量子信息导论
PHYS5251P

中国科学技术大学
物理学院/合肥微尺度物质科学国家研究中心

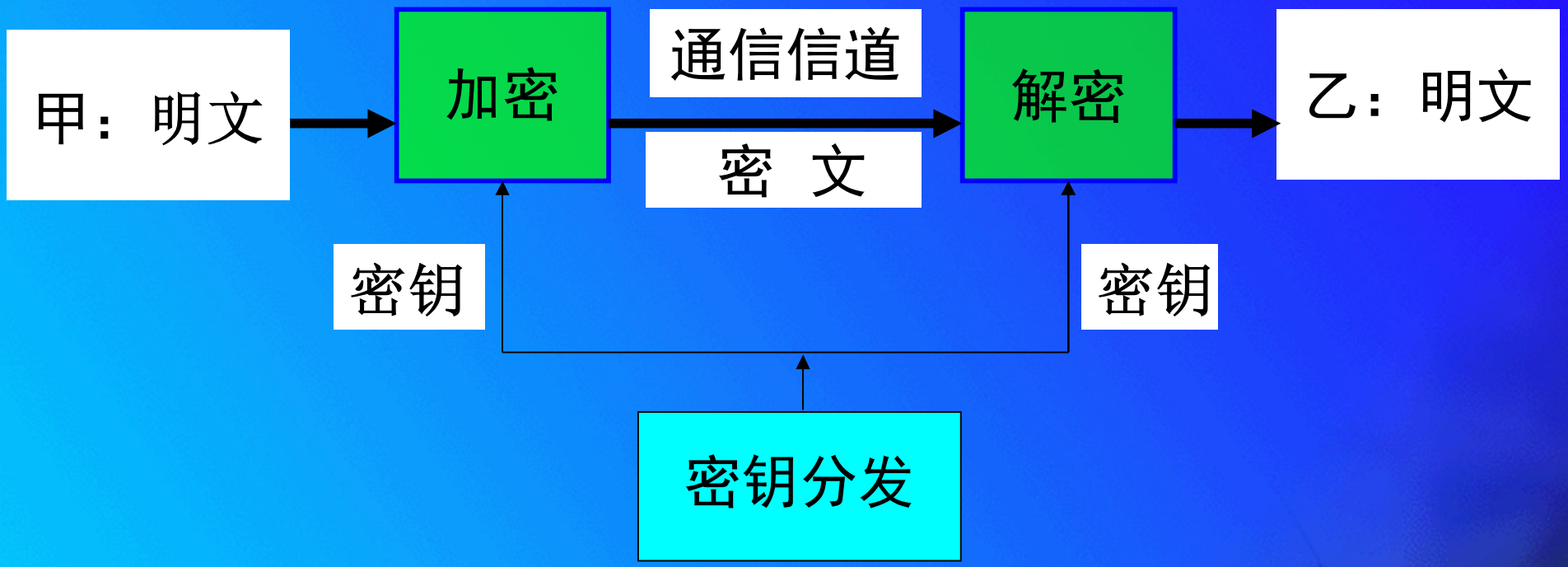
陈凯

2025.11

第四章 量子通信

1. 保密通信
2. QKD基本原理
3. BB84协议过程
4. QKD安全性
5. 诱骗态(Decoy-state QKD)
   - ① Decoy QKD原理
   - ② 实用Decoy QKD
   - ③ Decoy QKD实验
6. QKD的现实安全性
   - ① 探测端的安全性→MDI-QKD
   - ② 设备无关的→ DI-QKD
7. 量子隐形传态(Quantum Teleportation) [原理、实验]
8. 量子纠缠交换(Entanglement Swapping)
9. 量子通信网络
10. 量子通信商用公司
11. 量子通信发展与实用化QKD之路

常规保密通信体系



保密原理：系统保密性完全依赖于密钥的安全性，
不依赖于加密体制或算法

然而现有的保密通信体系不存在无条件安全的方案来分发密钥！

分配和使用密钥常规体制及安全性

- 对称密钥体制(私钥密码)—使用AES（高等数据加密标准）等进行密钥扩张和分配

- 非对称密钥体制(公钥密码)—使用基于大整数因子分解问题的RSA体制和Rabin体制、基于有限域上或者基于椭圆曲线上的离散对数问题的Diffie-Hellman公钥体制和ElGamal体制

然而这些体制均依赖于数学计算复杂性，并不是无条件安全的，而且其依赖的数学难问题并不是不可解决的。

常规保密通信体制安全性挑战

传统基于计算复杂性的密钥体制方法并不能杜绝可能存在的未知有效破解算法的存在

- 常规体制不存在多项式算法复杂性的假设并未得到证明。
- 目前，长达1024比特长度的RSA体制已经被破解。
- 基于Hash函数的世界通行密码标准系列算法MD5等被王小云教授等人破解
- Shor的大数分解量子算法可以以$O(N^3)$的复杂性破解RSA体制

  （例如，1分钟就可以破解1024比特RSA）
- 使用穷举破译法，量子计算机能够进行把$O(N)$复杂性降低为$O(\sqrt{N})$
- 大多数密码学家相信，发达国家允许出口的密码强度和型号的产品事实上能够被美国国家安全局等重要部门破译
- 技术进步导致破解能力大大提高（计算机芯片的摩尔定律）

传统的保密通信体系已经无法保证通信的无条件安全性

常规密钥安全性分析

AES等对称密钥
RSA等公开密钥
MD5等数字签名
→ 基于复杂算法的加密体系 →
更效的算法更快的运算可以破解
王小云等人破译了MD5等
Shor量子算法可破译RSA公开密钥
量子算法可以破译大多公开密钥体制

一次一密方式 → 与算法无关的加密体系 → 密钥可能在分发通道中被秘密截获
导致完全失密

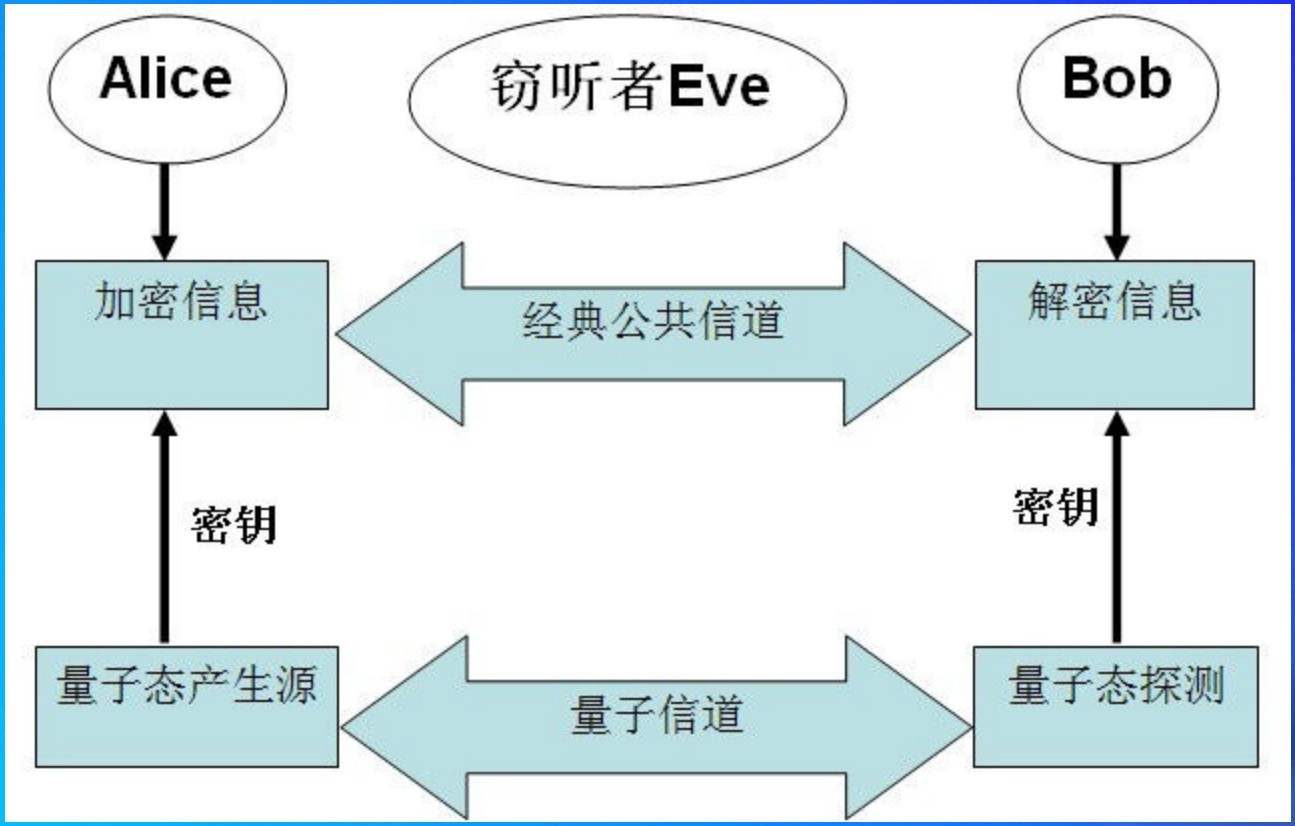
密钥的分配过程安全性无法保证

⇩

量子密钥分配彻底解决密钥分发过程的安全性问题

量子密钥分发

基于量子力学原理，1984年Bennett和Brassard在印度举行的一个IEEE会议上提出了世界上第一个量子密钥分发协议，俗称BB84协议



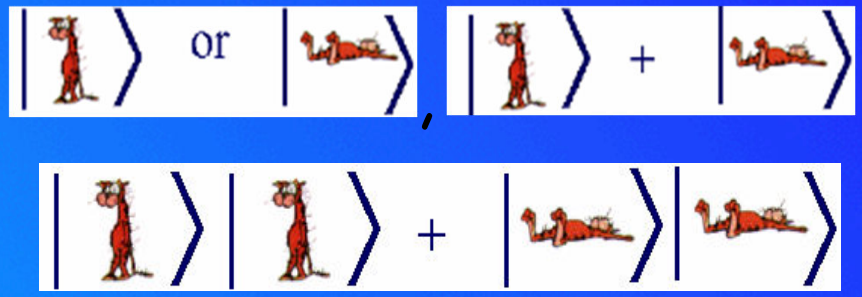
BB84协议示意图

What is QKD?

- Quantum Key Distribution is simultaneous generation of identical bit sequences in two distinct locations with quantum physical methods
- Quantum technology guarantees unconditional security
- QKD enables the implementation of a perfectly secure secret channel

量子密钥分配保密原理

量子态的相干叠加



单光子量子态不可克隆原理

未知量子态

$|\psi\rangle$

不可能的

复制到
另一量子体系

在不破坏原来量子态的前提下

单光子是安全的，不可分割，也不可克隆！

量子密钥分发安全性

窃听方式：截取　　单光子不可分割

甲方 ⟶ ⇢ 乙方

被窃取光子
不产生密钥

无条件安全
的密钥分发
依然可以
完成

甲方 ⟶ ⟶ 乙方

窃听方式：“复制”
再分发

单光子不可克隆

被复制光子
不产生密钥

- 实现了**无条件安全的**密钥分发的物理通道
- 彻底解决了经典密钥分发体系的安全漏洞

Quantum key distribution

A protocol that enables Alice and Bob to set up a secure secret key, provided that they have:

- A ***quantum channel***, where Eve can read and modify messages
- An ***authenticated classical channel***, where Eve can read messages, but cannot tamper with them (the authenticated classical channel can be simulated by Alice and Bob having a ***very short*** classical secret key)

BB84协议

The main issue in cryptography is how to establish a secret key between Alice and Bob. This is a string of zeros and ones which is in the possession of both parties, but is not known to any other unwanted parties—that is, eavesdroppers。

The BB84 protocol begins with Alice choosing a random string $x_1 \ldots x_4$ of bits to send to Bob.

Bit	x_1	x_2	x_3	x_4
Value	0	1	1	0

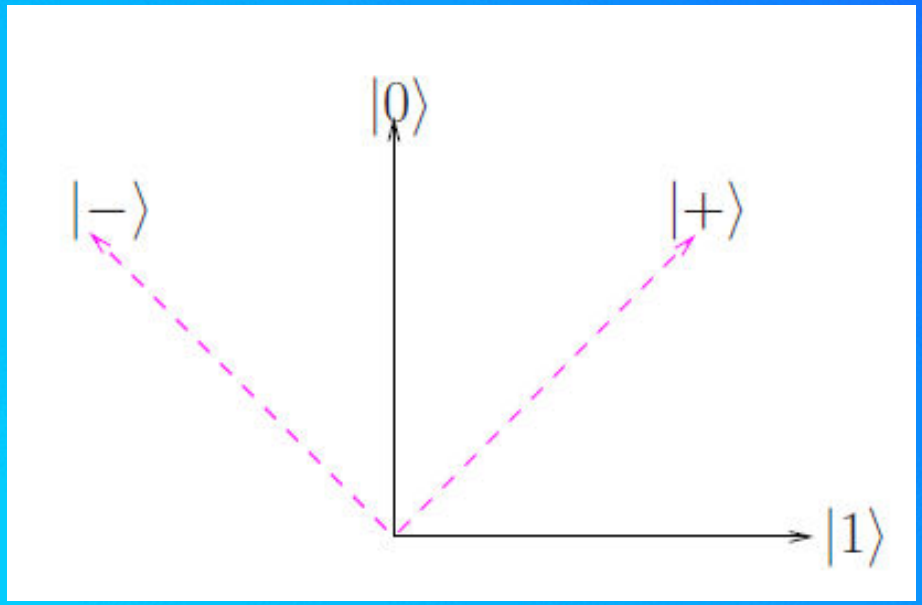
In order to prevent an eavesdropper from reading the bits, Alice randomly chooses to write each bit x_i as a qubit $|\psi_i\rangle$ in either the rectilinear basis as $|0\rangle$ or $|1\rangle$ or in the diagonal basis as $|+\rangle$ or $|-\rangle$

Classical value	0	1	1	0
Alice's basis	+	×	+	×
Quantum encoding	$\|\psi_1\rangle = \|0\rangle$	$\|\psi_2\rangle = \|-\rangle$	$\|\psi_3\rangle = \|1\rangle$	$\|\psi_4\rangle = \|+\rangle$

BB84协议

A logical "zero" is encoded either as $|0\rangle$ or $|+\rangle$, while a logical "one" is encoded as $|1\rangle$ or $|-\rangle$.

Classical value	0	1	1	0
Alice's basis	+	×	+	×
Bob's basis	×	×	+	+
In agreement	No	Yes	Yes	No



$|H\rangle$, codes for 0_+,

$|V\rangle$, codes for 1_+,

$|+45\rangle$, codes for $0_\times$,

$|-45\rangle$, codes for $1_\times$.

$$|\pm 45\rangle = (1/\sqrt{2})(|H\rangle \pm |V\rangle)$$

BB84协议执行流程

The BB84 QKD protocol

1: Alice chooses $(4+\delta)n$ random data bits.
2: Alice chooses a random $(4+\delta)n$-bit string b. She encodes each data bit as $\{|0\rangle, |1\rangle\}$ if the corresponding bit of b is 0 or $\{|+\rangle, |-\rangle\}$ if b is 1.
3: Alice sends the resulting state to Bob.
4: Bob receives the $(4+\delta)n$ qubits, announces this fact, and measures each qubit in the X or Z basis at random.
5: Alice announces b.
6: Alice and Bob discard any bits where Bob measured a different basis than Alice prepared. With high probability, there are at least $2n$ bits left (if not, abort the protocol). They keep $2n$ bits.
7: Alice selects a subset of n bits that will to serve as a check on Eve's interference, and tells Bob which bits she selected.
8: Alice and Bob announce and compare the values of the n check bits. If more than an acceptable number disagree, they abort the protocol.
9: Alice and Bob perform information reconciliation and privacy amplification on the remaining n bits to obtain m shared key bits.

BB84协议(一)

In the best-known quantum key distribution (QKD) scheme, BB84, Alice sends Bob a sequence of photons, each independently prepared in one of four polarizations (↔, ↕, ↗, or ↘). For each photon, Bob randomly picks one of the two (rectilinear and diagonal) bases to perform a measurement. He keeps the measurement outcome secret. Now Alice and Bob publicly compare their bases. They keep only the polarization data for which they measured in the same basis. In the absence of errors and eavesdropping by Eve, these data should agree.

To test for tampering, they now choose a random subset of the remaining polarization data, which they publicly announce. From there they can compute the error rate (that is,

BB84协议(二)

the fraction of data for which their values disagree). If the error rate is unreasonably high—above, say, 10%—they throw away all the data (and perhaps try again later). If the error rate is acceptably small, they perform error correction and also "privacy amplification" to distill a shorter string that will act as the secret key. These steps essentially ensure that their keys agree, are random, and are unknown to Eve.

Other QKD schemes have also been proposed. For example, Artur Ekert of the University of Oxford suggested one based on quantum mechanically correlated (that is, entangled) photons, using Bell inequalities as a check of security. In 1992, Charles Bennett of IBM proposed a simple QKD scheme, called B92, that uses only two nonorthogonal states.

Security issue

To serve as a secure key in cryptographic uses, there are two criteria:

- (a) Alice and Bob share the same key; that is, an identical key.
- (b) Eve has no information about the key; that is, a secure key.

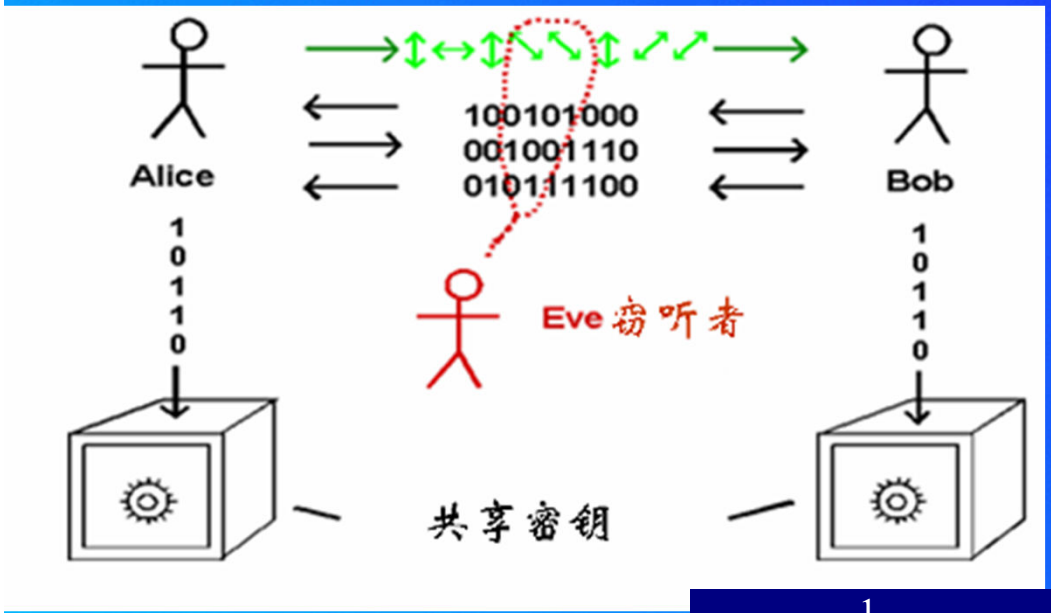
Is QKD secure?

- Dominic Mayers and subsequently by others, including Eli Biham and collaborators and Michael Ben-Or prove that the standard BB84 protocol is secure.

- Hoi-Kwong Lo and H. F. Chau, prove the security of a new QKD protocol that uses quantum error-correcting codes. The approach allows one to apply classical probability theory to tackle a quantum problem directly. It works because the relevant observables all commute with each other. While conceptually simpler, this protocol requires a quantum computer to implement.

- The two approaches have been unified by Peter Shor and John Preskill, who showed that a quantum error correcting protocol could be modified to become BB84 without compromising its security.

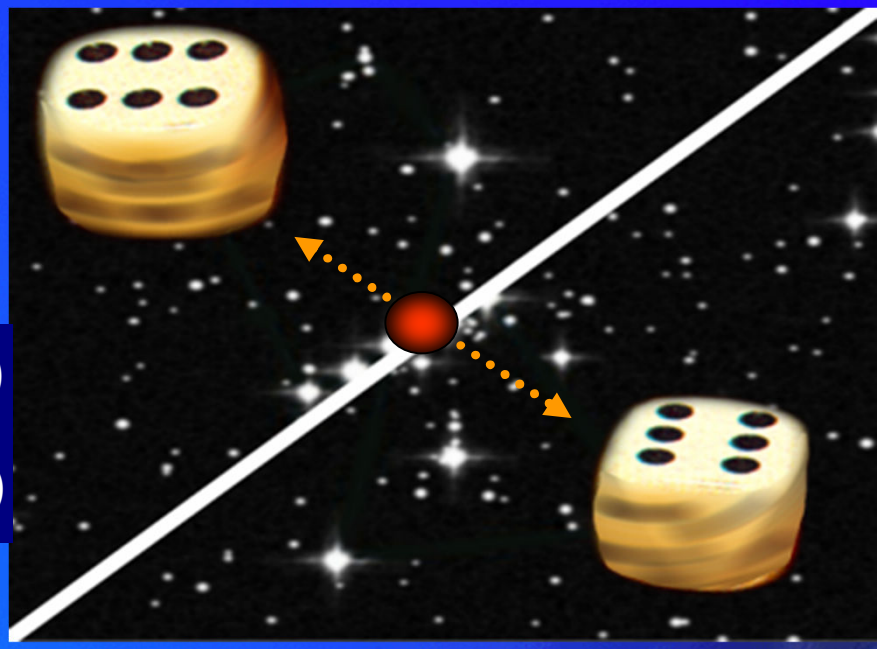
量子通信技术:量子加密术



无条件安全的密钥生成

纠缠态方案

Ekert, PRL 67, 661 (1991)



单粒子方案

Bennett & Brassard (1984)

$$|\Phi^{\pm}\rangle_{12}=\frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle_1|\leftrightarrow\rangle_2\pm|\updownarrow\rangle_1|\updownarrow\rangle_2\right)$$

$$|\Psi^{\pm}\rangle_{12}=\frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle_1|\updownarrow\rangle_2\pm|\updownarrow\rangle_1|\leftrightarrow\rangle_2\right)$$

量子不可克隆定理

量子不可分割

一次一密，完全随机

无条件安全

Sources

The output of a laser in a given mode is described by a coherent state of the field,

$$|\sqrt{\mu}e^{i\theta}\rangle \equiv |\alpha\rangle = e^{-\mu/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$$

where $\mu=|\alpha^2|$ is the average photon number

$$\rho = \int_0^{2\pi}\frac{d\theta}{2\pi}|\alpha\rangle\langle\alpha| = \sum_n P(n|\mu)|n\rangle\langle n|$$

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

Physical channels

Fiber links

$$t = 10^{-\alpha \ell / 10}$$

The value of α is strongly dependent on the wavelength and is minimal in the two "telecom windows" around 1330 nm ($\alpha \simeq 0.34$ dB/km) and 1550 nm ($\alpha \simeq 0.2$ dB/km).

Free-space links

Detectors

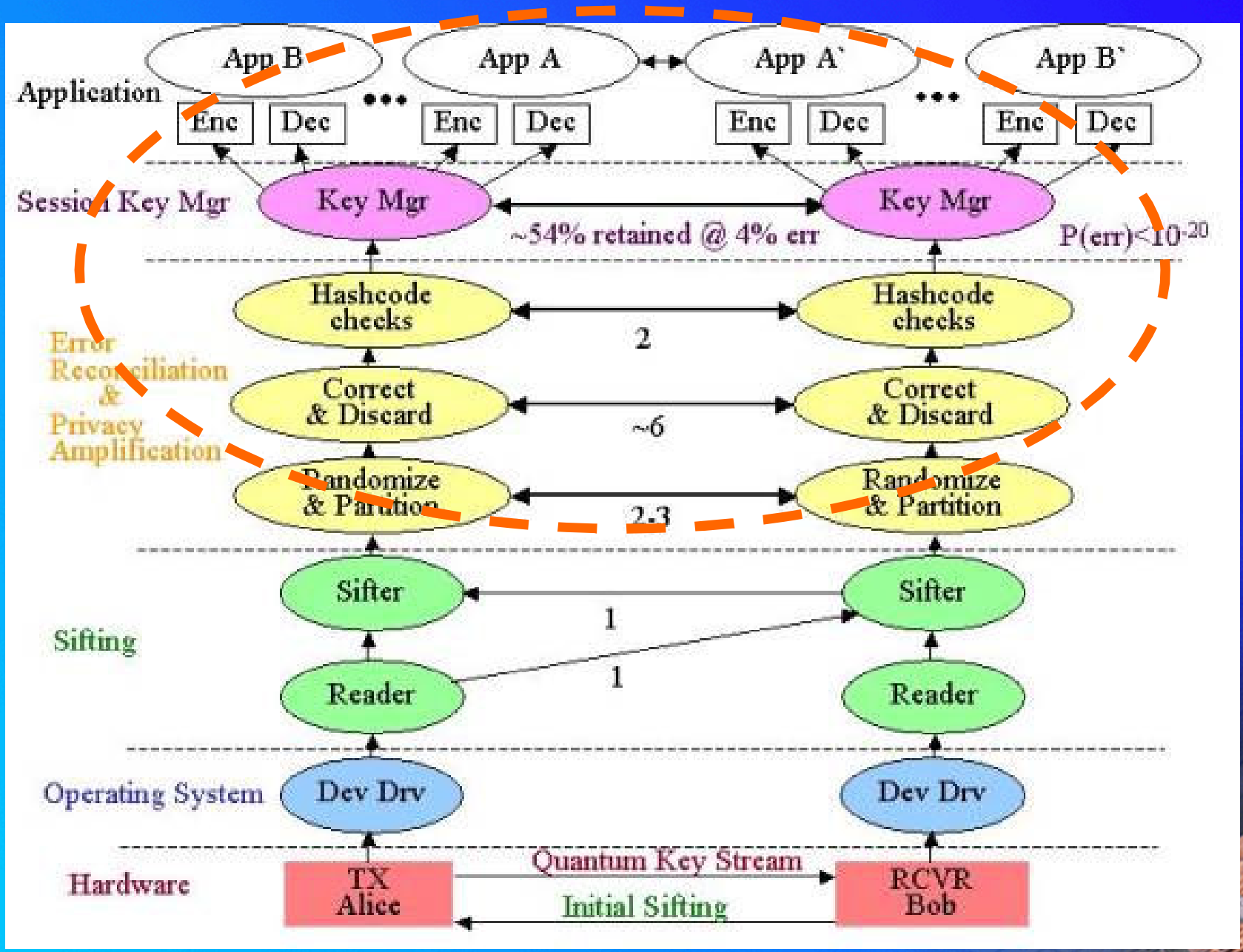
TABLE I. Typical parameters of single-photon detectors: detected wavelength λ, quantum efficiency η, fraction of dark counts p_d, repetition rate, maximum count rate, jitter, and temperature of operation T; the last column refers to the possibility of distinguishing the photon numbers. For acronyms and references, see text.

Name	λ (nm)	η	p_d	Rep. (MHz)	Count (MHz)	Jitter (ps)	T (K)	n
			APDs					
Si	600	50%	100 Hz	cw	15	50–200	250	N
InGaAs	1550	10%	10^{-5} per gate	10	0.1	500	220	N
Self-differencing				1250	100	60		
			Others					
VLPC	650	58–85 %	20 kHz	cw	0.015	N.A.	6	Y
SSPD	1550	0.9%	100 Hz	cw	N.A.	68	2.9	N
TES	1550	65%	10 Hz	cw	0.001	9×10^4	0.1	Y

Distillation procedure of secure keys

- real-time data acquisition
- key sifting
- error estimation
- error detection and correction (reconciliation) one-way, two-way
- privacy amplification

NIST QKD Protocol Stack



Correspondence between EDP and BB84 (Gottesman-Lo's proof)

EDP: Entanglement Distillation Protocol

2-way classical communications

CSS codes		BB84/six-state
bit-flip error detection	⟺	"advantage distillation"
bit flip error correction	⟺	error correction
phase error correction	⟺	privacy amplification

IEEE Trans. Inf. Theor. 49 (2003) 457

Quantum Distribution of Keys

- Produces raw classical key
- Observed error rate indicates amount of eavesdropper information and channel noise
- Error-correction is used to fix errors
- Random hash function is used to distill a smaller secret classical key

GLLP Formula for key generation rate

$$S \geq \tfrac{1}{2}\{-Q_\mu \cdot f(E_\mu) \cdot H_2(E_\mu) + Q_1 \cdot [1 - H_2(e_1)]$$

Error correction Privacy amplification

Q_μ is total # of detection events of signals.

E_μ is overall bit error rate of signals.

Q_1 is # of detection events due to single photon states.

e_1 is the bit error rate for single photon state.

$f(e) \geq 1$ is the error correction efficiency.

To prove security, one needs to lower bound Q_1 and upper bound e_1.

GLLP: D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Information and Computation. **4** (5) 2004 325-360, quant-ph/0212066

Combining Decoy with GLLP

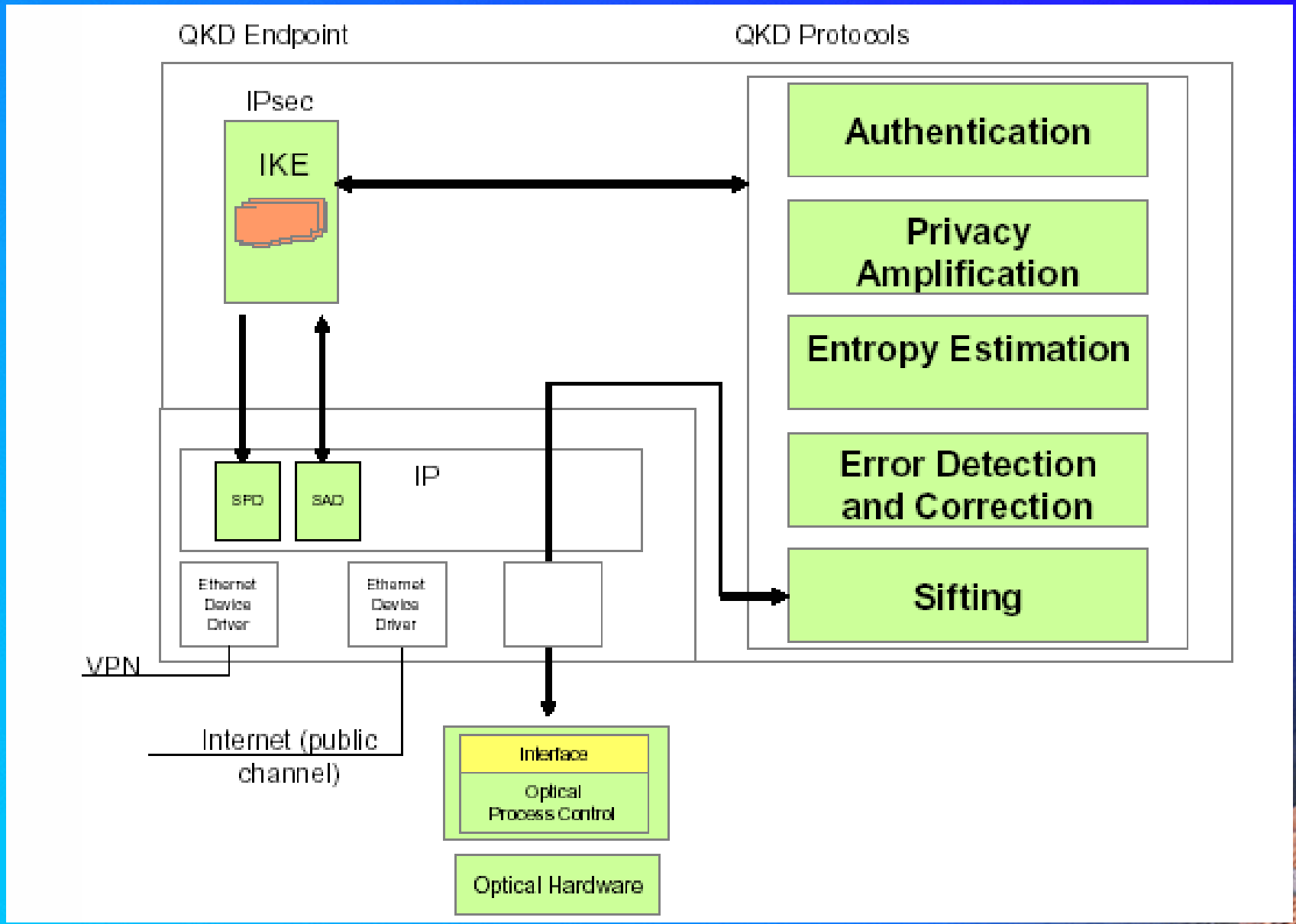
$$S \geq \tfrac{1}{2}\{-Q_{Signal} \cdot f(E_{Signal}) \cdot H_2(E_{Signal}) + Q_1 \cdot [1 - H_2(e_1)]\}$$

Error correction — Privacy amplification

- With the knowledge of yields $\{Y_n\}$, Alice can choose a much higher average photon number $\mu = O(1)$.
- Key generation rate $R = O(\eta)$ ☺

η : transmittance ~ 10^{-3}

QKD Software Suite and Protocols for the DARPA Quantum Network



Distill protocols for secret key

Error correction

One can use the algorithm **CASCADE**

Ref. Brassard G. and Salvail, L., 1993, Secret-Key Reconciliation by Public Discussion, proceedings of EUROCRYPT'94, Lecture Notes in Computer Science, 765, Springer-Verlag, 410-423.

Channel authentication

Protocol authentication algorithm should be implemented

Privacy amplification

Alice chooses a randomly a hashing function f, from some class F which is universal$_2$

$$f:\{0,1\}^N \rightarrow \{0,1\}^{N-L-S}$$

provided Eve knows at most L bits of an N-*bit* string common to Alice and Bob, they can publicly distill a shorter string of length $m=N-L-S$, where S is an arbitrary security parameter, on which Eve has less than $2^{-S}/\ln 2$ bits of information on average.

Error Correction I

We suggest the following algorithms:

(After obtaining experimentally measured Q_μ and E_μ, and estimated lower bound for Q_1 and upper bound e_1 of single photons)

Q_μ is total # of detection events of signals.

E_μ is overall bit error rate of signals.

Q_1 is # of detection events due to single photon states.

e_1 is the bit error rate for single photon state.

1. Using **CASCADE** procedure

   Alice and Bob publicly compare the parities of blocks of their data, and where these do not match, perform a bisective search within the block to identify and discard the error

Refs. Brassard G. and Salvail, L., 1993, Secret-Key Reconciliation by Public Discussion, proceedings of EUROCRYPT'94, Lecture Notes in Computer Science, 765, Springer-Verlag, 410-423.

C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, J. Cryptology, vol. 5, 3 1992 .

Error Correction II

2. Using a classical error correction code **C** (linear code of length n) which can correct errors with measured level of QBER E_μ with high probability (*up to 5~10 standard deviation, which promises a high confidence interval for statistical fluctuation*). Suppose one block data (of length n) for Alice is u, while it is $u+\varepsilon$ for Bob

a) Alice announces $u+v$, where v is a random code word in **C**.

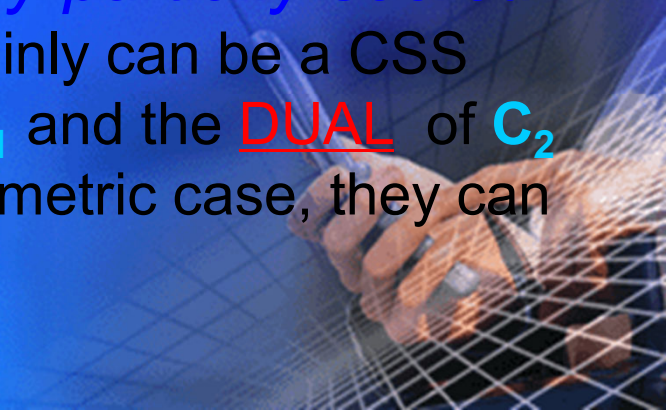
b) Bob computes $u+\varepsilon+u+v=v+\varepsilon$

c) Correction in **C** to obtain v, and decode to obtain the random sequence k (of length m) with code word v .

Remarks:

① The sequence k is error free, *but possibly only partially secret.*

② Here, the classical error correction code **C** certainly can be a CSS code C_1, with C_2 being a subcode of C_1. Both C_1 and the DUAL of C_2 can each correct up to $E_\mu * n$ errors. (In the asymmetric case, they can correct up to a different fraction of errors)



BBN's 'Niagara' LDPC Forward Error Correction

40x Less Comms Overhead, 16x Less CPU than Cascade

Inputs

Pseudo-random seed

k (block size)

D – density profile

p – number of parity constraints (revealed bits)

historic error rate

noise margin

margin for suboptimal code

Code

A low-density parity-check matrix

$$\begin{matrix} 1, & 0, & 0, & \ldots & 1 \\ 0, & 0, & 1, & \ldots & 0 \\ & & \vdots & & \\ 0, & 1, & 0, & \ldots & 0 \end{matrix}$$

Random, with constraints on row/column weights

A promising alternative to adding a safety margin is to add more parity bits when decoding fails

Average for 4096 bit blocks, 3% error rate	BBN Cascade	LDPC
Revealed bits	958	1006
% of Shannon limit	120%	126%
Delay (round trips)	68	**1**
Communication (bytes)	19200	**480**
CPU usage (secs / Mb, 800MHz x86)	17.4	**1.1**

DARPA BBN TECHNOLOGIES Harvard University BOSTON UNIVERSITY

中国科学技术大学 陈腾

Quantum information network in Defense Advanced Research Projects Agency (DARPA)

Privacy amplification

The privacy amplification *depends:*

- **Quantum bit error rate (QBER)**
- **Nature of the photon source**
- **Real life quantum channel properties (e.g. for single photon error rate and signal gain estimated from decoy states)**
- **Eavesdropping**

Privacy amplification (theory)

From unconditional security proof, we can use a *linear* hash function to N-bit key k

Applying a 0-1 $m*N$ matrix to k, Alice and Bob obtain a final m-bit key k' about which Eve has an exponentially small amount of information.

Use good hashing function

Alice chooses a randomly a hashing function f, from some class F which is ***(strongly) universal***$_2$

$$f:\{0,1\}^N \to \{0,1\}^{N-L-S}$$

provided Eve knows at most L bits of an N-*bit* string common to Alice and Bob, they can publicly distill a shorter string of length $m=N-L-S$, where S is an arbitrary security parameter, on which Eve has less than $2^{-S}/\ln 2$ bits of information on average.

good hashing function

Alice chooses a randomly a hashing function f, from some class F which is ***(strongly) universal$_2$***

A class *G* of functions *A* -> *B* is ***universal$_2$*** if for any distinct x_1 and x_2 in A, the probability that $g(x_1) = g(x_2)$ is at most 1/|*B*| when *g* is chosen at random from *G* according to the uniform distribution.

Future development

Authentication: foundation for QKD

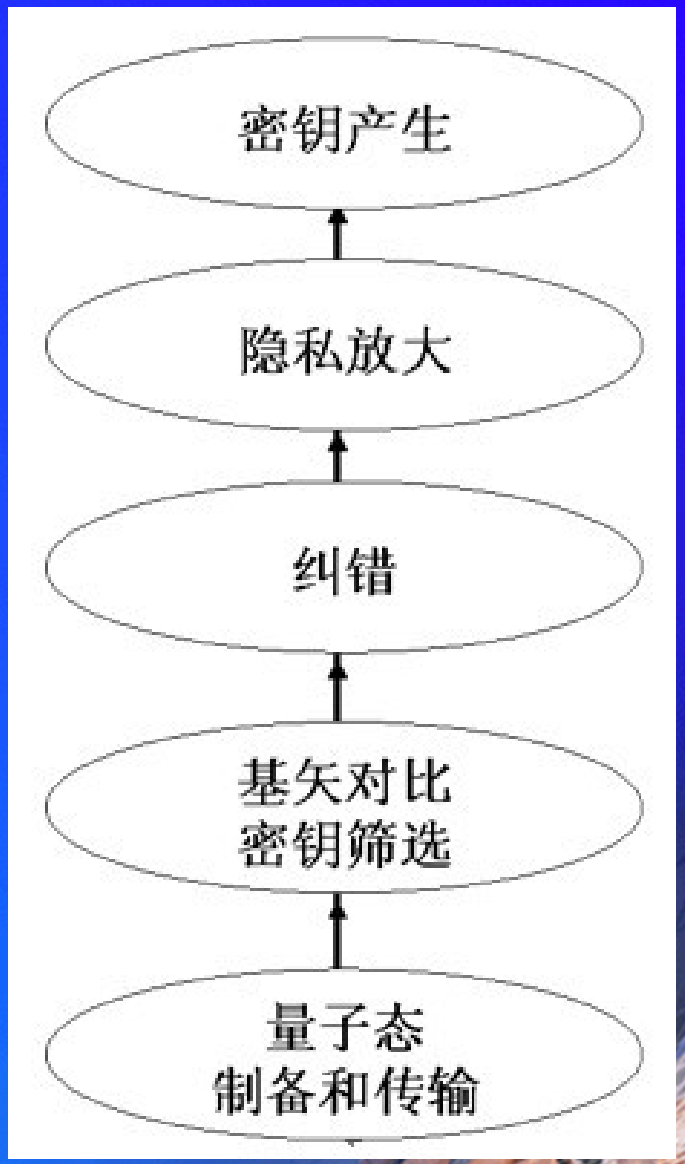
Error correction: efficient forward error correction algorithms capable of operating close to the Shannon limit

Privacy amplification: fast privacy amplification algorithms

Need REAL-TIME (hardware) implementation

QKD Protocols

- Sifting –Unmatched Bases; “stray” or “lost” qubits
- Error Correction – Noise & Eaves-dropping detected – Uses “cascade” protocol – Reveals information to Eve so need to track this.
- Privacy Amplification – reduces Eve’s knowledge obtained by previous EC
- Authentication – Continuous to avoid man-in-middle attacks – not required to initiate using shared keys



Decoy QKD Outline

1. Motivation and Introduction
2. Problem
3. Our Solution and its significance

1. Motivation and Introduction

Commercial Quantum Crypto products available on the market Today!

