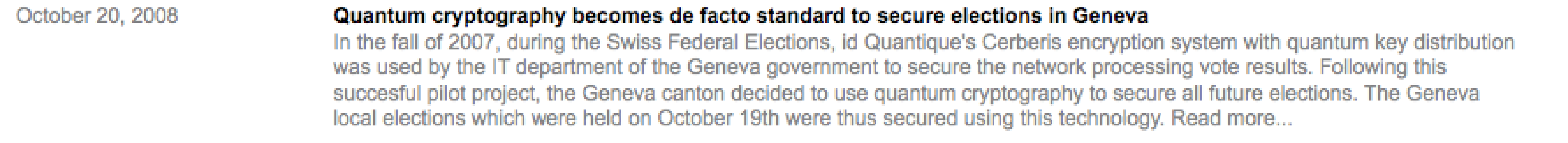
CERBERIS

A FAST AND SECURE SOLUTION: HIGH SPEED ENCRYPTION COMBINED WITH QUANTUM KEY DISTRIBUTION

Redefining Security!

IDQ is a leading supplier of high-speed layer 2 NETWORK ENCRYPTION solutions and QUANTUM KEY DISTRIBUTION equipment.

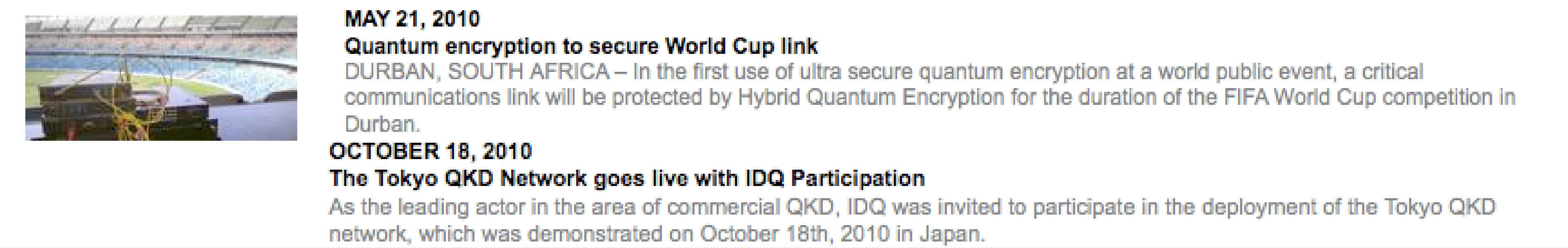
IDQ's Cerberis solution offers a radically new approach to network security, combining the sheer power of Centauris high-speed layer 2 encryption engines with the unconditional security of quantum key distribution (QKD) technology.



October 20, 2008

Quantum cryptography becomes de facto standard to secure elections in Geneva

In the fall of 2007, during the Swiss Federal Elections, id Quantique's Cerberis encryption system with quantum key distribution was used by the IT department of the Geneva government to secure the network processing vote results. Following this succesful pilot project, the Geneva canton decided to use quantum cryptography to secure all future elections. The Geneva local elections which were held on October 19th were thus secured using this technology. Read more...



MAY 21, 2010

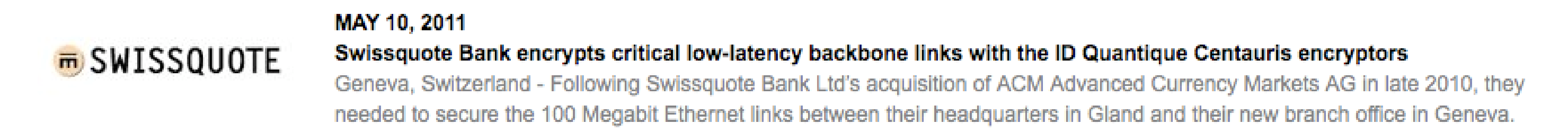
Quantum encryption to secure World Cup link

DURBAN, SOUTH AFRICA – In the first use of ultra secure quantum encryption at a world public event, a critical communications link will be protected by Hybrid Quantum Encryption for the duration of the FIFA World Cup competition in Durban.

OCTOBER 18, 2010

The Tokyo QKD Network goes live with IDQ Participation

As the leading actor in the area of commercial QKD, IDQ was invited to participate in the deployment of the Tokyo QKD network, which was demonstrated on October 18th, 2010 in Japan.



MAY 10, 2011

Swissquote Bank encrypts critical low-latency backbone links with the ID Quantique Centauris encryptors

Geneva, Switzerland - Following Swissquote Bank Ltd's acquisition of ACM Advanced Currency Markets AG in late 2010, they needed to secure the 100 Megabit Ethernet links between their headquarters in Gland and their new branch office in Geneva.

Is loss a problem for QKD?

PHYSICAL REVIEW LETTERS **121,** 190502 (2018)

Secure Quantum Key Distribution over 421 km of Optical Fiber

Alberto Boaron,[1,*] Gianluca Boso,[1] Davide Rusca,[1] Cédric Vulliez,[1] Claire Autebert,[1] Misael Caloz,[1] Matthieu Perrenoud,[1] Gaëtan Gras,[1,2] Félix Bussières,[1] Ming-Jun Li,[3] Daniel Nolan,[3] Anthony Martin,[1] and Hugo Zbinden[1]

We present a quantum key distribution system with a 2.5 GHz repetition rate using a three-state time-bin protocol combined with a one-decoy approach. Taking advantage of superconducting single-photon detectors optimized for quantum key distribution and ultralow-loss fiber, we can distribute secret keys at a maximum distance of 421 km and obtain secret key rates of 6.5 bps over 405 km.

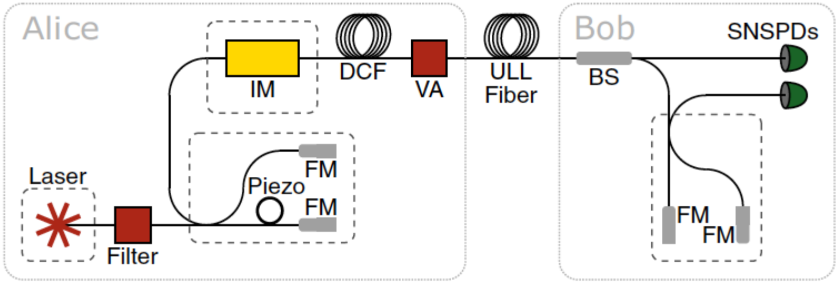


FIG. 1. Schematics of the experimental setup. Laser: 1550 nm distributed feedback laser; filter: 270 pm bandpass filter; piezo: piezoelectric fiber stretcher; FM: Faraday mirror; IM: intensity modulator; DCF: dispersion compensating fiber; VA: variable attenuator; ULL fiber: ultralow-loss single-mode fiber; BS: beam splitter; SNSPDs: superconducting nanowire single-photon detectors. Dashed lines represent temperature stabilized boxes.

The quantum channel (QC) is composed of spools of SMF-28® ultralow-loss (ULL) single-mode fiber (SMF) (Corning) which has an attenuation of about 0.16 dB/km

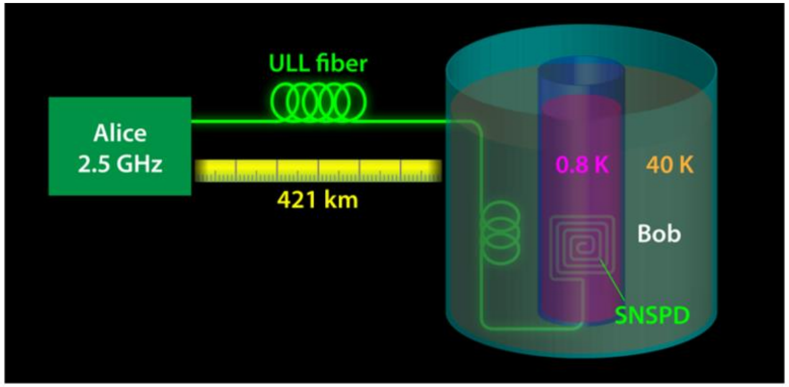


Figure 1: Sketch of the scheme used by Boaron *et al.* to demonstrate QKD over a record distance of 421 km. The setup uses an ultralow-loss (ULL) optical fiber, an electro-optical system with a high repetition rate (2.5 GHz), and a low-noise detection unit based on superconducting nanowire single-photon detectors

in a spiraling pattern on a flat surface. To reduce the dark counts in the detectors, the team cooled them down to 0.8 K and used a fiber filter cooled to 40 K to cut off the black body emission of the optical fiber connected to the detectors. These measures reduced the dark count rate to an impressive 0.1 Hz, about 2 orders of magnitude lower than commercially available SNSPDs. With these technical tricks, the probability of detecting a dark count when a photon was expected was lowered to 10^{-11}.