MAGIQ TECH.

- Distance over 100 km of commercial Telecom fibers.

ID QUANTIQUE

Bad News (for theorists)

Theory of quantum key distribution (QKD) is **behind** experiments.

Opportunity:

By developing theory, one can bridge gap between theory and practice.

Happy Marriage

Theory and Experiment go hand in hand.

中国科学技术大学 陈凯

Key Distribution Problem

Alice and Bob would like to communicate in unconditional security in the presence of an eavesdropper, Eve.

To do so, they need to share a common random string of number----key

Bennett and Brassard's scheme (BB84)

Alice Bob

ASSSUMPTIONS:

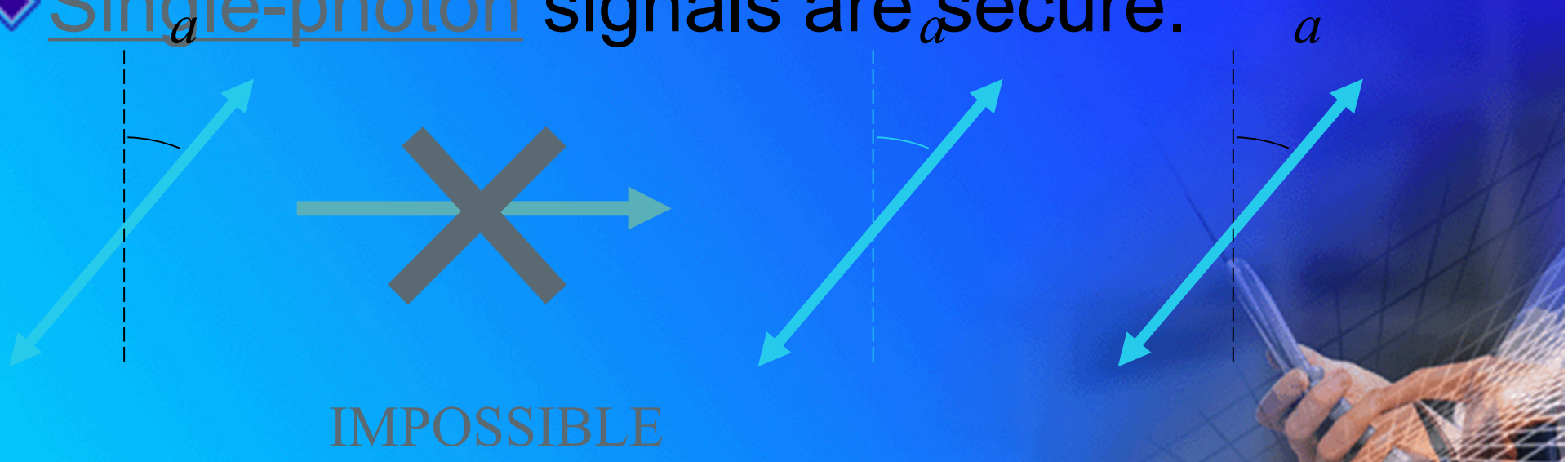
1. Source: Emits perfect single photons. (No multi-photons)
2. Channel: noisy but lossless. (No absorption in channel)
3. Detectors: a) Perfect detection efficiency. (100 %)
4. Basis Alignment: Perfect. (Angle between X and Z basis is exactly 45 degrees.)

Assumptions lead to security proofs:
Mayers (BB84), Lo and Chau (quantum-computing protocol), Biham et al. (BB84), Ben-Or (BB84), Shor-Preskill (BB84), …

Conclusion: QKD is secure in theory.

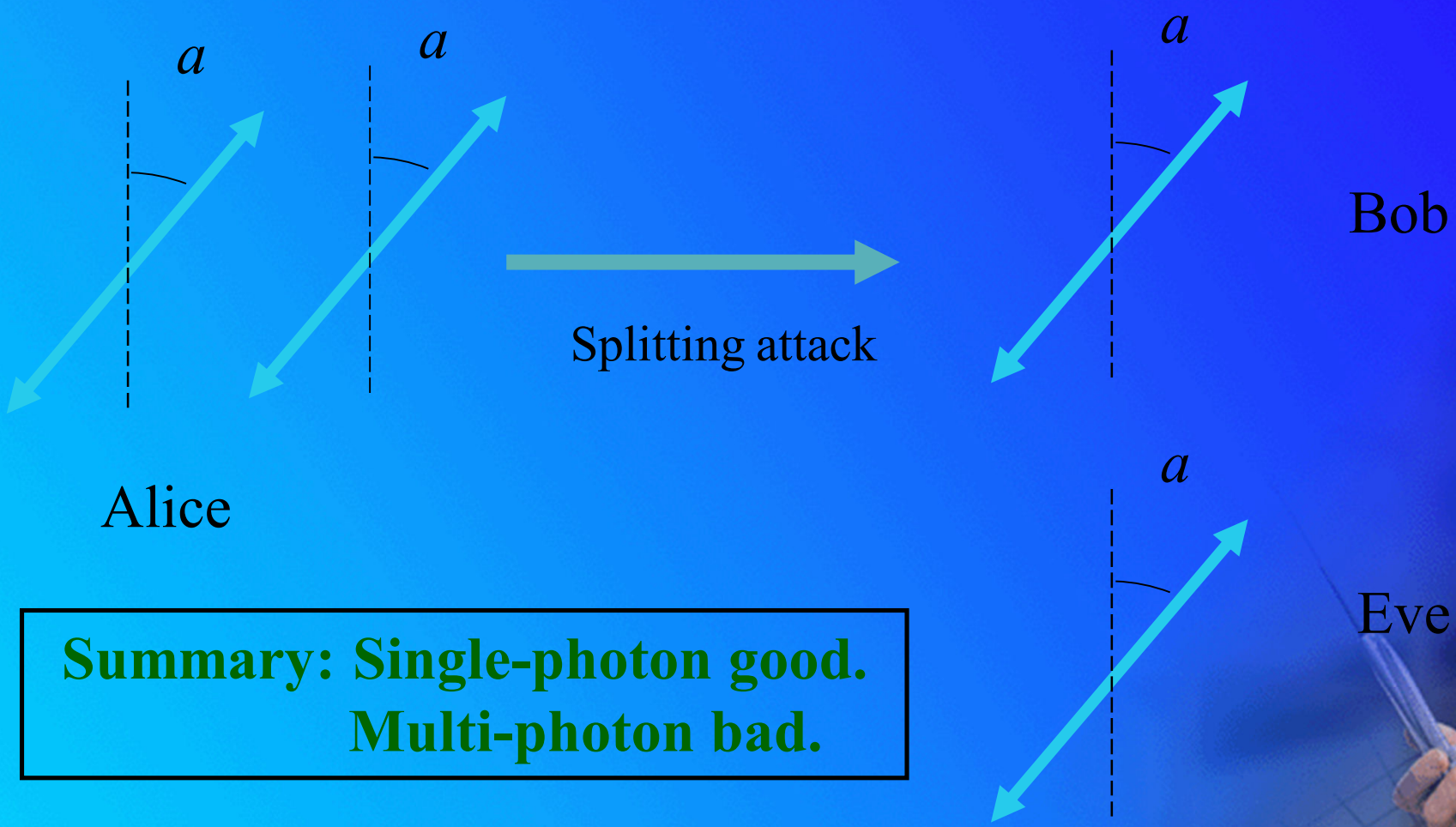
Reminder: Quantum No-cloning Theorem

- An unknown quantum state **CANNOT** be cloned. Therefore, eavesdropper, Eve, cannot have the same information as Bob.
- Single-photon signals are secure.



Photon-number splitting attack against multi-photons

A multi-photon signal CAN be split.
(Therefore, insecure.)



Summary: Single-photon good.
Multi-photon bad.

QKD : Practice

Reality:

1. Source: (**Poisson photon number distribution**)
   Mixture. Photon number = k with probability: $\frac{\alpha^k}{k!}e^{-\alpha}$
   Some signals are, in fact, double photons!
2. Channel: Absorption inevitable. (e.g. 0.2 dB/km)
3. Detectors:
   (a) Efficiency ~15% for Telecom wavelengths
   (b) "Dark counts": Detector's erroneous fire.
   Detectors will claim to have detected signals with some probability even when the input is a vacuum.
4. Basis Alignment: Minor misalignment inevitable.

Question: Is QKD secure in practice?

Prior art on BB84 with imperfect devices

1. Inamori, Lutkenhaus, Mayers (ILM)
2. Gottesman, Lo, Lutkenhaus, Preskill (GLLP)

GLLP: Under (semi-) realistic assumptions,
if imperfections are sufficiently small,
then BB84 is secure.

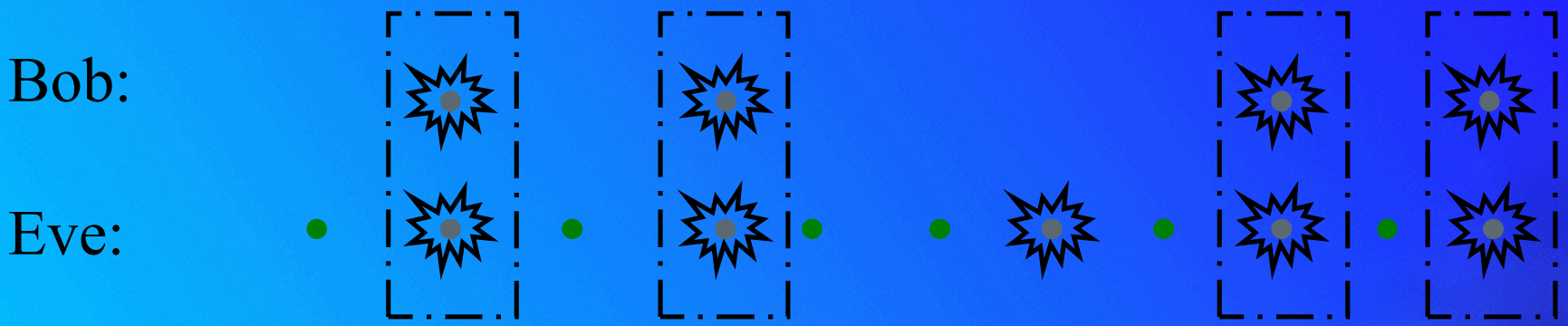
Question: Can we go beyond these results

2. Problem

Big Problem: Nice guys come last

Problems: 1) Multi-photon signals (bad guys) can be split.

2) Eve may suppress single-photon signals (Good guys).

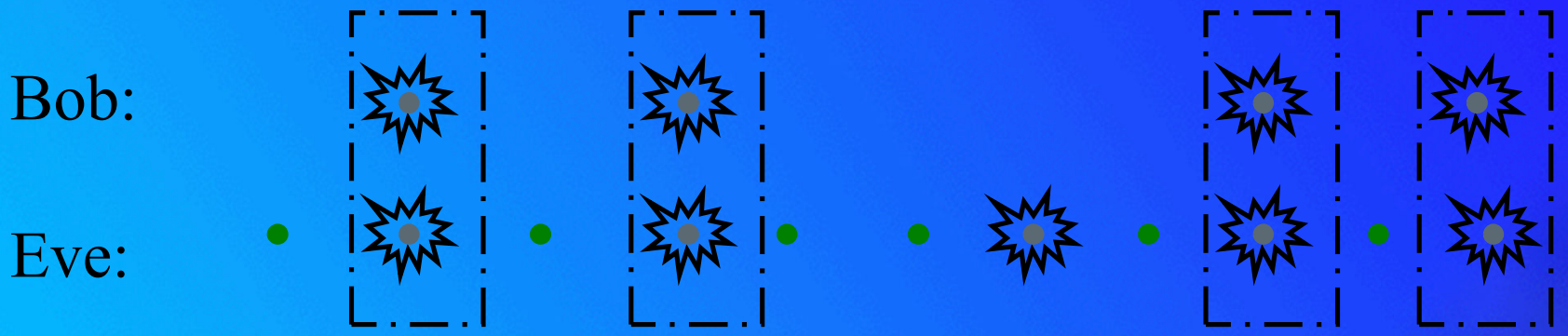


Eve may disguise herself as absorption in channel.
QKD becomes INSECURE as Eve has whatever Bob has.

Signature of this attack: Multi-photons are much more likely to reach Bob than single-photons.
(Nice guys come last).

Yield as a function of photon number

Let us define Y_n = yield
= conditional probability that a signal will be detected by Bob, given that it is emitted by Alice as an **n-photon** state.



For example, with photon number splitting attack:

$Y_2 = 1$: all two-photon states are detected by Bob.
$Y_1 = 0$: all single-photon states are lost.

Figures of merits in QKD

- # of Secure bits per signal (emitted by Alice).

  How long is the final key that Alice and Bob can generate?
- (Maximal) distance of secure QKD.

  How far apart can Alice and Bob be from each other?

Prior Art Result

Consider the worst case scenario where **all** signals received by Bob are bad guys. (Insecure.)

To prevent this from happening, we need:

# of signals received by Bob

$>$ # of multi-photon signals emitted by Alice.

Consider **channel transmittance η**.

For security, we use **weak** Poisson photon number distribution: $\mu = O(\eta)$.

Secure bits per signal $S = O(\eta^2)$.

Big Gap between theory and practice of BB84

	Theory	Experiment
Key generation rate:	$S = O(\eta^2)$.	$S = O(\eta)$.
Maximal distance:	d ~ 35km.	d >120km.

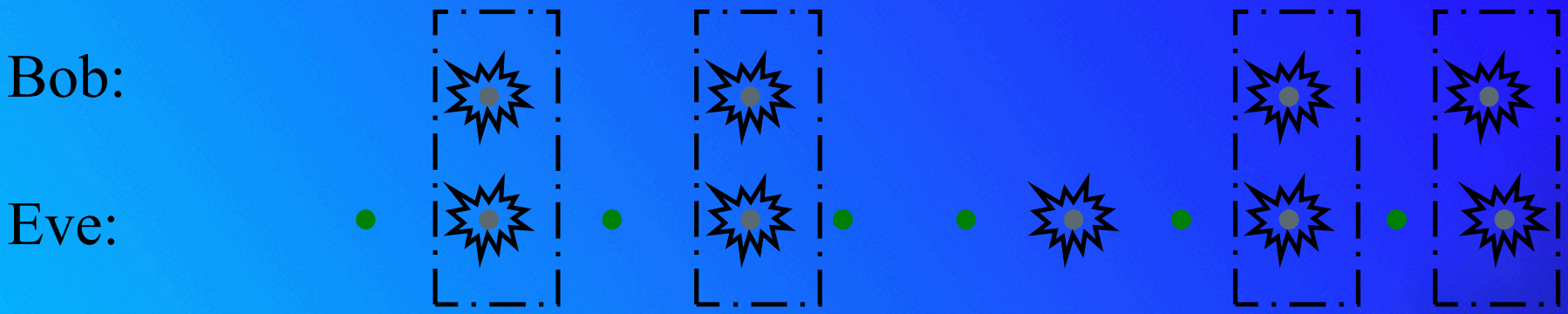
Prior art solutions (All bad):

1) Use Ad hoc security: Defeat main advantage of Q. Crypto. : unconditional security. (Theorists unhappy ☹.)
2) Limit experimental parameters: Substantially reduce performance. (Experimentalists unhappy ☹.)
3) Better experimental equipment (e.g. Single-photon source. Low-loss fibers. Photon-number-resolving detectors): Daunting experimental challenges. Impractical in near-future. (Engineers unhappy ☹.)

Question: How can we make everyone happy ☺?

(Recall) Problem: Photon number splitting attack

Let us define Y_n = yield
= conditional probability that a signal will be detected by Bob, given that it is emitted by Alice as an **n-photon** state.



For example, with photon number splitting attack:

$Y_2 = 1$: all two-photon states are detected by Bob.

$Y_1 = 0$: all single-photon states are lost.

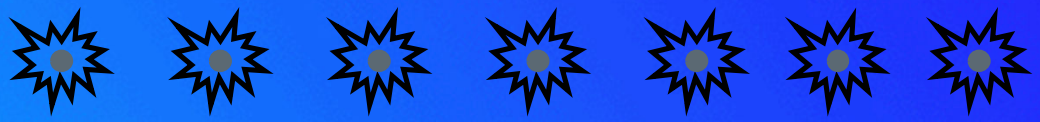
Yield for multi-photons may be much higher than single-photons.

Is there any way to detect this?

A solution: Decoy State (Toy Model)

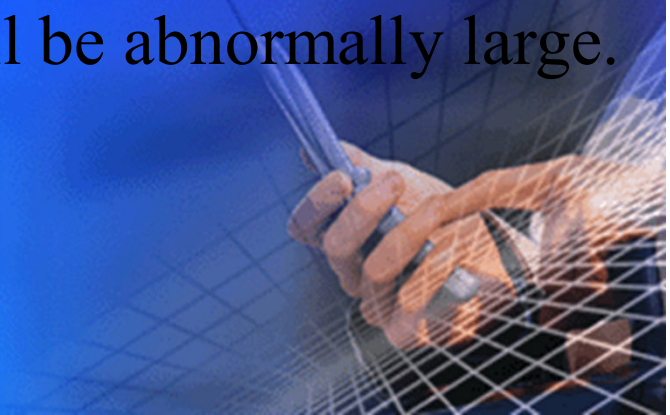
Goal: Design a method to test experimentally the yield (i.e. transmittance) of multi-photons.

Method: Use two-photon states as decoys and test their yield.

Alice: N signals 

Bob: x signals 

Alice sends N two-photon signals to Bob.
Alice and Bob estimate the yield $Y_2 = x/N$.
If Eve selectively sends multi-photons, Y_2 will be abnormally large.
Eve will be caught!



Procedure of Decoy State QKD (Toy Model).

A) Signal state: Poisson photon number distribution α (at Alice).

B) Decoy state: = two-photon signals

1) Alice randomly sends either a signal state or decoy state to Bob.
2) Bob acknowledges receipt of signals.
3) Alice publicly announces which are signal states and which are decoy states.
4) Alice and Bob compute the transmission probability for the signal states and for the decoy states respectively.

If Eve selectively transmits two-photons, an abnormally high fraction of the decoy state B) will be received by Bob. Eve will be caught.

Practical problem with toy model

- Problem: Making perfect two-photon states is hard, in practice
- Solution: Make **another mixture** of good and bad guys with a **different weight**.

Decoy state idea (Heuristic)

1) Signal state: Poisson photon number distribution: α (at Alice). Mixture 1.

2) **Decoy state: Poisson photon number distribution: μ~ 2 (at Alice). Mixture 2**

W.-Y. Hwang's **heuristic** idea (PRL):

- If Eve lets an abnormally high fraction of multi-photons go to Bob, then decoy states (which has high weight of multi-photons) will have an abnormally high transmission probability.
- Therefore, Alice and Bob can catch Eve!

Can we make things rigorous?

YES!

3. Our solution:

I Come!

Experimental observation

Yield: $$Q(\mu) = Y_0 e^{-\mu} + Y_1 e^{-\mu}\mu + Y_2 e^{-\mu}(\mu^2/2) + \ldots + Y_n e^{-\mu}(\mu^n/n!) + \ldots.$$

Error Rate $$E(\mu) = Y_0 e^{-\mu} e_0 + Y_1 e^{-\mu}\mu e_1 + Y_2 e^{-\mu}(\mu^2/2) e_2 + \ldots + Y_n e^{-\mu}(\mu^n/n!) e_n + \ldots.$$

If Eve cannot treat the decoy state any differently from a signal state

$$Y_n(\text{signal}) = Y_n(\text{decoy}),\ e_n(\text{signal}) = e_n(\text{decoy})$$

Y_n: yield of an n-photon signal

e_n : quantum bit error rate (QBER) of an n-photon signal.

Our ideas

Try **every** Poisson distribution μ!

We propose that Alice *switches power of her laser up and down*, thus producing as decoy states Poisson photon number distributions, μ's for **all** possible values of μ's.

Each μ gives Poisson photon number distribution:

$$Q(\mu), E(\mu) \forall \mu \Rightarrow Y_n, e_n \forall n$$

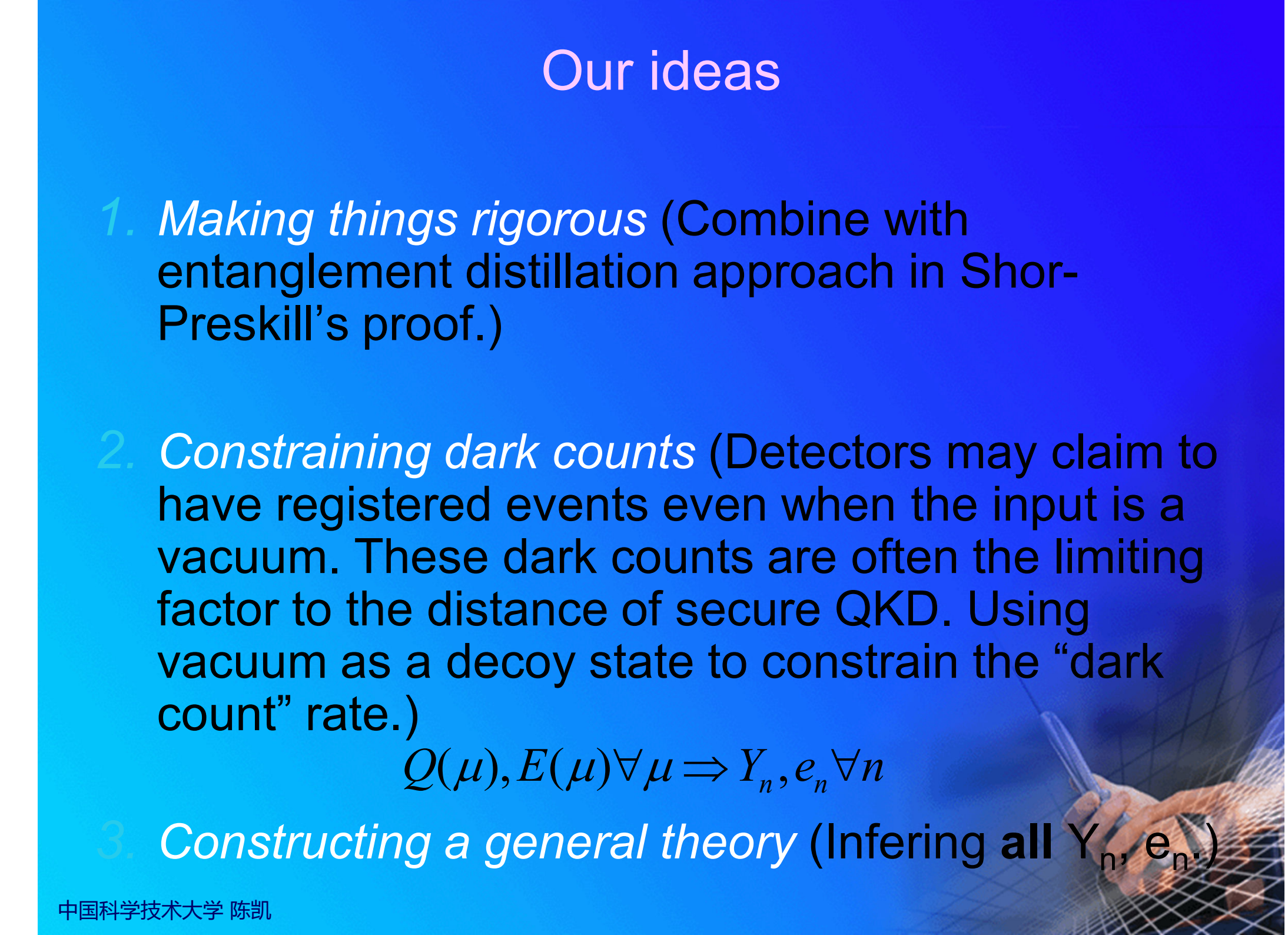
Our ideas

1. *Making things rigorous* (Combine with entanglement distillation approach in Shor-Preskill's proof.)

2. *Constraining dark counts* (Detectors may claim to have registered events even when the input is a vacuum. These dark counts are often the limiting factor to the distance of secure QKD. Using vacuum as a decoy state to constrain the "dark count" rate.)

$$Q(\mu), E(\mu) \forall \mu \Rightarrow Y_n, e_n \forall n$$

3. *Constructing a general theory* (Infering **all** Y_n, e_n.)



Our ideas

Conclusion: We severely limit Eve's eavesdropping strategies.

Any attempt by Eve to change <u>any</u> of Y_n, e_n 's will, in principle be caught.

$$Q(\mu), E(\mu) \forall \mu \Rightarrow Y_n, e_n \forall n$$

Old Picture

Theory

Experiment

Secure bits per signal: $S = O(\eta^2)$.

$S = O(\eta)$.

Maximal distance: $d \sim 35$km.

$d > 120$km.

There is a big gap between theory and practice of BB84.

NEW Picture

Theory

Experiment

Secure bits per signal: S = O (η).

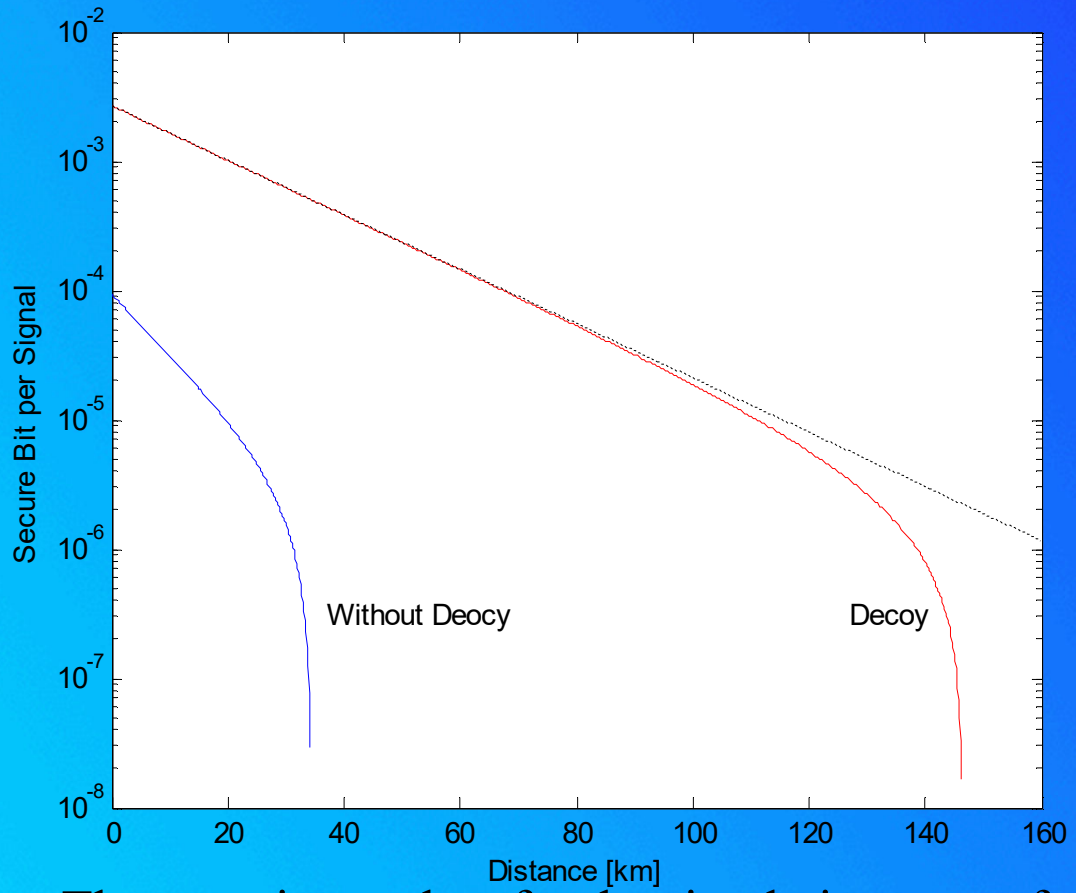
S= O (η).

Maximal distance: d >120 km.

d >120km.

Even with imperfect devices, one gets highest performance possible without compromising security.

Compare the results with and without decoy states



Key parameter:

Wavelength: 1550nm

Channel loss: 0.21dB/km

Signal error rate: 3.3%

Dark count: $8.5*10^{-7}$ per pulse

Receiver loss and detection efficiency: 4.5%

The experiment data for the simulation come from the recent paper:

C. Gobby, Z. L. Yuan, and A. J. Shields, Applied Physics Letters, (2004)

Related Work

Decoy QKD

W.-Y. Hwang, *Phys. Rev. Lett. 91, 057901 (2003);*
H.-K. Lo, X.-F. Ma, and K. Chen, *Phys. Rev. Lett. 94, 230504 (2005);*
X.-B. Wang, *Phys. Rev. Lett. 94, 230503 (2005).*

- Using another approach (strong reference pulse), another protocol (essentially B92) has recently been proven to be secure with R=O(η). [Koashi, Phys. Rev. Lett. 93, 120501 (2004)]
- It will be interesting to compare this approach with ours.

Related Work

PNS attack

B. Huttner, and N. Imoto, N. Gisin, T. Mor, Quantum cryptography with coherent states, *Phys. Rev. A 51, 1863–1869 (1995)*

Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders, Limitations on Practical Quantum Cryptography, *Phys. Rev. Lett. 85, 1330–1333 (2000)*

实用Decoy QKD

首先我们假设使用的弱相干态光源是相位随机的，则从Alice端发射的量子态可以写为

$$\rho_A = \sum_{i=0}^{\infty} p_i |i\rangle\langle i| = \sum_{i=0}^{\infty} \frac{\mu^i}{i!} e^{-\mu} |i\rangle\langle i|$$

其中 μ 为平均光子数密度。另外我们定义n光子数态的计数率(yield)为，当Alice发射一个n光子数态时Bob端得到探测事件的条件概率。

X.-F. Ma, B. Qi, Y. Zhao and H.-K. Lo, Practical decoy state for quantum key distribution. Phys. Rev. A, 72,012326 (2005).

实用Decoy QKD

Bob端总的接收率为

$$Q_\mu = \sum_{i=0}^{\infty} Q_i = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu}$$

同时总的量子误码率QBER满足

$$E_\mu Q_\mu = \sum_{i=0}^{\infty} e_i Q_i = \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} e^{-\mu}$$

这里 Y_0 为只有背景光时的计数率，e_i 为n光子数态的量子误码率。

X.-F. Ma, B. Qi, Y. Zhao and H.-K. Lo, Practical decoy state for quantum key distribution. Phys. Rev. A, 72,012326 (2005).

实用Decoy QKD

以一个信号态(平均光子数密度为μ)和2个诱骗态（平均光子数密度分别为ν_1,ν_2）为例，假设 $\nu_1 \geq \nu_2 \geq 0, \mu > \nu_1 + \nu_2$

则有

$$Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} = Y_1(\nu_1 - \nu_2) + \sum_{i=2}^{\infty} \frac{Y^i}{i!}(\nu_1^i - \nu_2^i) \leq Y_1(\nu_1 - \nu_2) + \frac{(\nu_1^2 - \nu_2^2)}{\mu^2} \sum_{i=2}^{\infty} Y^i \frac{\mu^i}{i!}$$

$$= Y_1(\nu_1 - \nu_2) + \frac{(\nu_1^2 - \nu_2^2)}{\mu^2}(Q_\mu e^\mu - Y_0 - Y_1\mu)$$

其中我们用到了一个不等式，

当$0 < a + b < 1$并且$i \geq 2$时，总有 $a^i - b^i \leq a^2 - b^2$

X.-F. Ma, B. Qi, Y. Zhao and H.-K. Lo, Practical decoy state for quantum key distribution. Phys. Rev. A, 72,012326 (2005).

实用Decoy QKD

可得单光子态的接收率的下限

$$Q_1 \geq Q_1^L = \mu e^{-\mu} Y_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2}[Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2}(Q_\mu e^\mu - Y_0)]$$

对于平均光子数密度分别为 的两个诱骗态来说，均满足关于 $E_\mu Q_\mu$ 的公式,两式相减可得单光子态的QBER的上限，

$$e_1 \leq e_1^U = \frac{E_{\nu_1} Q_{\nu_1} e^{\nu_1} - E_{\nu_2} Q_{\nu_2} e^{\nu_2}}{(\nu_1 - \nu_2) Y_1^L}$$

X.-F. Ma, B. Qi, Y. Zhao and H.-K. Lo, Practical decoy state for quantum key distribution. Phys. Rev. A, 72,012326 (2005).

实用Decoy QKD

最终的成码率

$$R \geq = q\{-Q_\mu f(Q_\mu) H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}$$

GLLP的结果对于计算安全密钥率需要四个重要参数：量子光源的总接收率和总QBER，单光子态的接收率和QBER

其中

μ 为光源的平均光子数密度；

Q_μ 为光源信号态接收率；

E_μ 是接收到的信号态误码率；

$H_2(x)$ 为二元熵函数；

q 为系统效率，对于BB84协议来说为1/2，这是因为只有一半的情形是Alice和Bob选定了相同的基矢；

$f(Q_\mu)$ 为双边纠错效率；

Q_1 为单光子态的接收率；

e_1 为单光子误码率

GLLP: D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Information and Computation. **4** (5) 2004 325-360, quant-ph/0212066

Combining Decoy with GLLP

$$S \geq \tfrac{1}{2}\{-Q_{Signal}\cdot f(E_{Signal})\cdot H_2(E_{Signal}) + Q_1\cdot[1-H_2(e_1)]\}$$

Error correction — Privacy amplification

- With the knowledge of yields $\{Y_n\}$, Alice can choose a much higher average photon number $\mu=O(1)$.
- Key generation rate $R=O(\eta)$ ☺

η : transmittance ~ 10^{-3}

Decoy QKD Summary

1. Decoy state BB84 allows:
   - Secure bits per signal: O (η)
     where η : channel transmittance.
   - Distance > 100km

2. Easy to implement. Alice just switches power of laser up and down (and measure transmittance and error rate).

3. Theory and experiment go hand-in-hand for standard BB84 quantum key distribution protocol.

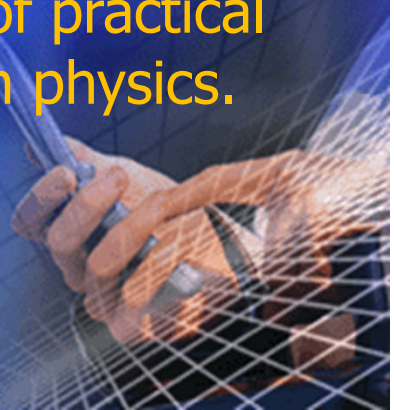
Requirements for unconditional security

1. Eve cannot intrude into Alice's and Bob's devices to access either the emerging key or their choices of settings.

2. Alice and Bob must trust the random number generators that select the state to be sent or the measurement to be performed.

3. The classical channel is authenticated with unconditionally secure protocols, which exist.(Carter and Wegman, 1979; Wegman and Carter, 1981; Stinson, 1995)

4. Eve is limited by the laws of physics. This requirement can be sharpened: in particular, one can ask whether security can be based on a restricted set of laws. In this review, as in the whole field of practical QKD, we assume that Eve has to obey the whole of quantum physics.



Several techniques for security proofs

1. The very first proofs by Mayers were somehow based on the uncertainty principle Mayers, 1996, 2001. This approach has been revived recently by Koashi 2006a, 2007.

2. Most of the subsequent security proofs have been based on the correspondence between entanglement distillation and classical post processing, generalizing the techniques of Shor and Preskill 2000. For instance, the most developed security proofs for imperfect devices follow this pattern Gottesman, Lo, Lütkenhaus, and Preskill, 2004.

3. The most recent techniques use instead information theoretical notions Ben-Or, 2002; Kraus, Gisin, and Renner, 2005; Renner, 2005; Renner, Gisin, and Kraus, 2005.

BOUNDS ON THE BIT ERROR RATE FOR BB84 AND THE SIX-STATE SCHEME

TABLE I

BOUNDS ON THE BIT ERROR RATE FOR BB84 AND THE SIX-STATE SCHEME USING ONE-WAY AND TWO-WAY CLASSICAL POST-PROCESSING. THE LOWER BOUNDS FOR TWO-WAY POST-PROCESSING, 18.9% FOR BB84 AND 26.4% FOR THE SIX-STATE SCHEME, COME FROM THE CURRENT WORK

BB84

	one-way	two-way
Upper bound	14.6%	1/4
Lower bound	11.0%	18.9%

Six-state Scheme

	one-way	two-way
Upper bound	1/6	1/3
Lower bound	12.7%	26.4%

Daniel Gottesman and Hoi-Kwong Lo, Proof of Security of Quantum Key Distribution With Two-Way Classical Communications, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 49, 457-475 (2003)

Decoy-state quantum key distribution with two-way classical postprocessing

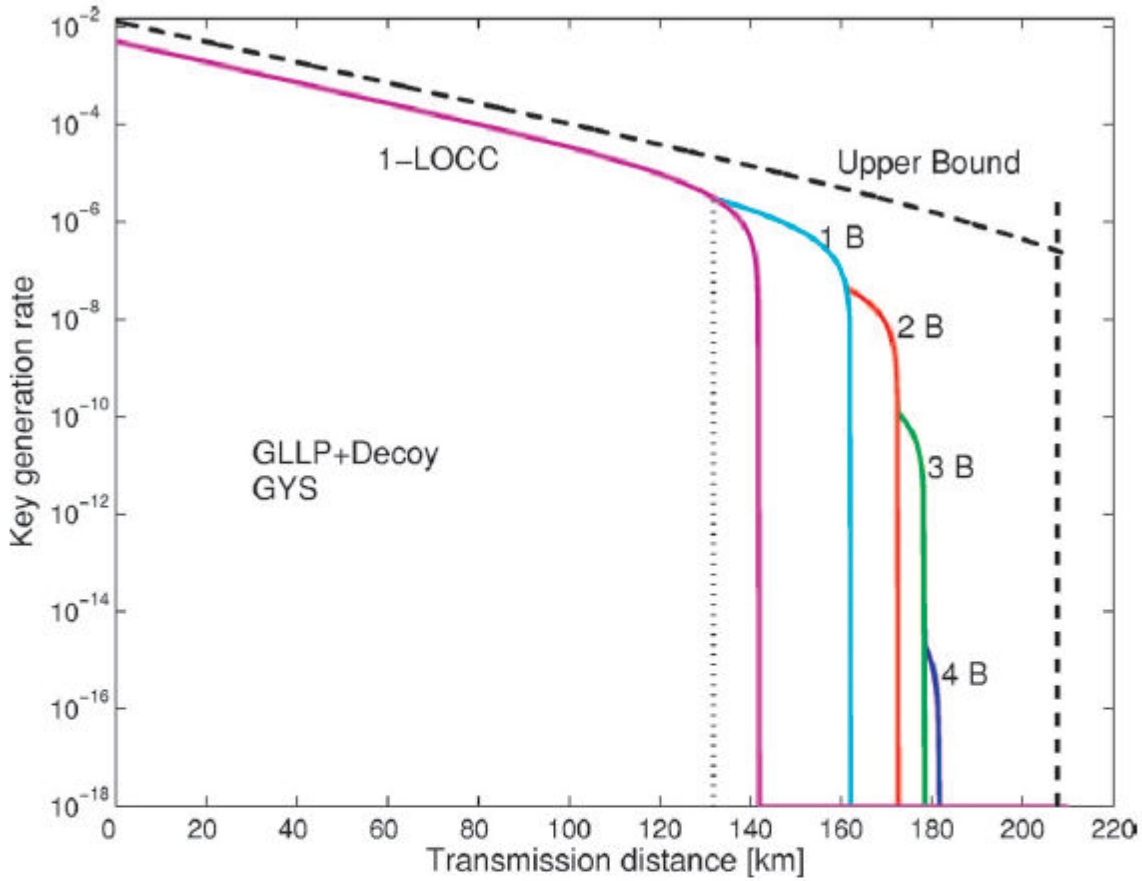


FIG. 3. (Color online) Plot of the key generation rate as a function of the transmission distance with the data postprocessing scheme of GLLP+decoy+B steps method. The parameters used are from the GYS experiment [19] listed in Table I. The GLLP +decoy+B steps scheme surpasses the scheme with 1-LOCC at a distance of 132 km. The maximal secure distance using four B steps is 181 km, which is not far from the upper bound of 208 km.

X.-F. Ma, C,-H. Fred Fung,† F. Dupuis, K. Chen, K. Tamaki,and H.-K. Lo, Phys. Rev. A 74, 032330 (2006)

Decoy-state quantum key distribution with both source errors and statistical fluctuations

Xiang-Bin Wang, C.-Z. Peng, J. Zhang, L. Yang, Jian-Wei Pan
General theory of decoy-state quantum cryptography with source errors
Phys. Rev. A 77, 042311 (2008)

Xiang-Bin Wang, Lin Yang, Cheng-Zhi Peng, Jian-Wei Pan, Decoy-state quantum key distribution with both source errors and statistical fluctuations, New. J. Phys., 11, 075006 (2009)

量子通信国际动态

欧洲

- 欧盟“基于量子密码的安全通信”工程集中了12个国家的41个研究组，发布了技术和商业白皮书，启动了技术标准化的制定，实现了多节点城域量子通信网络
- 欧空局以国际空间站为平台，计划于2013年开始进行空间量子通信实验

美国

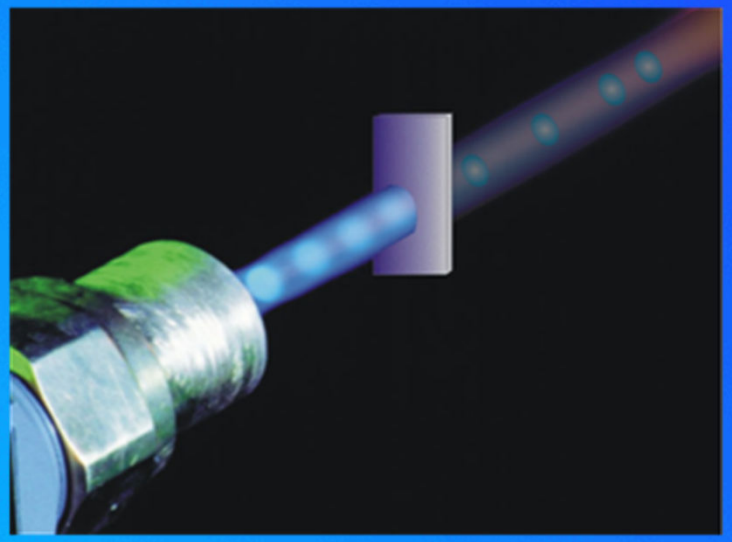
- “保持国家竞争力”计划中，量子信息为重点支持课题
- 09年信息科学白皮书中要求各科研机构一起协调开展量子信息技术研究
- 09年，美国军方完成了飞机与地面间的自由空间量子通信演示实验

日本

- 提出了量子信息技术长期研究战略，目前年投入2亿美元
- 通过洲际合作建成了多节点城域量子通信网络(Tokyo QKD Network)
- 5-10年内建成全国性的高速量子通信网

其它如加拿大、澳大利亚、巴西、印度等进行了大幅投入。商业领域包括AT&T、Bell实验室、IBM、HP、Hitachi、Toshiba等对量子通信技术投入了大量研发资本，推进产业化

早期弱光脉冲量子密钥分发的实验演示



准单光子源：弱光脉冲

- 每个脉冲 $P \ll 1$ → 近似单光子源
- 问题： P^2 每个脉冲里有两个光子

↓

光子数分束攻击

- 2005年以前所有的基于弱相干脉冲方案都存在安全漏洞

1. 2004，剑桥Toshiba 122km
2. 2004，日本NEC 150km **误码率7%左右**
3. 2005，中国 125km，初始成码率0.001比特/秒

- 该问题于1985年被首次提出

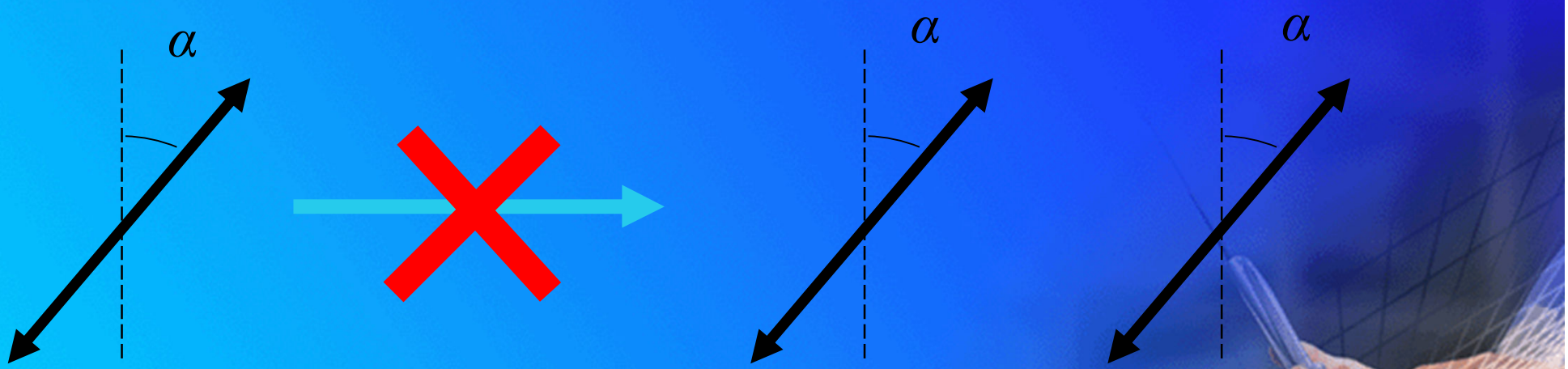
B. Huttner et al, PRA 51, 1863 (1985)
G. Brassard et al., PRL 85, 1330 (2000)

- 即使在理想情况下，

信息安全传输的最远距离也只有10公里量级，且成码率极低

量子不可克隆定理

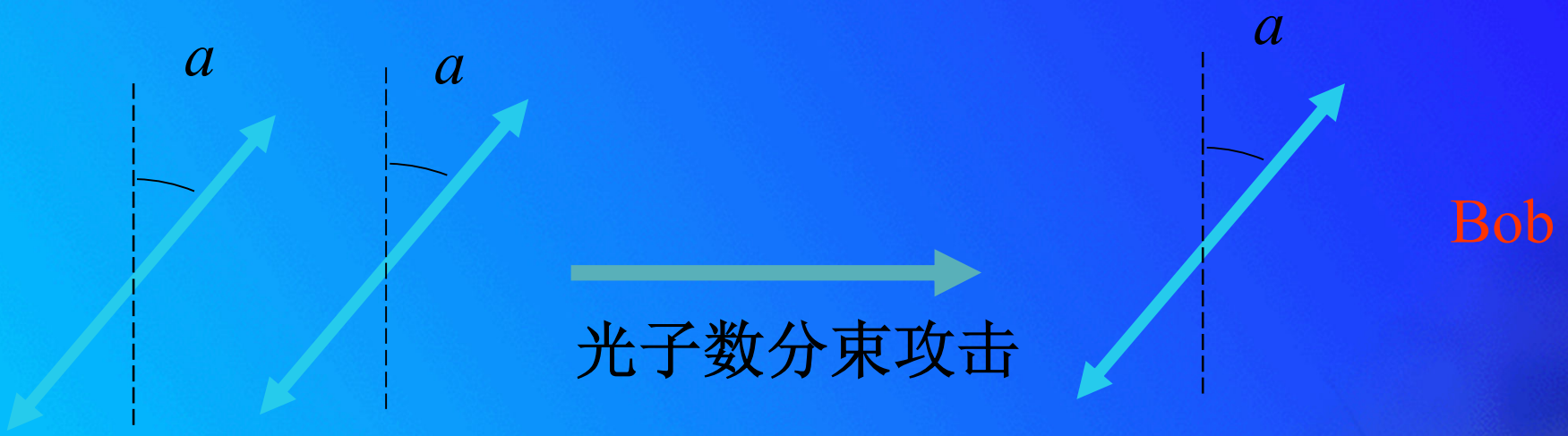
- 任意量子态不能被精确克隆。因此窃听者不能够获取到和接收方同样的信息。
- 单光子信号是安全的



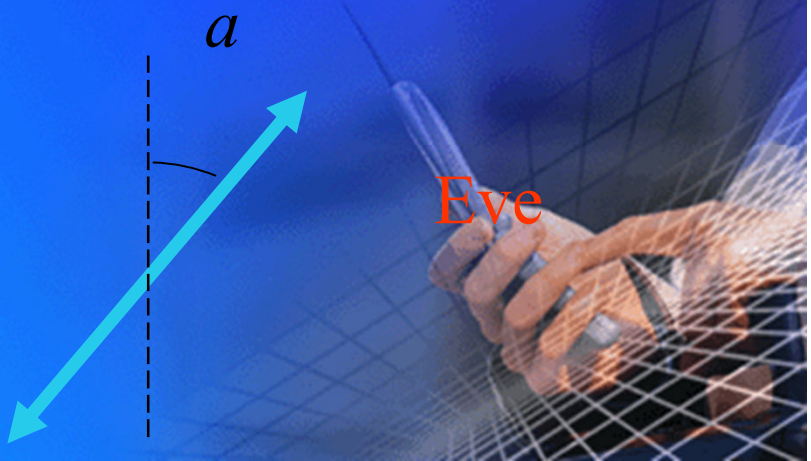
不可能的

多光子信号是不安全的

- 多光子信号原则上可以分束，因而是不安全的



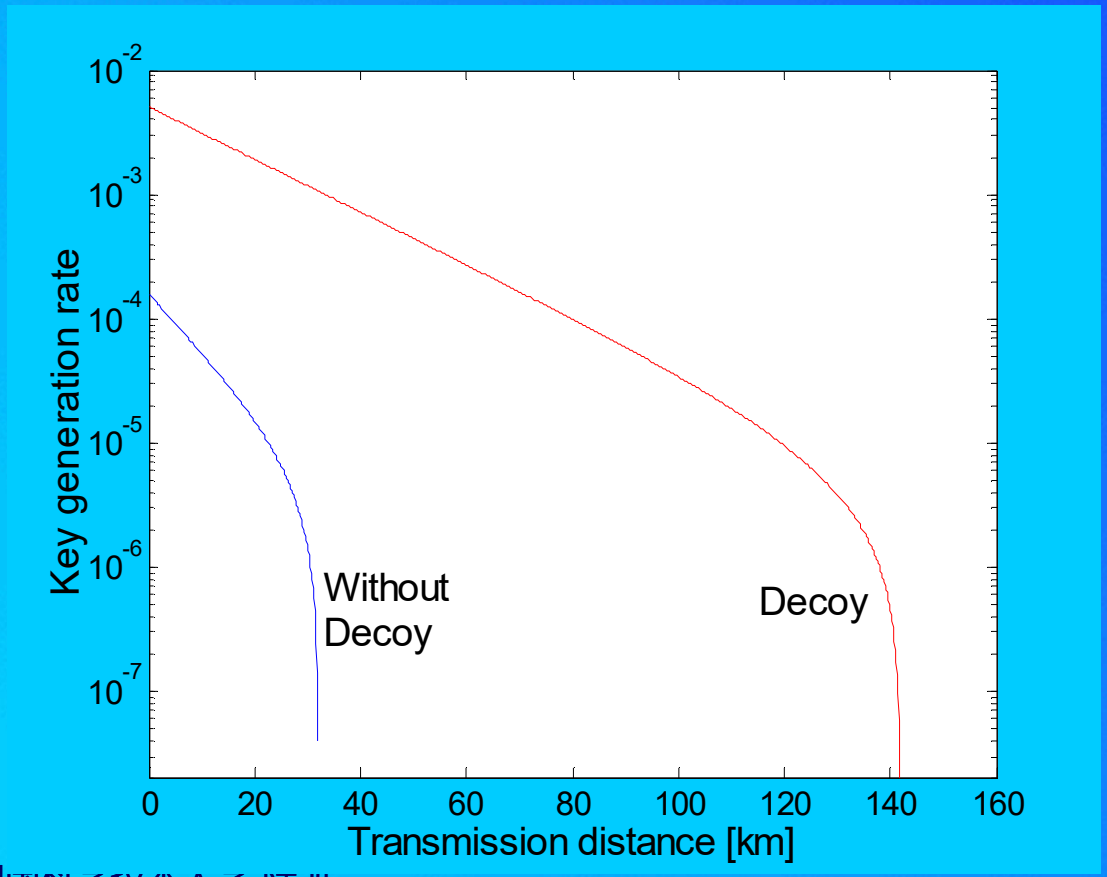
结论：单光子好的
多光子不好



基于诱骗态（Decoy State) 量子通信

W.-Y. Hwang, *Phys. Rev. Lett.* 91, 057901 (2003);
H.-K. Lo, X.-F. Ma, and K. Chen, *Phys. Rev. Lett.* 94, 230504 (2005);
X.-B. Wang, *Phys. Rev. Lett.* 94, 230503 (2005).

利用诱骗态方案安全通信的距离可达100公里以上!
在同等距离下可大幅度提高密钥的成码率



实验参数来自C. Gobby, Z. L. Yuan, and A. J. Shields, Applied Physics Letters, 84, 3762 (2004)

基于诱骗态量子通信的实验进展

2005年，第一个实验演示15km电信光纤通道(**Hoi-Kwong Lo教授研究组**)

Y. Zhao et al., *Phys.Rev.Lett.* 96,070502 (2006)

2006年，国内外3个小组几乎同时实现了超过100公里基于诱骗态的量子通信

- **光纤通道**(*telecom wavelength*)

  潘建伟教授研究组(102km)

  C.-Z. Peng et al., *Phys.Rev.Lett.* 98,010505(2007)

  美国Los Alamos国家实验室和NIST：R. Hughes(107km)

  D. Rosenberg et al., *Phys.Rev.Lett.* 98,010503(2007)

  郭光灿教授研究组：(25km)

  Q. Wang et al., *Phys.Rev.Lett.* 100, 090501(2008)

- **自由空间通道**

  欧洲联合实验组：H. Weinfurter & A. Zeilinger (144km)

  T. Schmitt-Manderbach et al.,*Phys.Rev.Lett.* 98,010504(2007)

基于诱骗态量子通信的实验

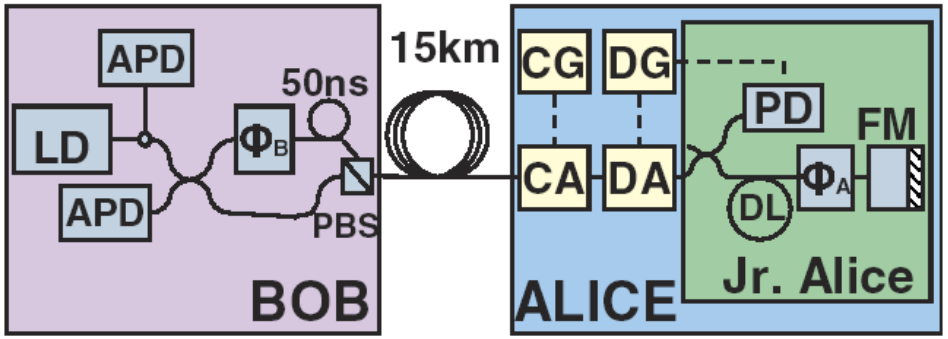


FIG. 1 (color online). Schematic of the experimental setup in our system. Inside Bob (Jr. Alice): Components in Bob's (Alice's) package of id Quantique QKD system. Our modifications: CA, compensating AOM; CG, compensating generator; DA, decoy AOM; DG, decoy generator. Original QKD system: LD, laser diode; APD, avalanche photon diode; Φ_i, phase modulator; PBS, polarization beam splitter; PD, classical photo detector; DL, delay line; FM, faraday mirror. Solid line, SMF28 single mode optical fiber; dashed line, electric cable.

潘建伟教授研究组**(102km)**
C.-Z. Peng et al., *Phys.Rev.Lett.* 98,010505(2007)

Hoi-Kwong Lo教授研究组
Y. Zhao et al., *Phys.Rev.Lett.* 96,070502 (2006)

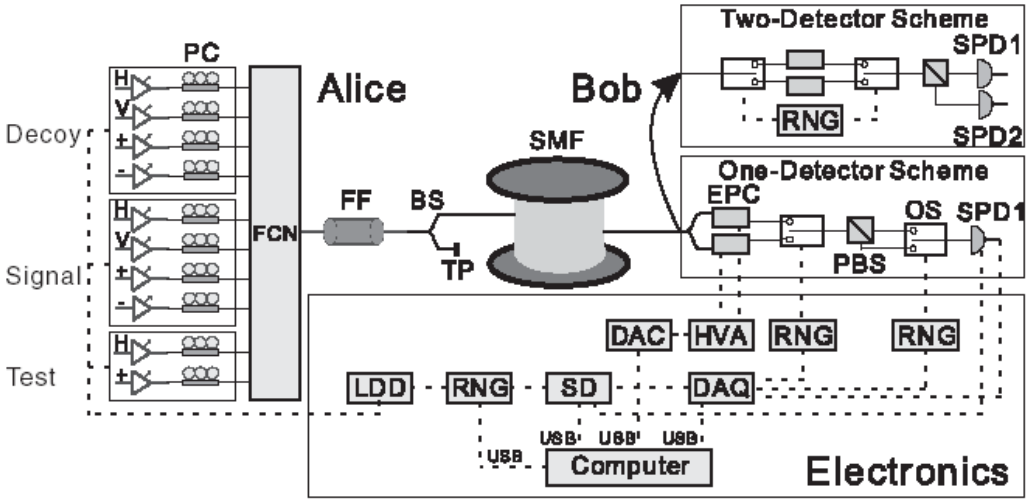


FIG. 1. Schematic diagram of the experimental setup. Solid lines and dashed lines represent the optical fiber and electric cable, respectively. See the text for the abbreviations.

基于诱骗态量子通信的实验

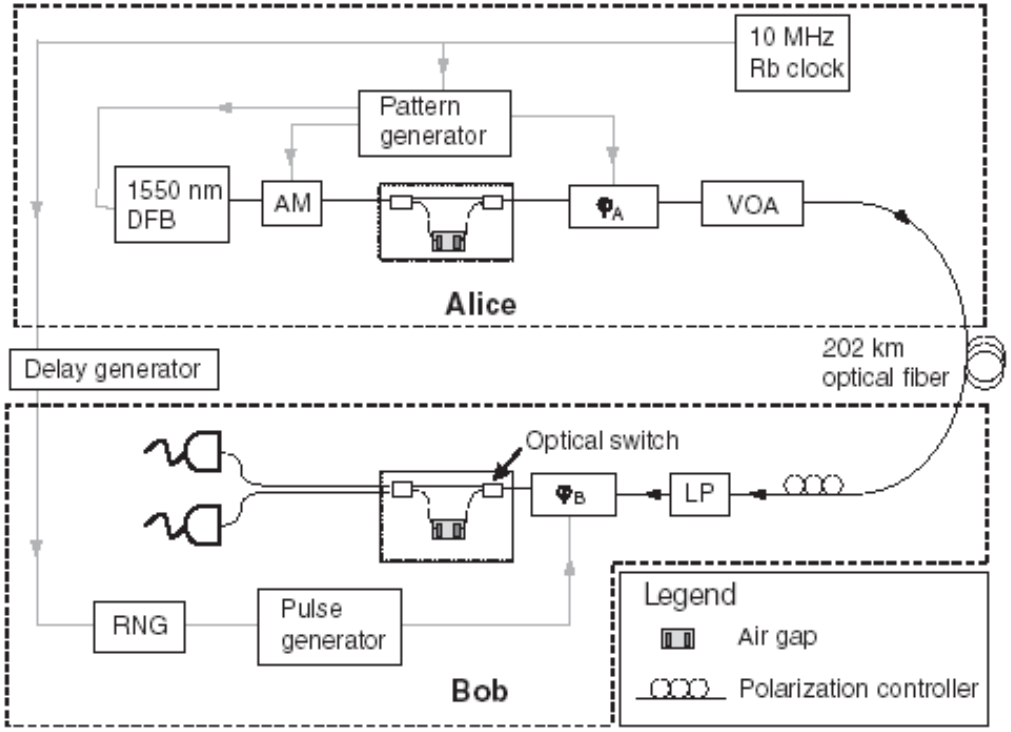


FIG. 1. QKD system used in this work. DFB, distributed feedback laser; VOA, variable optical attenuator; AM, amplitude modulator; LP, linear polarizer; RNG, random number generator.

欧洲联合实验组：**H. Weinfurter & A. Zeilinger (144km)**

T. Schmitt-Manderbach et al., *Phys.Rev.Lett.* 98,010504(2007)

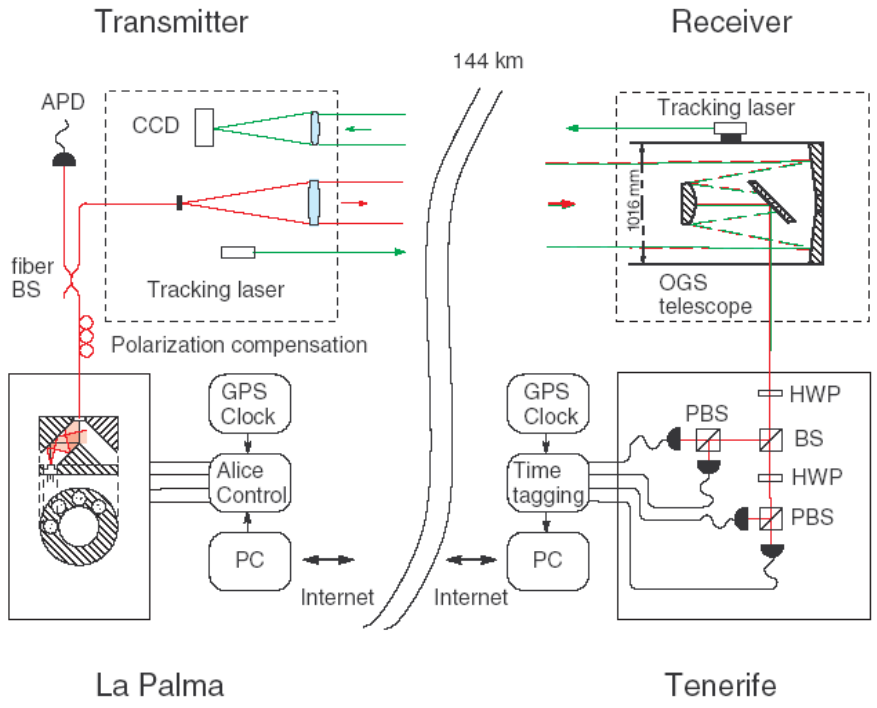


FIG. 2 (color online). Schematics of the experimental setup on the two canary islands. BS, beam splitter; PBS, polarizing beam splitter; HWP, half-wave plate; APD, avalanche photo diode.

美国**Los Alamos**国家实验室和**NIST**：

R. Hughes (107km)

D. Rosenberg et al., *Phys.Rev.Lett.* 98,010503(2007)

基于诱骗态
量子通信的实验

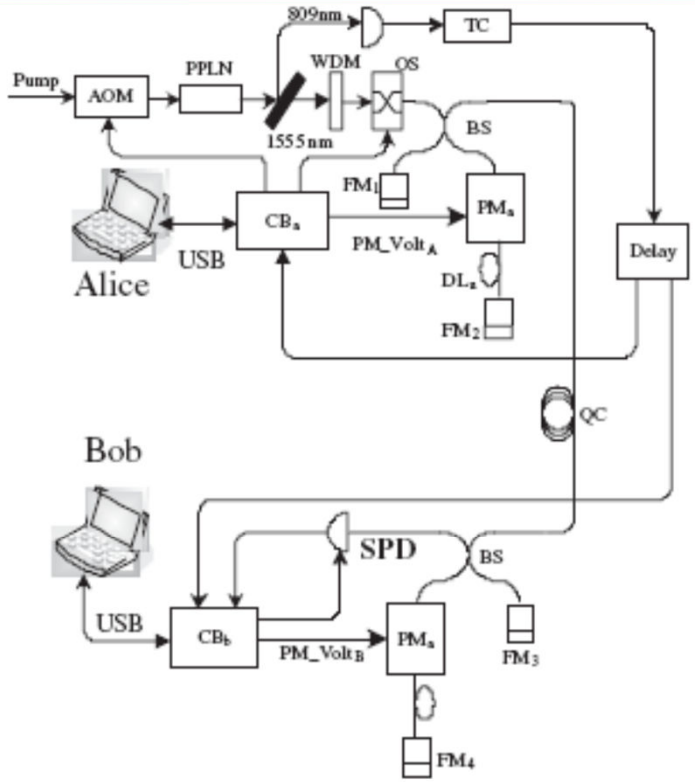


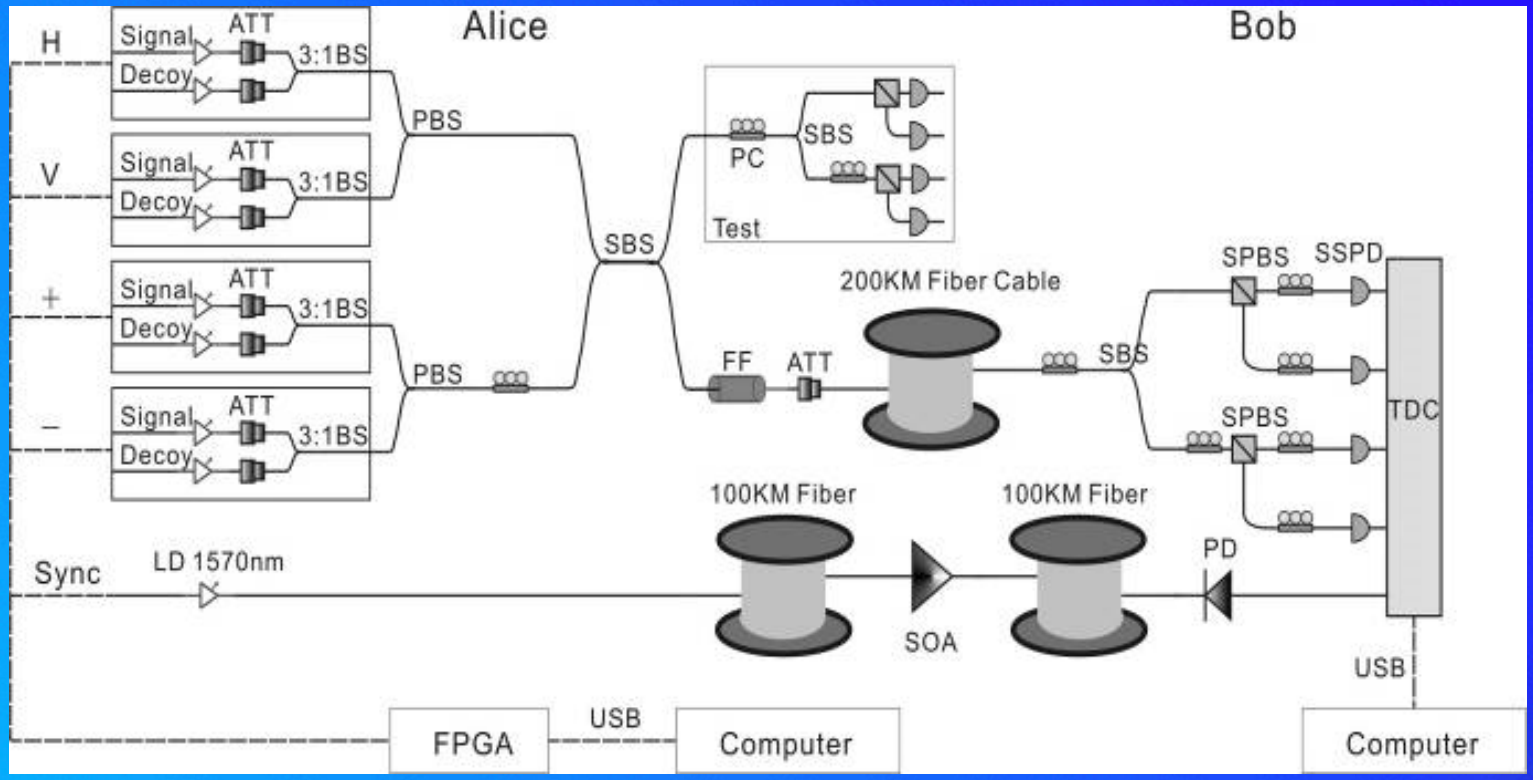
FIG. 2. The experimental setup of our quantum key transmission system. PPLN: periodically-poled $LiNbO_3$, AOM: acousto-optical-modulator, WDM: wavelength-division multiplexing, OS: optical switch, TC: time chopper, BS: beam-splitter, FM: Faraday Mirror, PM: phase modulator, DL: delay line, QC: quantum channel, SPD: single-photon detector, CB: control board.

郭光灿教授研究组：**(25km)**

Q. Wang et al., *Phys.Rev.Lett.* 100, 090501(2008)

使用通过参量下转换过程
的条件单光子源

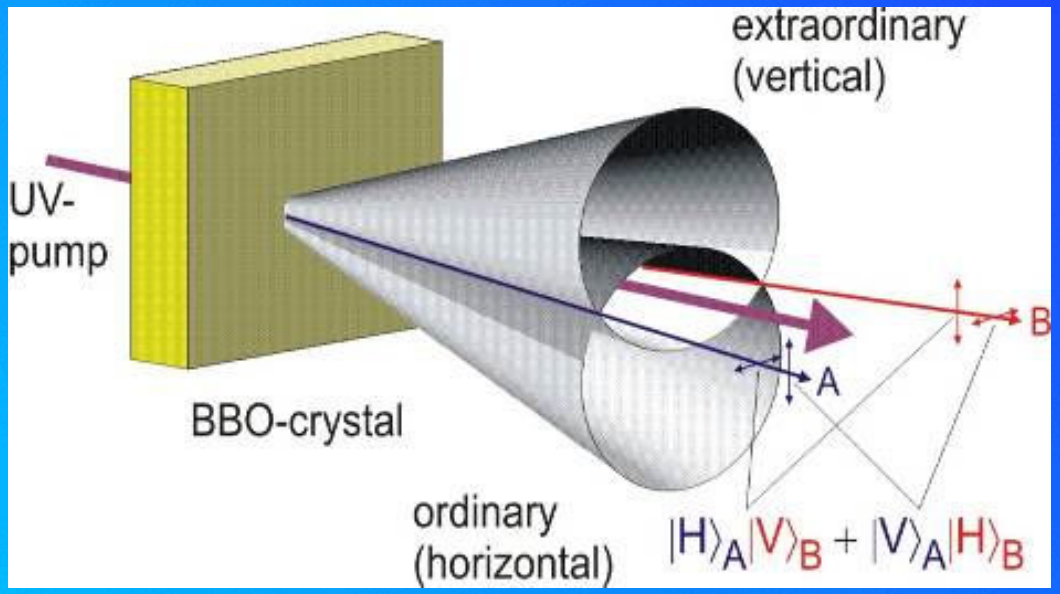
基于诱骗态的200km光纤量子通信

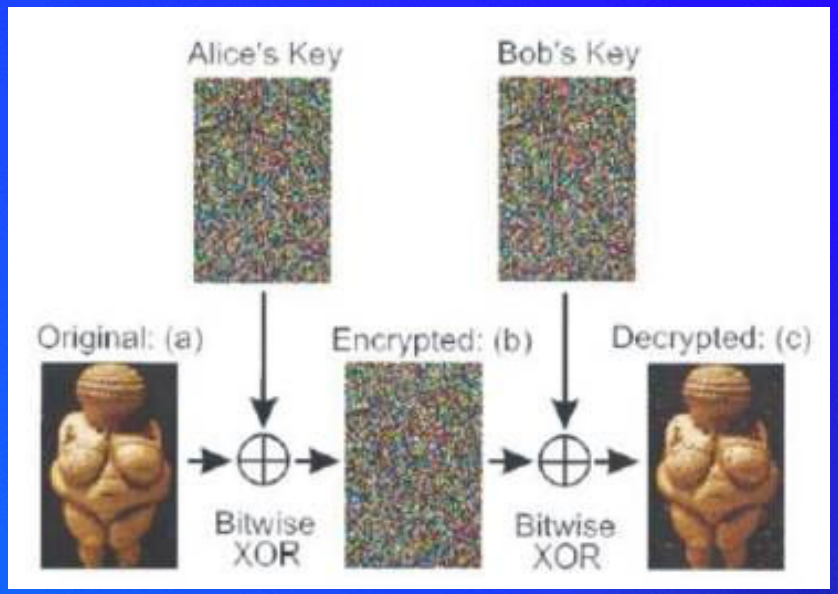


- 极化编码，**BB84**协议
- 量子信道**: 320MHz, 1550 nm**
- 使用双光纤, 信号和诱骗态脉冲**: 1550nm; 40kHz** 同步脉冲**:1550nm**
- 信号态平均光子数**μ=0.6,** 诱骗态平均光子数**v=0.2**
- 最终成码率 **~10bits/s**

Y. Liu *et al.*, *Optics Express* Vol. 18, Iss. 8, pp.8587-8594(2010).

早期纠缠光子量子密钥分发研究



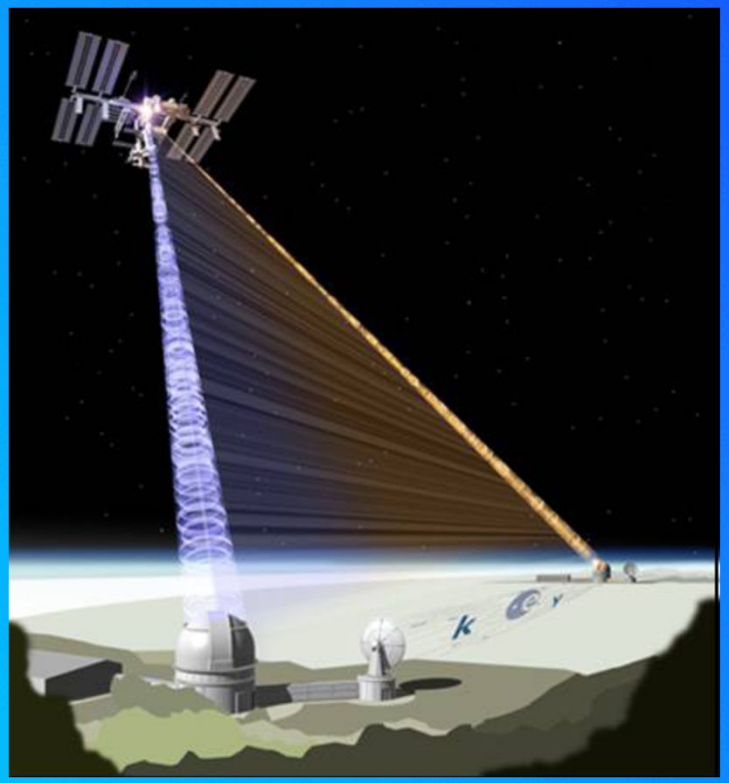


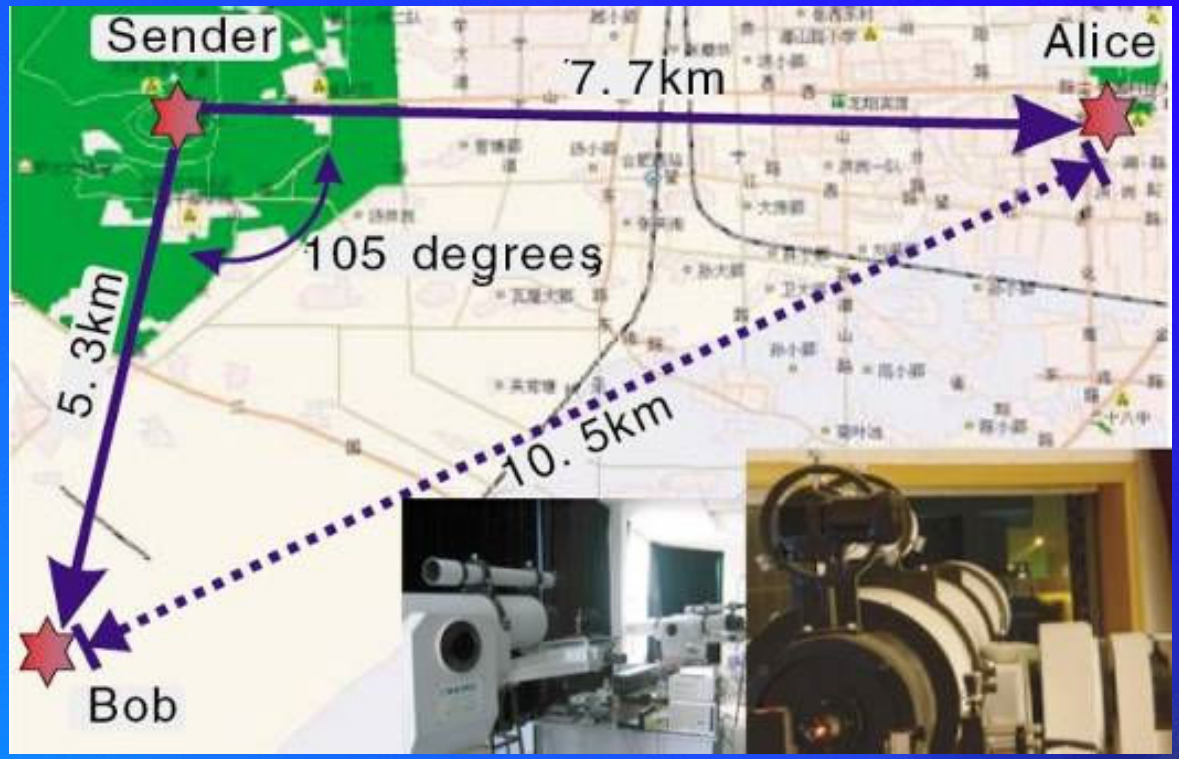
光纤: [T. Jennewein et al., PRL 84, 4729 (2000).]

[D. S. Naik, et al., PRL 84, 4733 (2000).] 1公里左右

[W. Tittel et al., PRL 84, 4737 (2000).]

远程量子通信：自由空间纠缠光子分发





- 1km　M. Aspelmeyer et al., Science 301, 621 (2003)
- 13km C.-Z. Peng et al., PRL 94, 150501 (2005)


QUANTEN
TELEP ATION


Teleport Exit
< Baggage
< Hover Cabs
< Skyway
< Rentals


fiz.iks

中国科学技术大学 陈凯

对现实量子通信的攻击

量子通信原理上具有无条件安全性。
但在现实条件下，由于设备的性能缺陷和非完美的物理实现，量子通信系统有可能遭到攻击。

- 相位重映射攻击
- 时间错位旁路攻击
- 高能破坏攻击
- ……

这些攻击方式都可以有相应的防范措施 ☺

可能的未知安全威胁

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

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.