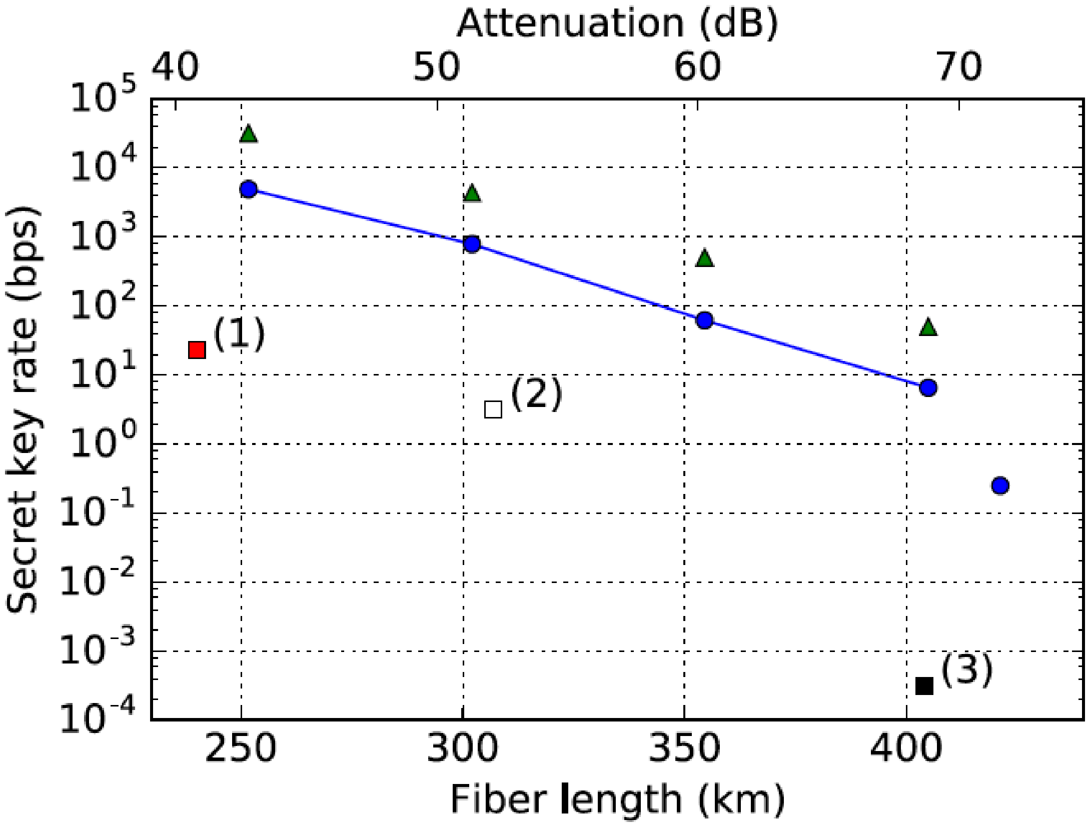


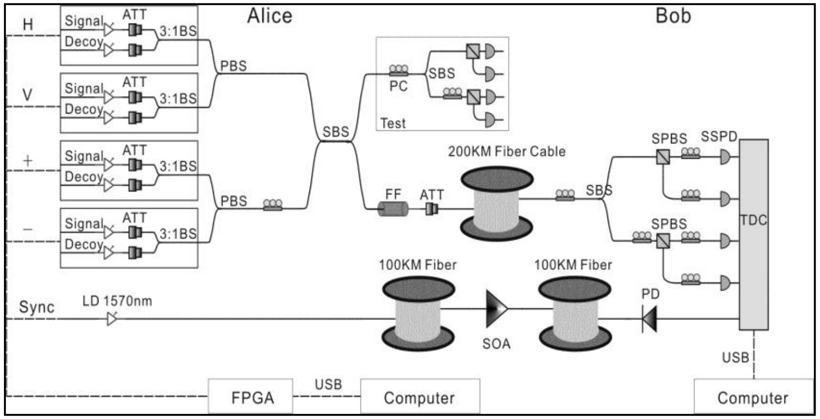
FIG. 2. Circles denote experimental final SKR versus fiber length. Triangles denote simulation of an idealized BB84 protocol with the same block sizes as the corresponding experimental points. Squares denote results of other long-distance QKD experiments using finite-key analysis: (1) BB84, Frölich *et al.* [22]; (2) coherent one-way, Korzh *et al.* [23]; (3) measurement-device-independent QKD, Yin *et al.* [3]. (Average fiber loss for: (1): 0.185 dB/km; (2): 0.169 dB/km; (3): 0.168 dB/km; this work: 0.171 dB/km.) The upper axis indicates the overall attenuation based on a fiber loss of 0.17 dB/km.

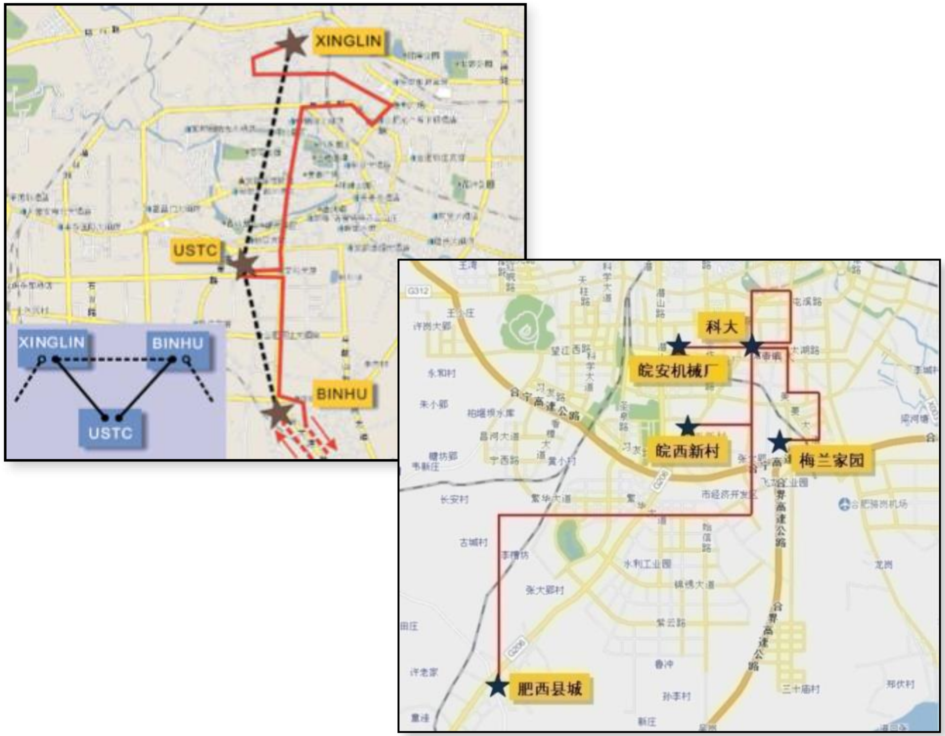
Bringing quantum secured key exchange to the consumer

University of BRISTOL
BANK OF THE FUTURE
Artwork By RWN 09
Thursday 4th 2015
GENERATING SECURE KEYS VIA QKD

Could use one-time-pad to protect the PIN
Generate one-time-pad using quantum secured key exchange
Key exchange at ATM allows user to ‘top-up’ a personal one-time-pad.

Practical Quantum Cryptography





- **Fiber-based decoy state QKD over 100km**

Peng *et al.*, PRL 98, 010505 (2007)

- **Fiber-based decoy state QKD over 200km**

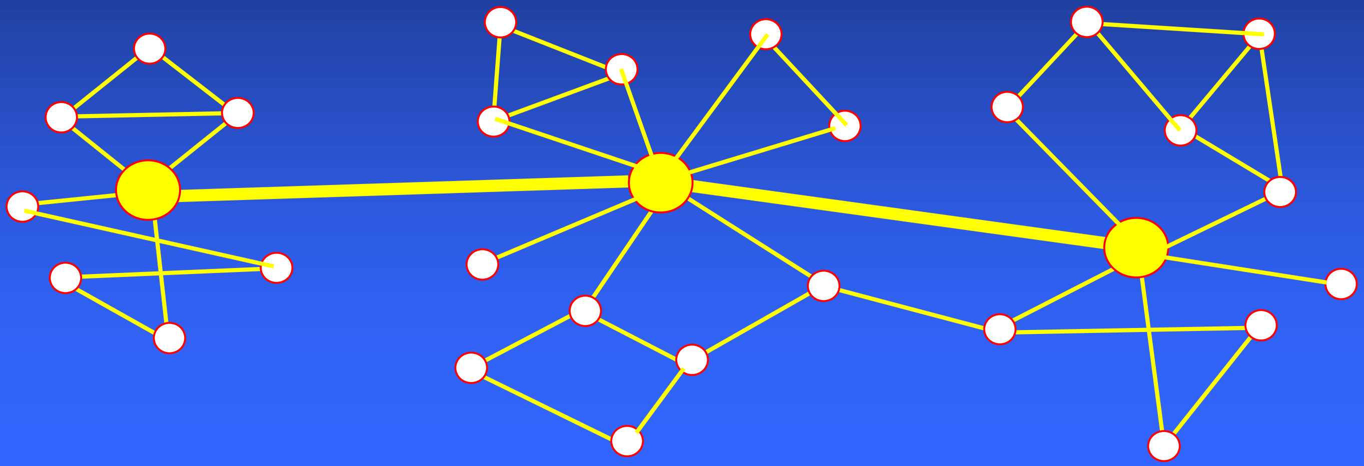
Liu *et al.*, Optics Express 18, 8587 (2010)

- **Intra-city network**

Chen et al., Optics Express 17, 6540 (2009)

Chen et al., Optics Express 18, 27217 (2010)

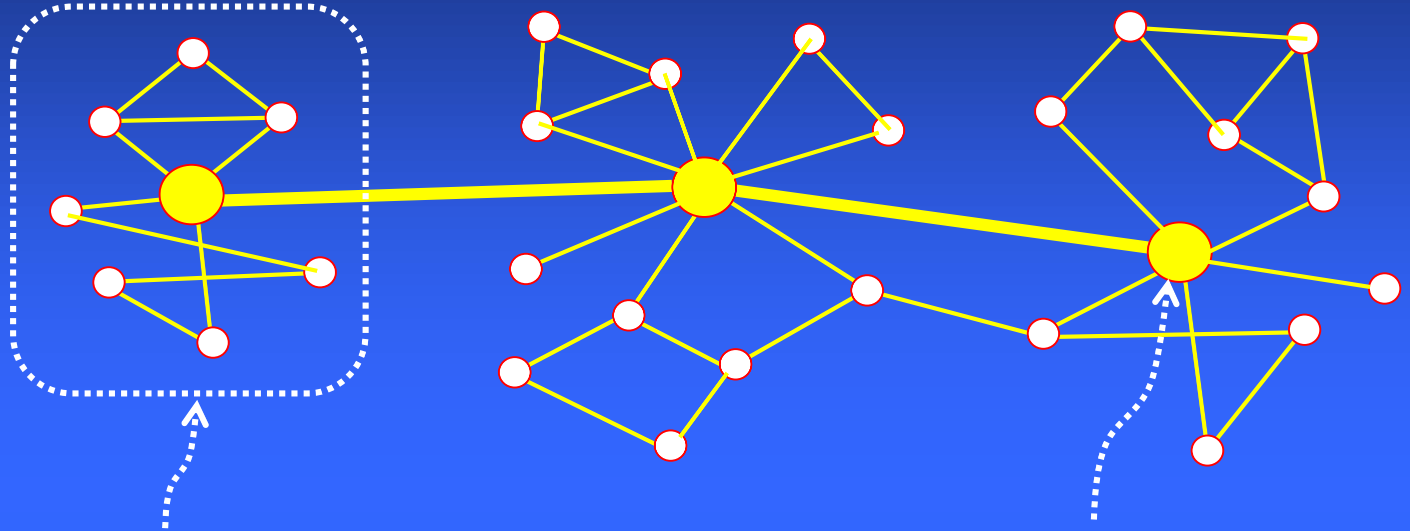
Scalable multi-user QKD network



- QKD clusters and small number of strong hubs
- Most of nodes in the clusters have only 2 or 3 links
- No isolated nodes

Secure key can be relayed over the entire network only by a few hops.