致盲单光子探测器攻击

此攻击可以通过监测系统工作状态而防范

Measurement Device Independent (MDI)-QKD

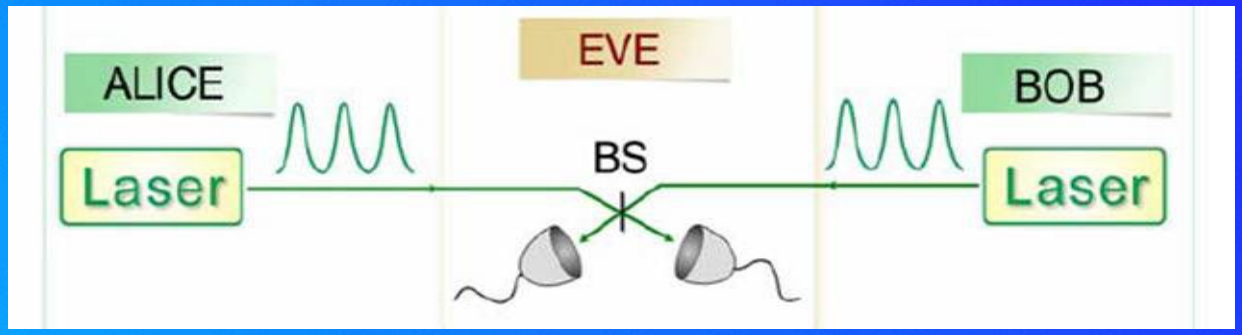
Immune to any attacks on detector

Scheme:

Lo *et al*., PRL 108, 130503 (2012)

Experiment:

Liu *et al*., PRL 111, 130502 (2013)

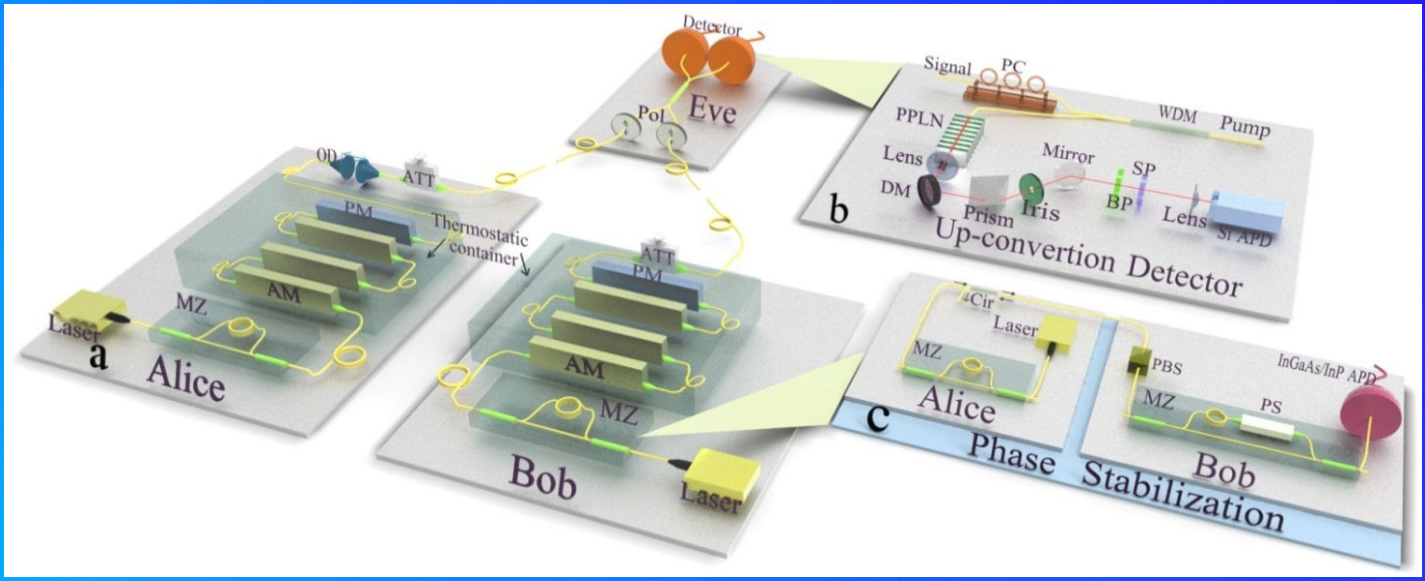


Bell-state measurement (BSM)

- ☑ Creating raw key: If Alice and Bob's polarization choice are same, there would not be coincidence event
- ☑ Even measurement station is fully controlled by Eve, she can only implement BSM to avoid be revealed, but she can not gain any information of key

Measurement Device Independent (MDI)-QKD

Since coincidence detection is needed, the detection efficiency is very important



- Typical efficiency of single-photon InGaAs/InP APD at communication wavelength (1550nm): 10%
- Low noise up-conversion detector: 34%

→ increase coincidence probability for ~11 times

☑ MDI-QKD in 50km fiber

☑ Can achieve a transmission of more than 400km currently

第四章 量子通信

1. 保密通信
2. QKD基本原理
3. BB84协议过程
4. QKD安全性
5. 诱骗态(Decoy-state QKD)
   - ① Decoy QKD原理
   - ② 实用Decoy QKD
   - ③ Decoy QKD实验
6. QKD的现实安全性
   - ① 探测端的安全性→MDI-QKD
   - ② 设备无关的→ DI-QKD
7. **量子隐形传态(Quantum Teleportation) [原理、实验]**
8. 量子纠缠交换(Entanglement Swapping)
9. 量子通信网络
10. 量子通信商用公司
11. 量子通信发展与实用化QKD之路

QUANTUM TELEPORTATION

Teleportation of unknown quantum state encompasses the complete transfer of information from one particle to another

Unknown quantum state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

EPR source

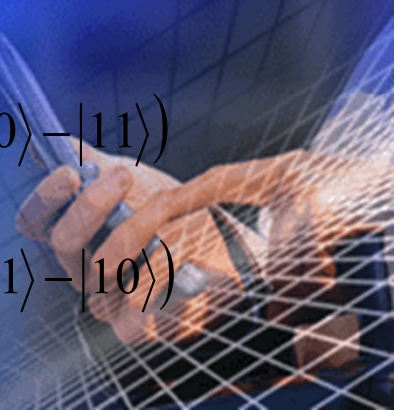
$$|EPR-pair\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Total state

$$|\psi\rangle|EPR-pair\rangle = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right)$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$



QUANTUM TELEPORTATION

The joint state of three particles

$$|\psi\rangle|EPR-pair\rangle=\frac{1}{\sqrt{2}}\left(\alpha|000\rangle+\alpha|011\rangle+\beta|100\rangle+\beta|111\rangle\right)$$

can be rephrased as follows:

$$|\psi\rangle|EPR-pair\rangle=|\Phi^{+}\rangle\frac{1}{2}\left(\alpha|0\rangle+\beta|1\rangle\right)+|\Psi^{+}\rangle\frac{1}{2}\left(\beta|0\rangle+\alpha|1\rangle\right)$$

$$+|\Phi^{-}\rangle\frac{1}{2}\left(\alpha|0\rangle-\beta|1\rangle\right)+|\Psi^{-}\rangle\frac{1}{2}\left(-\beta|0\rangle+\alpha|1\rangle\right)$$

Therefore Bell measurements on the first two particles would project the state of Bob's particle into a variant of $|\psi_1\rangle$ of the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where

$|\psi_1\rangle$ = either $|\psi\rangle$ or $\sigma_x|\psi\rangle$ or $\sigma_z|\psi\rangle$ or $\sigma_x\sigma_z|\psi\rangle$

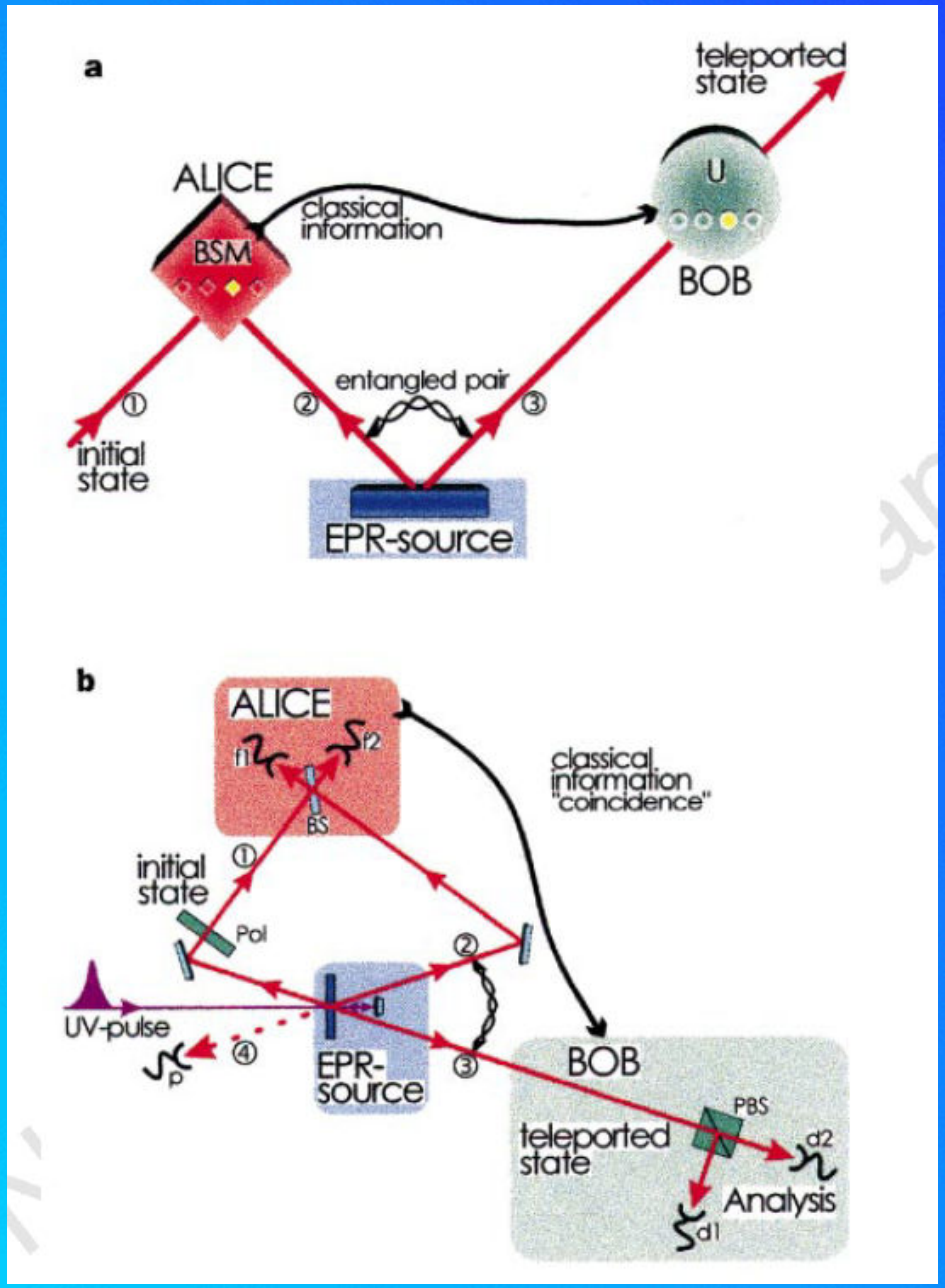
The unknown state $|\psi\rangle$ can therefore be obtained from $|\psi_1\rangle$ by applying one of the four operations

$$I, \sigma_x, \sigma_y, \sigma_z,$$

and the result of the Bell measurement provides two bits specifying which of the above four operations should be applied.

Alice can send to Bob these two bits of classical information using a classical channel (by phone, email for example).

Quantum Teleportation

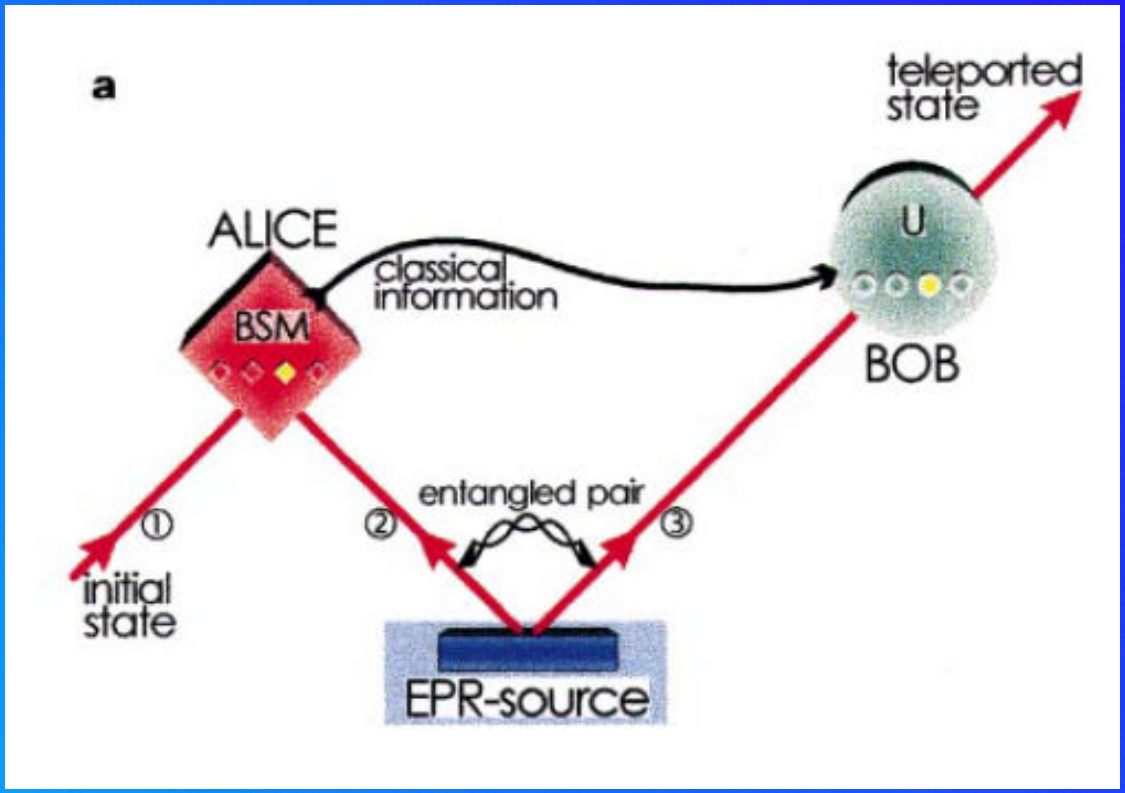


Scheme showing principles involved in quantum teleportation (a) and the experimental set-up (b).

- EPR correlations used as a source
- Teleporting an unknown quantum state not the particle
- Entanglement between photon 2 and 3
- Bell-state measurement plus classical communication and recovery operation lead to successful teleportation

D. Bouwmeester *et al.*, Experimental quantum teleportation, *Nature 390*, 575-579 (1997);
M. Zukowski, A. Zeilinger, & H. Weinfurter, Entangling photons radiated by independent pulsed sources. Ann. NY Acad. Sci. 755, 91–102 (1995).

Quantum Teleportation

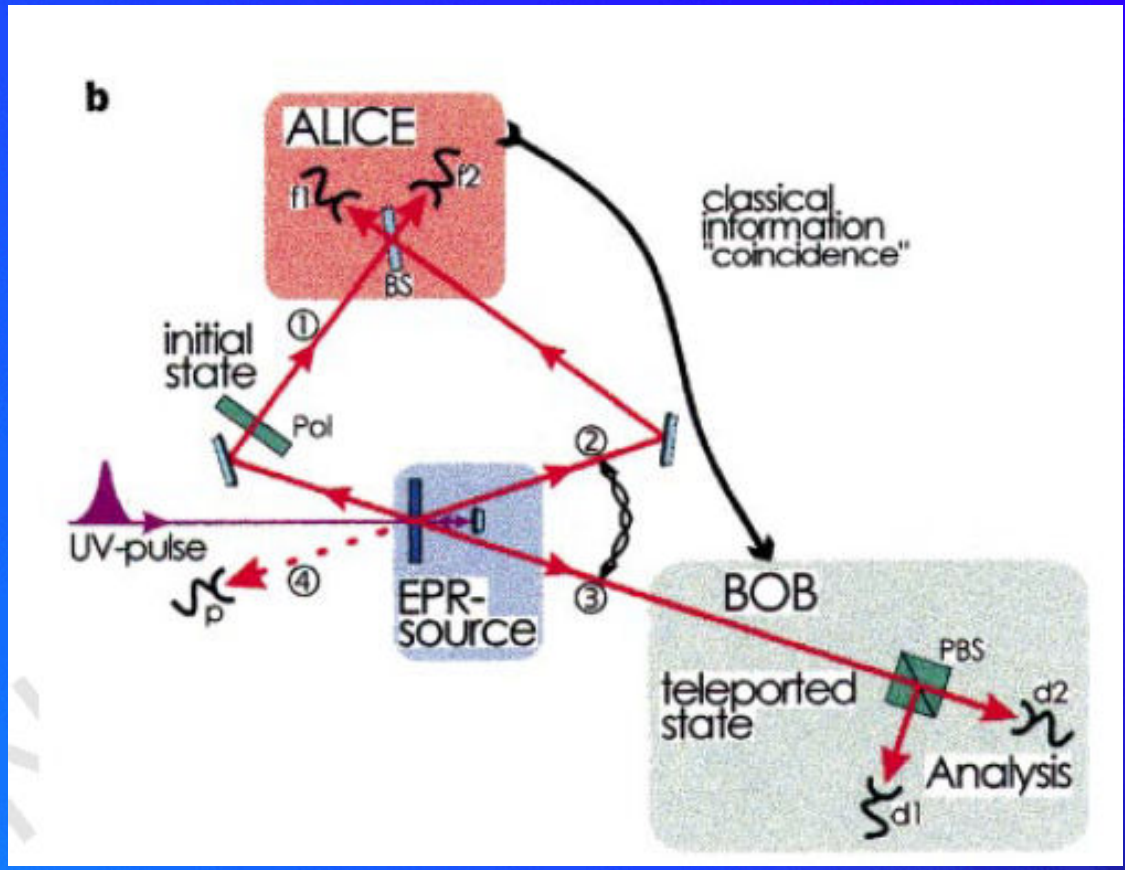


Alice has a quantum system, particle 1, in an initial state which she wants to teleport to Bob. Alice and Bob also share an ancillary entangled pair of particles 2 and 3 emitted by an Einstein–Podolsky–Rosen (EPR) source. Alice then performs a joint Bell-state measurement (BSM) on the initial particle and one of the ancillaries, projecting them also onto an entangled state. After she has sent the result of her measurement as classical information to Bob, he can perform a unitary transformation (U) on the other ancillary particle resulting in it being in the state of the original particle.

D. Bouwmeester *et al., Nature 390*, 575-579 (1997)

Quantum Teleportation

A pulse of ultraviolet radiation passing through a nonlinear crystal creates the ancillary pair of photons 2 and 3. After retroflection during its second passage through the crystal the ultraviolet pulse creates another pair of photons, one of which will be prepared in the initial state of photon 1 to be teleported, the other one serving as a trigger indicating that a photon to be teleported is under way.



Alice then looks for coincidences after a beam splitter BS where the initial photon and one of the ancillaries are superposed. Bob, after receiving the classical information that Alice obtained a coincidence count in detectors f1 and f2 identifying the $|\psi^-\rangle_{12}$ Bell state, knows that his photon 3 is in the initial state of photon 1 which he then can check using polarization analysis with the polarizing beam splitter PBS and the detectors d1 and d2. The detector p provides the information that photon 1 is under way.

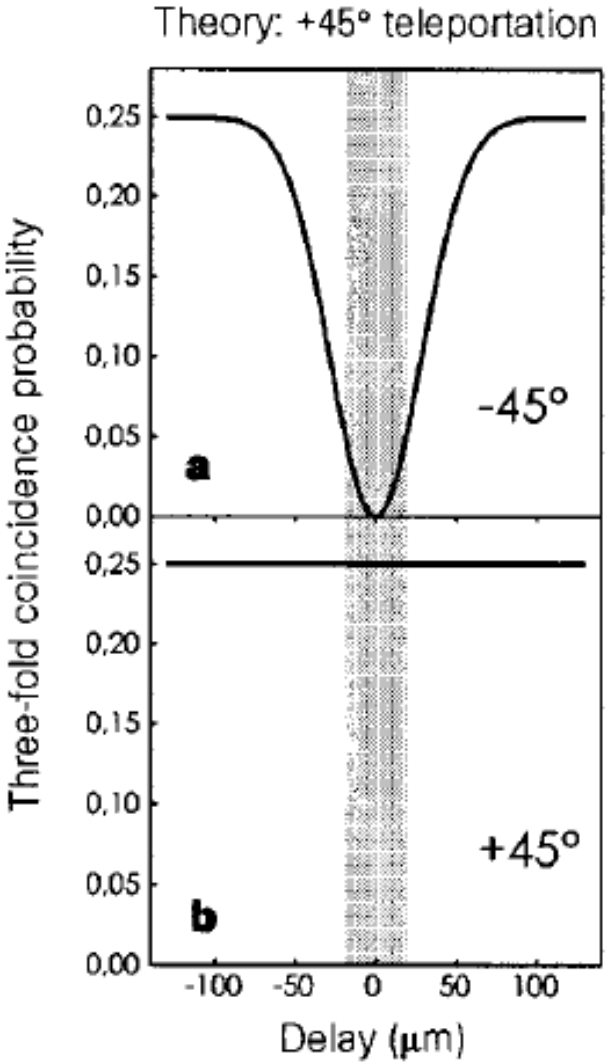
D. Bouwmeester *et al.*, *Nature 390*, 575-579 (1997)

Quantum Teleportation

Results

In the first experiment photon 1 is polarized at 45°. Teleportation should work as soon as photon 1 and 2 are detected in the $|\psi^-\rangle_{12}$ state, which occurs in 25% of all possible cases. The $|\psi^-\rangle_{12}$ state is identified by recording a coincidence between two detectors, f1 and f2, placed behind the beam splitter (Fig. 1b).

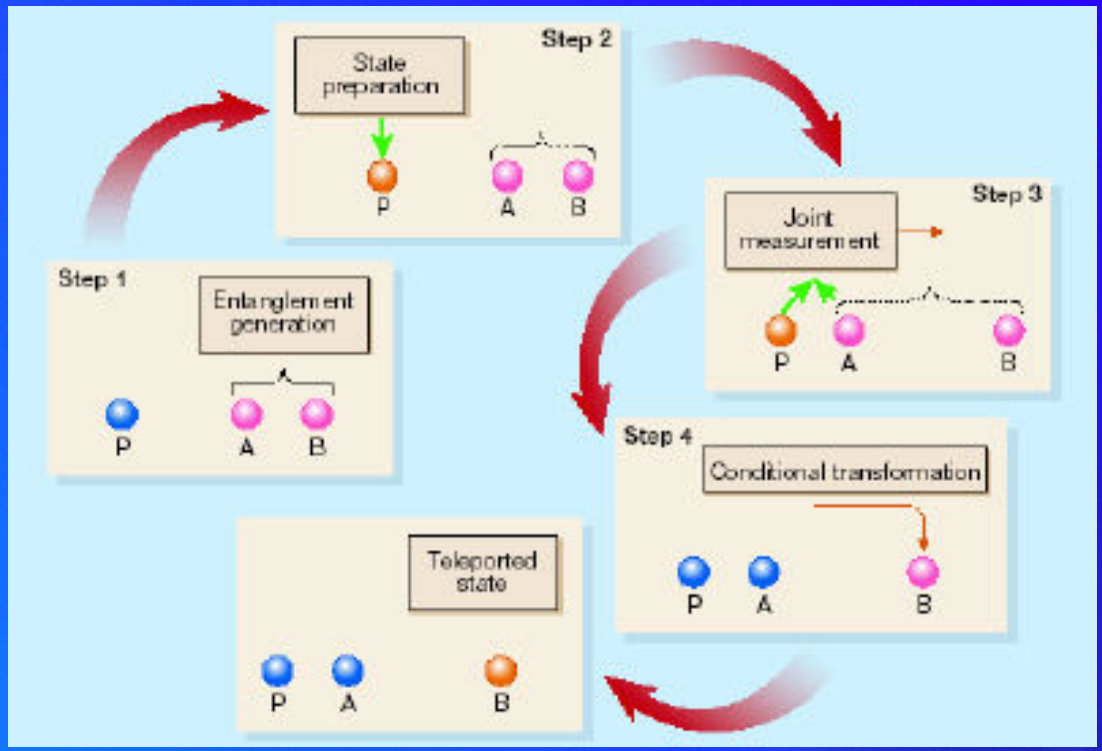
If we detect a f1f2 coincidence (between detectors f1 and f2), then photon 3 should also be polarized at 45°. The polarization of photon 3 is analysed by passing it through a polarizing beam splitter selecting +45° and –45° polarization. To demonstrate teleportation, only detector d2 at the +45° output of the polarizing beam splitter should click (that is, register a detection) once detectors f1 and f2 click. Detector d1 at the –45° output of the polarizing beam splitter should not detect a photon. Therefore, recording a three-fold coincidence d2f1f2 (+45° analysis) together with the absence of a three-fold coincidence d1f1f2 (–45° analysis) is a proof that the polarization of photon 1 has been teleported to photon 3.



D. Bouwmeester *et al., Nature 390*, 575-579 (1997)

Teleportation of Massive Particles

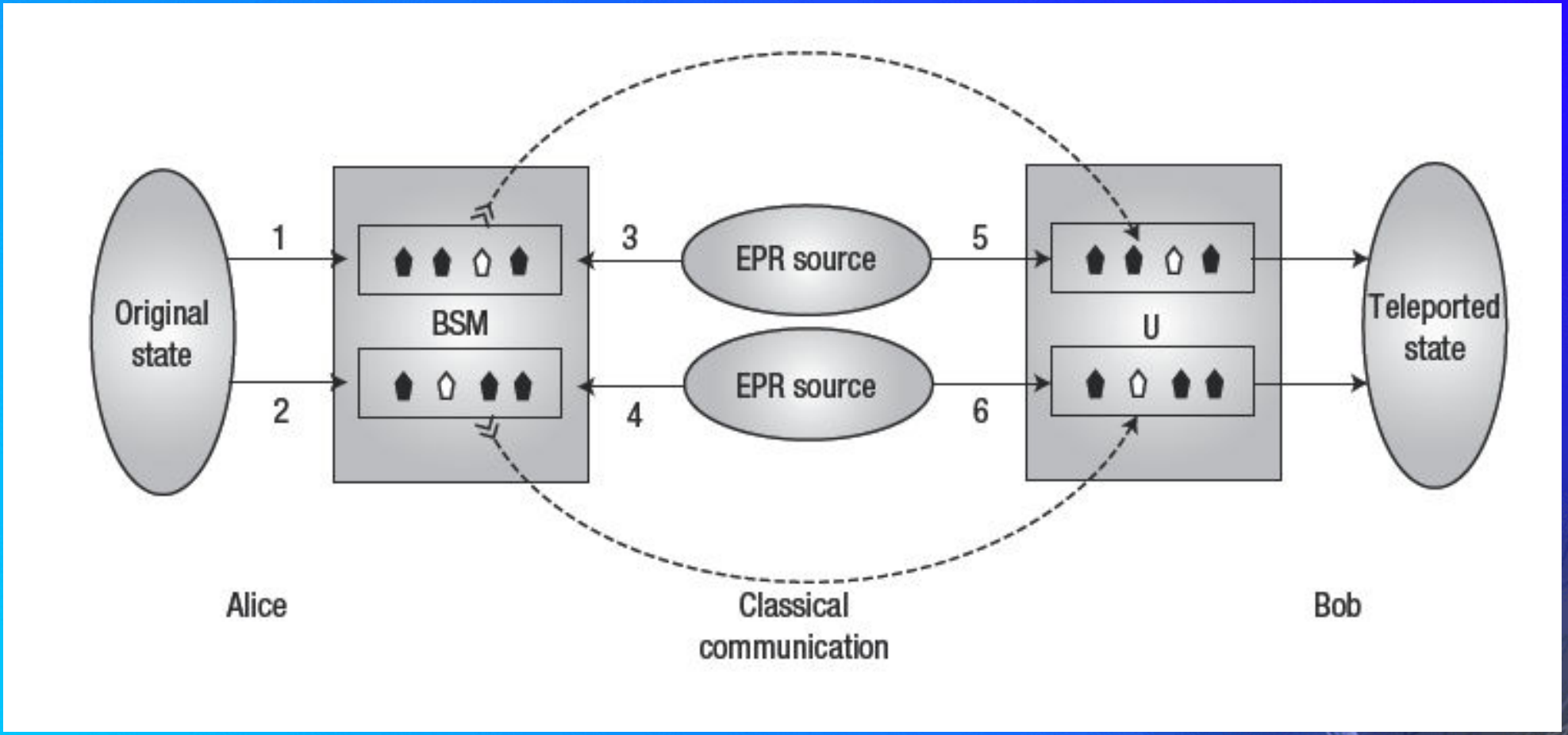
David Wineland and colleagues from the National Institute of Standards and Technology (NIST) in Colorado began by creating a superposition of spin up and spin down states in a single trapped beryllium ion (*Nature* **429** 737 [2004]). Using laser beams, they teleported these quantum states to a second ion with the help of a third, auxiliary ion (see figure). The NIST technique relied on being able to move the ions within the trap.



Meanwhile, Rainer Blatt and co-workers at the University of Innsbruck performed a similar experiment using trapped calcium ions (*Nature* **429** 734 [2004]). However, rather than moving the ions, they "hide" them in a different internal state.

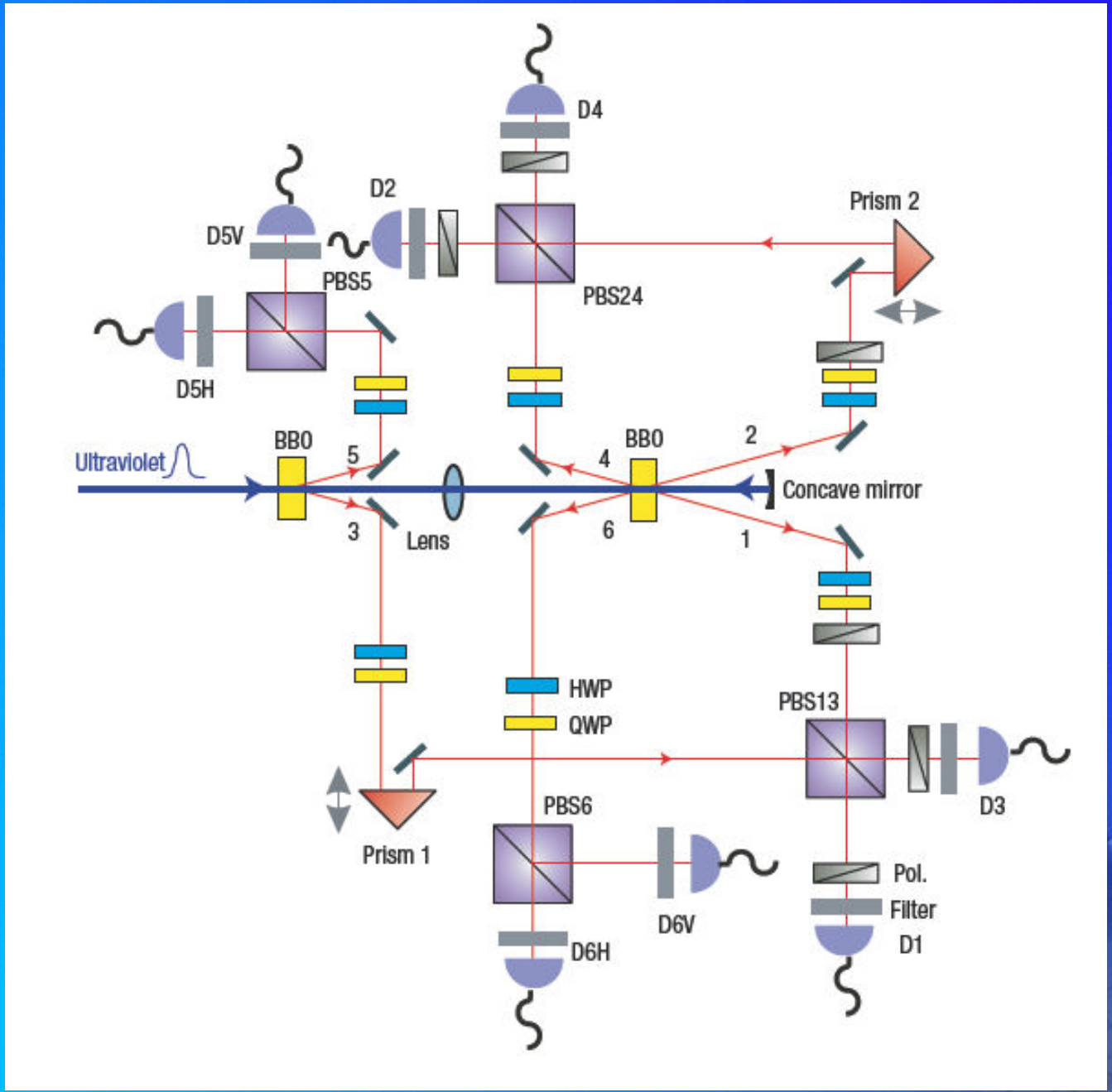
http://physicsworld.com/cws/article/news/19690

Experimental quantum teleportation of a two-qubit composite system



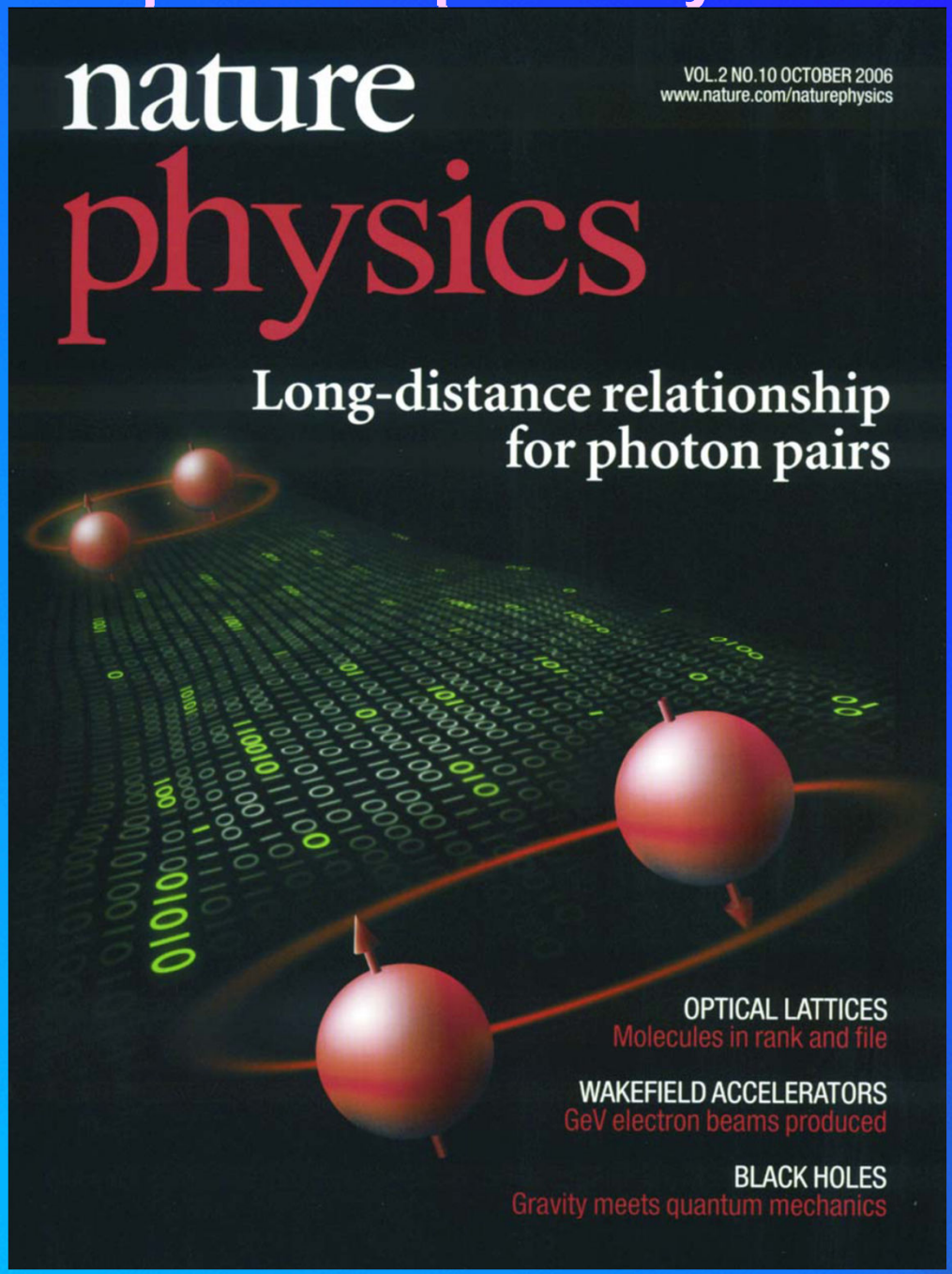
Qiang Zhang *et al., Nature Physics* 2, 678-682 (2006)

Experimental quantum teleportation of a two-qubit composite system



Qiang Zhang *et al., Nature Physics* 2, 678-682 (2006)

Experimental quantum teleportation of a two-qubit composite system



中国科学技术大学 陈凯

Qiang Zhang *et al., Nature Physics* 2, 678-682 (2006)

Memory-built-in quantum teleportation with photonic and atomic qubits

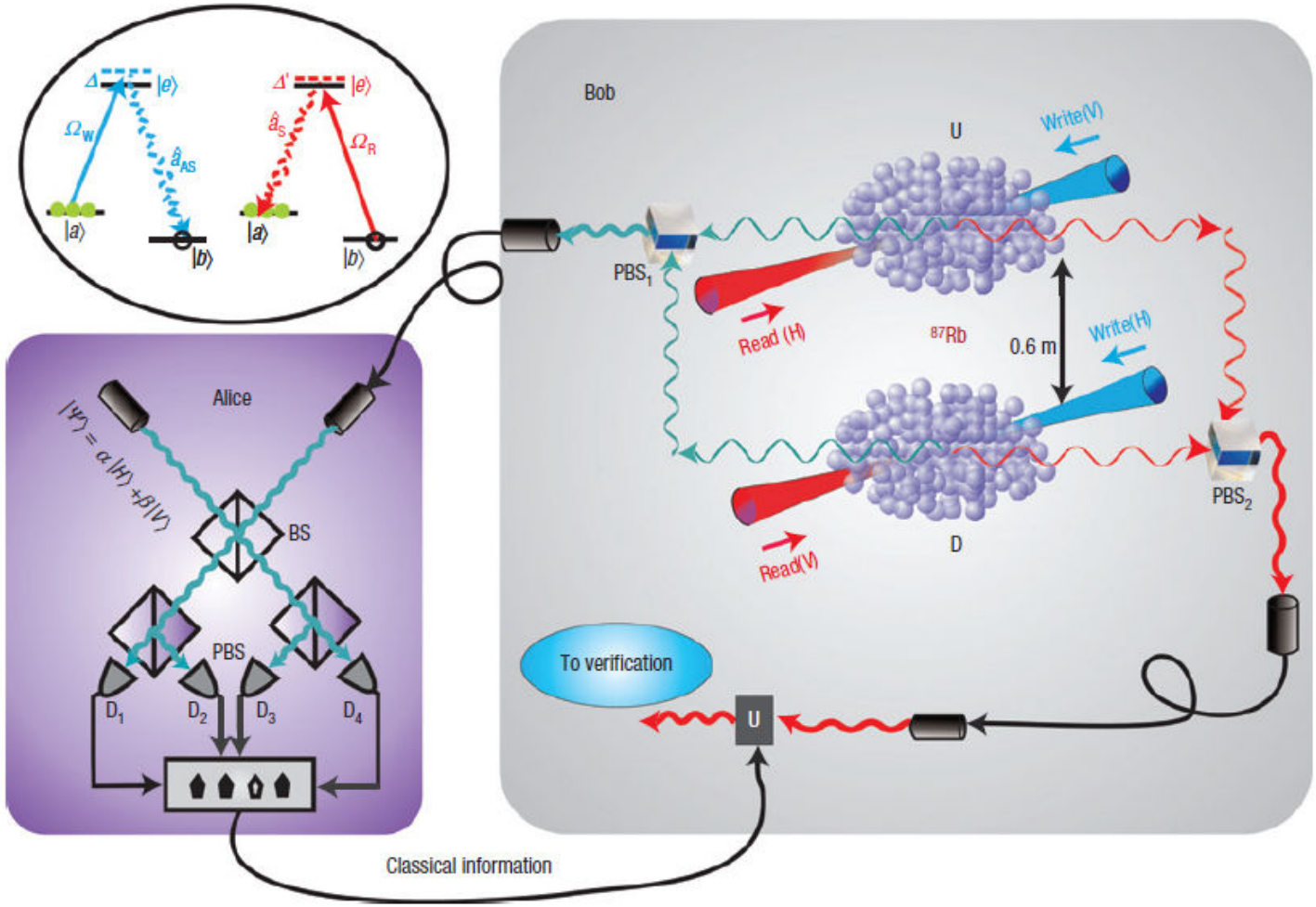


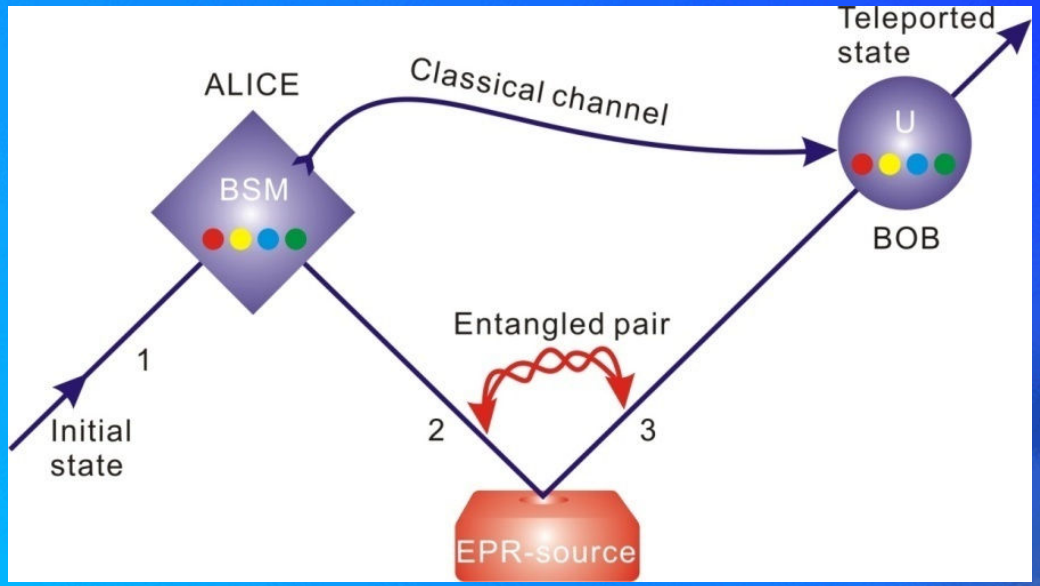
Figure 1 Experimental set-up for teleportation between photonic and atomic qubits. The top-left diagram shows the structure and the initial populations of atomic levels for the two ensembles. At Bob's site, the anti-Stokes fields emitted from U and D are collected and combined at PBS_1, selecting perpendicular polarizations. Then the photon travels 7 m through the fibres to Alice's site to overlap with the initial unknown photon on a beam splitter (BS) to carry out the BSM. The results of the BSM are sent to Bob through a classical channel. Bob then carries out the verification of the teleported state in the U and D ensembles by converting the atomic excitation to a photonic state. If the state $|\Psi^+\rangle$ is registered, Bob directly carries out a polarization analysis on the converted photon to measure the teleportation fidelity. On the other hand, if the state $|\Psi^-\rangle$ is detected, the converted photon is sent through a half-wave plate via the first-order diffraction of an AOM (not shown). The half-wave plate is set at 0° serving as the unitary transformation of $\hat{\sigma}_z$. Then the photon is sent through the polarization analyser to obtain the teleportation fidelity.

Yu-Ao Chen *et al., Nature Physics* **4**, 103-107 (2008)

Motivation: longer and not only longer

- Fundamental interest: faithfully transfer of quantum state between two distant locations without physically transmitting carrier itself:

- Long-distance quantum communication network: quantum relay, quantum repeater.