Scalable multi-user QKD network



QKD cluster

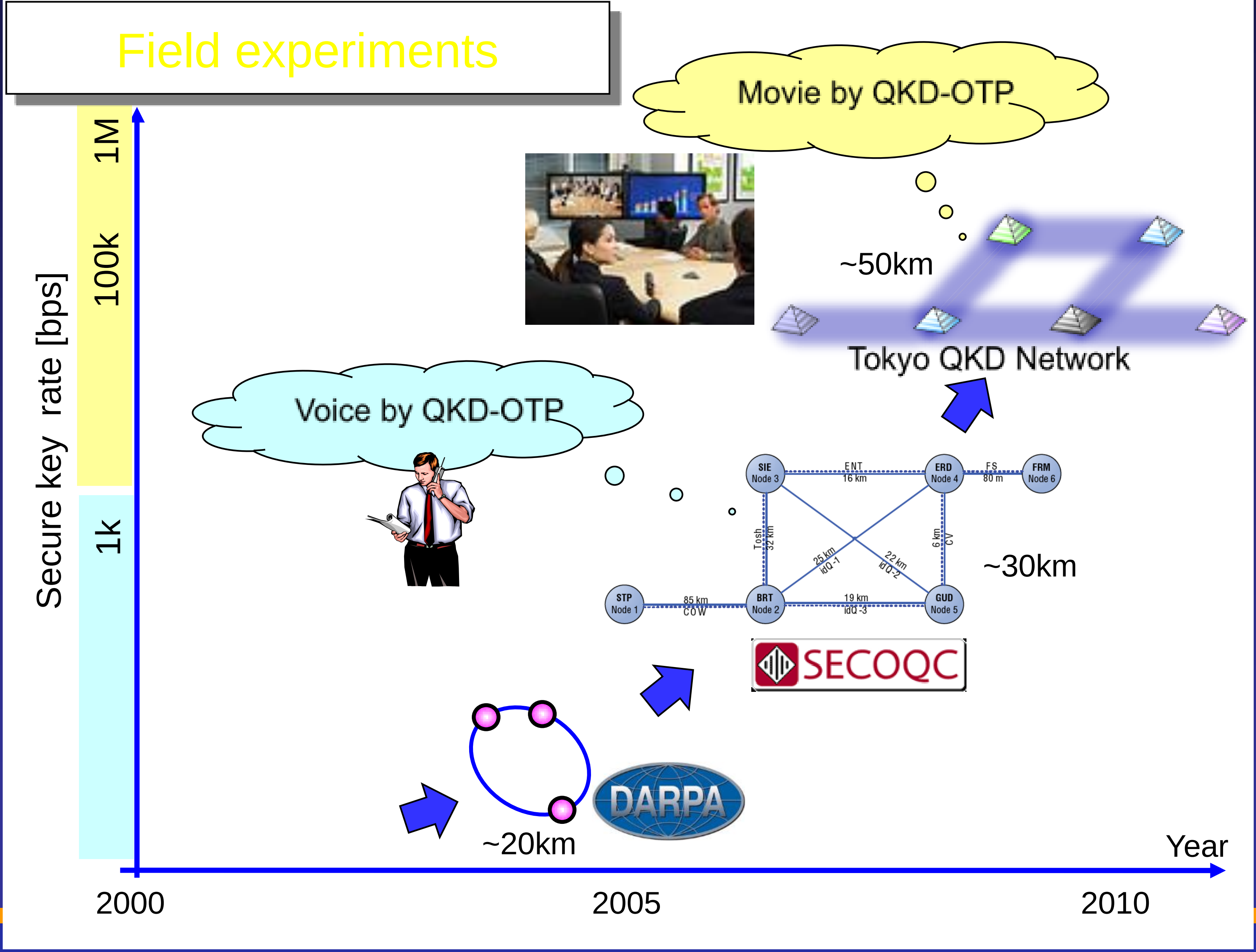
Hub (key management center)

- Photon routers
- Compact QKD systems
- APDs

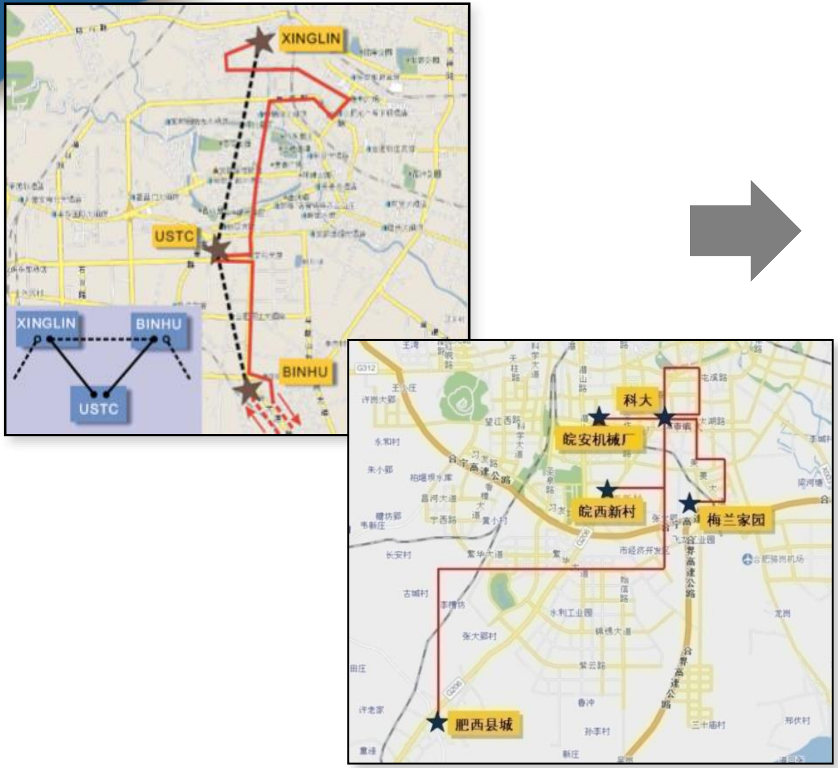
- Trusted nodes
- WDM-QKD systems
- SSPDs for long distance QKD

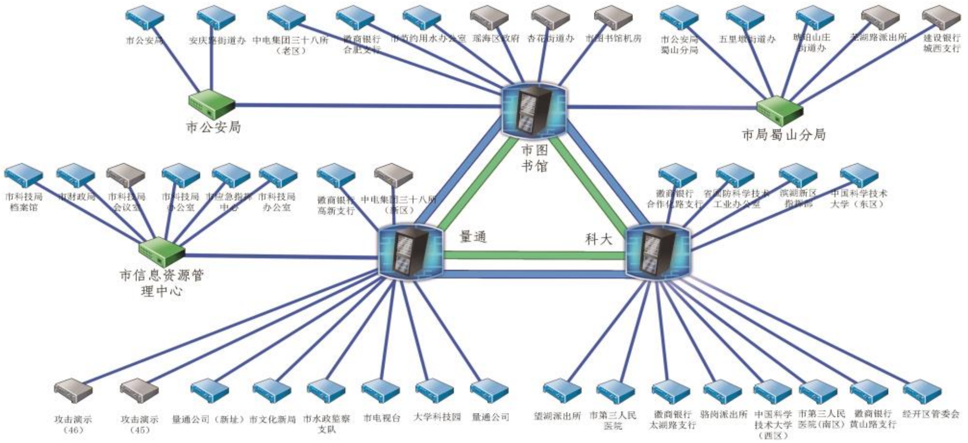
High cost and control complexity must be absorbed
by small number of hubs.

Quantum Networking

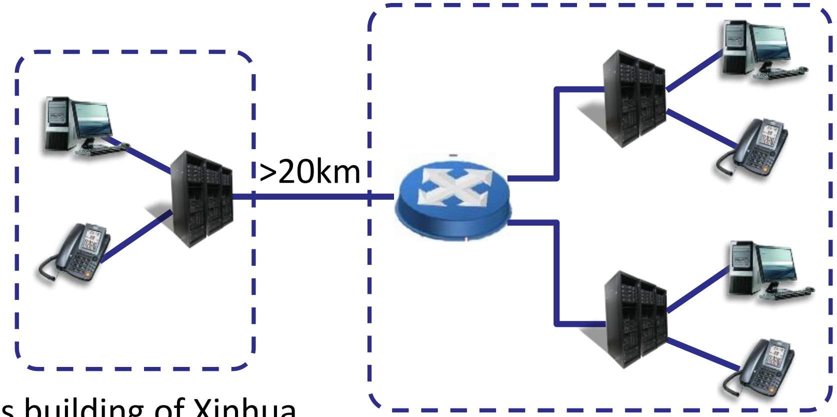


Practical Metropolitan QKD Networks





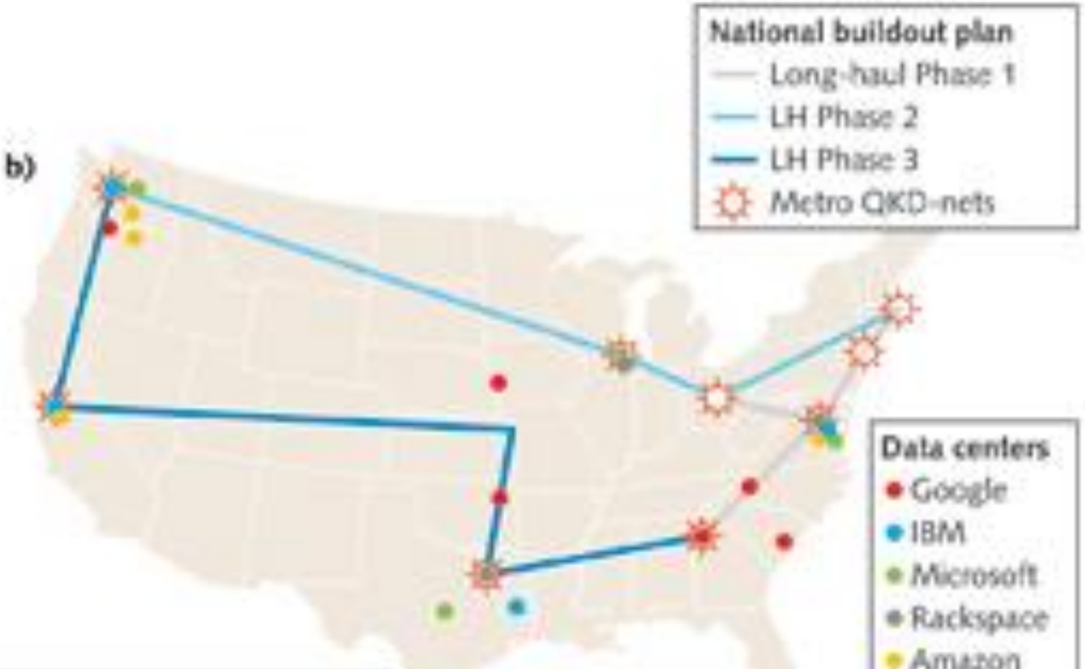
Hefei intra-city QKD network (46 nodes, 2012)



News building of Xinhua News Agency

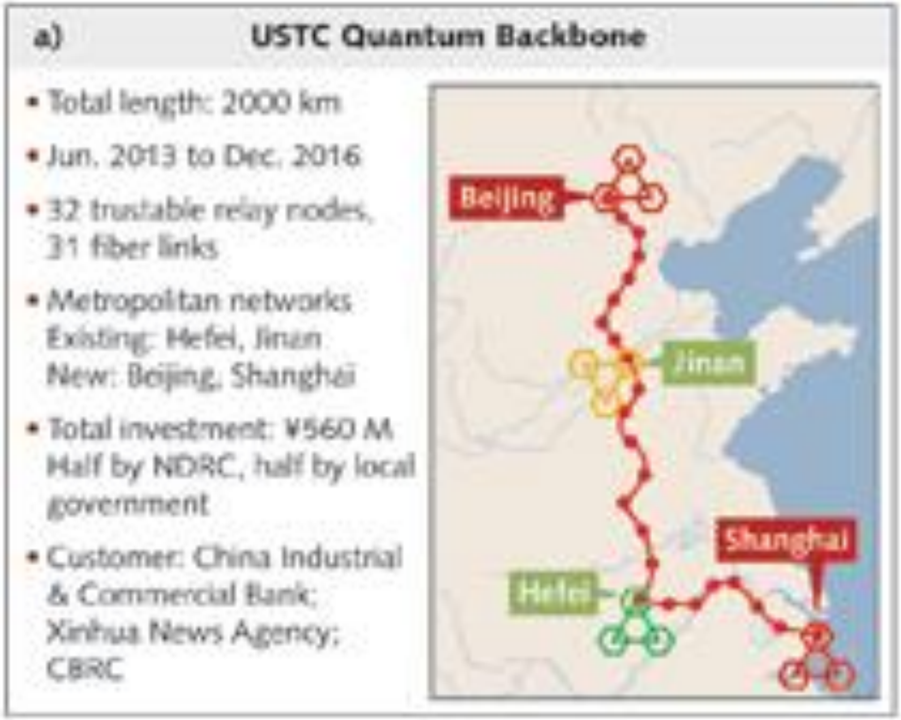
Financial Information Exchange of Xinhua News Agency

Quantum communication-based transmission network of financial information (Beijing, 2012)



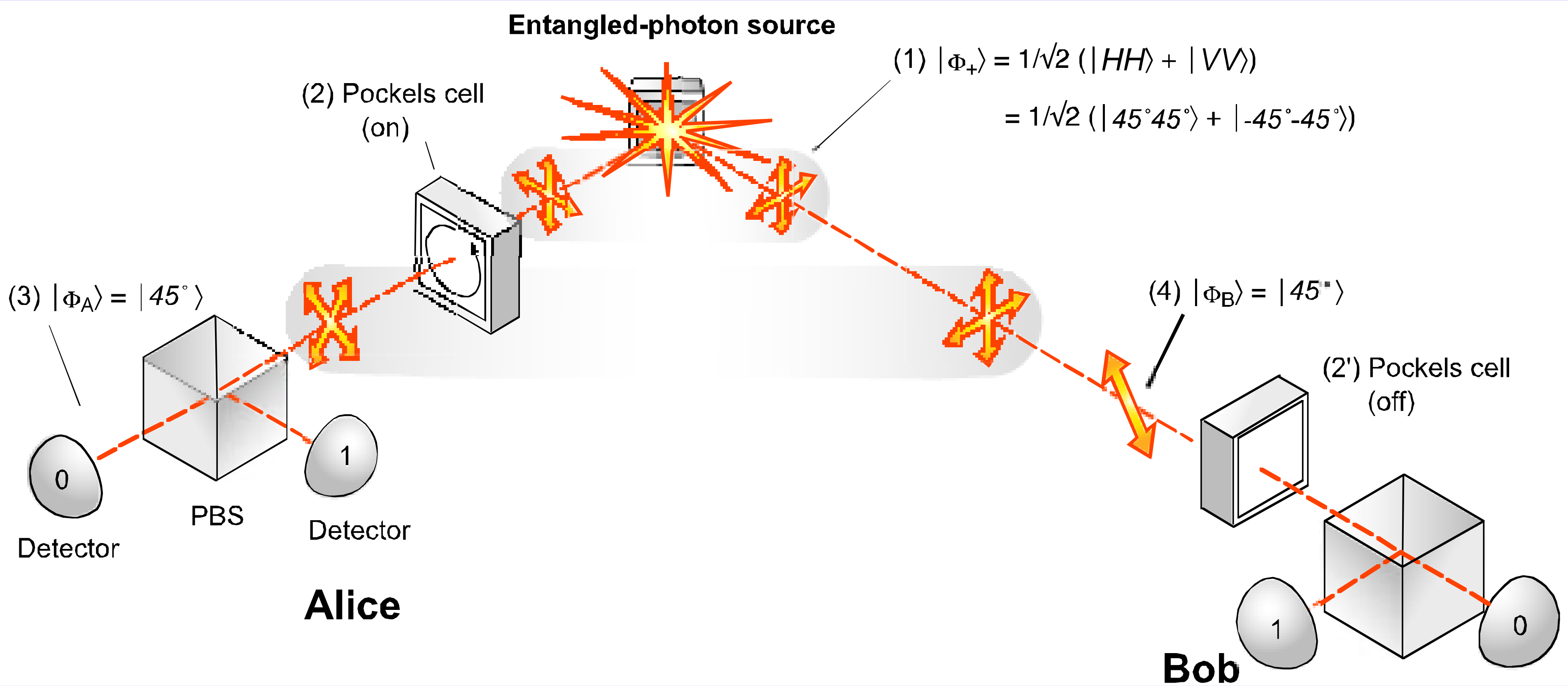
a) **USTC Quantum Backbone**

- Total length: 2000 km
- Jun. 2013 to Dec. 2016
- 32 trustable relay nodes, 31 fiber links
- Metropolitan networks Existing: Hefei, Jinan New: Beijing, Shanghai
- Total investment: ¥560 M Half by NDRC, half by local government
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC



The University of Science and Technology of China (USTC) has created a metropolitan quantum key distribution (QKD) "backbone" with 50 nodes and 90 users in Jinan, China (a). Battelle and idQuantique are working on a quantum backbone extending from Ohio to Washington, DC (with further extensions later). **ORNL → electrical grid via QKD**

Entangled-Photon Quantum Cryptography


Entangled-photon source
(1) $|\Phi_+\rangle = 1/\sqrt{2}\,(|HH\rangle + |VV\rangle)$
$= 1/\sqrt{2}\,(|45^\circ 45^\circ\rangle + |-45^\circ -45^\circ\rangle)$
(2) Pockels cell (on)
(3) $|\Phi_A\rangle = |45^\circ\rangle$
0
Detector
PBS
1
Detector
Alice
(4) $|\Phi_B\rangle = |45^\circ\rangle$
(2') Pockels cell (off)
1
0
Bob

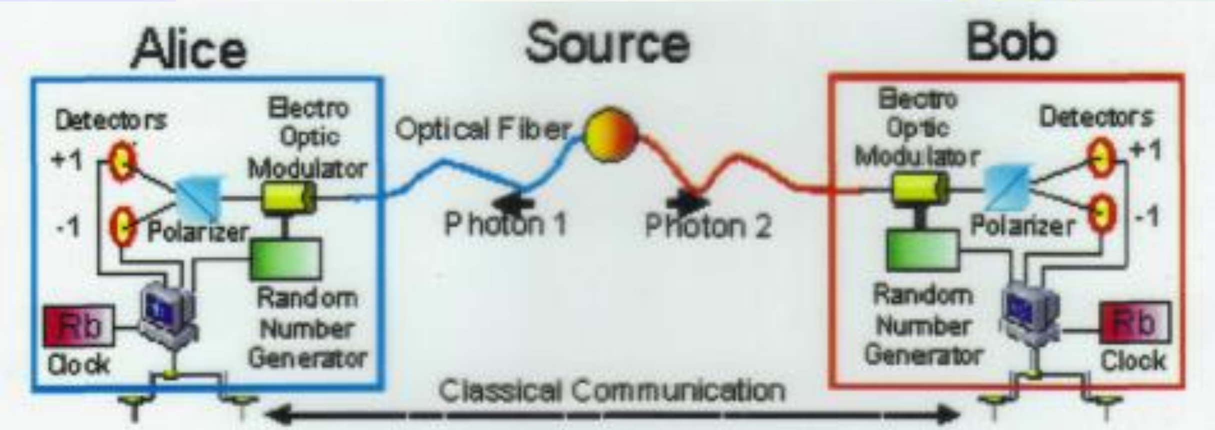
- Alice & Bob randomly measure polarization in the (HV) or the (45 -45) basis.
- Discuss via a "public channel" which bases they used, *but not the results*.
- Discard cases (50%) where they used different bases → uncorrelated results.
- Keep cases where they used the same basis → *perfectly correlated results!*
- Define H ="0" = 45, V ="1" = -45.   **They now share a secret key.**