Quantum Teleportation Progress

- First proof-of-principle verification

Bouwmeester, D. et al. Nature, 390, 575(1997).

Boschi, D. et al. Phys. Rev. Lett., 80,1121(1998).

Furusawa, A. et al. Science 282, 706–709 (1998).

Sherson, J. F. et al. Nature 443, 557–560 (2006).

- Fiber-based long-distance teleportation :

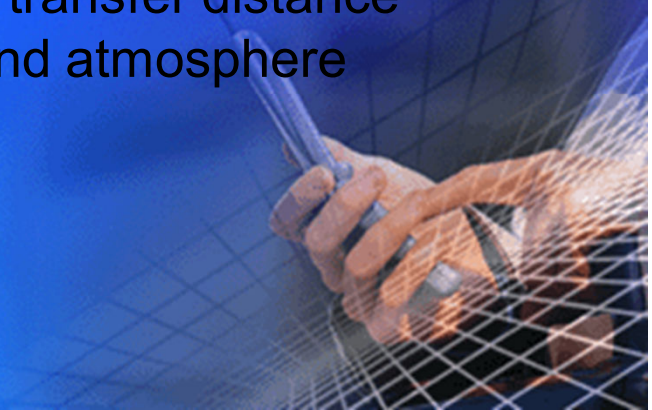
55m： Marcikic, I. et al. Nature 421, 509-513 (2003)

600m： Ursin, R. et al. Nature 430, 849 (2004)

- Optical free-space link is highly desirable for extending the transfer distance

Effective aerosphere thickness: ~equivalent to 5-10 km ground atmosphere

How to **exceed this?**



Polarization Entanglement Source

Bell states – maximally entangled states:

$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 \pm |V\rangle_1|V\rangle_2\right)$$

$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2\right)$$

Singlet:

$$|\Psi^{-}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2)$$

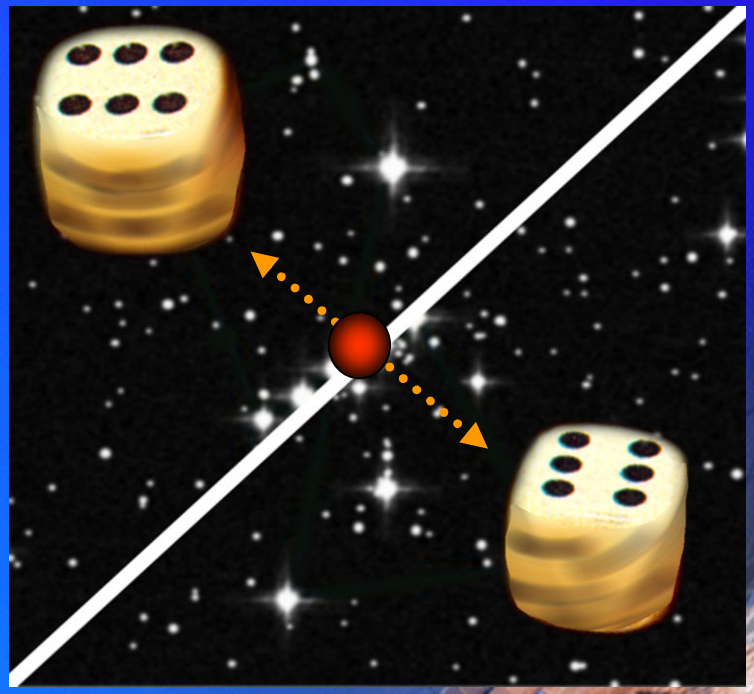
$$= \frac{1}{\sqrt{2}}(|H'\rangle_1|V'\rangle_2 - |V'\rangle_1|H'\rangle_2)$$

where

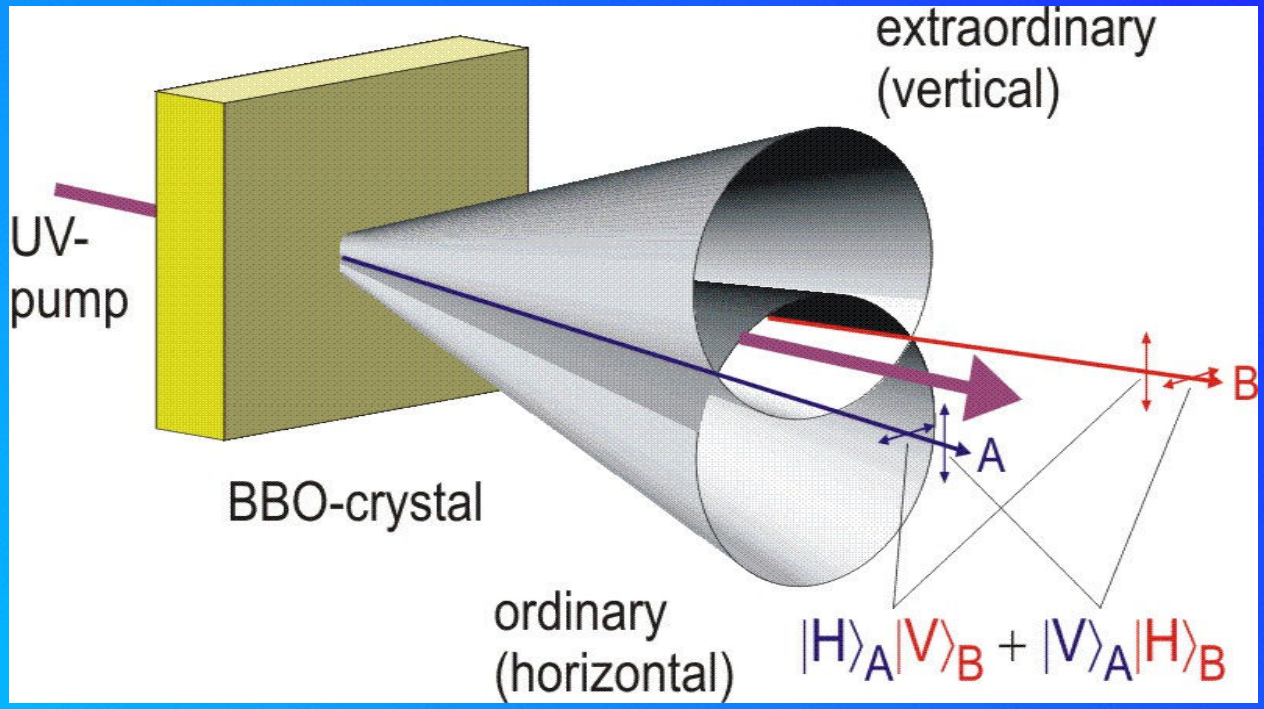
$$|H'\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

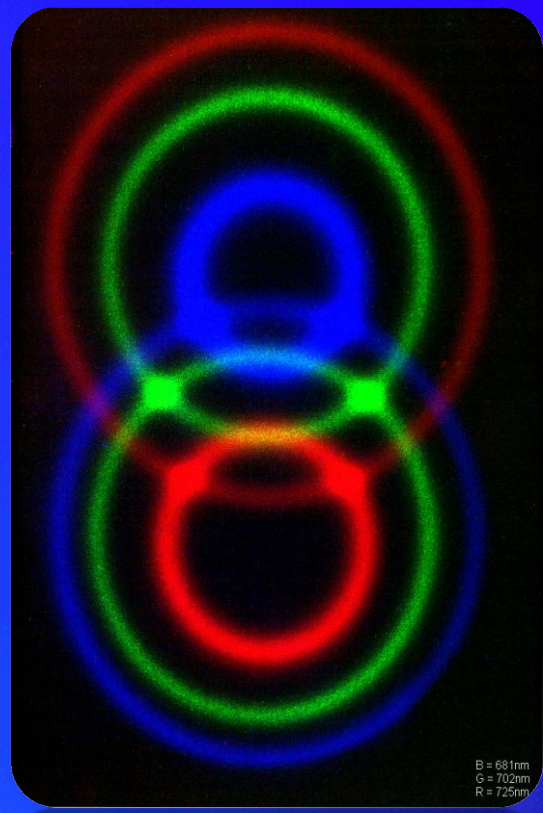
$$|V'\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$

45-degree polarization



Polarization Entanglement Source





PDC

$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 \pm |V\rangle_1|V\rangle_2\right)$$

$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2\right)$$

- P. G. Kwiat et al., Phys. Rev. Lett. 75, 4337 (1995)

Modified Rome quantum teleportation scheme

$$\left|\Psi^{-}\right\rangle_{1w2p}=\left|V\right\rangle_{1p}\otimes\frac{1}{\sqrt{2}}\left(\left|R\right\rangle_{1w}\left|V\right\rangle_{2p}-\left|L\right\rangle_{1w}\left|H\right\rangle_{2p}\right)$$

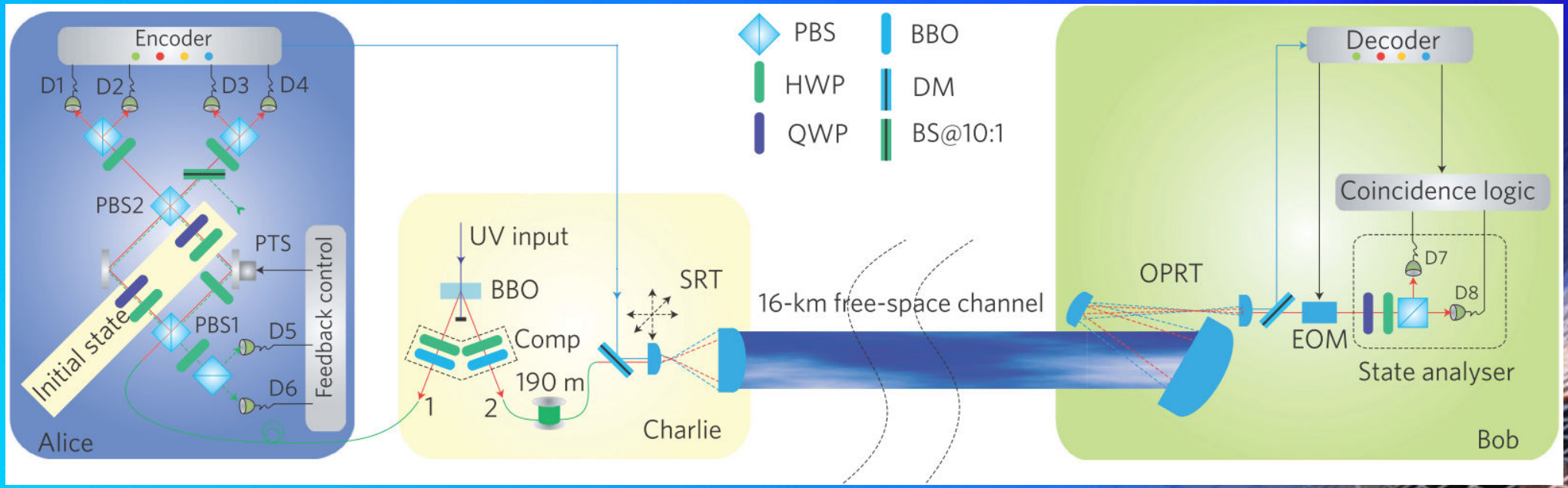
- Initial state: $\left|\Psi\right\rangle_{1p}=\alpha\left|H\right\rangle_{1p}+\beta\left|V\right\rangle_{1p}$
- Bell state:

$$\left|\Psi^{\pm}\right\rangle_{1w1p}=\left(\left|R\right\rangle_{1w}\left|V\right\rangle_{1p}\pm\left|L\right\rangle_{1w}\left|H\right\rangle_{1p}\right)\Big/\sqrt{2}$$

$$\left|\Phi^{\pm}\right\rangle_{1w1p}=\left(\left|R\right\rangle_{1w}\left|H\right\rangle_{1p}\pm\left|L\right\rangle_{1w}\left|V\right\rangle_{1p}\right)\Big/\sqrt{2}$$

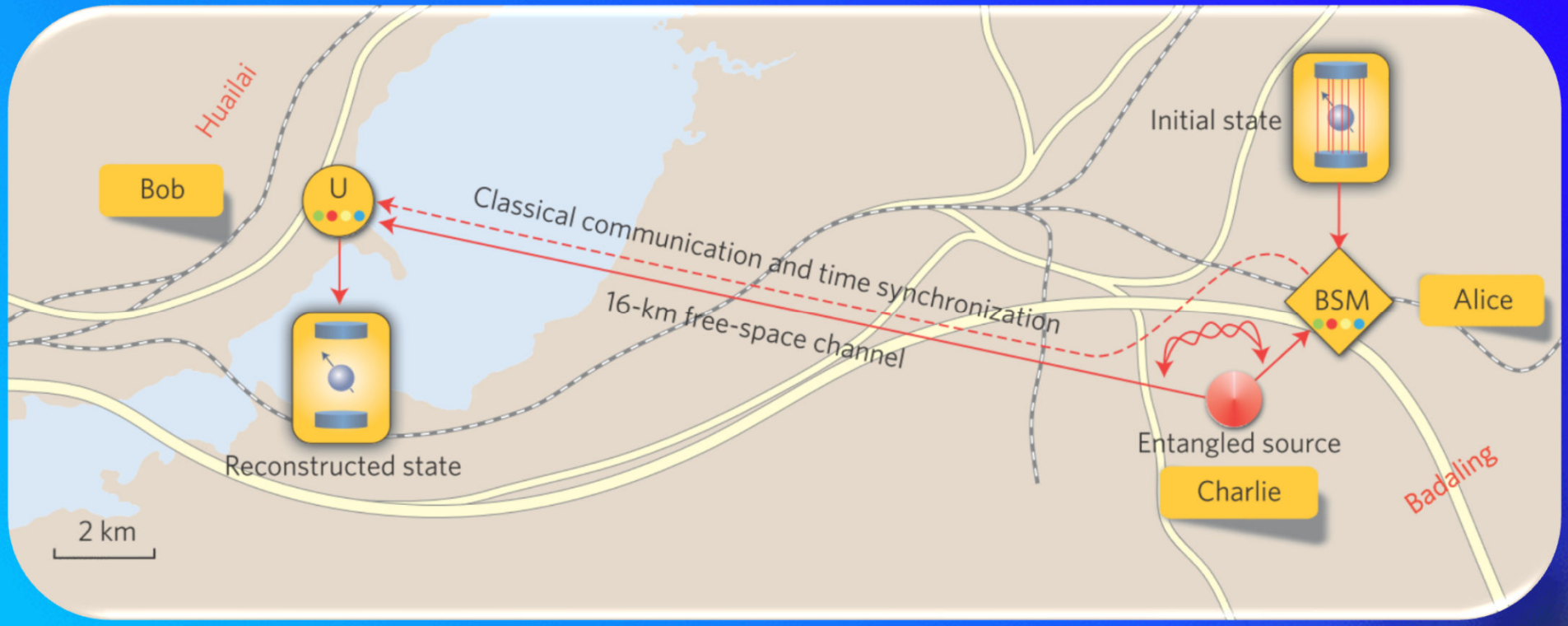
$$\left|\Psi\right\rangle_{1p1w2p}=\left|\Psi\right\rangle_{1p}\otimes\left|\Psi^{-}\right\rangle_{1w2p}$$

$$=\frac{1}{2}(\left|\Psi^{-}\right\rangle_{1p1w}+\left|\Phi^{-}\right\rangle_{1p1w}\hat{\sigma}_x-\left|\Phi^{+}\right\rangle_{1p1w}i\hat{\sigma}_y-\left|\Psi^{+}\right\rangle_{1p1w}\hat{\sigma}_z)\left|\Psi\right\rangle_{2p}$$

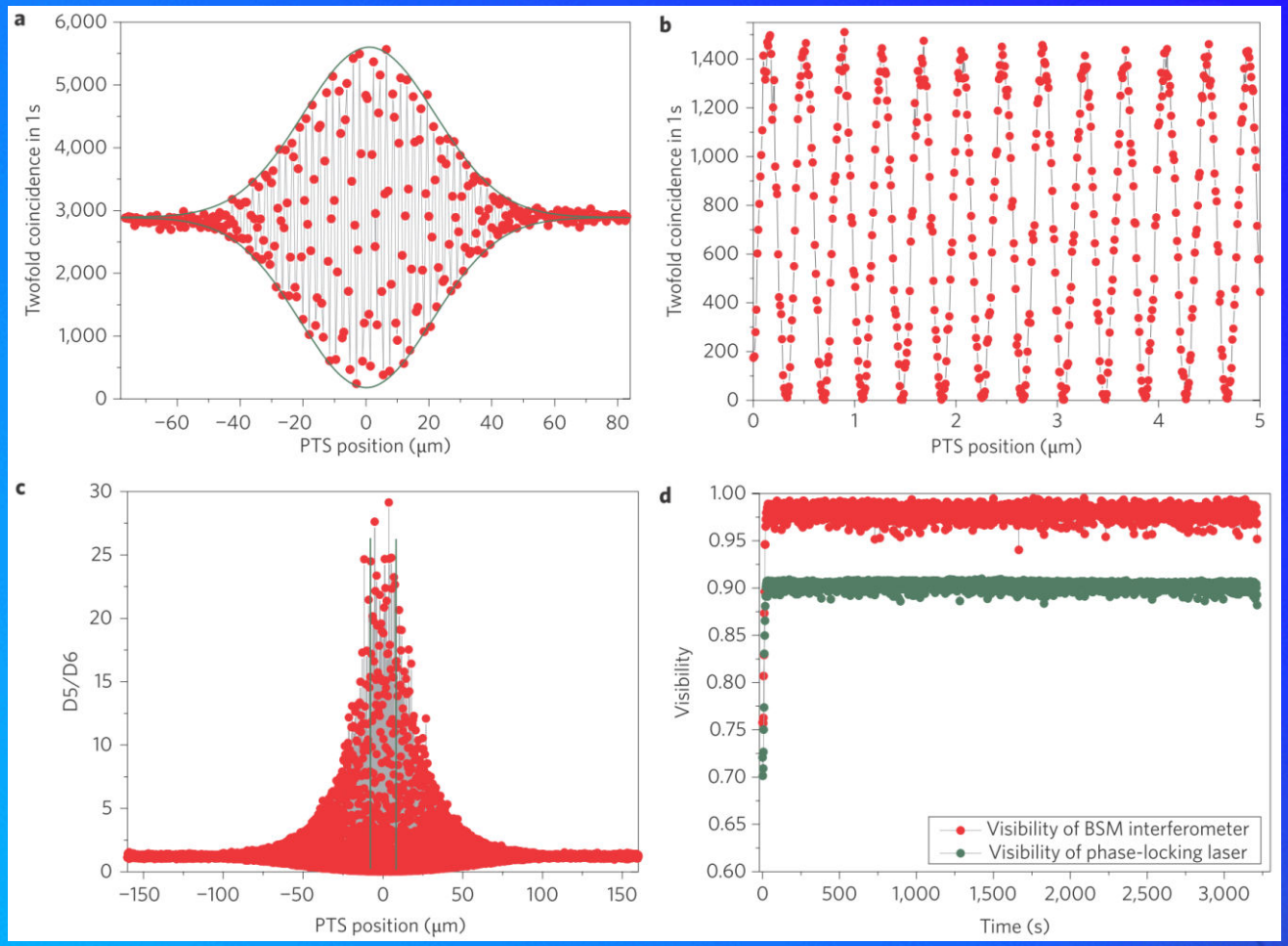


Free-space channel + Stable BSM + Active Feedforward

- Split-type refracting telescope(SRT): f=2.372, d=0.2m, 0.42μrad per step, 0.4~1m(point)
- Off-axis parabolic reflecting telescope (OPRT):d=0.4m, 1000kg, stability 0.3μrad/hour
- Optical link efficiency between SRT and OPRT:-14 dB ~ -31 dB.



Free-space channel + Stable BSM + Active Feedforward



- Perfect overlap :spatial, temporal, spectral.

Visibility of BSM:~99.2%

- Active lock BSM interferometer: reverse propagating direction, 633nm

The instability can be suppressed within λ/52

Teleportation Fidelities

$$F = Tr(\hat{\rho}|\Psi\rangle_{1p\ 1p}\langle\Psi|) = Tr(\hat{\rho}(|\alpha|^2(\hat{I}+\hat{\sigma}_z)+\alpha\beta^*(\hat{\sigma}_x+i\hat{\sigma}_y)+\beta\alpha^*(\hat{\sigma}_x-i\hat{\sigma}_y)+|\beta|^2(\hat{I}-\hat{\sigma}_z)))/2$$

$$F_{|H\rangle} = Tr(\hat{\rho}(\hat{I}+\hat{\sigma}_z))/2$$

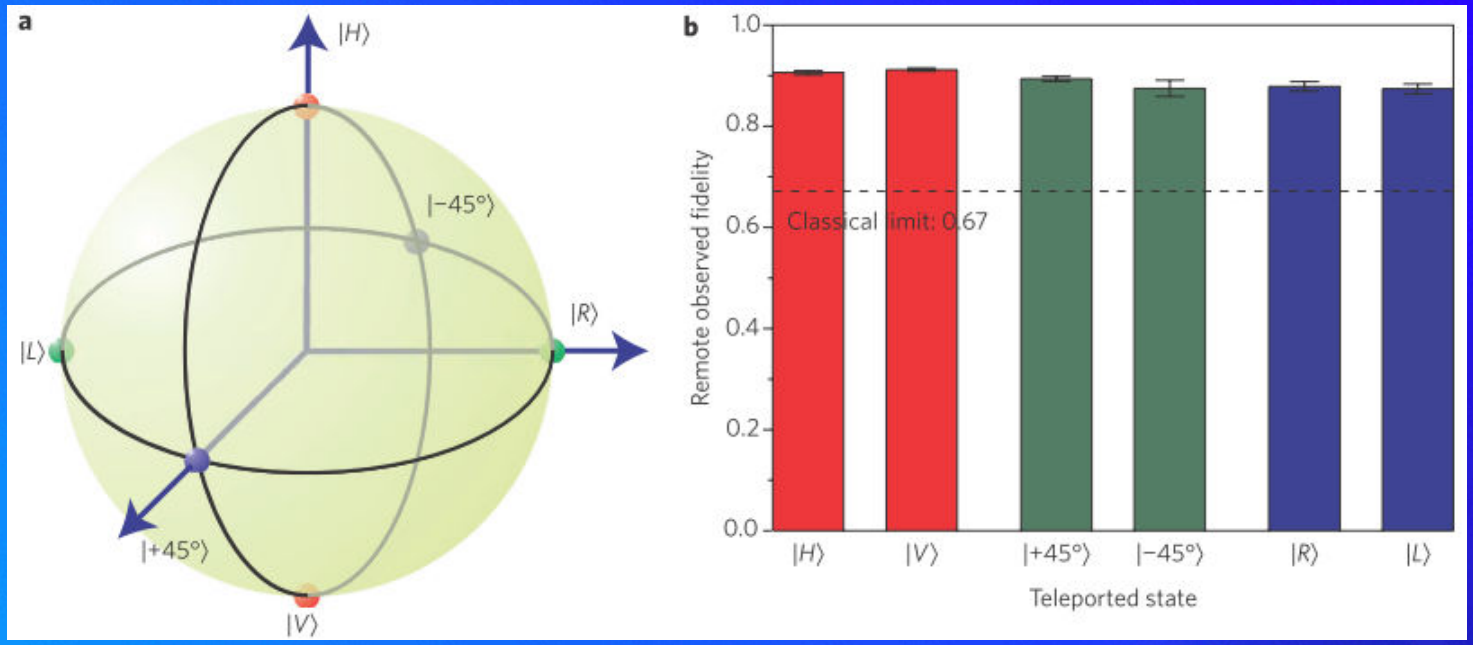
$$F_{|V\rangle} = Tr(\hat{\rho}(\hat{I}-\hat{\sigma}_z))/2$$

$$F_{|+45^\circ\rangle} = Tr(\hat{\rho}(\hat{I}+\hat{\sigma}_x))/2$$

$$F_{|-45^\circ\rangle} = Tr(\hat{\rho}(\hat{I}-\hat{\sigma}_x))/2$$

$$F_{|R\rangle} = Tr(\hat{\rho}(\hat{I}+\hat{\sigma}_y))/2$$

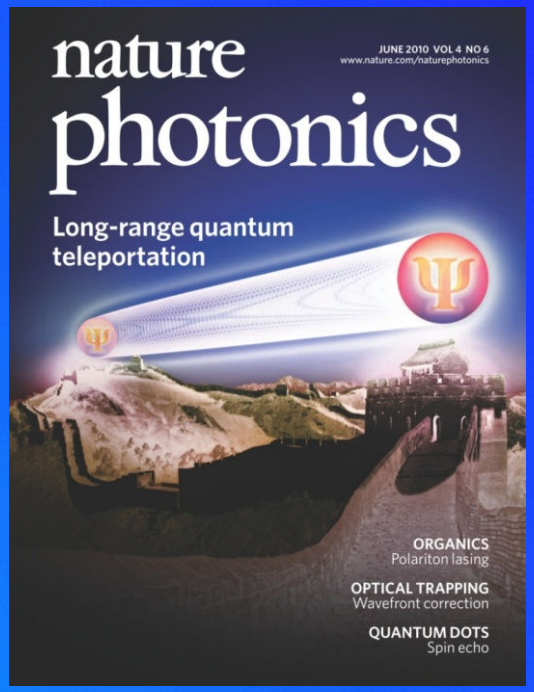
$$F_{|L\rangle} = Tr(\hat{\rho}(\hat{I}-\hat{\sigma}_y))/2$$



- Swap projection: Eliminate the biased effect caused by different detection efficiencies of D7 and D8
- The real teleportation fidelity: $F = 1/(1+\sqrt{C_7' C_8 / C_7 C_8'})$

Table 1 | Experimental measurement for teleportation fidelities.

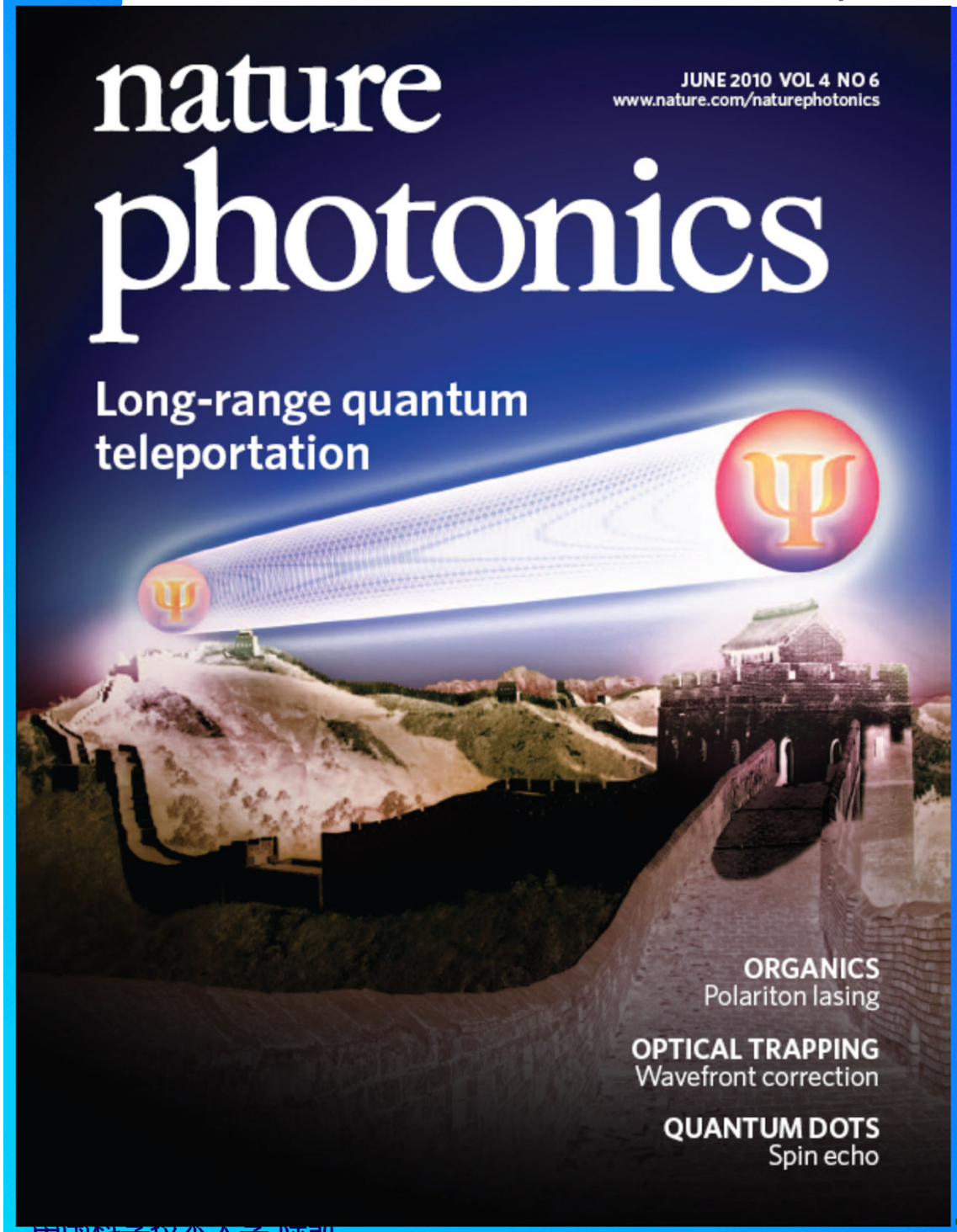
Initial states	$\|H\rangle$	$\|V\rangle$	$\|+45°\rangle$	$\|-45°\rangle$	$\|R\rangle$	$\|L\rangle$
$\|\Psi\rangle_{1p}$ (D7)	2,936	4,939	2,027	213	591	631
$\|\Psi\rangle_{1p}^{\perp}$ (D8)	225	391	276	30	83	103
$\|\Psi\rangle_{1p}$ (D8)	3,232	5,125	1,279	152	553	300
$\|\Psi\rangle_{1p}^{\perp}$ (D7)	458	605	131	22	74	38
Fidelities	0.906(4)	0.912(3)	0.894(5)	0.875(16)	0.879(9)	0.874(11)



Xian-Min Jin *et al.*, Experimental Free-Space Quantum Teleportation, **Nature Photonics 4, 376-381** (2010).

- *Developed techniques:*
- *Real-time feedback control for high stability interferometer for single photon Bell state measurement*
- *Active feed-forward manipulation on single photon state for reconstruction of the initial teleported qubit*
- *Novel design of telescopes tailored for teleportation experiment*
- *Achieve quantum teleportation in free-space at a distance 16 km, 20 times longer than the previous implementation*
- *confirms the feasibility of space-based experiments, and presents an important step towards quantum communication applications on a global scale.*

Nature Photonics 4, 376-381 (2010)封面文章



Beam Us Up Teleportation doesn't work for humans — yet — but it works over long distances, a new study reports. *Time Magazine*

隐形传态过程虽然不能够传送人类， 然而一个最新的研究显示，它的确可以远距离地传送信息。 美国《时代杂志》

大众科学・美国

Homepage
Current content
Featured this month
Subject archive
User recommended papers
About the site
Meet the editors
Contact us
FAQs
Terms & Conditions
natureasia.com

NPG Journals
by Subject Area

Chemistry
Chemistry
Drug discovery
Biotechnology
Materials
Methods & Protocols

Clinical Practice & Research
Cancer
Cardiovascular medicine
Dentistry
Endocrinology
Gastroenterology & Hepatology
Methods & Protocols
Pathology & Pathobiology
Urology

Earth & Environment
Earth sciences
Evolution & Ecology

Research Highlights

Subject Category: Physics

Published online: 2 June 2010 | doi:10.1038/nchina.2010.65

Quantum physics: Teleportation goes long distance

Felix Cheung

Researchers in China have achieved quantum teleportation in free space over a distance of 16 km

Original article citation
Jin, X. M. *et al.* Experimental free-space quantum teleportation. *Nature Photon.* doi:10.1038/nphoton.2010.87 (2010).

Full text article available for download

© (2010) istockphoto.com/Andrey Volodin

Quantum communication promises the world a completely secure way of transferring information, and quantum teleportation is an information transfer protocol that will one day make quantum communication over long distance possible. Previous studies have demonstrated quantum teleportation using an optical fibre, but photon losses due to decoherence in the fibre are large and the transmission distance is limited to 600 metres. Jianwei Pan at the University of Science and Technology of China in Hefei, Chengzhi Peng at Tsinghua University in Beijing and co-workers[1] have now achieved quantum teleportation in an optical free-space channel over a distance of 16 kilometres.

The researchers generated an entangled photon pair at Badaling in Beijing using a semiconductor, a blue laser beam and a beta-barium borate crystal. They sent one photon in the pair to 'Alice', situated at Badaling, for measurement. They then sent the other photon in the pair and the results of Alice's measurement to 'Bob' at Huailai in Hebei province — 16 kilometres away — through the free-space channel.

The researchers used specially designed telescopes to optimize the transmission efficiency and improve the stability of the free-space channel. They found that Bob could recover the results of Alice's measurements using the photon it received, thus demonstrating quantum teleportation. The study confirms the feasibility of quantum teleportation in free space and represents an important step towards quantum communication on a global scale.

Physicists Achieve Quantum Teleportation Across a Distance of 10 Miles

How far can you beam information instantaneously? Try 10 miles, according to a study in *Nature Photonics* that pushes the limits of quantum teleportation to its greatest distance yet. At that distance, the scientists say, one can begin to consider the possibility of someday using quantum teleportation to communicate between the ground and a satellite in orbit.

As stories about quantum teleportation usually note, this isn't the Starship Enterprise's transporter: The weird quantum phenomenon makes it possible to send information, not matter, across a distance.

> It works by entangling two objects, like photons or ions. The first teleportation experiments involved beams of light. Once the objects are entangled, they're connected by an invisible wave, like a thread or umbilical cord. That means when something is done to one object, it immediately happens to the other object, too. Einstein called this "spooky action at a distance." [Popular Science]

自然·中国

中国科学技术大学 陈凯

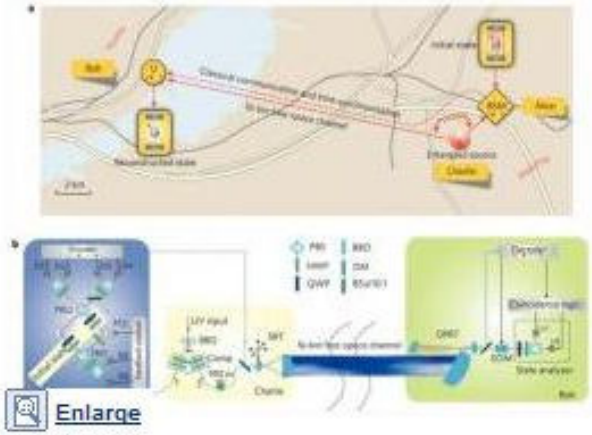
PHYSORG.COM
SCIENCE : PHYSICS : TECH : NANO : NEWS

Home | Nanotechnology | Physics | Space & Earth | Electronics

General Physics | Condensed Matter | Optics & Photonics | Superco

Quantum teleportation achieved over 16 km

May 20, 2010 by Lin Edwards



Enlarge

a, A birds-eye view of the 16-km free-space quantum teleportation experiment. Charlie sends photon 1 to Alice for BSM. Classical information, including the results of the BSM and the signal for time synchronization, is sent through the free-space channel with photon 2, to Bob, before decoding and triggering of the corresponding unitary transformation. b, Sketch of the experimental system. See the original paper for more details. Image copyright: Nature Photonics, doi:10.1038/nphoton.2010.87

(PhysOrg.com) -- Scientists in China have succeeded in teleporting information between photons further than ever before. They transported quantum information over a free space distance of 16 km (10 miles), much further than the few hundred meters previously achieved, which brings us closer to transmitting information over long distances without the need for a traditional signal.

physicstoday.org Physics Update
The latest in research

PHYSICS TODAY HOME | JOBS | BUYERS GUIDE |

« Electron microsco

Quantum teleportation through open air

By Physics Today on May 17, 2010 10:17 AM | No Comments | No TrackBacks

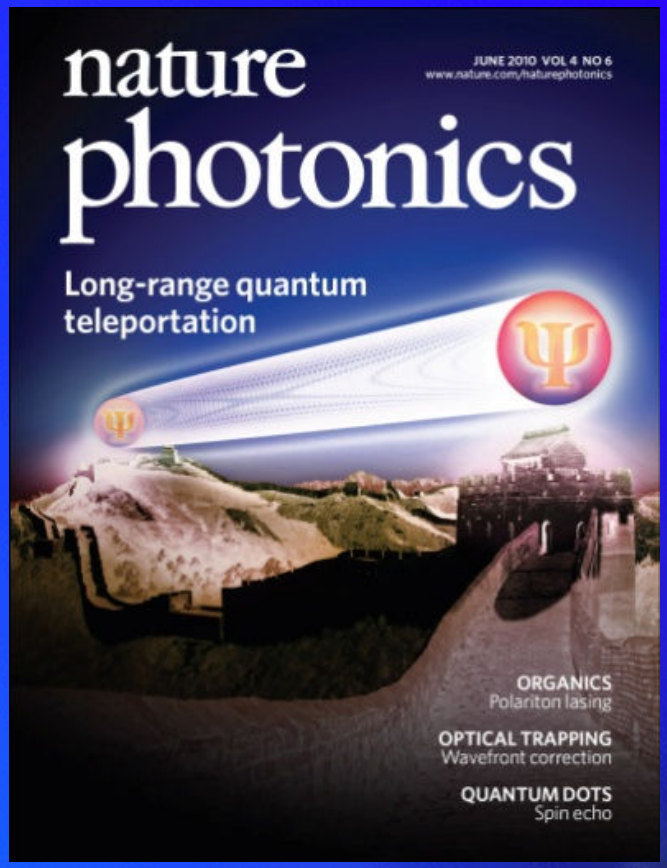
A central tenet of quantum information processing asserts that an unknown qubit cannot be cloned (see *Physics Today*, February 2009, page 76). But the unknown state of one qubit can be transferred to another qubit in a process termed quantum teleportation. The first experimental demonstrations succeeded in teleporting a qubit state a meter or so (see *Physics Today*, February 1998, page 18). Subsequent experiments with photons, whose polarizations form a convenient basis for quantum information, have used fiber optics to achieve teleportation over hundreds of meters. But practical quantum communication will require teleportation over much greater distances. Jian-Wei Pan, Cheng-Zhi Peng, and coworkers at the University of Science and Technology of China and Tsinghua University have now transferred a qubit state through free space over a distance of 16 km, from "Alice" in the Beijing suburb of Badaling, across towns and roads, to "Bob" in Huailai, on the other side of Guanting Reservoir. The experiment employed a standard teleportation protocol: Alice and Bob each receive one of a pair of entangled photons; Alice measures hers in combination with an unknown qubit and sends the result, by classical means, to Bob; armed with that result, Bob projects his photon onto the state of the unknown qubit. The new work, though, adds many refinements, including novel telescope designs for open-air transmission, active feedback control for increased stability, and synchronized real-time information transfer. The resulting teleportation fidelity was nearly 90%. Such high-fidelity transmission, say the researchers, could help enable quantum teleportation to orbiting satellites. (X.-M. Jin et al., *Nat. Photon.*, in press, doi:10.1038/nphoton.2010.87.)—Richard J. Fitzgerald

自由空间量子通信

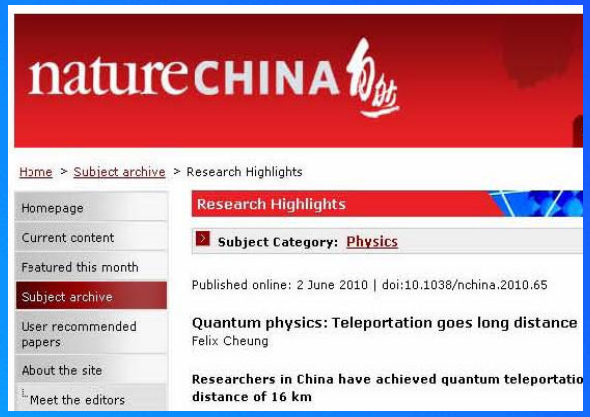
- 国际上距离最远的(16公里)自由空间量子隐形传态 [Nature Photonics 4, 376] (2010)

两院院士评为
“中国十大科技进展新闻

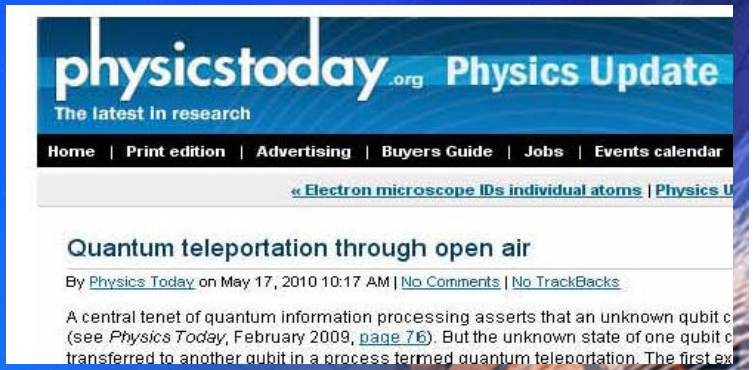
科技部评为
“中国科学十大进展”



美国物理学家组织的报道

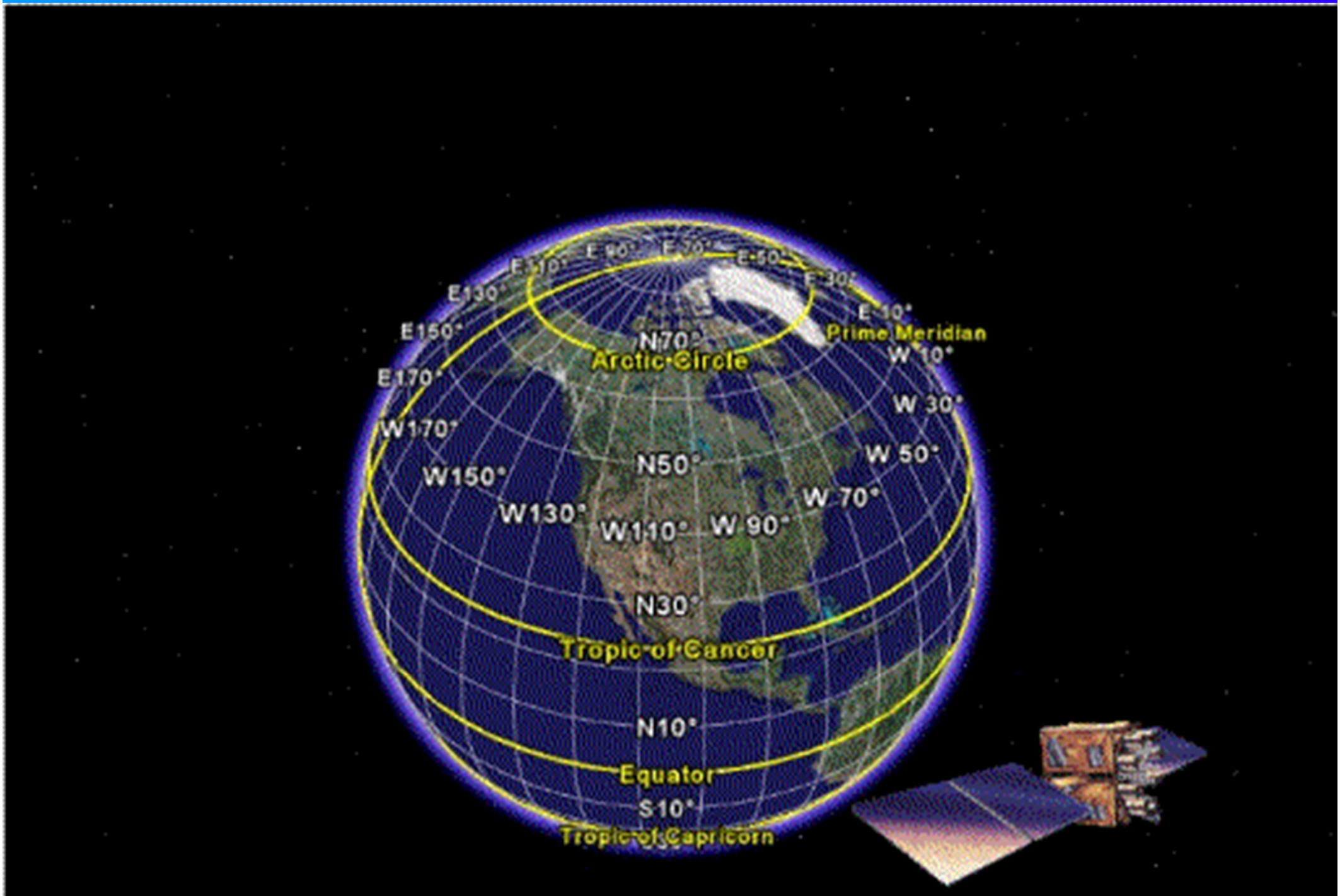


《自然·中国》的报道



美国《今日物理》的报道

Global Quantum Communication Network



About Quantum Teleportation

- In a quantum teleportation an unknown quantum state can be disambled into, and later reconstructed from, two classical bit-states and an maximally entangled pure quantum state.
- Using quantum teleportation an unknown quantum state can be *teleported* from one place to another by a sender who does not need to know - for teleportation itself - neither the state to be teleported nor the location of the intended receiver.
- The teleportation procedure can not be used to transmit information faster than light

but

- it can be argued that quantum information presented in unknown state is transmitted instanteneously (except two random bits to be transmitted at the speed of light at most).
- EPR channel is irreversibly destroyed during the teleportation process.