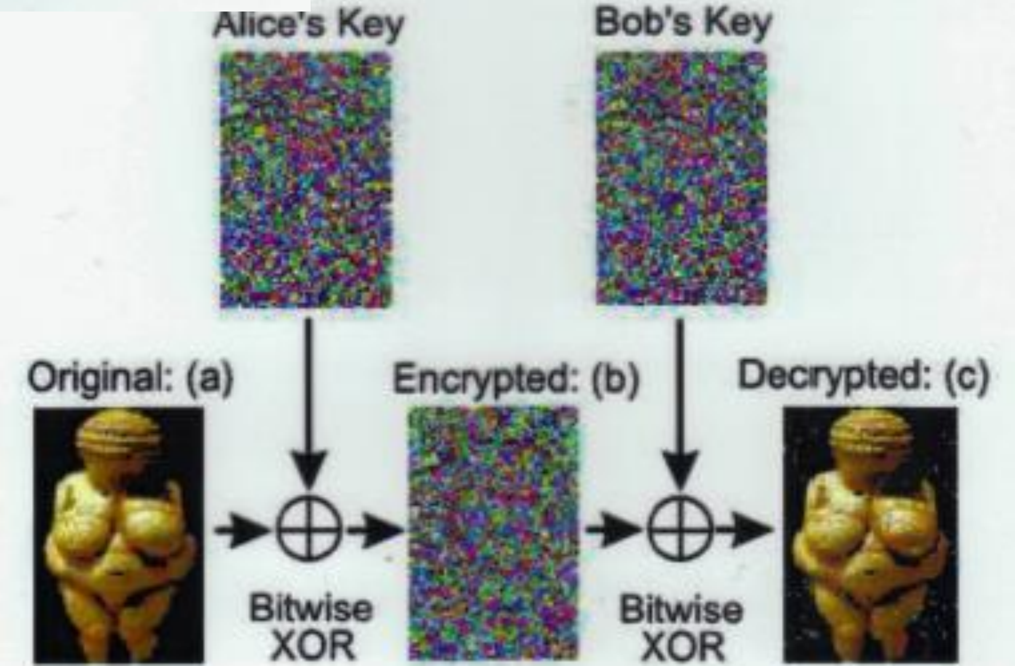
Entangled-photon Q. Cryptography

T. Jennewein, *et al*., Phys. Rev. Lett. **84**, 4729 (2000)

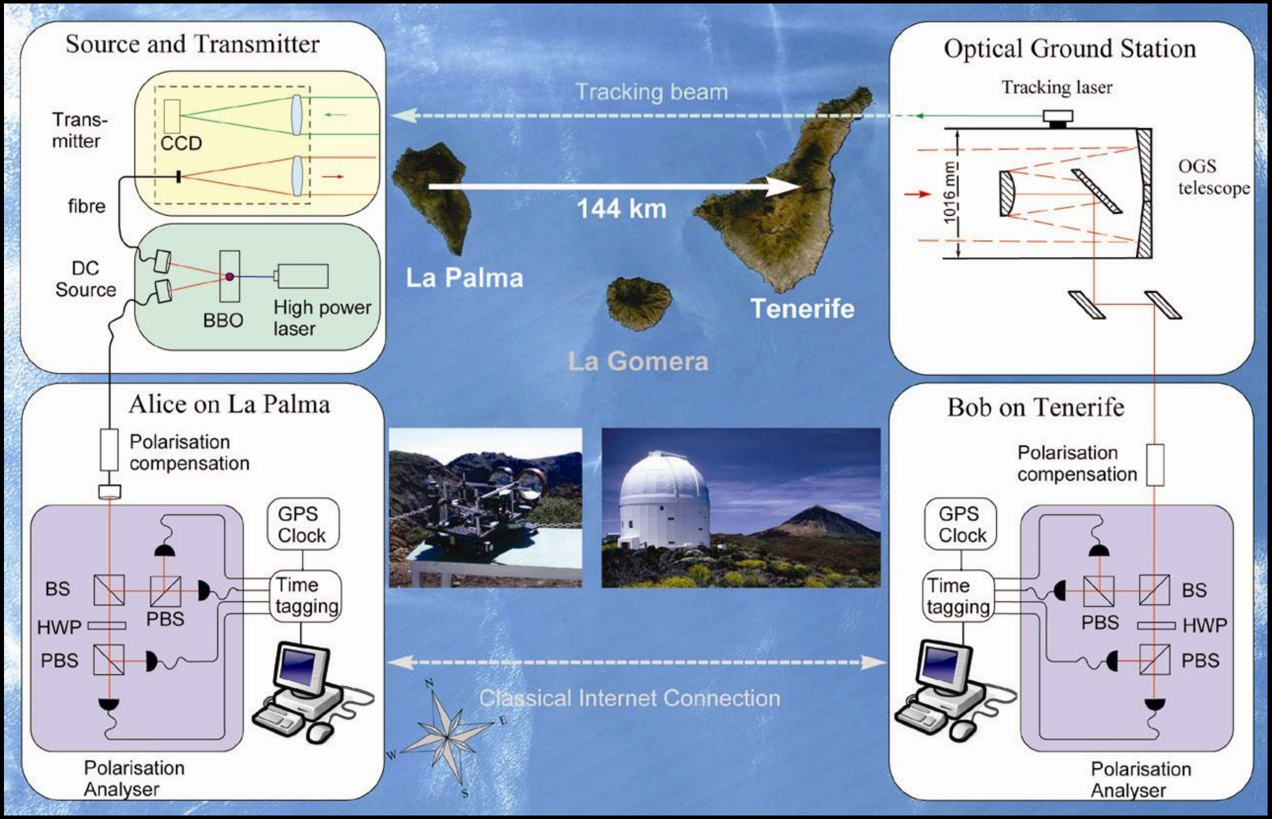
D. S. Naik, *et al*., *ibid.* 4733 (2000)

W. Tittel, *et al*., *ibid.* 4737 (2000)

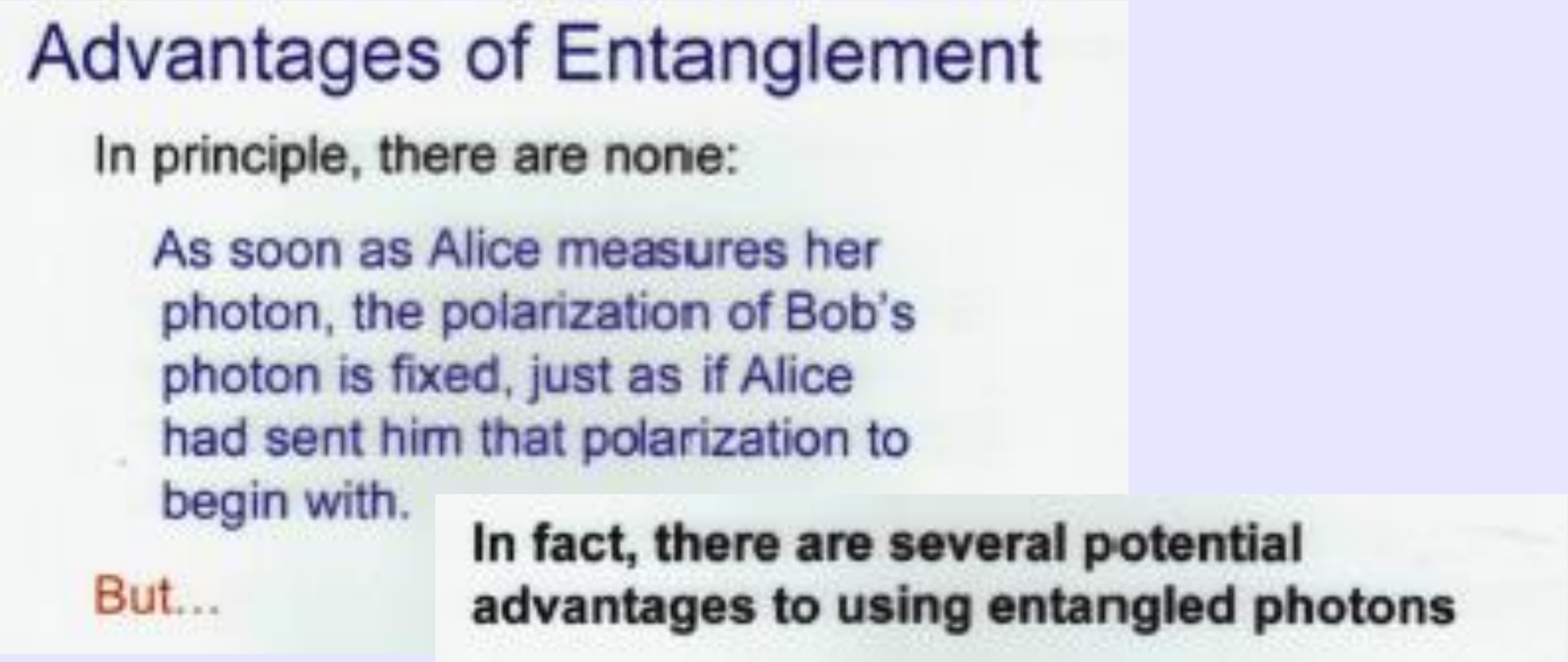




144 km set-up



- locally 98% (H/V) and 96%(P/M)
- QBER 4.8 % ± 1 % (798 coinc/75s – 417 bit – 178 bit)
- Ekert 91: S = 2.508 ± 0.037



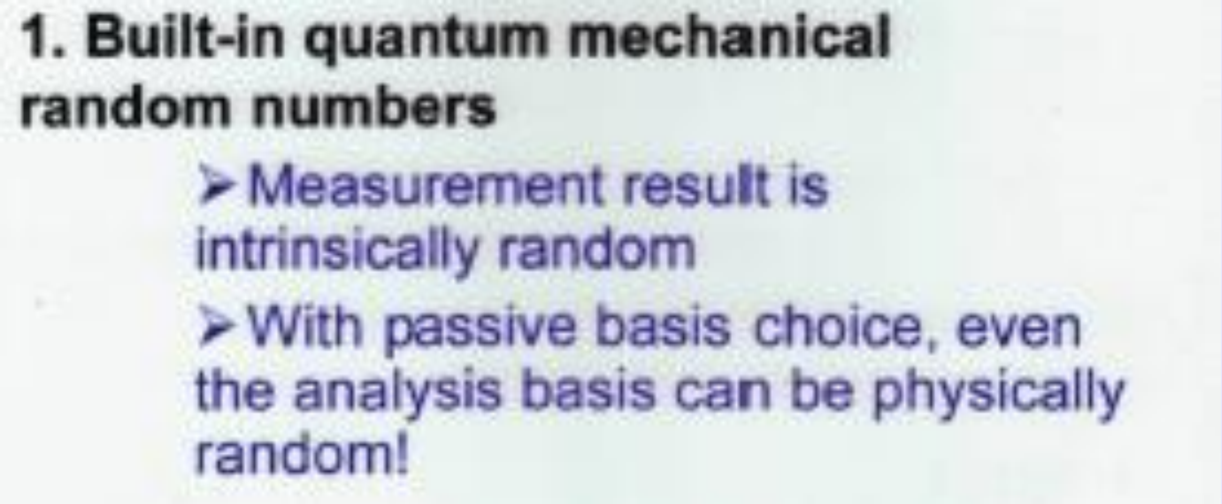
Advantages of Entanglement

In principle, there are none:

As soon as Alice measures her photon, the polarization of Bob's photon is fixed, just as if Alice had sent him that polarization to begin with.

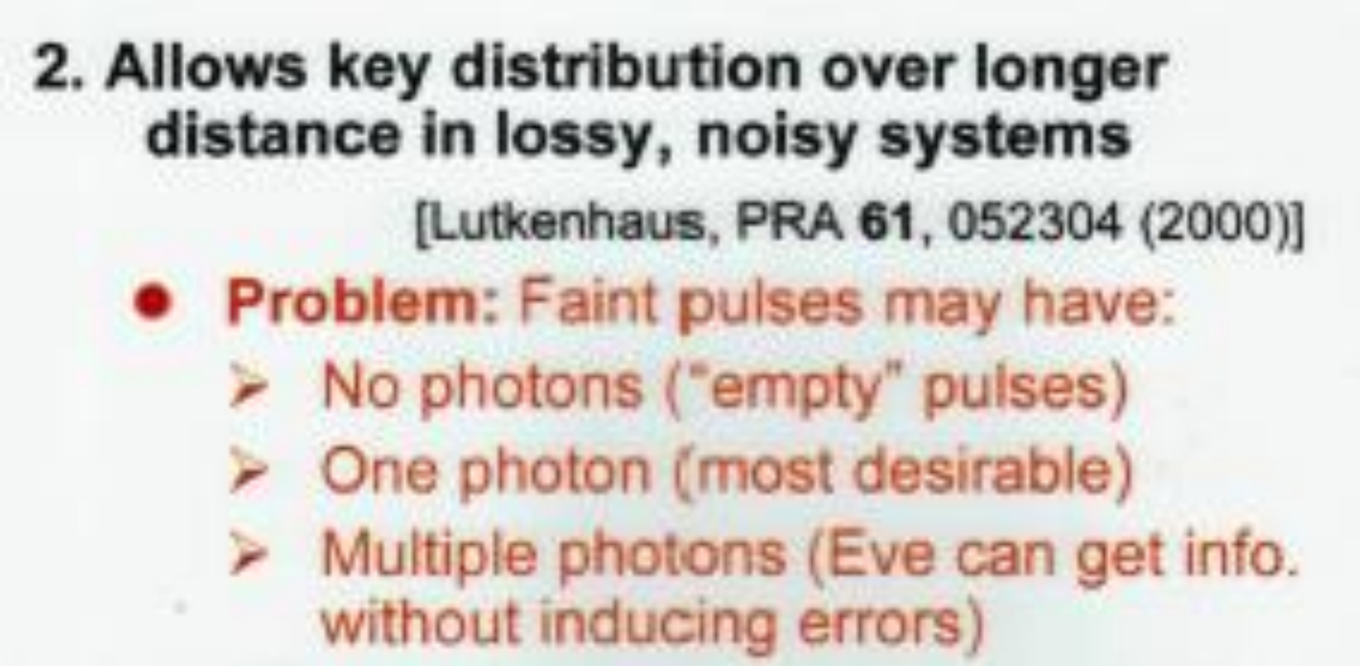
But…

In fact, there are several potential advantages to using entangled photons



1. Built-in quantum mechanical random numbers

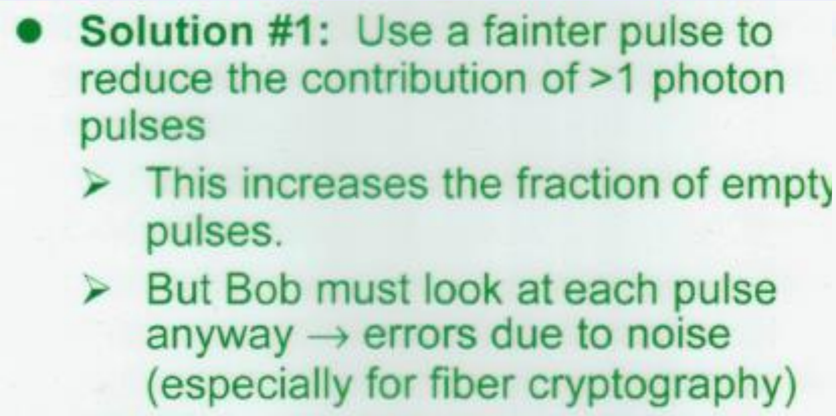
- ➢Measurement result is intrinsically random
- ➢With passive basis choice, even the analysis basis can be physically random!



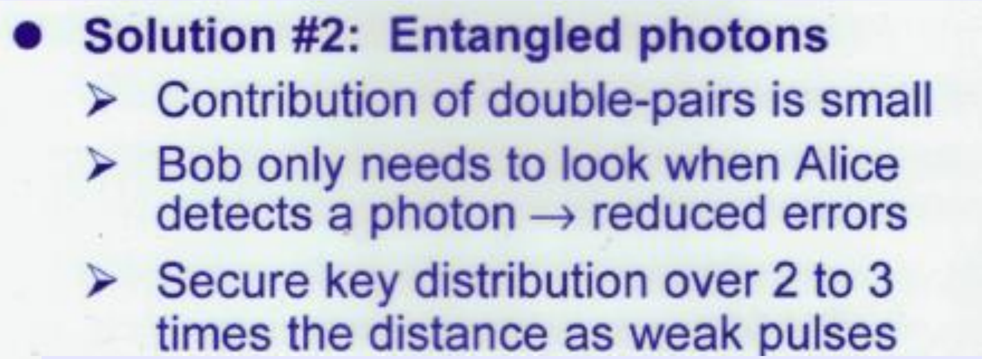
2. Allows key distribution over longer distance in lossy, noisy systems

[Lutkenhaus, PRA **61**, 052304 (2000)]

- **Problem:** Faint pulses may have:
  - ➢ No photons ("empty" pulses)
  - ➢ One photon (most desirable)
  - ➢ Multiple photons (Eve can get info. without inducing errors)



- **Solution #1:** Use a fainter pulse to reduce the contribution of >1 photon pulses
  - ➢ This increases the fraction of empty pulses.
  - ➢ But Bob must look at each pulse anyway → errors due to noise (especially for fiber cryptography)



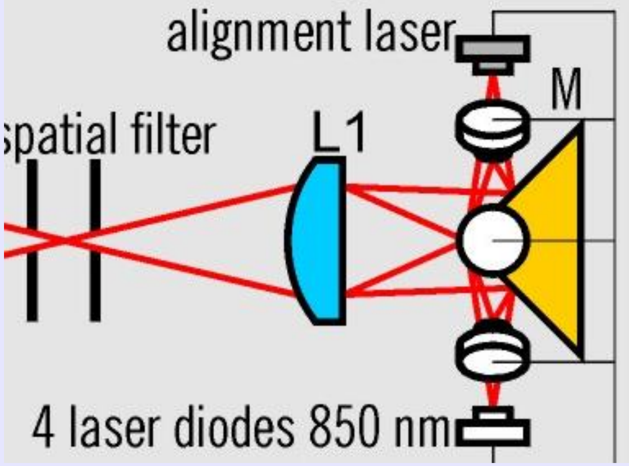
- **Solution #2: Entangled photons**
  - ➢ Contribution of double-pairs is small
  - ➢ Bob only needs to look when Alice detects a photon → reduced errors
  - ➢ Secure key distribution over 2 to 3 times the distance as weak pulses

Solution #3: Decoy states

3. Explicit source verification

[Mayers, IEEE Comput. Soc. 1998, p. 503]

- **Problem: Information may "leak" via other degrees of freedom**
  - Assume Alice sends single photons to Bob
  - Polarization correlated to some other degree of freedom
  - Does not affect BER -- allows Eve to eavesdrop undetected!
  - Extra information could hide in frequency, spatial modes, or precise timing/pulse shapes, and *could even change over time*!
- **Solution #1:** *Constantly* check the source (may be difficult)
- **Solution #2: Entangled states**
  - Entangling polarization to another degree of freedom will *necessarily* result in an increased BER (in some basis)
  - *Alice and Bob automatically detect the possible loss of information*



$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H,\lambda_H\rangle_1 |H,\lambda\rangle_2 + |V,\lambda_V\rangle_1 |V,\lambda\rangle_2\right)$$

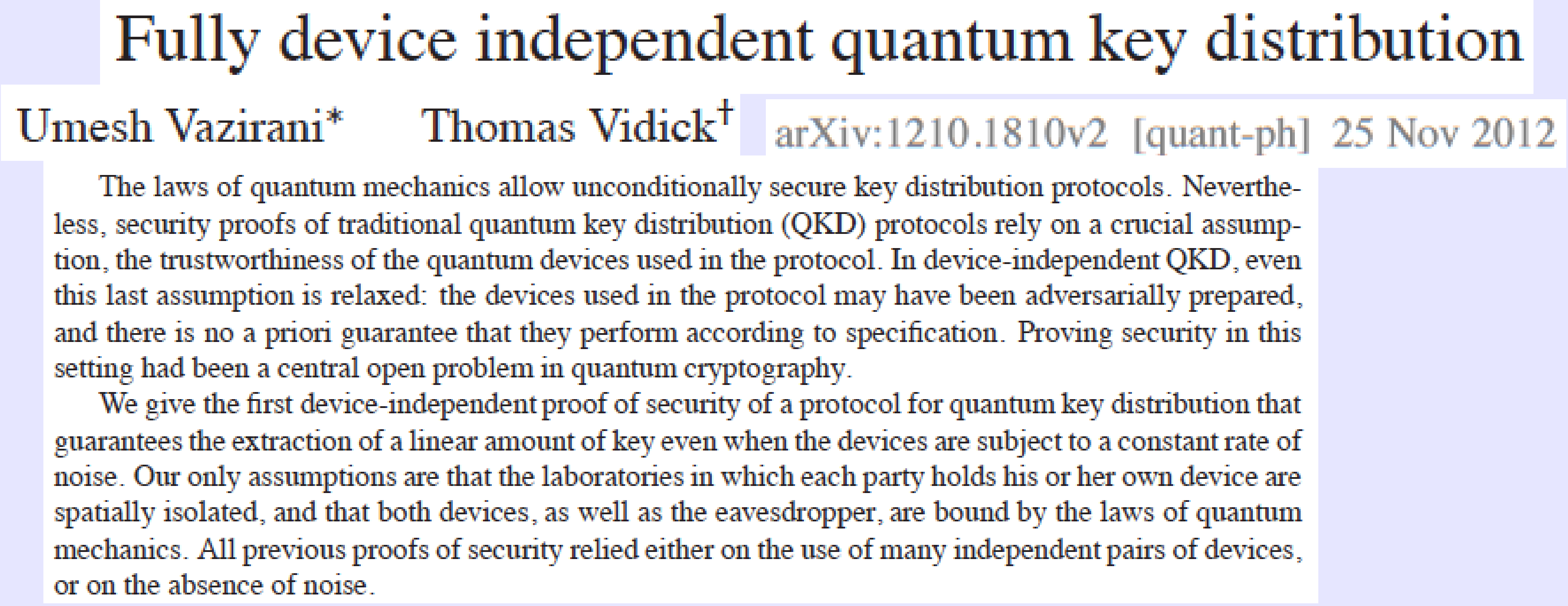
$$= \frac{1}{2\sqrt{2}}(|D,\lambda_H\rangle_1|D\rangle_2 + |d,\lambda_H\rangle_1|d\rangle_2 + |d,\lambda_H\rangle_1|D\rangle_2 + |D,\lambda_H\rangle_1|d\rangle_2$$
$$+|D,\lambda_V\rangle_1|D\rangle_2 + |d,\lambda_V\rangle_1|d\rangle_2 - |d,\lambda_V\rangle_1|D\rangle_2 - |D,\lambda_V\rangle_1|d\rangle_2)$$

$$P(Dd) = |\langle Dd\|\psi\rangle|^2 = \frac{1}{4}\left[1 - |\langle\lambda_H\|\lambda_V\rangle|\right]$$

If $\langle\lambda_H|\lambda_V\rangle = 1$,

no distinguishing information → BER=0.