第四章 量子通信

1. 保密通信
2. QKD基本原理
3. BB84协议过程
4. QKD安全性
5. 诱骗态(Decoy-state QKD)
   - ① Decoy QKD原理
   - ② 实用Decoy QKD
   - ③ Decoy QKD实验
6. QKD的现实安全性
   - ① 探测端的安全性→MDI-QKD
   - ② 设备无关的→ DI-QKD
7. 量子隐形传态(Quantum Teleportation) [原理、实验]
8. **量子纠缠交换(Entanglement Swapping)**
9. 量子通信网络
10. 量子通信商用公司
11. 量子通信发展与实用化QKD之路

Entanglement Swapping: Entangling Photons That Never Interacted

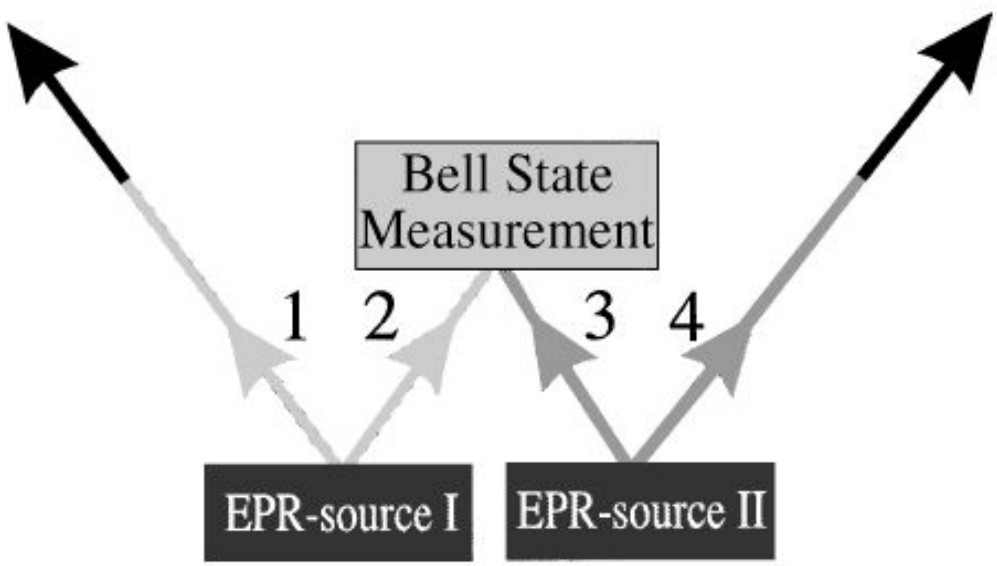


FIG. 1. Principle of entanglement swapping. Two EPR sources produce two pairs of entangled photons, pair 1-2 and pair 3-4. One photon from each pair (photons 2 and 3) is subjected to a Bell-state measurement. This results in projecting the other two outgoing photons 1 and 4 onto an entangled state. Change of the shading of the lines indicates the change in the set of possible predictions that can be made.

Jian-Wei Pan *et al.*, Phys. Rev. Lett. 80, 3891-3894 (1998)

Entanglement Swapping: Entangling Photons That Never Interacted

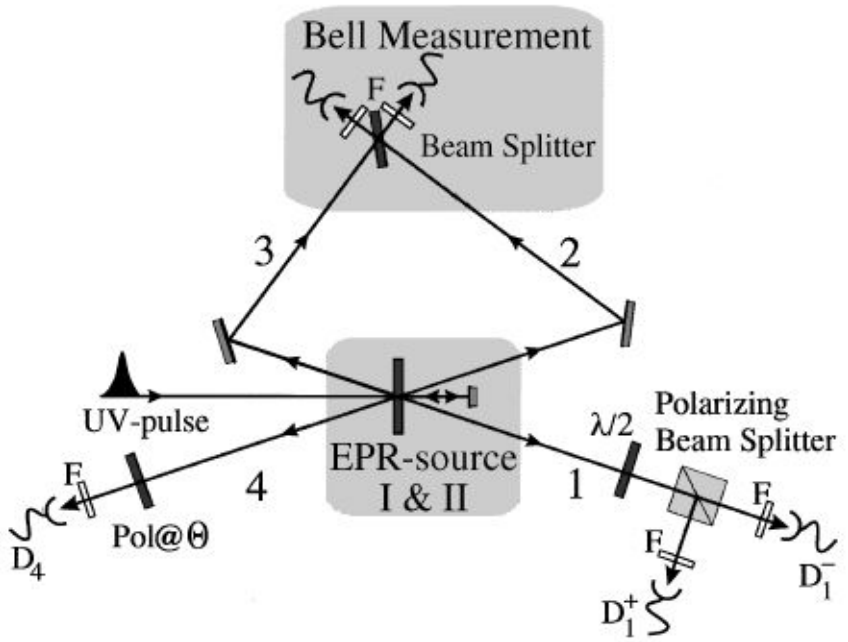


FIG. 2. Experimental setup. A UV pulse passing through a nonlinear crystal creates pair 1-2 of entangled photons. Photon 2 is directed to the beam splitter. After reflection, during its second passage through the crystal the UV pulse creates a second pair 3-4 of entangled photons. Photon 3 will also be directed to the beam splitter. When photons 2 and 3 yield a coincidence click at the two detectors behind the beam splitter, they are projected into the $|\Psi^-\rangle_{23}$ state. As a consequence of this Bell-state measurement the two remaining photons 1 and 4 will also be projected into an entangled state. To analyze their entanglement we look at coincidences between detectors D_1^+ and D_4, and between detectors D_1^- and D_4, for different polarization angles Θ. By rotating the $\lambda/2$ plate in front of the two-channel polarizer we can analyze photon 1 in any linear polarization basis. Note that, since the detection of coincidences between detectors D_1^+ and D_4, and D_1^- and D_4 are conditioned on the detection of the Ψ^- state, we are looking at fourfold coincidences. Narrow bandwidth filters (F) are positioned in front of each detector.

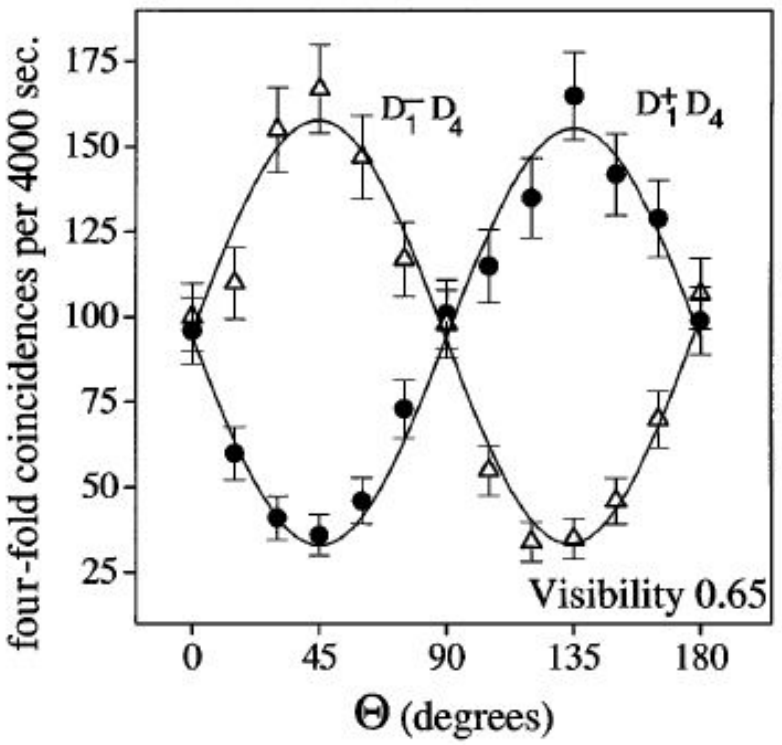


FIG. 3. Entanglement verification. Fourfold coincidences, resulting from twofold coincidence $D1^+D4$ and $D1^-D4$ conditioned on the twofold coincidences of the Bell-state measurement, when varying the polarizer angle Θ. The two complementary sine curves with a visibility of 0.65 ± 0.02 demonstrate that photons 1 and 4 are polarization entangled.

Jian-Wei Pan *et al.*, Phys. Rev. Lett. 80, 3891-3894 (1998)

Multistage Entanglement Swapping

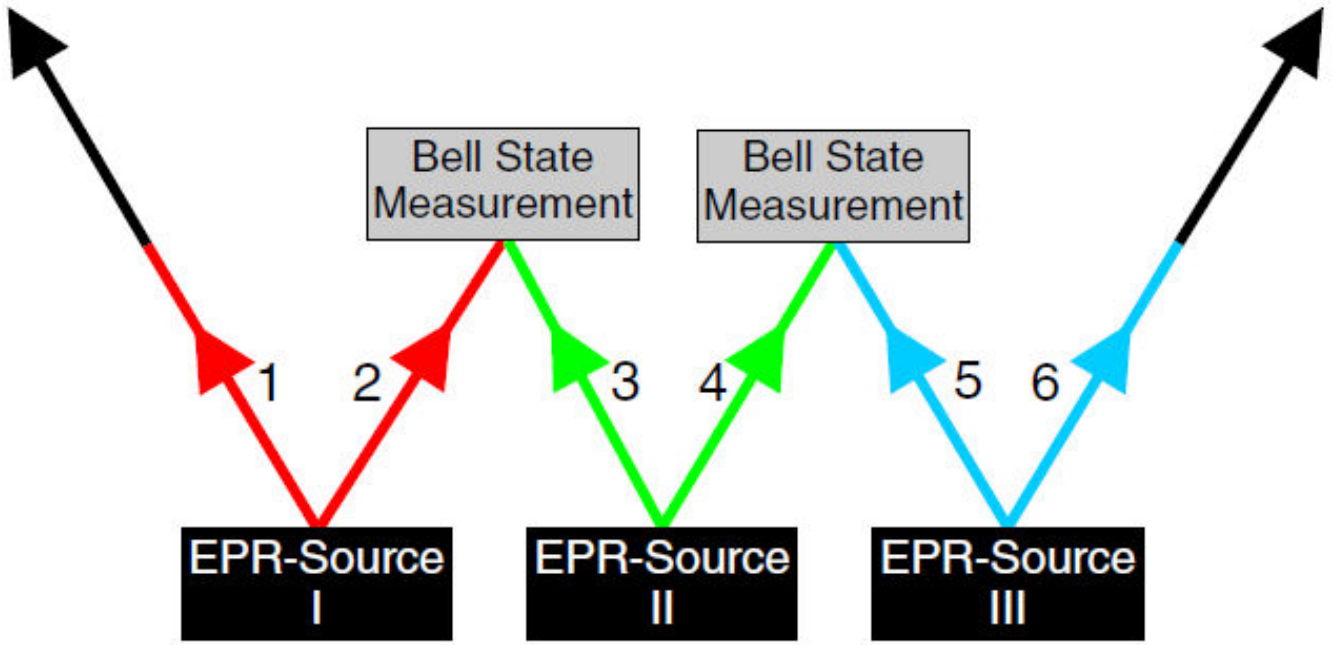


FIG. 1 (color online). Principle of multistage entanglement swapping: three EPR sources produce pairs of entangled photons 1–2, 3–4, and 5–6. Photon 2 from the initial state and photon 3 from the first ancillary pair are subjected to a joint BSM, and so are photon 4 from the first ancillary and photon 5 from the second acillary pair. The two BSMs project outgoing photons 1 and 6 onto an entangled state. Thus the entanglement of the initial pair is swapped to an entanglement between photons 1 and 6.

Alexander M. Goebel *et al.*, Phys. Rev. Lett. 101, 080403 (2008)

Multistage Entanglement Swapping

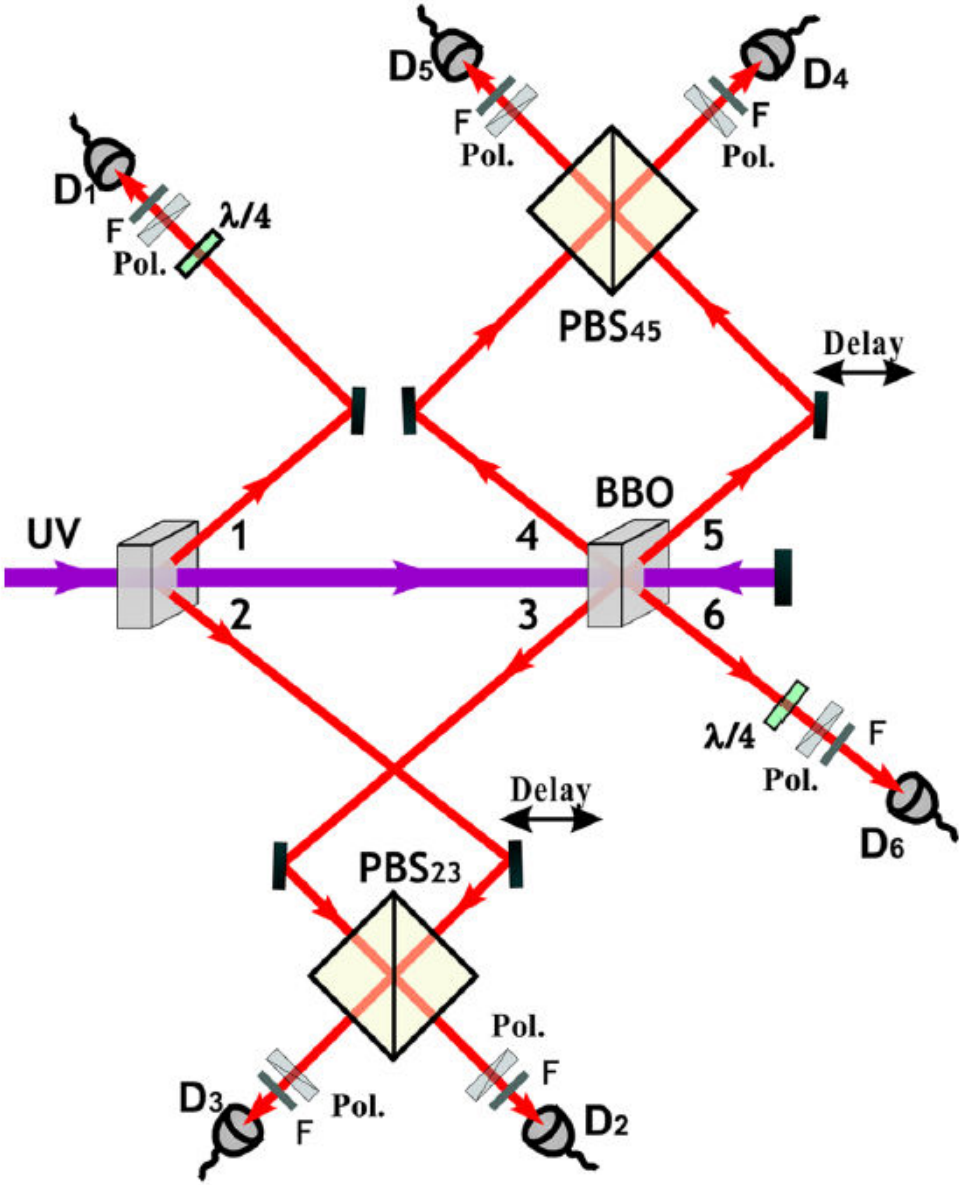


FIG. 2 (color online). The focused ultraviolet laser beam passes the first BBO generating photon pair 1–2. Refocused, it passes the second BBO generating the ancillary pair 5–6 and again retroreflected through the second BBO generating pair 3–4. In order to achieve indistinguishability at the interference PBS23 and PBS45 the spatial and temporal overlap are maximized by adjusting the delays and observing "Shih-Alley-Hong-Ou-Mandel-type" interference fringes [19] behind the PBS23 (PBS45) in the ± basis [20]. With the help of polarizers and half or quarter wave plates, we are able to analyze the polarization of photons in arms 1 and 6. All photons are spectrally filtered by narrow band filters with $\Delta\lambda_{\mathrm{FWHM}} \approx 2.8$ nm and are monitored by silicon avalanche single-photon detectors [21]. Coincidences are counted by a laser clocked field-programmable gate array based coincidence unit.

Alexander M. Goebel *et al.*, Phys. Rev. Lett. 101, 080403 (2008)

Experimental Multiparticle Entanglement Swapping for Quantum Networking

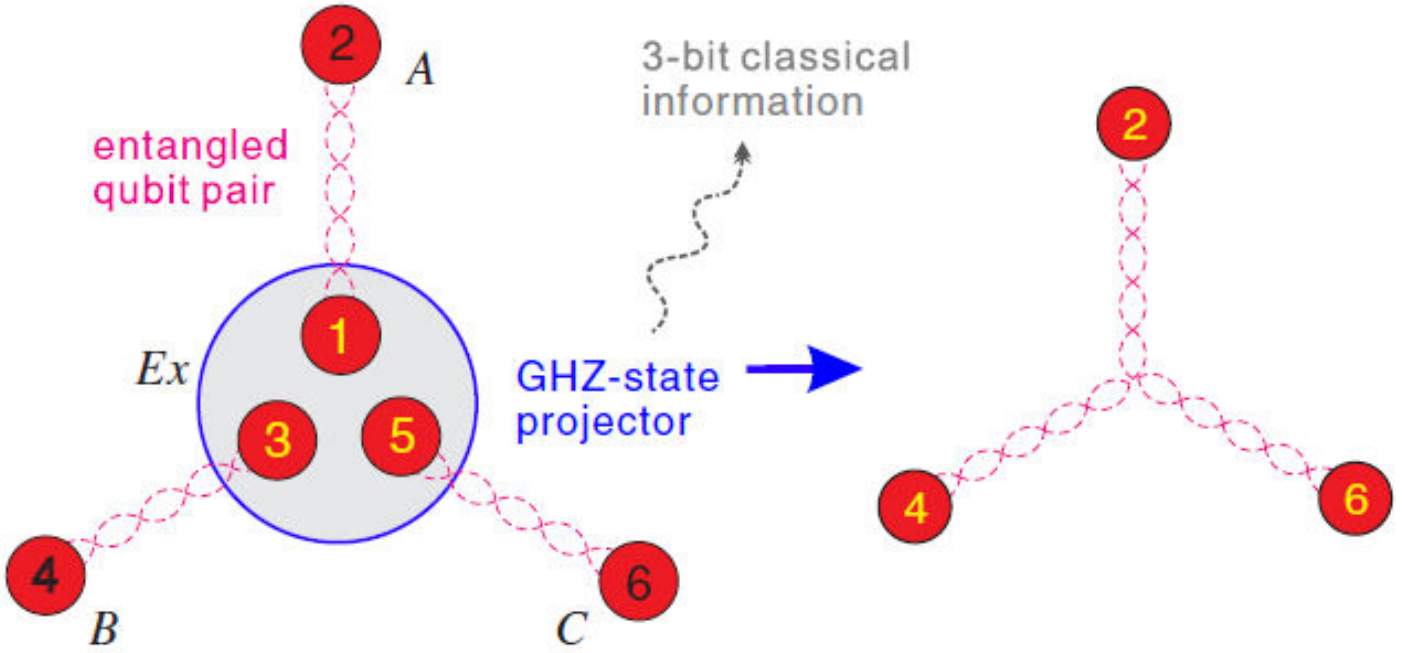


FIG. 1 (color online). Configuration of a multiparty quantum network and GHZ entanglement swapping. Initially, users A, B, and C share entangled qubit pairs with the central exchange Ex. If Ex projects the three particles, 1, 3, and 5, into a GHZ state, the other three particles, 2, 4, and 6 belonging to A, B, and C respectively, will be entangled into a GHZ state by entanglement swapping.

Chao-Yang Lu, Tao Yang, and Jian-Wei Pan, Phys. Rev. Lett. 103, 020501 (2009)

Experimental Multiparticle Entanglement Swapping for Quantum Networking

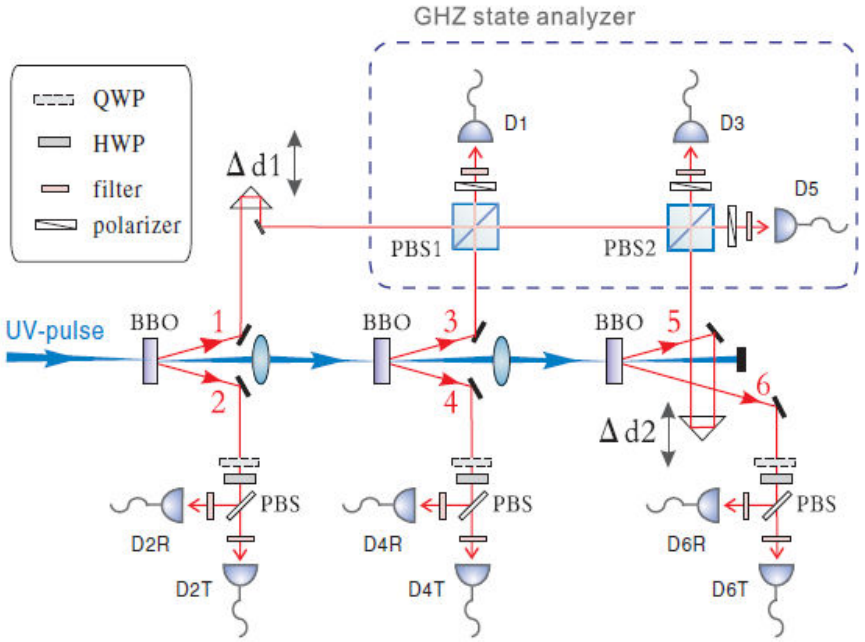


FIG. 2 (color online). Experimental setup for entanglement swapping of a three-photon GHZ state. Ultraviolet laser pulses (with a central wavelength of ~394 nm, a pulse duration of ~120 fs, and a repetition rate of ~76 MHz) are focused on three BBO crystals, producing entangled photon pairs emitted into spatial modes 1–2, 3–4, and 5–6. Photons 1, 3, and 5 are projected into a GHZ state (dashed box, see text and Ref. [18]), and the photons 2, 4, and 6 are analyzed by a combination of a quarter-wave plate (QWP), a half-wave plate (HWP) and a PBS. The photons are spectrally filtered by narrow-band filters ($\Delta\lambda_{\mathrm{FWHM}} = 3.2$ nm) and monitored by fiber-coupled silicon avalanche single-photon detectors (D1, D2T, $\cdots$, D6R). The multiphoton events are registered by a laser clocked multichannel coincidence unit.

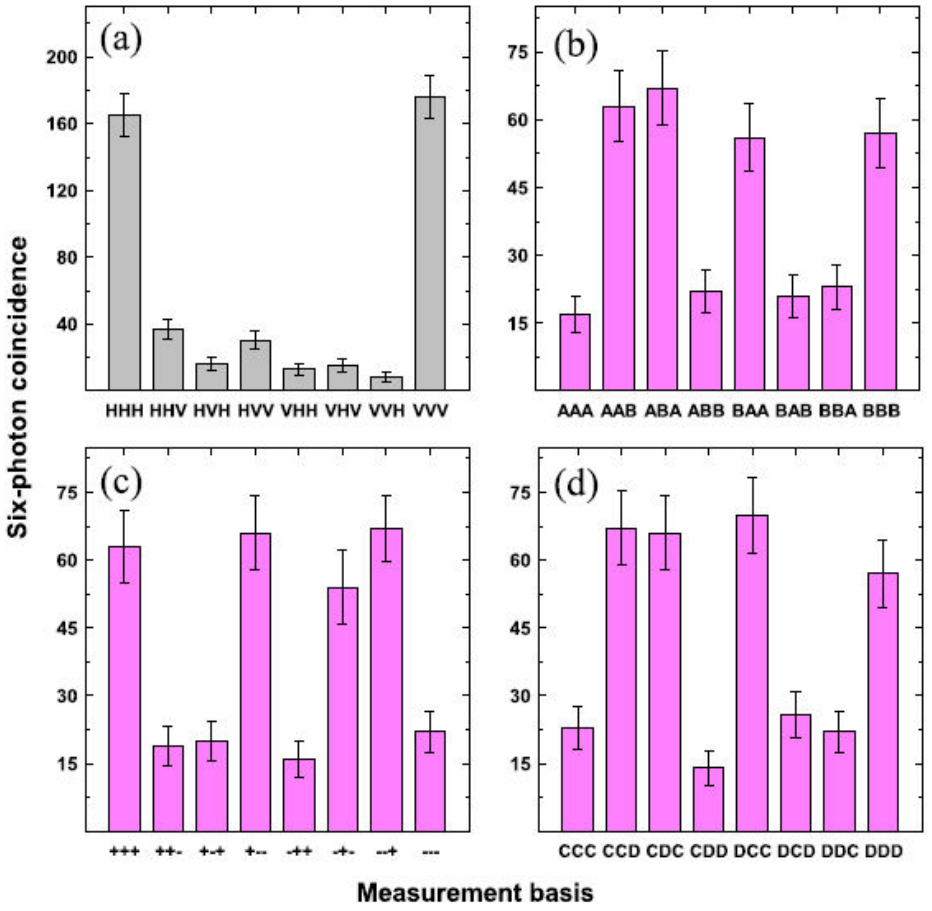


FIG. 4 (color online). Sixfold coincidence in the measurement basis of: (a) H/V, (b) A/B, (c) $+/-$, and (d) C/D for witnessing the genuine entanglement of the three emerging photons 2, 4, and 6. The accumulation time for each data set is 24 h in (a) and 18 h in (b),(c), and (d). The error bars represent 1 standard deviation deduced from Poissonian counting statistics of the raw detection events.

Chao-Yang Lu, Tao Yang, and Jian-Wei Pan, Phys. Rev. Lett. 103, 020501 (2009)

课后作业

Entanglement Swapping的原理推导

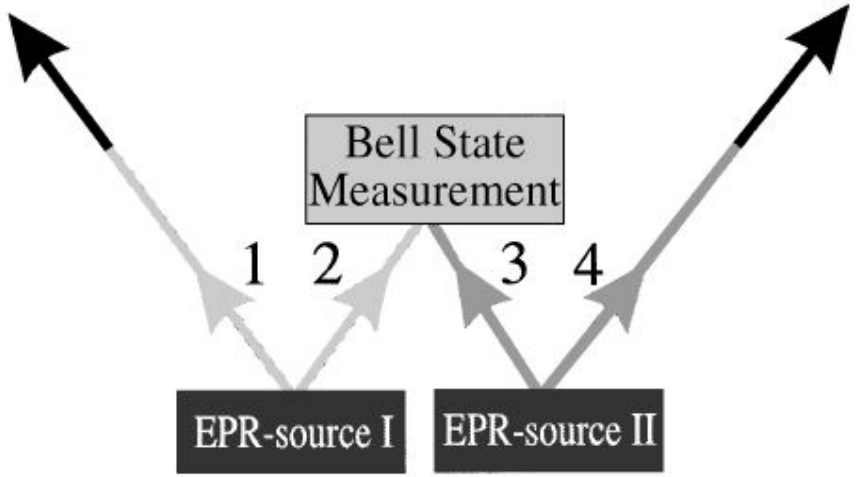


FIG. 1. Principle of entanglement swapping. Two EPR sources produce two pairs of entangled photons, pair 1-2 and pair 3-4. One photon from each pair (photons 2 and 3) is subjected to a Bell-state measurement. This results in projecting the other two outgoing photons 1 and 4 onto an entangled state. Change of the shading of the lines indicates the change in the set of possible predictions that can be made.

第四章 量子通信

1. 保密通信
2. QKD基本原理
3. BB84协议过程
4. QKD安全性
5. 诱骗态(Decoy-state QKD)
   - ① Decoy QKD原理
   - ② 实用Decoy QKD
   - ③ Decoy QKD实验
6. QKD的现实安全性
   - ① 探测端的安全性→MDI-QKD
   - ② 设备无关的→ DI-QKD
7. 量子隐形传态(Quantum Teleportation) [原理、实验]
8. 量子纠缠交换(Entanglement Swapping)
9. **量子通信网络**
10. 量子通信商用公司
11. 量子通信发展与实用化QKD之路

量子通信网络进展

US

- DARPA 网络，连接波士顿市区的哈佛大学、波士顿大学和BBN公司 10km 链接。其3个节点之后增加到了10个。
- NIST 3节点网络 1km 链接。

EU

- 欧盟从2006年起，成立了“基于密码的安全通信（SECOQC）”网络，囊括了来自英国、法国、德国、意大利、奥地利和西班牙等12个国家的41个相关领域的机构和组织 。典型的网络 6个节点，8个链接。 2008年10月在维也纳演示。采用混合类型的协议和可信中继架构。光纤的环形网络63 km，一个额外节点85 km。

Japan

- 日本国家情报通信研究机构（NICT） 主导联合项目‘Seamless QKD in Metropolitan- and Backbone- Networks’. NEC & Mitsubishi的互联于2006年演示。2010年10月，NICT主导，联合日本电信电话株式会社(NTT)、NEC和三菱电机，并邀请东芝欧洲有限公司，瑞士ID Quantique公司和奥地利的All Vienna共同协作在东京建成和演示了6节点城域量子通信网络”Tokyo QKD Network”。最远通信距离为90公里，45公里距离上点对点通信速率可达60kbps（使用超导探测器）

量子通信网络进展

China

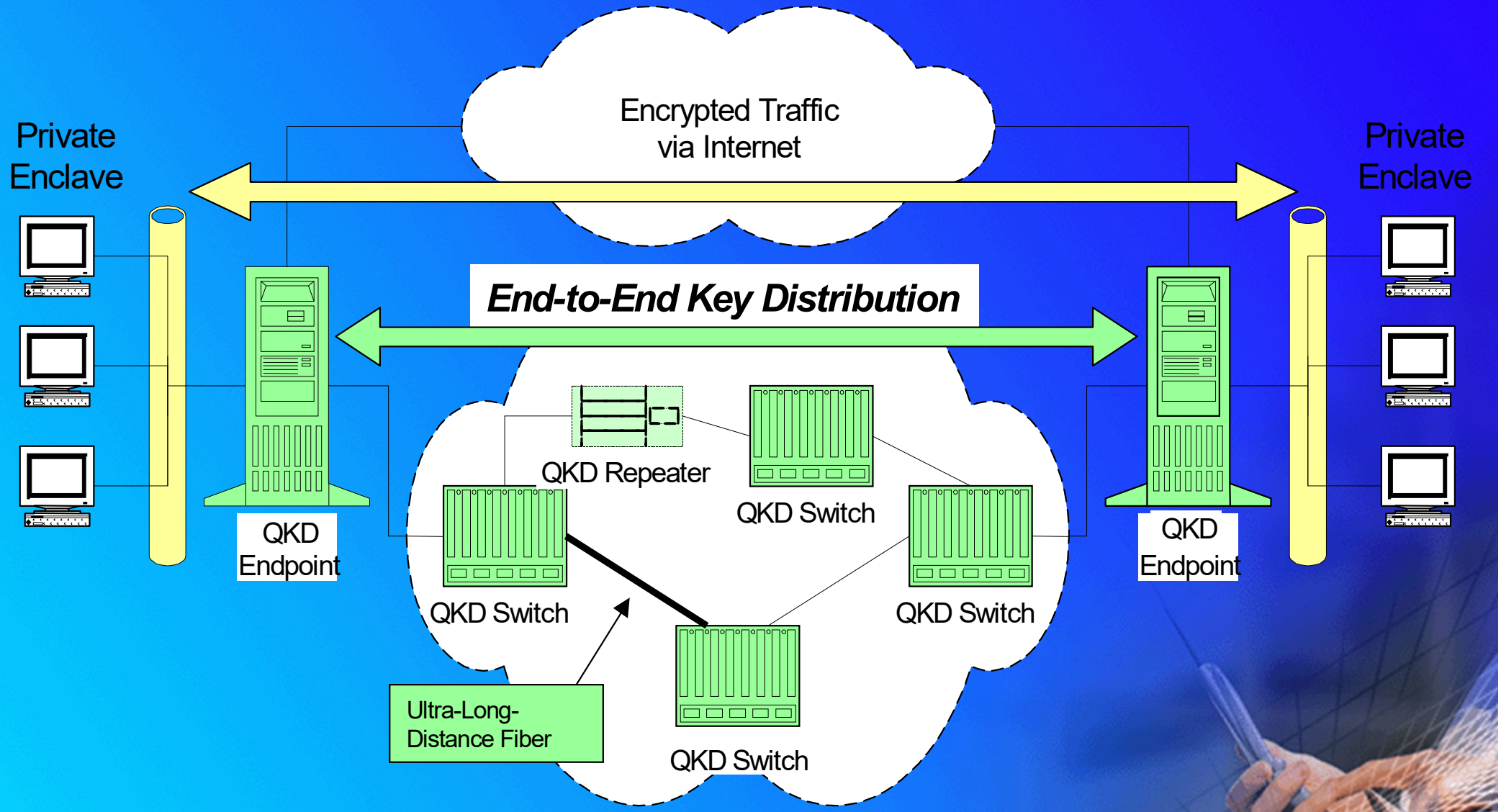
- **USTC** 潘建伟教授团队 **5**节点大于**16km**链接。最远链接**60km**（延伸至**130km**）。所有节点互联互通。
- **USTC** 郭光灿教授团队**7**个节点最远**10km**链接。**4**节点互通**5.6km**。

商用量子通信产品公司

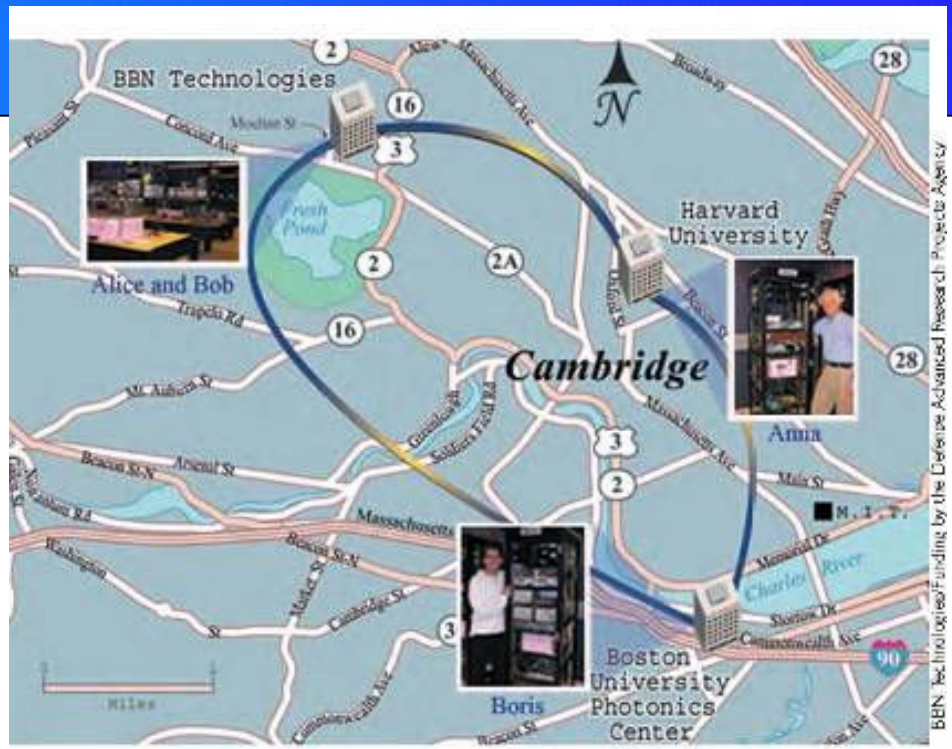
- **id Quantique: Geneva, Switzerland**
- **MagiQ Technologies: US, New York**
- **SmartQuantum，France，Lannion**（破产）
- **QuintessenceLabs, Australia, Canberra**

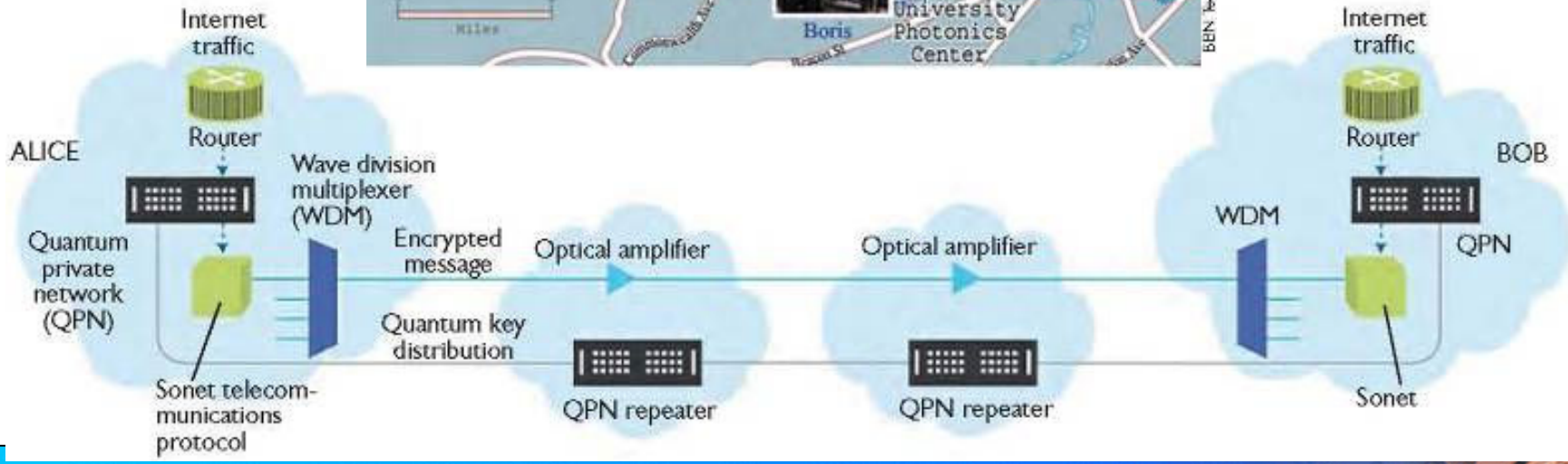
etc.