Entangled photons → automatic source verification

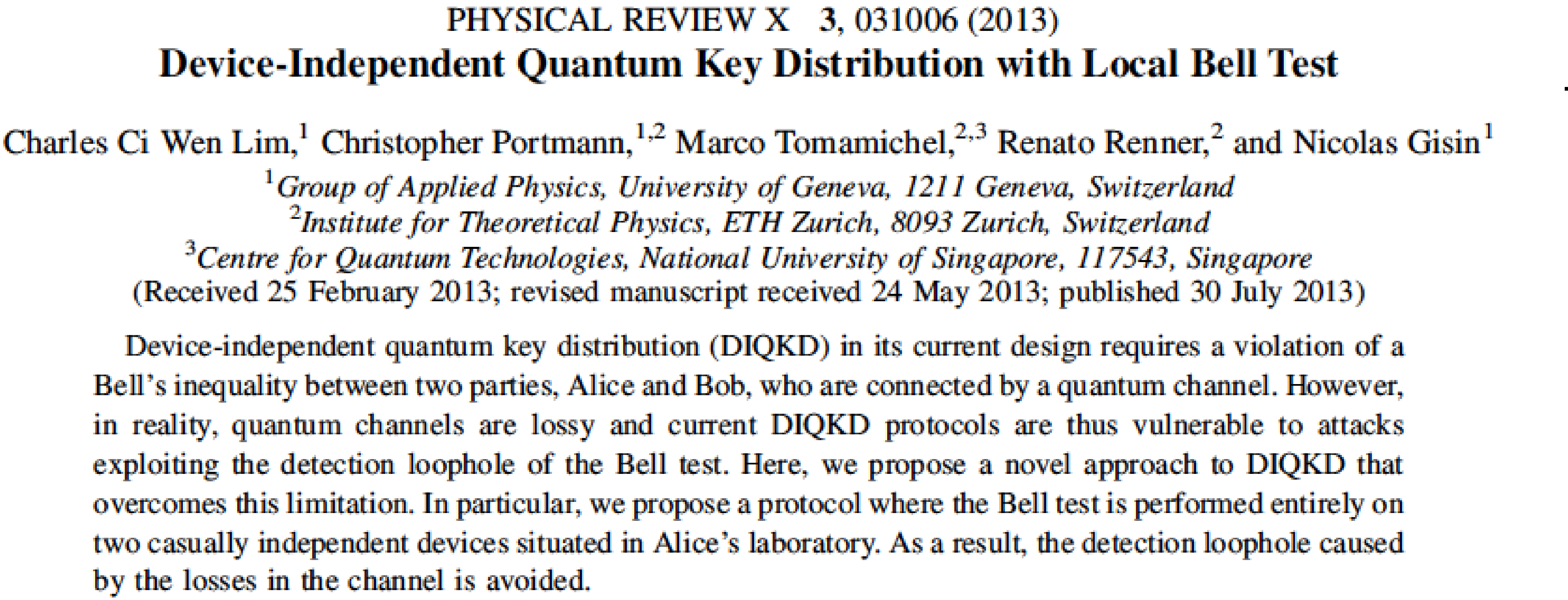


Fully device independent quantum key distribution

Umesh Vazirani* Thomas Vidick† arXiv:1210.1810v2 [quant-ph] 25 Nov 2012

The laws of quantum mechanics allow unconditionally secure key distribution protocols. Nevertheless, security proofs of traditional quantum key distribution (QKD) protocols rely on a crucial assumption, the trustworthiness of the quantum devices used in the protocol. In device-independent QKD, even this last assumption is relaxed: the devices used in the protocol may have been adversarially prepared, and there is no a priori guarantee that they perform according to specification. Proving security in this setting had been a central open problem in quantum cryptography.

We give the first device-independent proof of security of a protocol for quantum key distribution that guarantees the extraction of a linear amount of key even when the devices are subject to a constant rate of noise. Our only assumptions are that the laboratories in which each party holds his or her own device are spatially isolated, and that both devices, as well as the eavesdropper, are bound by the laws of quantum mechanics. All previous proofs of security relied either on the use of many independent pairs of devices, or on the absence of noise.



PHYSICAL REVIEW X **3**, 031006 (2013)

Device-Independent Quantum Key Distribution with Local Bell Test

Charles Ci Wen Lim,[1] Christopher Portmann,[1,2] Marco Tomamichel,[2,3] Renato Renner,[2] and Nicolas Gisin[1]

[1] *Group of Applied Physics, University of Geneva, 1211 Geneva, Switzerland*
[2] *Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*
[3] *Centre for Quantum Technologies, National University of Singapore, 117543, Singapore*
(Received 25 February 2013; revised manuscript received 24 May 2013; published 30 July 2013)

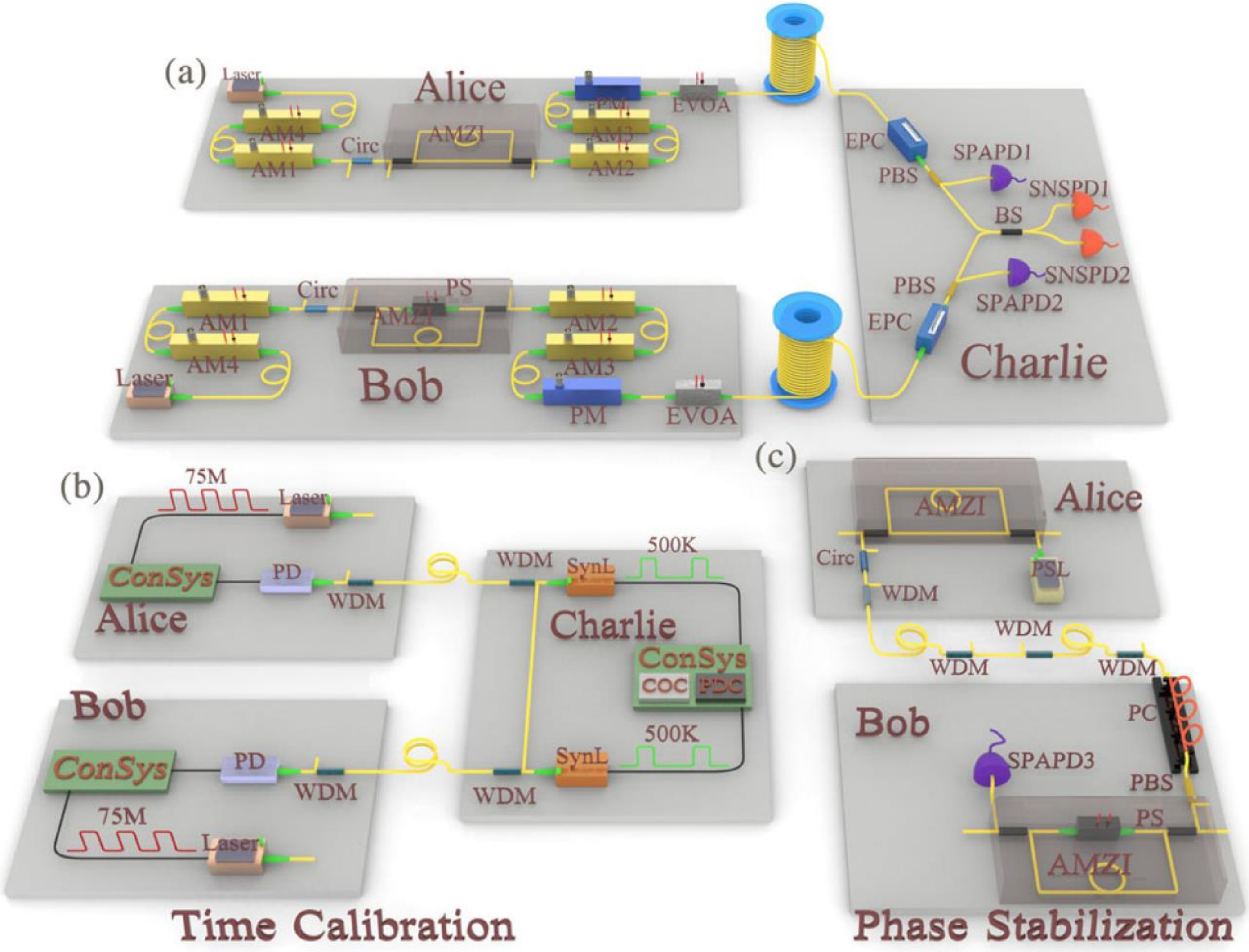
Device-independent quantum key distribution (DIQKD) in its current design requires a violation of a Bell's inequality between two parties, Alice and Bob, who are connected by a quantum channel. However, in reality, quantum channels are lossy and current DIQKD protocols are thus vulnerable to attacks exploiting the detection loophole of the Bell test. Here, we propose a novel approach to DIQKD that overcomes this limitation. In particular, we propose a protocol where the Bell test is performed entirely on two casually independent devices situated in Alice's laboratory. As a result, the detection loophole caused by the losses in the channel is avoided.

MDI-QKD – how it works

Measurement-Device-Independent Quantum Key Distribution over 200 km

Yan-Lin Tang,[1,2] Hua-Lei Yin,[1,2] Si-Jing Chen,[3] Yang Liu,[1,2] Wei-Jun Zhang,[3] Xiao Jiang,[1,2*] Lu Zhang,[3] Jian Wang,[1,2] Li-Xing You,[3] Jian-Yu Guan,[1,2] Dong-Xu Yang,[1,2] Zhen Wang,[3] Hao Liang,[1,2] Zhen Zhang,[4,2] Nan Zhou,[1,2] Xiongfeng Ma,[4,2†] Teng-Yun Chen,[1,2‡] Qiang Zhang,[1,2§] and Jian-Wei Pan[1,2]

Measurement-device-independent quantum key distribution (MDIQKD) protocol is immune to all attacks on detection and guarantees the information-theoretical security even with imperfect single-photon detectors. Recently, several proof-of-principle demonstrations of MDIQKD have been achieved. Those experiments, although novel, are implemented through limited distance with a key rate less than 0.1 bit/s. Here, by developing a 75 MHz clock rate fully automatic and highly stable system and superconducting nanowire single-photon detectors with detection efficiencies of more than 40%, we extend the secure transmission distance of MDIQKD to 200 km and achieve a secure key rate 3 orders of magnitude higher. These results pave the way towards a quantum network with measurement-device-independent security.



is included [30]. Operated at 2.2 K, two SNSPDs provide the system detection efficiencies of 46% and 40% at the dark count rate of 10 Hz, respectively, which are almost 2 or 3

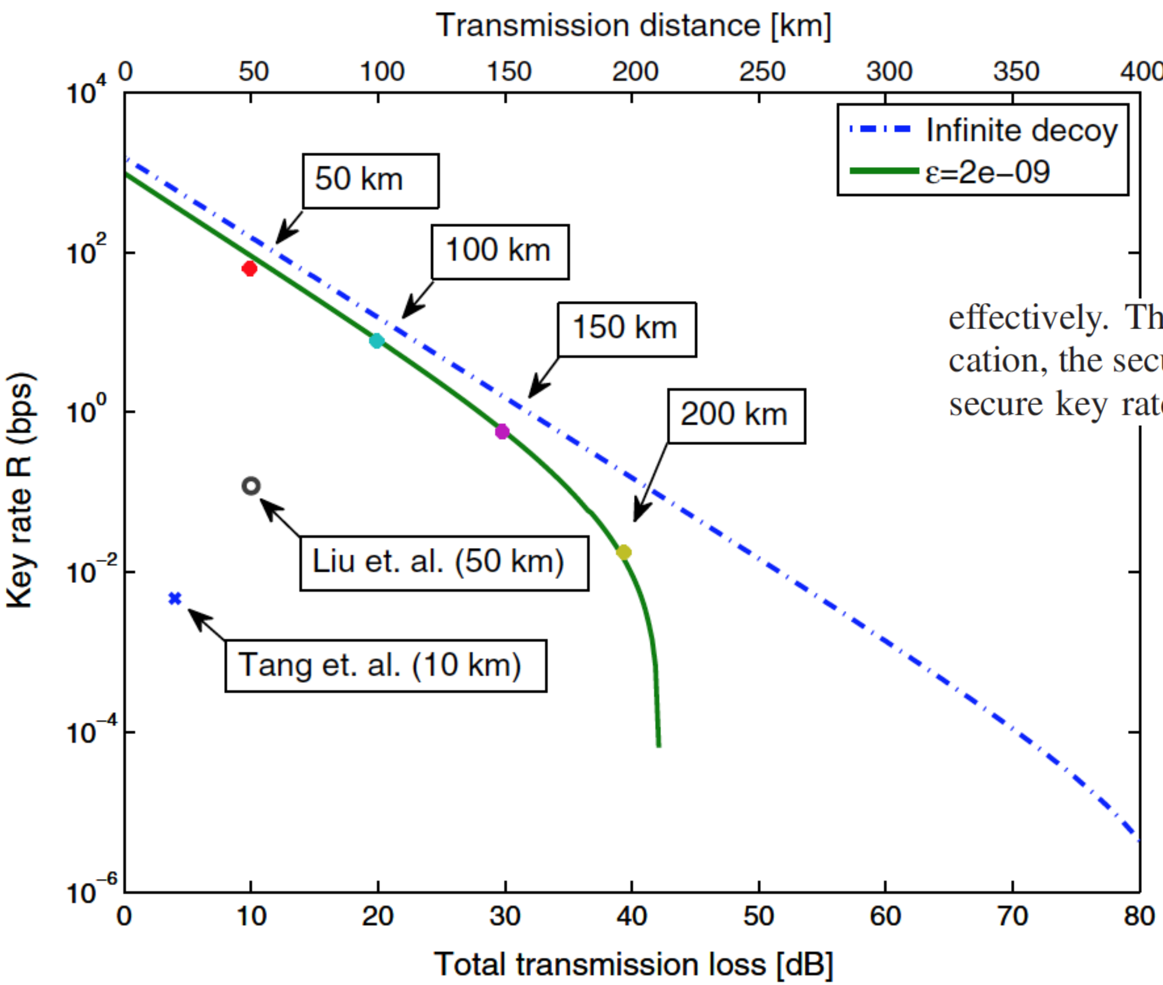
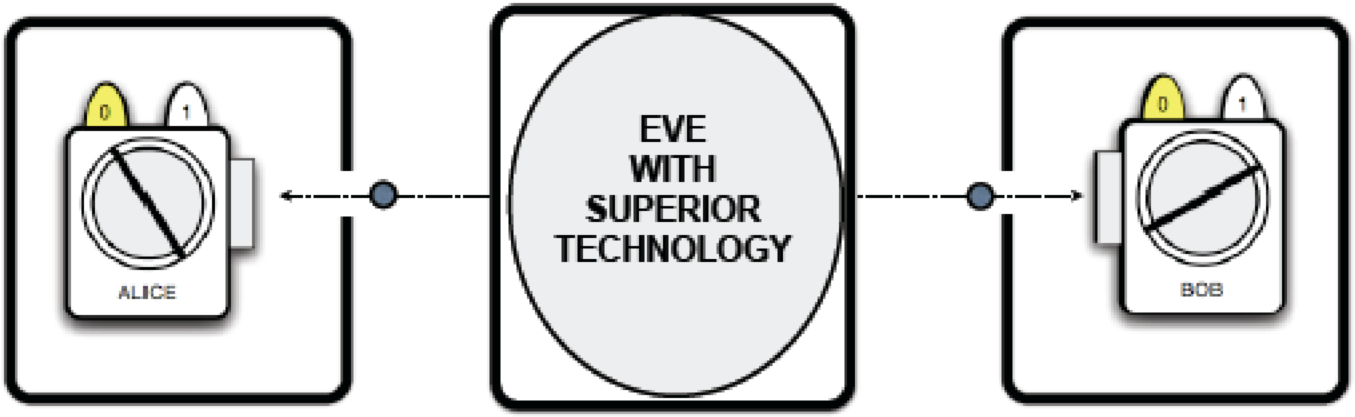


FIG. 2 (color online). Secure key rates of experiments in the laboratory as well as the simulation results. The four dots correspond to the experimental results with the fiber transmitting loss of 9.9 dB (50 km), 19.9 dB (100 km), 29.8 dB (150 km), and 39.6 dB (200 km). The solid curve shows the result calculated by simulating the vacuum + weak decoy-state scheme with the experimental parameters. The dashed curve represents the optimal result with infinite number of decoy states.

effectively. Through error correction and privacy amplification, the secure key length obtained is 8.31 kbits and the secure key rate is 0.018 bit/s.

Assumptions



- 🟢 Alice's and Bob's labs are secure - no information leaks
- 🟢 Alice and Bob have free will and can **choose** their observables
- 🔴 Alice and Bob control and trust devices in their labs
- 🔴 Alice and Bob know the carriers, e.g. dimensionality of associated Hilbert space

LETTERS

PUBLISHED ONLINE: 29 AUGUST 2010 | DOI: 10.1038/NPHOTON.2010.214

nature photonics

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen[1,2]*, Carlos Wiechers[3,4,5], Christoffer Wittmann[3,4], Dominique Elser[3,4], Johannes Skaar[1,2] and Vadim Makarov[1]

The peculiar properties of quantum mechanics allow two remote parties to communicate a private, secret key, which is protected from eavesdropping by the laws of physics[1–4]. So-called quantum key distribution (QKD) implementations always rely on detectors to measure the relevant quantum property of single photons[5]. Here we demonstrate experimentally that the detectors in two commercially available QKD systems can be fully remote-controlled using specially tailored bright illumination. This makes it possible to tracelessly acquire the full secret key; we propose an eavesdropping apparatus built from off-the-shelf components. The loophole is likely to be present in most QKD systems using avalanche photodiodes to detect single photons. We believe that our findings are crucial for strengthening the security of practical QKD, by identifying and patching technological deficiencies.

cracked. We show experimentally that Eve can blind the gated detectors in the QKD systems using bright illumination, thereby converting them into classical, linear detectors. The detectors are then fully controlled by classical laser pulses superimposed over the bright continuous-wave (c.w.) illumination. Remarkably, the detectors exactly measure what is dictated by Eve; with matching measurement bases Bob detects exactly the bit value sent by Eve, whereas

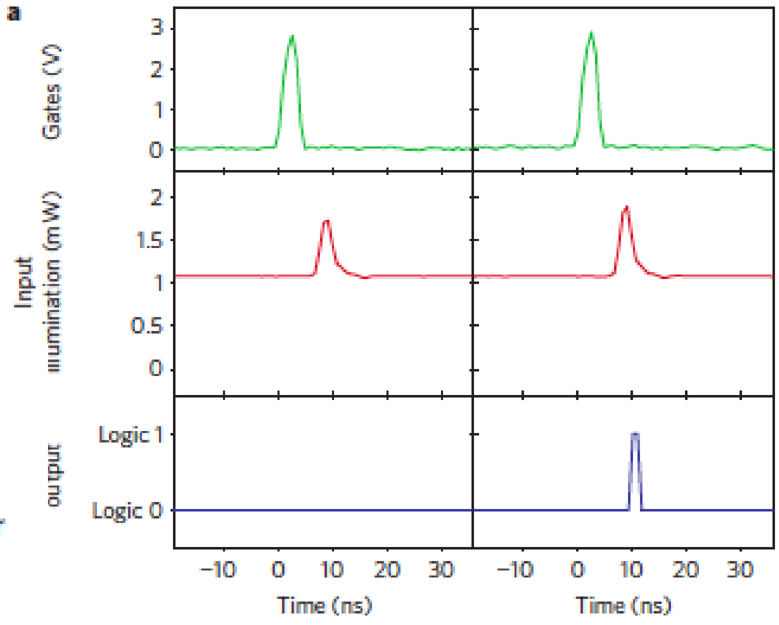


Figure 4 | Detector control. a, Electrical and optical signal oscillograms when detector 0 in Clavis2 is blinded by 1.08 mW c.w. illumination, and controlled by a superimposed 2.5-ns-long laser pulse timed slightly behind the gate (see Supplementary Section III for detailed measurement setup). The superimposed $P_{\mathrm{never},0} = 647$ µW (detector 1: $P_{\mathrm{never},1} = 697$ µW) trigger pulse never causes a detection event, whereas the $P_{\mathrm{always},0} = 808$ µW ($P_{\mathrm{always},1} = 932$ µW) trigger pulse always causes a detection event. **b,** Click

Talk at QCRYPT conference, Zurich, Switzerland, September 12-16, 2011

Loopholes in implementations

of quantum cryptography

Vadim Makarov

UNIK UNIVERSITY GRADUATE CENTER

NTNU Det skapende universitet

Photo ©2010 NTNU Info / Geir Mogen

Attack	Target component	Tested system	Demonstrated eavesdr. (% key)?	Keeps full key rate?
Time-shift Y. Zhao *et al.*, Phys. Rev. A **78**, 042333 (2008)	detector	ID Quantique	**no** (fraction)	**no**
Phase-remapping F. Xu, B. Qi, H.-K. Lo, New J. Phys. **12**, 113026 (2010)	phase modulator	ID Quantique	**no** (full inf.-th.)	**yes** (@ transm.≪1)
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011)	Faraday mirror	(theory)	(full inf.-th.)	**yes** (@ transm.≪1)
Channel calibration N. Jain *et al.*, Phys. Rev. Lett. **107**, 110501 (2011)	detector	ID Quantique	**no** (full inf.-th.)	**yes**
Detector control L. Lydersen *et al.*, Nat. Photonics **4**, 686 (2010)	detector	ID Quantique, MagiQ Tech.	**no** (**100%**)	**yes**
Detector control I. Gerhardt *et al.*, Nat. Commun. **2**, 349 (2011)	detector	research syst.	**yes** (**100%**)	**yes**
Deadtime H. Weier *et al.*, New J. Phys. **13**, 073024 (2011)	detector	research syst.	**yes** (**98.8%**)	**no, 1/4**

Countermeasures (technical)

"Quick and intuitive" patches

- Lead away from provable security model of QKD
- Can often be defeated by hacking advances

Z. L. Yuan, J. F. Dynes, A. J. Shields, Appl. Phys. Lett. **98**, 231104 (2011); *comment:* L. Lydersen, V. Makarov, J. Skaar, arXiv:1106.3756
L. Lydersen *et al.*, arXiv:1106.2119

Integrate imperfection into security proof

- May require deep modification of protocol, hardware, and security proof

Ø. Marøy *et al.*, Phys. Rev. A **82**, 032337 (2010)
L. Lydersen *et al.*, Phys. Rev. A **83**, 032306 (2011)

H.-K. Lo, M. Curty, B. Qi, arXiv:1109.1473