The DARPA Quantum Network

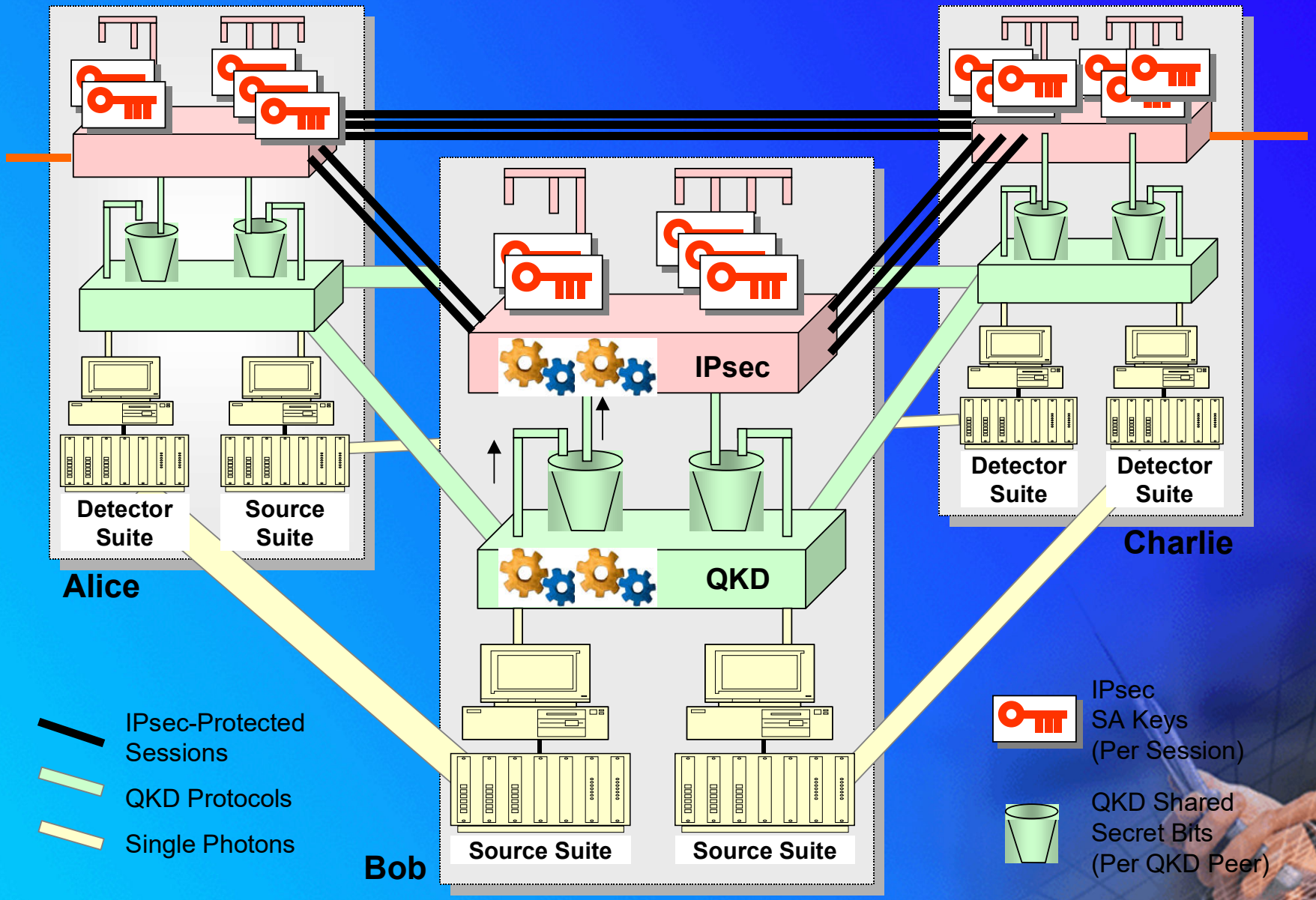


The DARPA Quantum Network

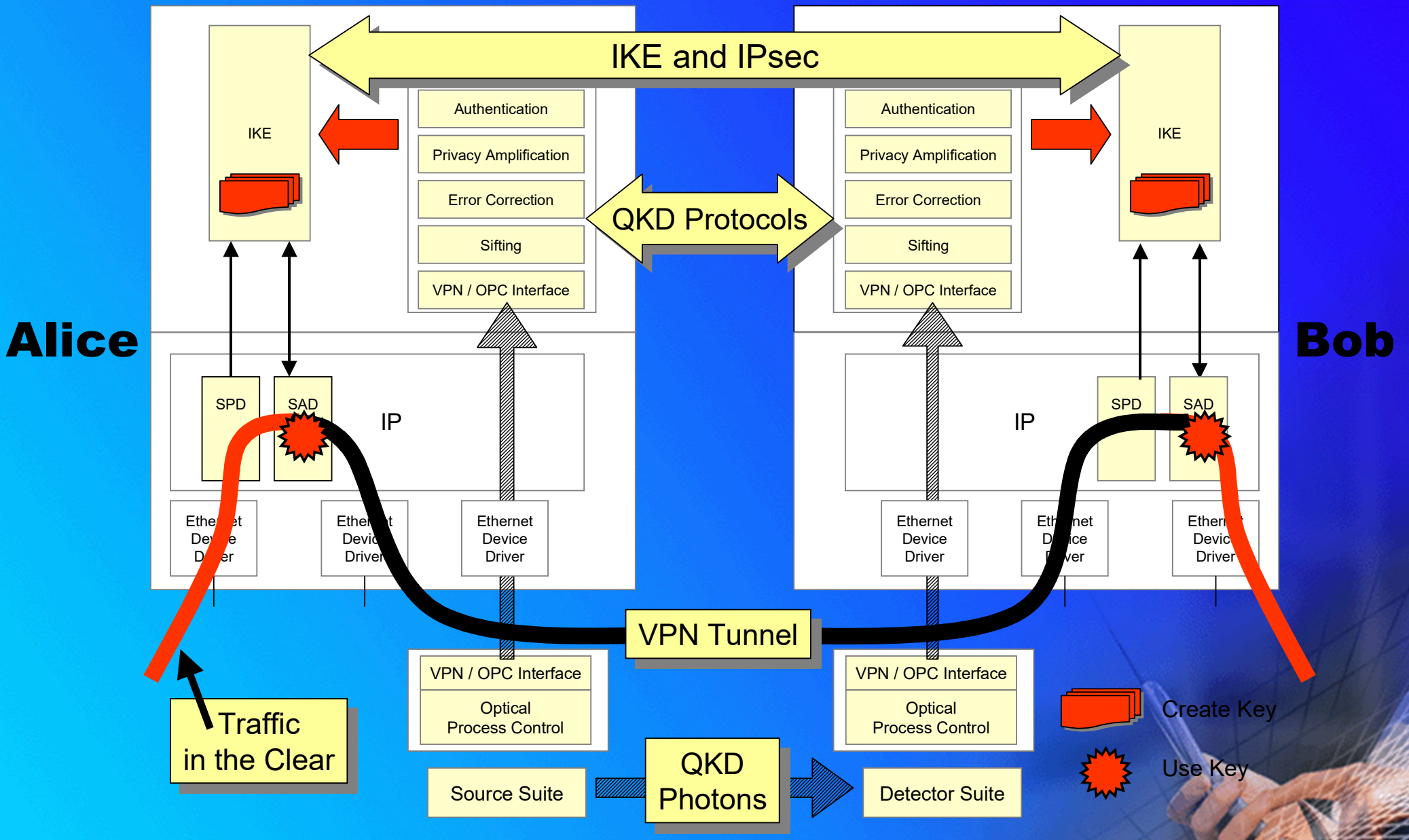




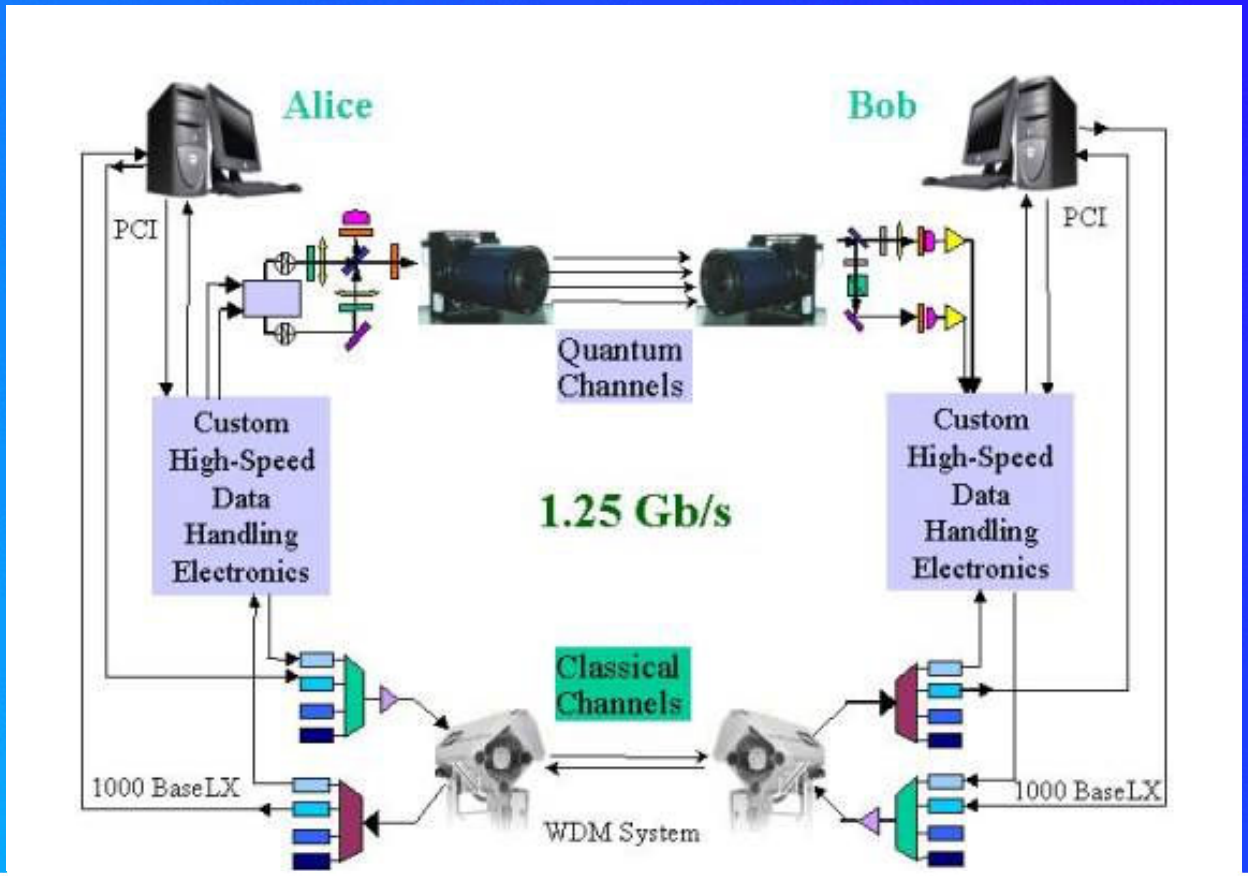
The DARPA Quantum Network架构



The DARPA Quantum Network架构



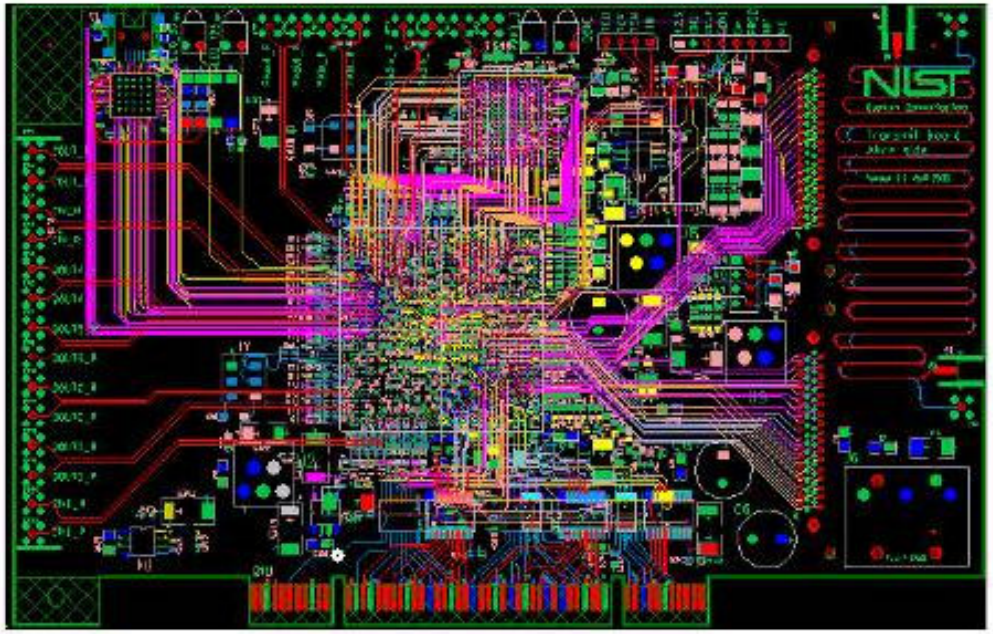
NIST Quantum Communication Testbed



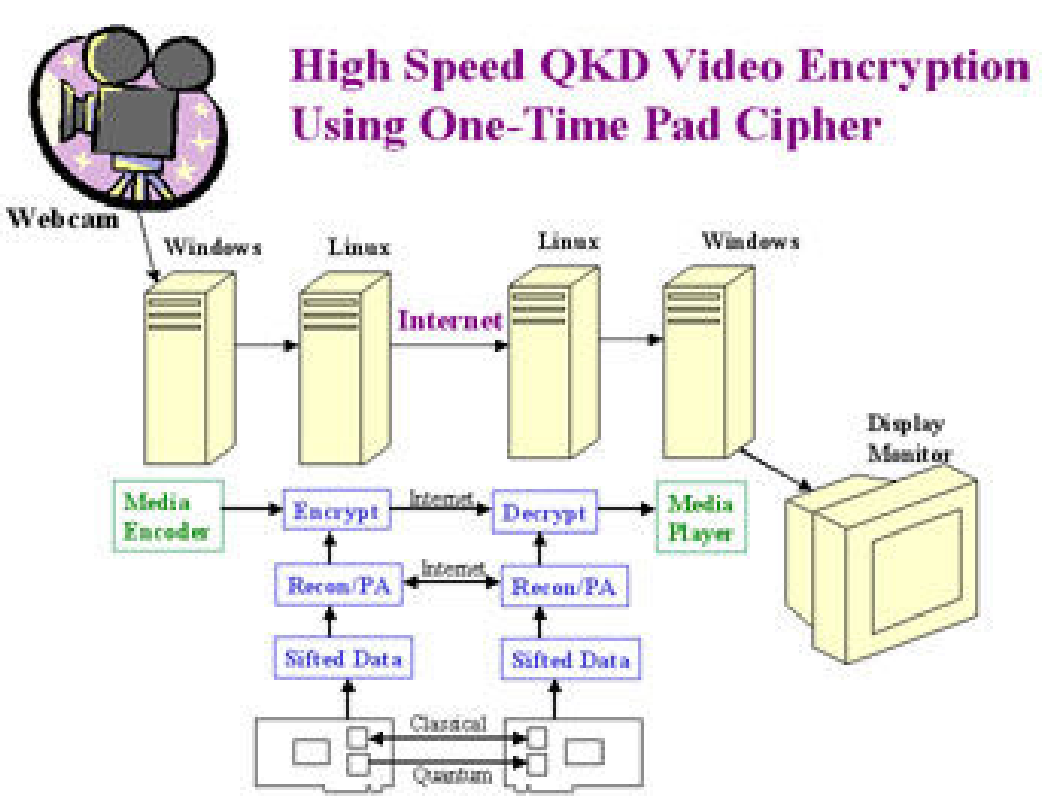
PCI interface high-speed electronics boards for Alice (left) and Bob (right).

1 Mbit/s over 4km (2006年)

NIST 量子网络

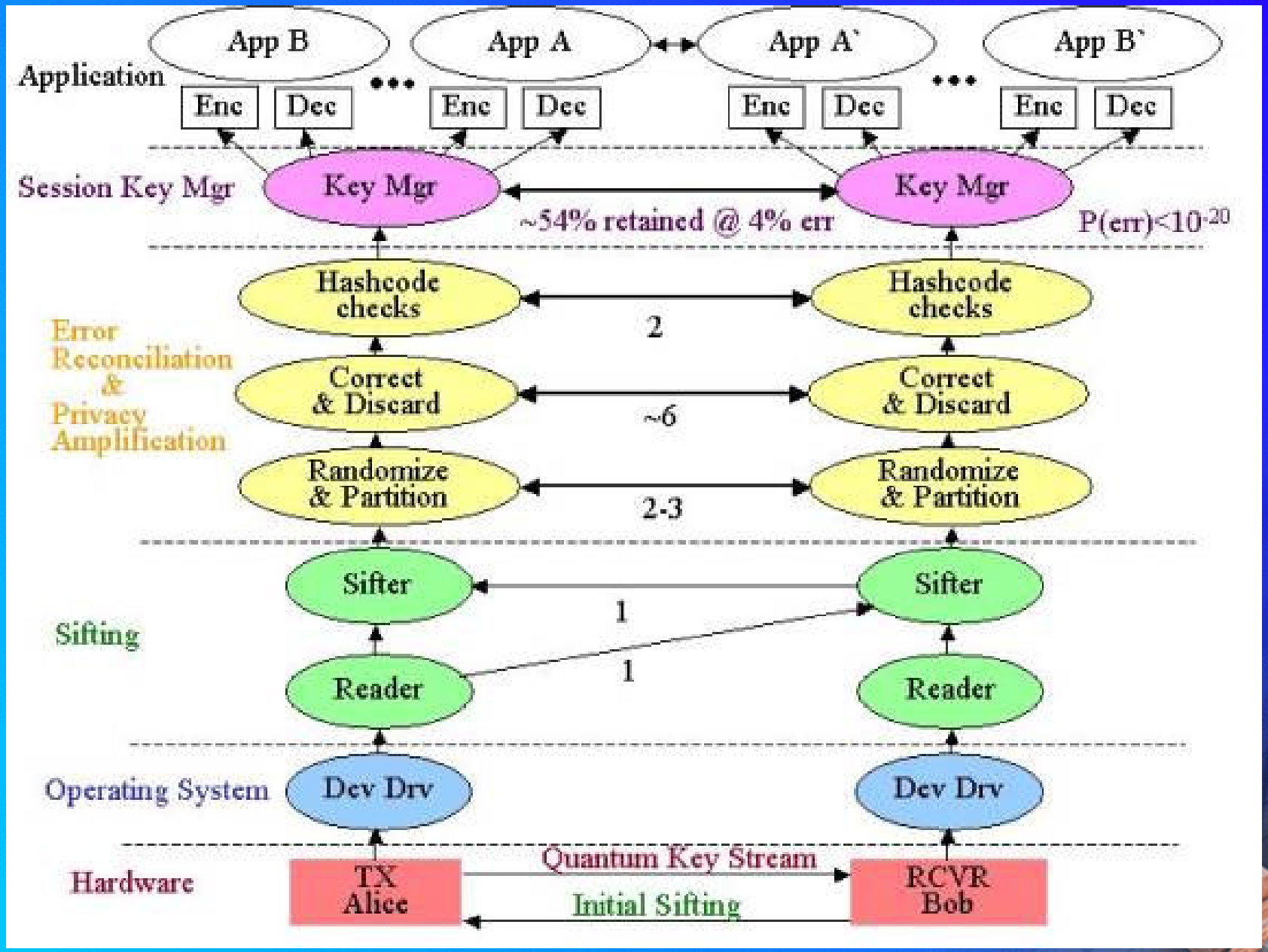


集成的高速电路板



视频会议演示

NIST QKD Protocol Stack (2006)



SECOQC QKD网络拓扑和分布

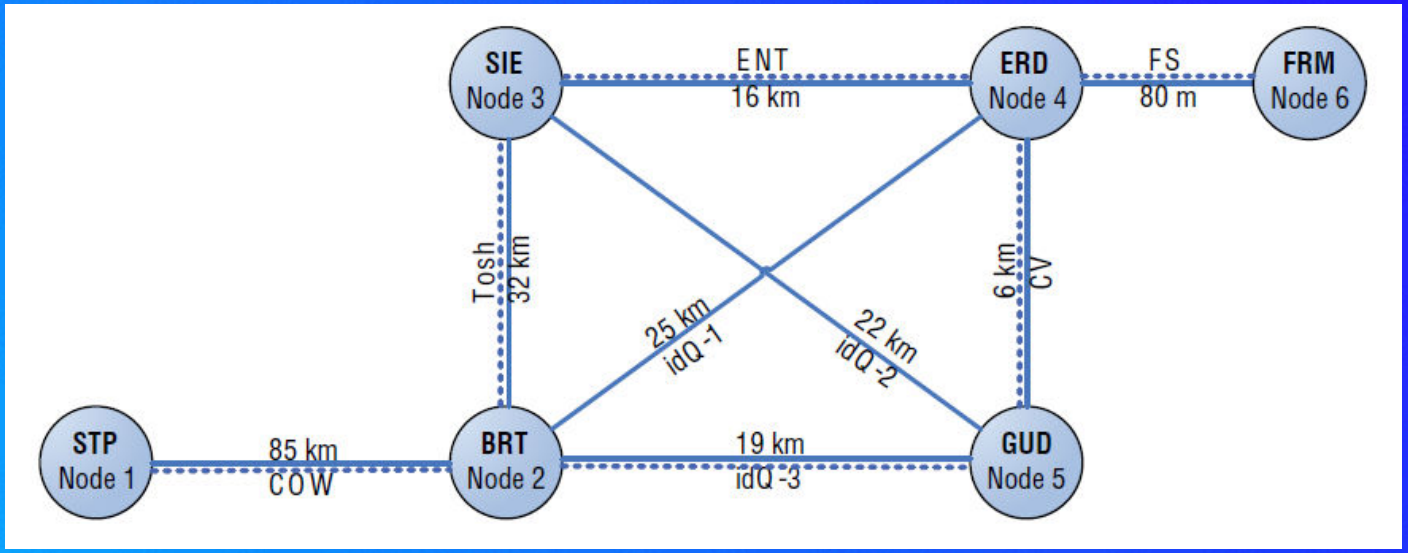


Figure 3. Satellite map with the locations of the nodes of the prototype.

SECOQC QKD-链接协议和设备

- Attenuated Laser Pulses (Id Quantique)
- Coherent-One-Way (University of Geneva)
- One-way, decoy states (Toshiba UK)
- Entangled photons (University of Vienna)
- Continuous Variables (Prof. Grangier)
- Access Free Space Link (LMU of Munich)
  - The “last mile“ (80 m, >10kbit/s)

SECOQC QKD节点组成

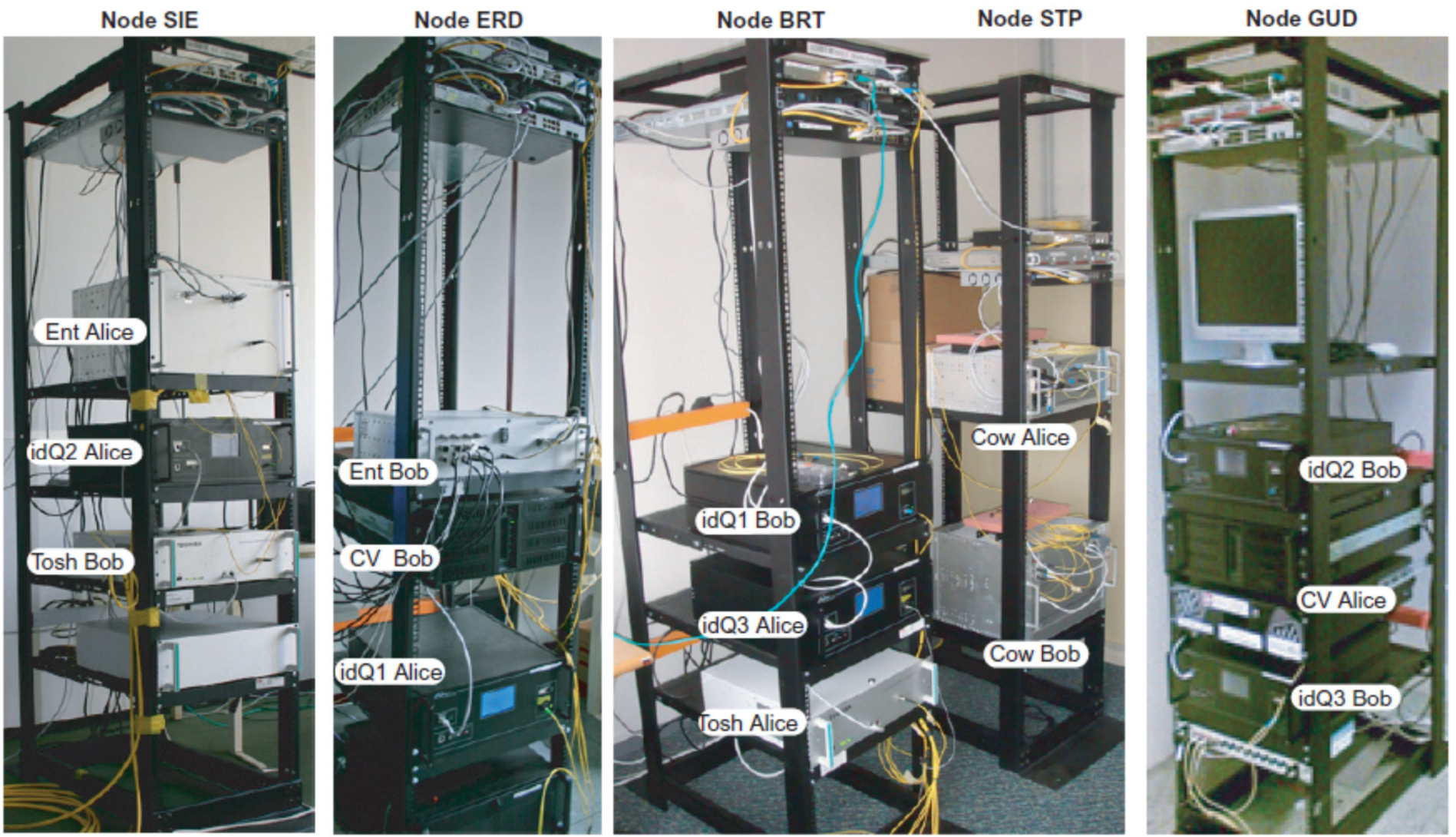
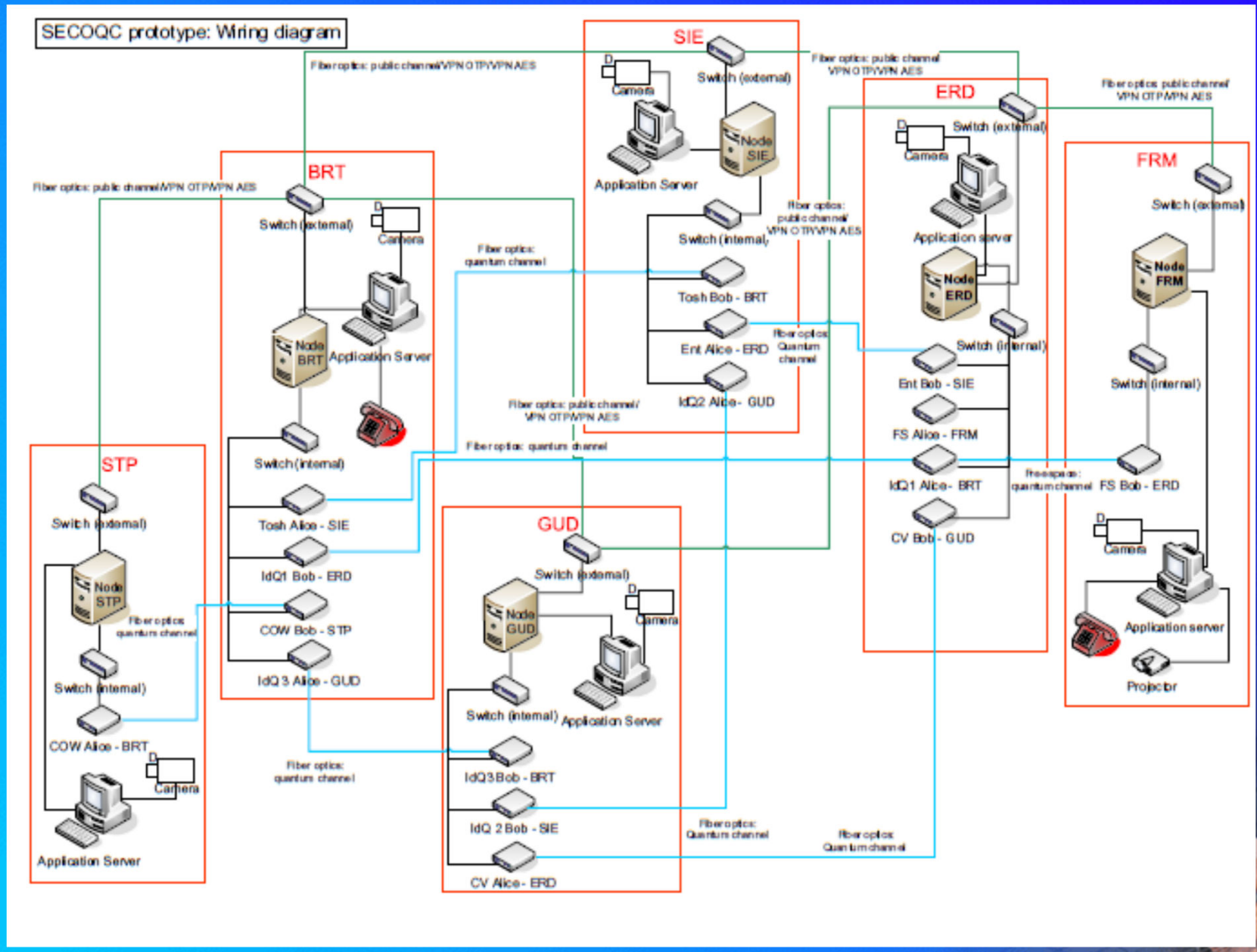


Figure 5. Photographs of the SECOQC network node racks.

成码率：0.6～10kbps

SECOQC QKD链接方式



SECOQC QKD节点模块

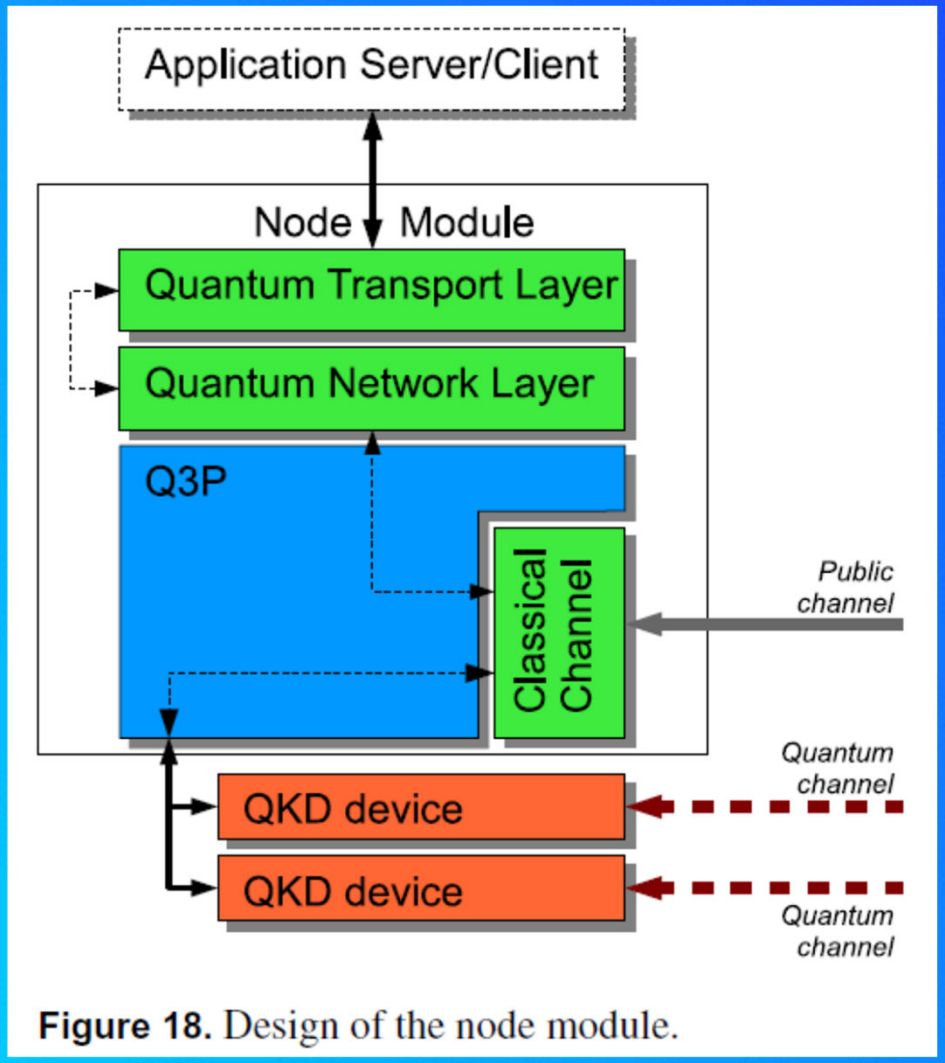
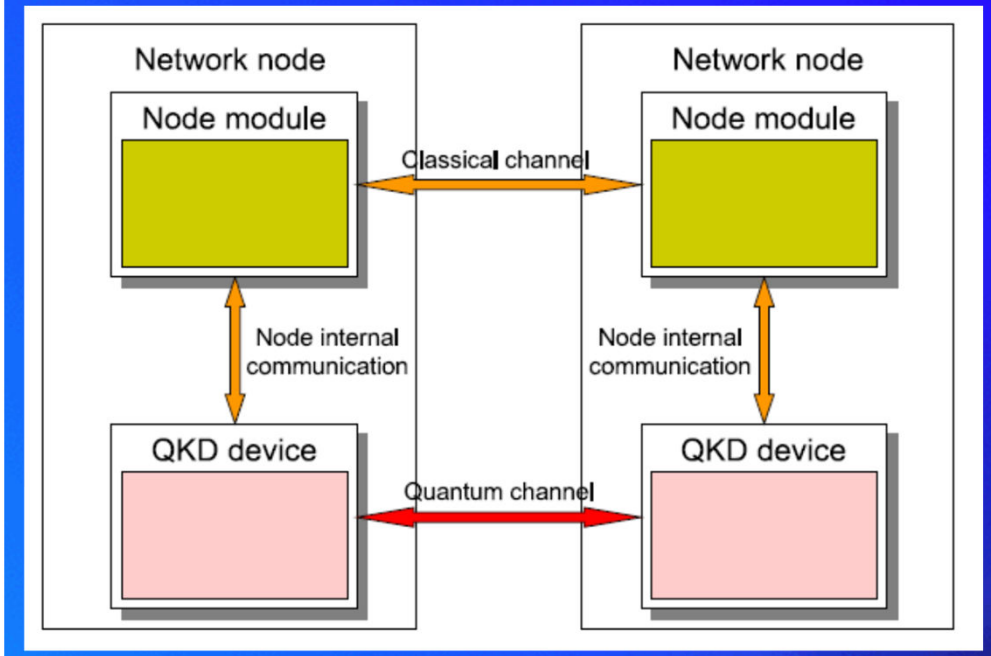
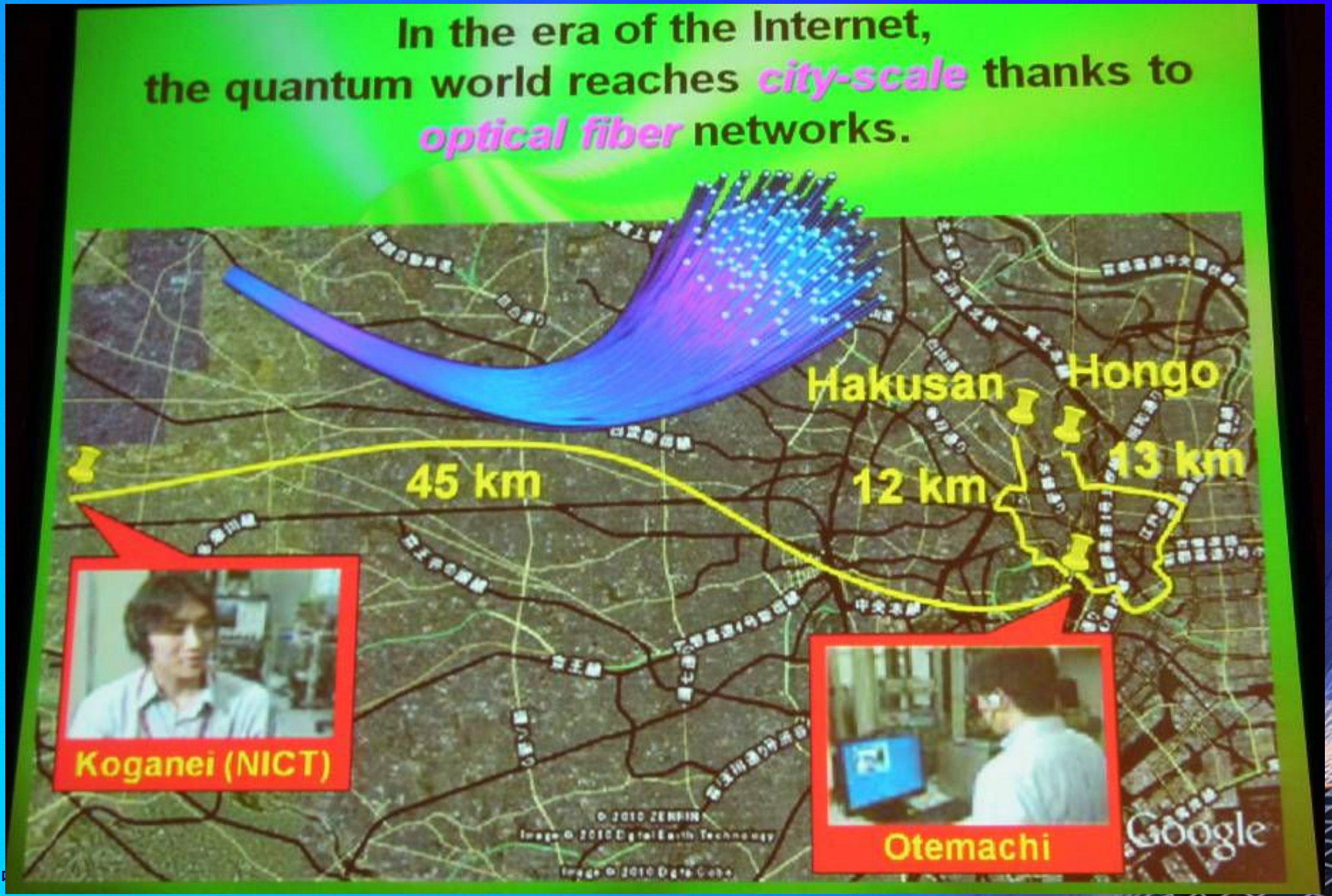


Figure 18. Design of the node module.



Tokyo QKD network



NiCT

Empowered by Innovation

NEC

MITSUBISHI

三菱電機

Changes for the Better

NTT

TOSHIBA

Leading Innovation >>>

Toshiba Research Europe Ltd (TREL)

IDQ

Id Quantique (IDQ)

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Austrian Institute of Technology

IQI

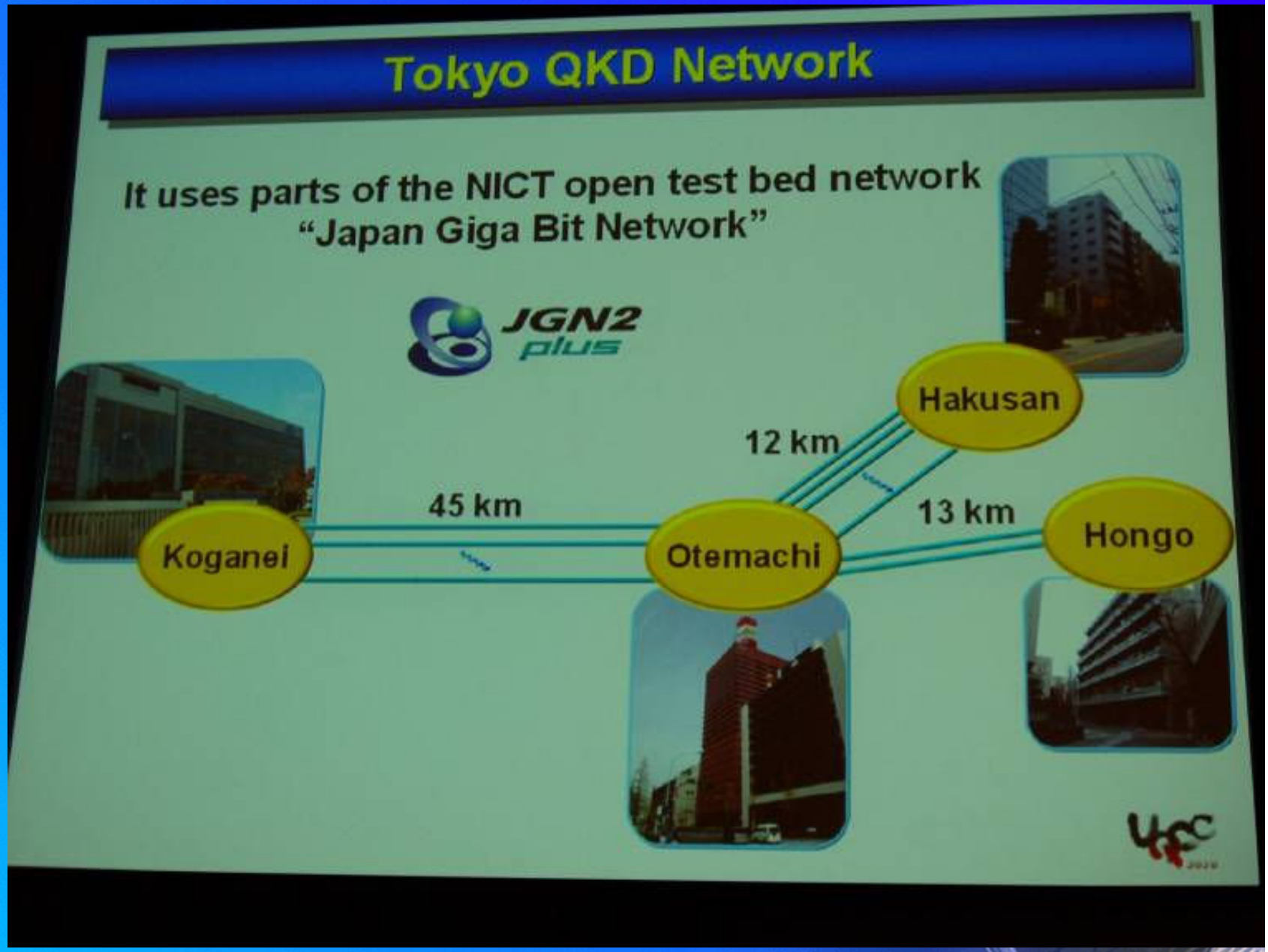
Institute of Quantum Optics and Quantum Information

universität wien

University of Vienna

All Vienna

连接点



东京网络基于日本的一个光纤实验床，有6个节点，3个在Koganei，2个在Otemachi，1个在Hongo

Tokyo QKD Network网络拓扑、距离和损耗

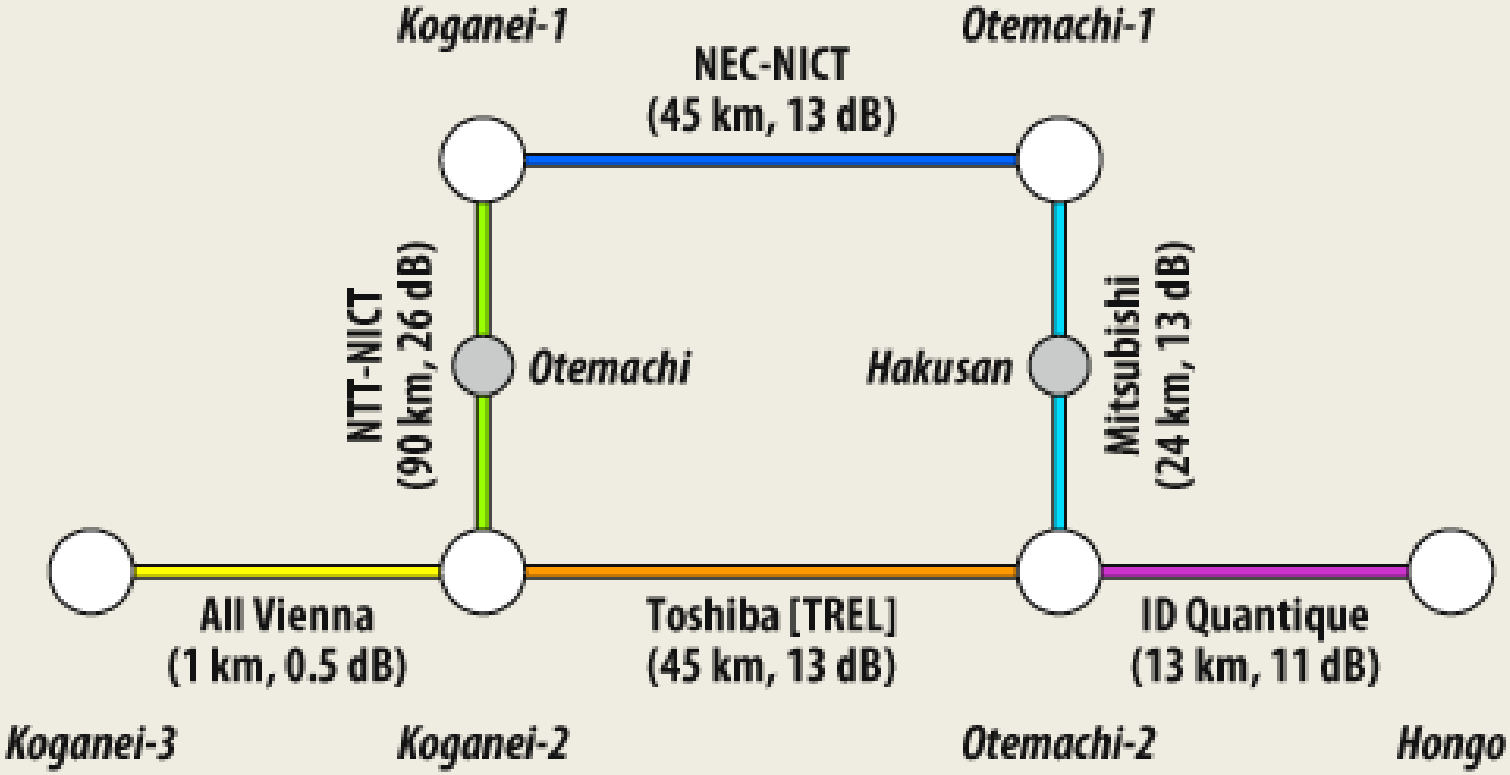


Fig. 3 Topological Map of the Tokyo QKD Network

NEC, Mitsubishi Electric, NTT, NICT, Toshiba Research Europe Ltd. (UK)

ID Quantique (Switzerland) All Vienna (Austria)

网络架构

- 基于JGN2plus（Japan's Gigabit Network ）
- 星形结构

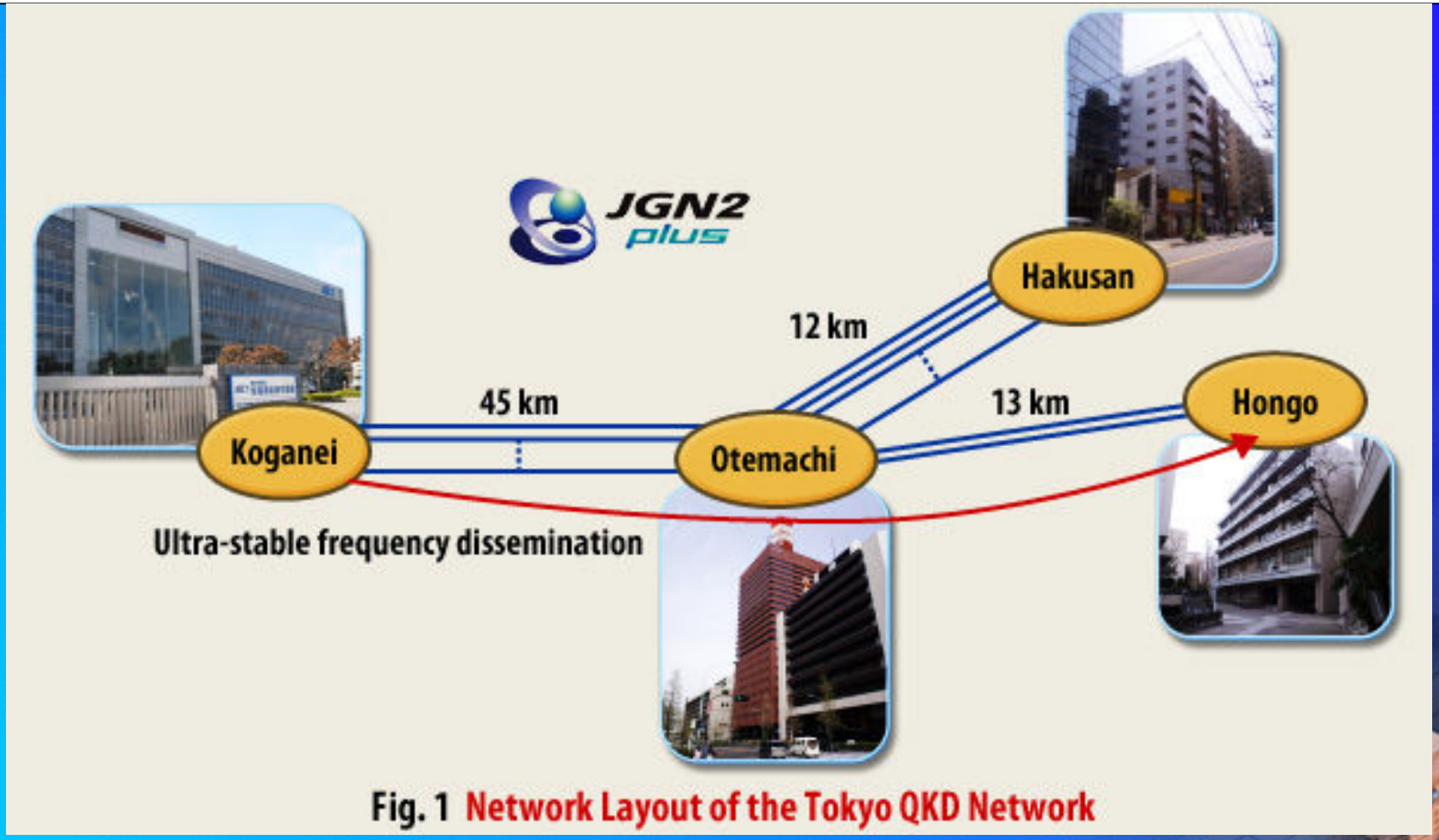


Fig. 1 Network Layout of the Tokyo QKD Network

Network Layer结构

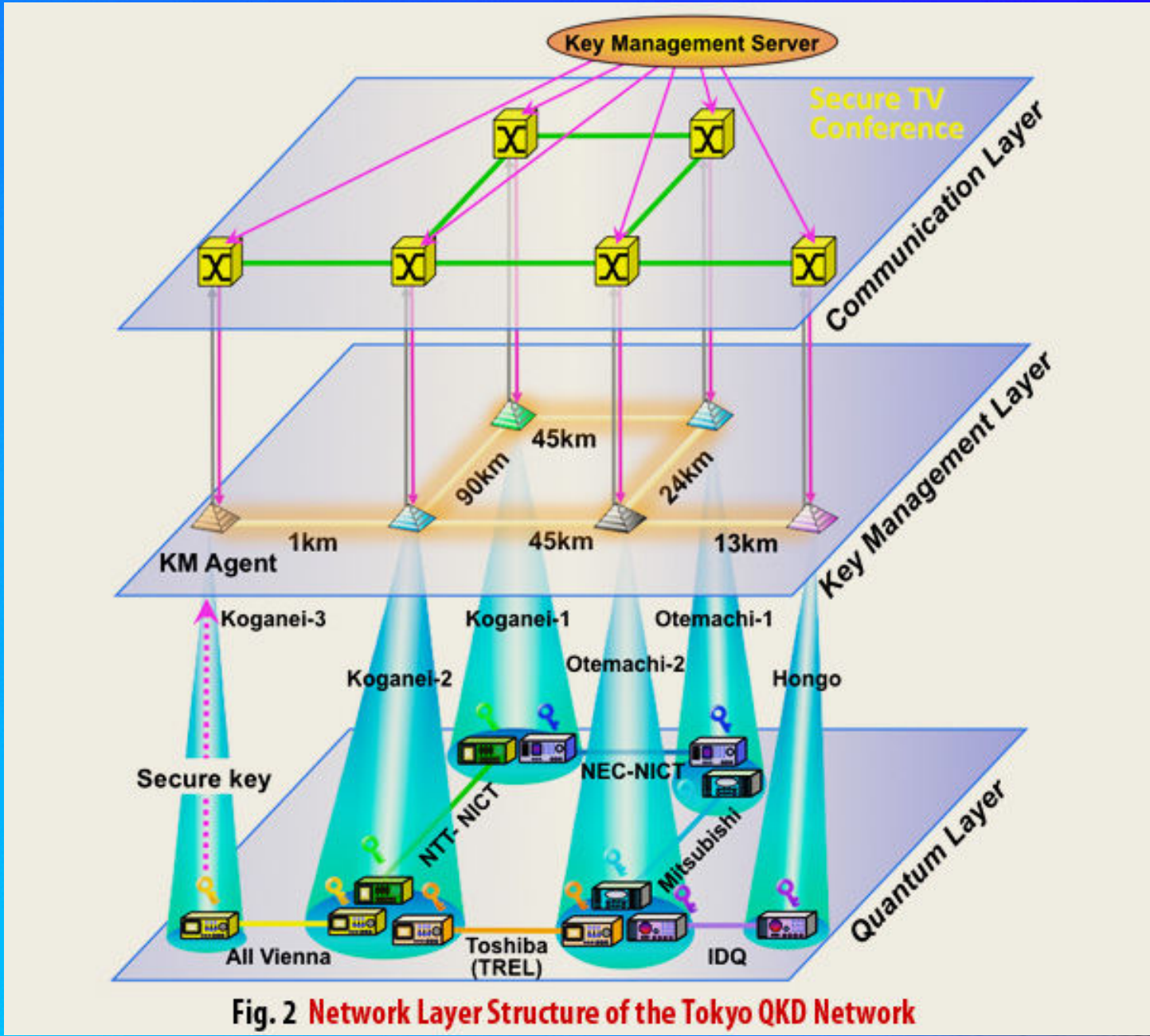
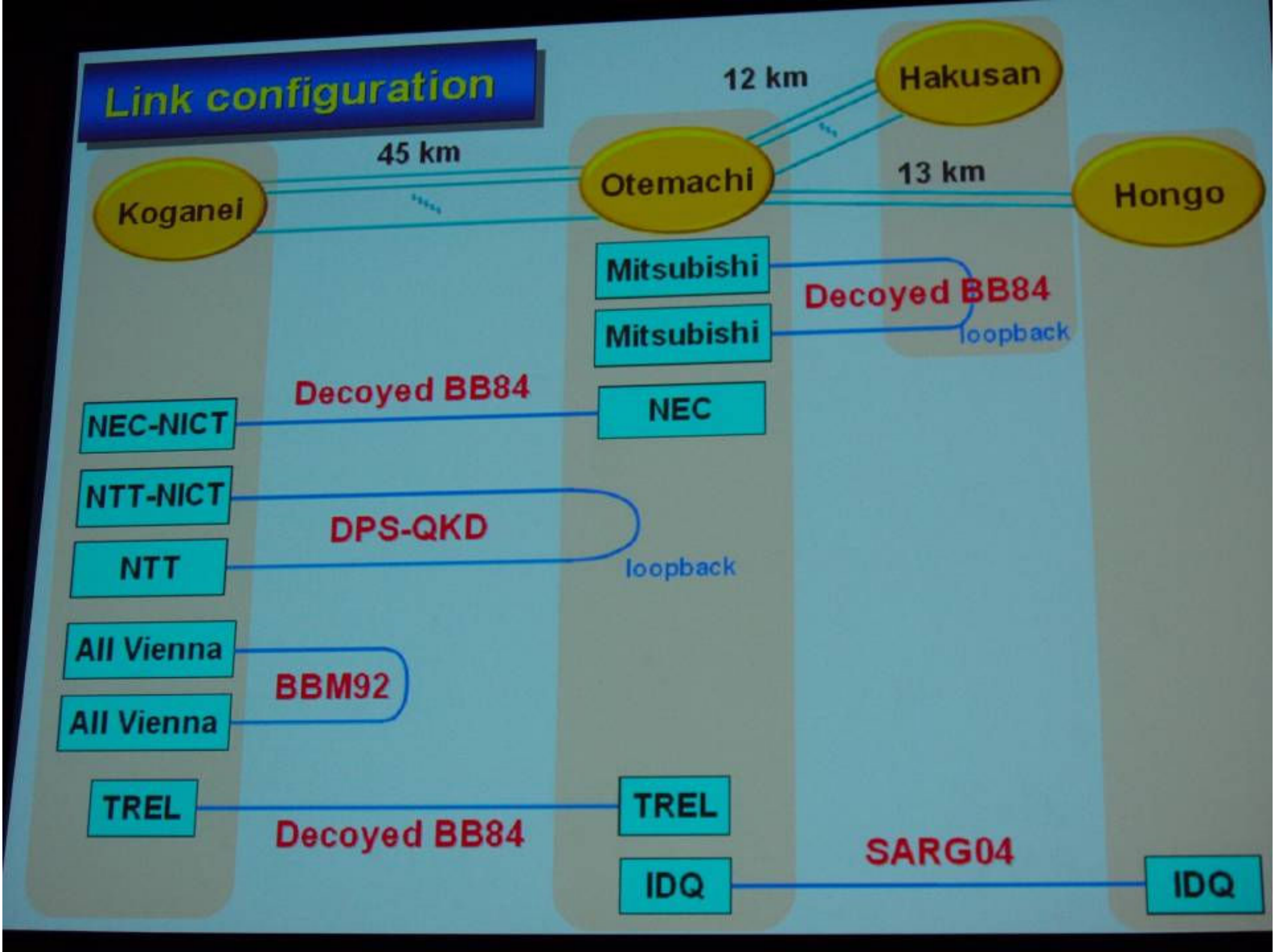
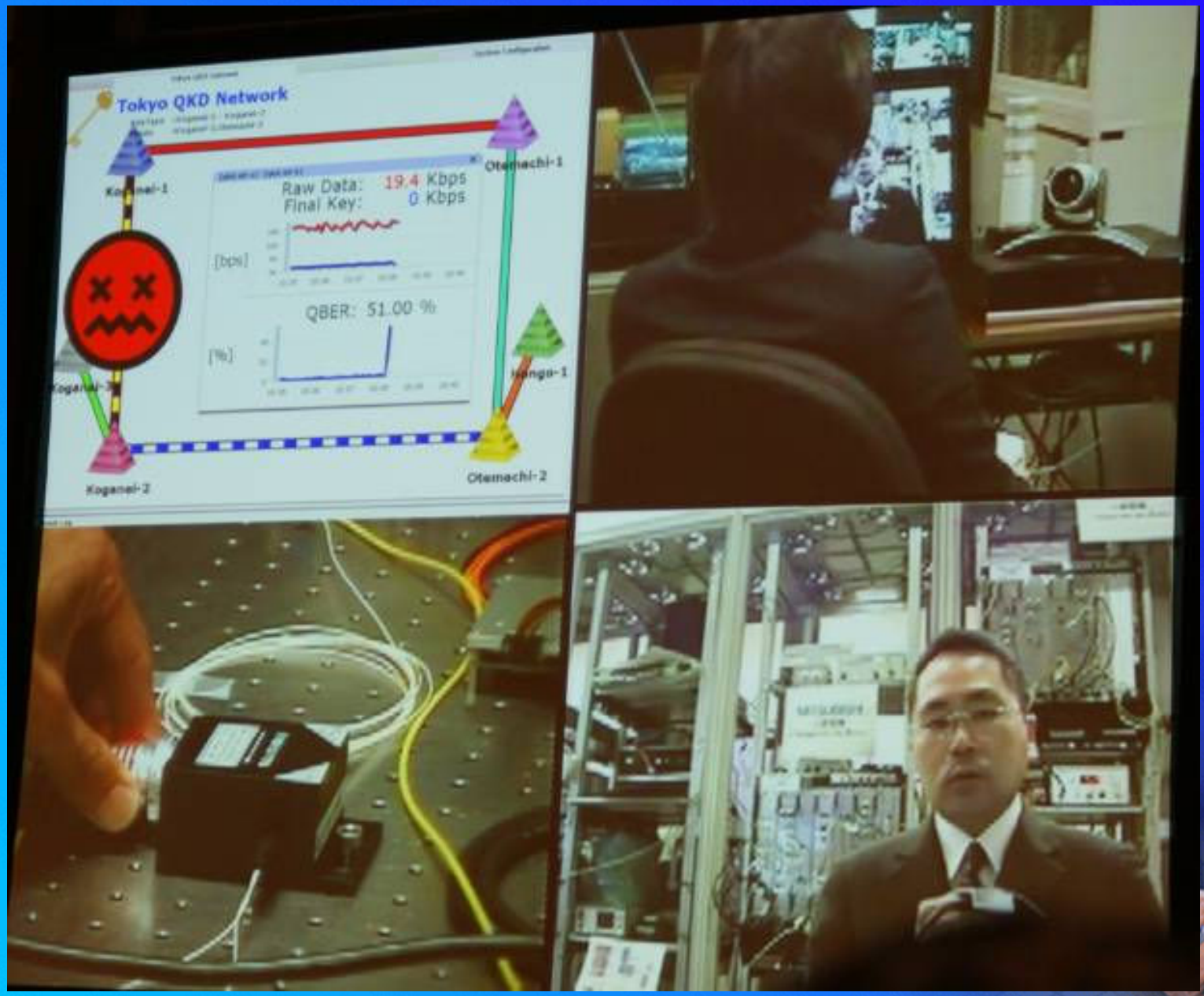


Fig. 2 Network Layer Structure of the Tokyo QKD Network


Link configuration
12 km
Hakusan
45 km
Otemachi
13 km
Hongo
Koganei
Mitsubishi
Mitsubishi
Decoyed BB84
loopback
Decoyed BB84
NEC-NICT
NEC
NTT-NICT
DPS-QKD
NTT
loopback
All Vienna
BBM92
All Vienna
TREL
TREL
Decoyed BB84
SARG04
IDQ
IDQ

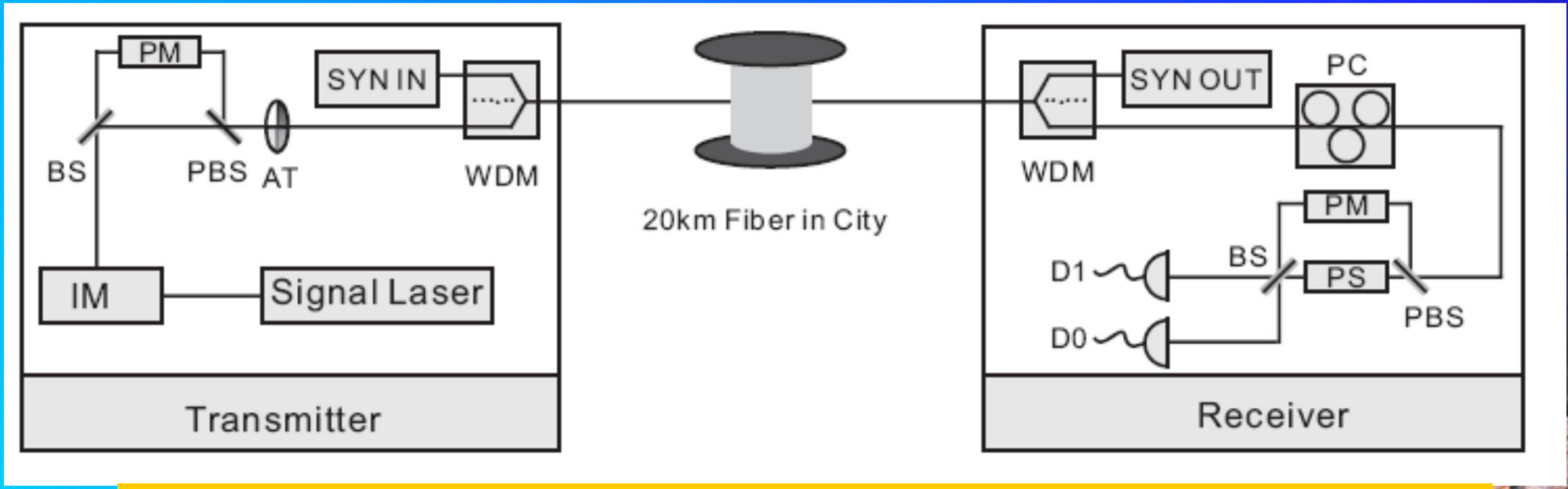
Tokyo QKD Network视频会议演示



3节点光量子电话网络

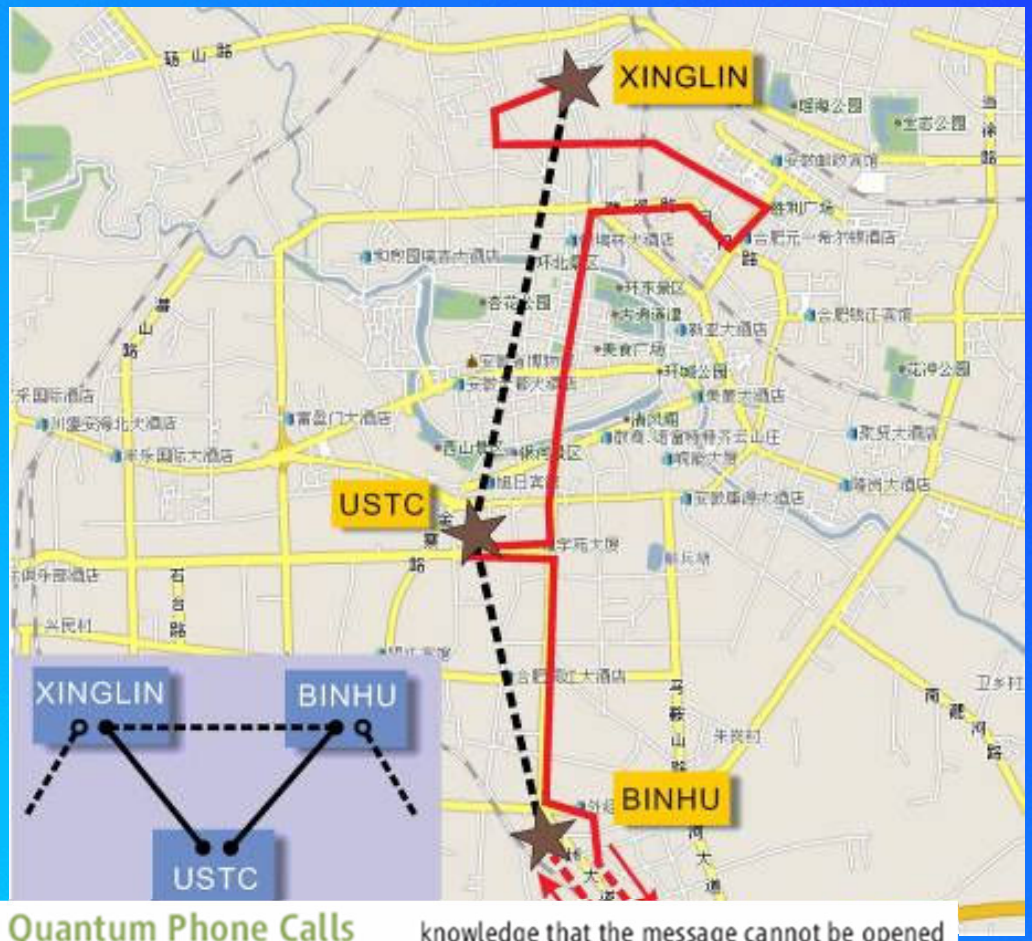
- 极化编码
- **4 MHz**
- **Decoy BB84**
- 可信中继架构
- 任意两节点通信距离≥**20 km**
- 信号和诱骗态脉冲**: 1550nm;** 同步脉冲**:1310 nm** 使用**WDM**

- 相位涨落的实时稳相
- 最终成码率≥**1.5kbps**
- 无条件安全，考虑了有限长度的密钥统计涨落。



T.-Y. Chen *et al.*, *Optics Express* Vol. 17, Iss. 8, pp. 6540–6549 (2009).

3节点光量子电话网络



- 任意两节点间的量子电话
- 任意节点对于另外两个节点的加密广播

physicsworld.com News & Analysis

Applications

China creates quantum network

Researchers in China claim to have built what they say is "the world's first quantum cryptography network for telephony". They have used the network to send completely secure telephone messages between three nodes located in Hefei, Anhui Province, in the east of the country. They say that the new system is better suited to real-world applications than networks developed by rival researchers.

Quantum cryptography exploits the principles of quantum mechanics to create keys for encoding and decoding messages with complete security. These keys are made up of the quantum states of subatomic particles, which means that an eavesdropper who tries to observe the keys will alter them and therefore reveal their presence. Several firms, such as Toshiba and the start-up firms id Quantique and MagiQ Technologies, have built commercial quantum cryptographic devices but usually these are limited to sending encrypted data between two fixed points.

The Chinese network, developed by Jianwei Pan and colleagues at the University of Science and Technology of China, involves three nodes connected in a chain by two 20 km-long commercial fibre-optic cables. Quantum keys consisting of photons with varying phase are shared between the adjacent nodes. Pan and colleagues claim to have used their network to send telephone messages in real time between three users as well as broadcast voice messages from one user to the other two (*Optics Express* 17 6540).

According to Pan's colleague Zeng-Bing Chen, the network has a number of advantages over quantum-cryptographic networks built in other countries because it uses "decoy" photon pulses. He points out that not only do the decoy pulses make the network more secure – by preventing eavesdroppers siphoning off the excess photons generated by imperfect single-photon sources – but they also allow faster key generation and offer potentially longer distances between nodes – up to some 100 km, compared with 30 km for rival technologies. In addition, he says that the equipment used at each node is compact, cheap – costing about €50 000 – and reliable.

However, Christian Monyk, project manager of the European-Union funded Secure Communication based on Quantum Cryptography consortium, which displayed a six-node quantum-cryptography network in Vienna last year (see *Physics World* November 2008 p10), believes the Chinese set-up is not really a network because messages cannot be rerouted if faults occur. He also says that quantum key distribution in the Chinese network is integrated into the telephony applications and so other kinds of secure data transmission – such as document exchange – would require the development of new apparatus, whereas key exchange in the Austrian network is application independent.

Chen says that quantum-key exchange and applications are in fact completely independent in his group's network. He believes that the technology could be used commercially within two or three years, but that the size of the market will depend on further increasing key-generation speeds and extending the maximum distance between links.

Edwin Cartlidge

Coded conversation
The quantum network in Hefei, China, allows secure communication down 20 km fibre-optic cables.

Physics World的报道

Quantum Phone Calls

Certain conversations or transactio
meant to be private. Yet despite th
of digital communication in one fo

有了这样的演示，量子隐私进入千家万户不会是很遥远的未来。

mechanics closes that loophole
Sharing quantum mechanically–en
photons can provide a secure key
to encrypt and send a message, sa

knowledge that the message cannot be opened by an eavesdropper, at least not without alerting you to the breach. Chen *et al.* demonstrate a quantum key distribution protocol in a real-world application scenario, with the quantum uted over a network consisting of ons linked by 20 km of commercial er. The generated keys can be used tely in the context of encrypted real-telephone conversations between the separated stations. With such a demonstration, quantum privacy in your own home may not be a too distant prospect. — ISO

Science的报道

T.-Y. Chen *et al.*, *Optics Express* Vol. 17, Iss. 8, pp. 6540–6549 (2009).

5节点星型量子密钥分配网络系统

全通型量子通信网络

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

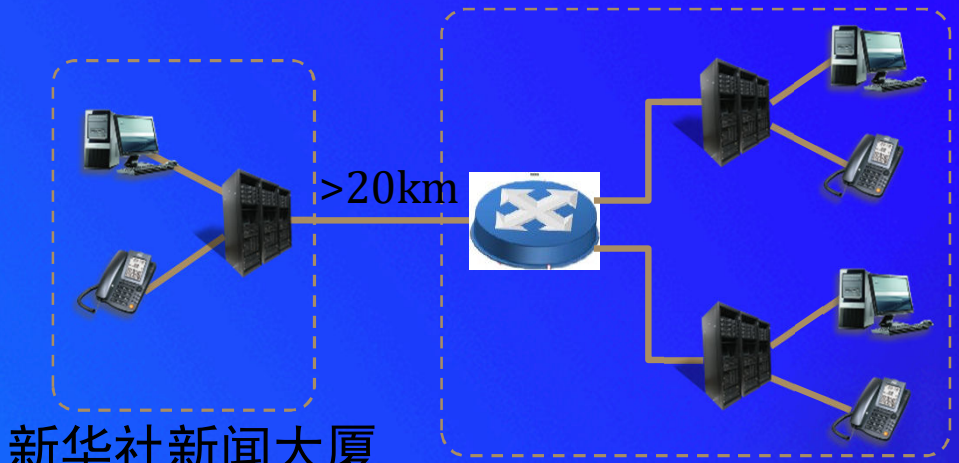
中国科学技术大学 陈凯

实用化城域量子通信网络

合肥全通型城域量子通信网络

Chen *et al.*, Opt. Express 17, 6540 (2009)

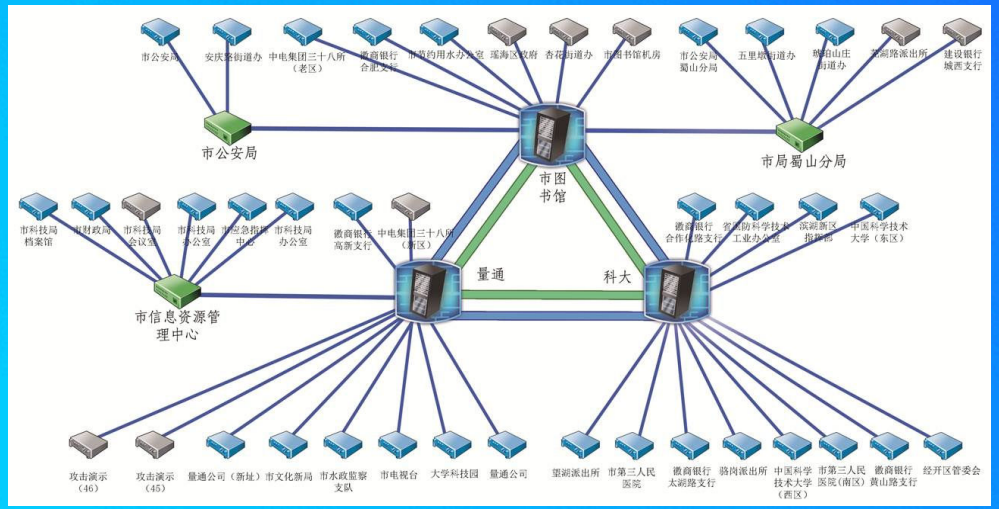
Chen *et al.*, Opt. Express 18, 27217 (2010)



新华社新闻大厦

新华社金融信息交易所

金融信息量子通信验证网(2012)



合肥城域量子通信试验示范网
(46个节点, 2012年)

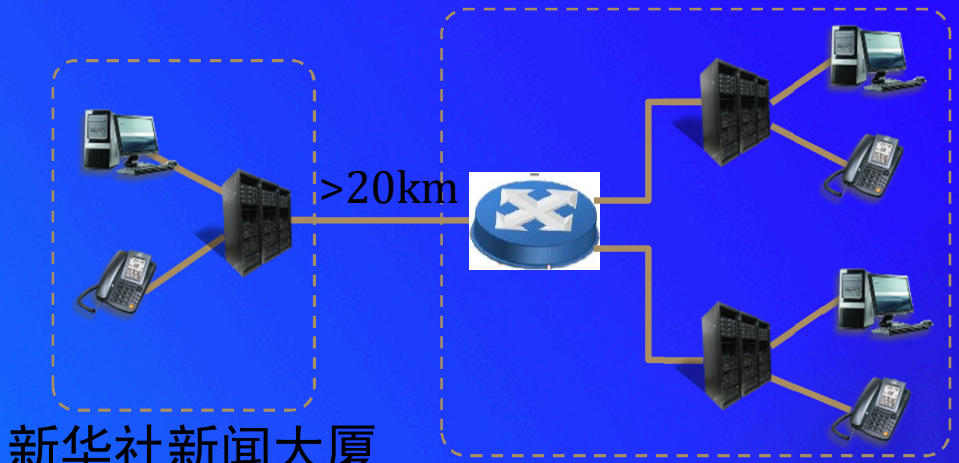
系统集成

实用化城域量子通信网络

合肥全通型城域量子通信网络

Chen *et al.*, Opt. Express 17, 6540 (2009)

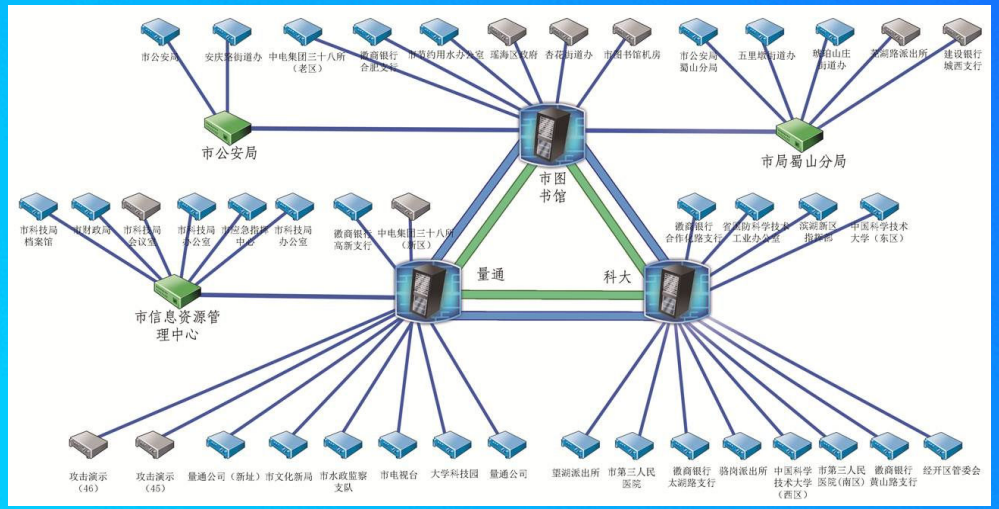
Chen *et al.*, Opt. Express 18, 27217 (2010)



新华社新闻大厦

新华社金融信息交易所

金融信息量子通信验证网(2012)



合肥城域量子通信试验示范网
(46个节点, 2012年)

第四章 量子通信

1. 保密通信
2. QKD基本原理
3. BB84协议过程
4. QKD安全性
5. 诱骗态(Decoy-state QKD)
   - ① Decoy QKD原理
   - ② 实用Decoy QKD
   - ③ Decoy QKD实验
6. QKD的现实安全性
   - ① 探测端的安全性→MDI-QKD
   - ② 设备无关的→ DI-QKD
7. 量子隐形传态(Quantum Teleportation) [原理、实验]
8. 量子纠缠交换(Entanglement Swapping)
9. 量子通信网络
10. **量子通信商用公司**
11. 量子通信发展与实用化QKD之路

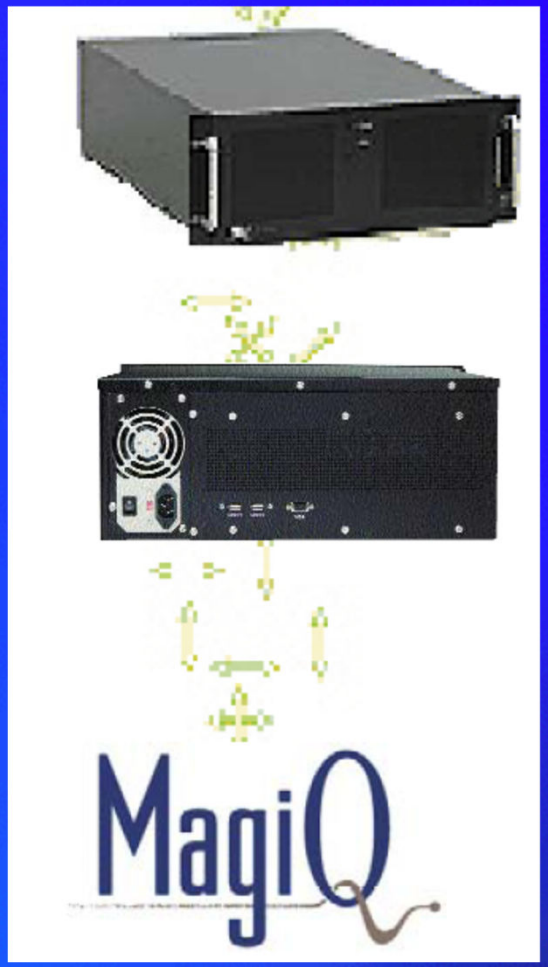
商用QKD产品

MagiQ

id Quantique

MagiQ

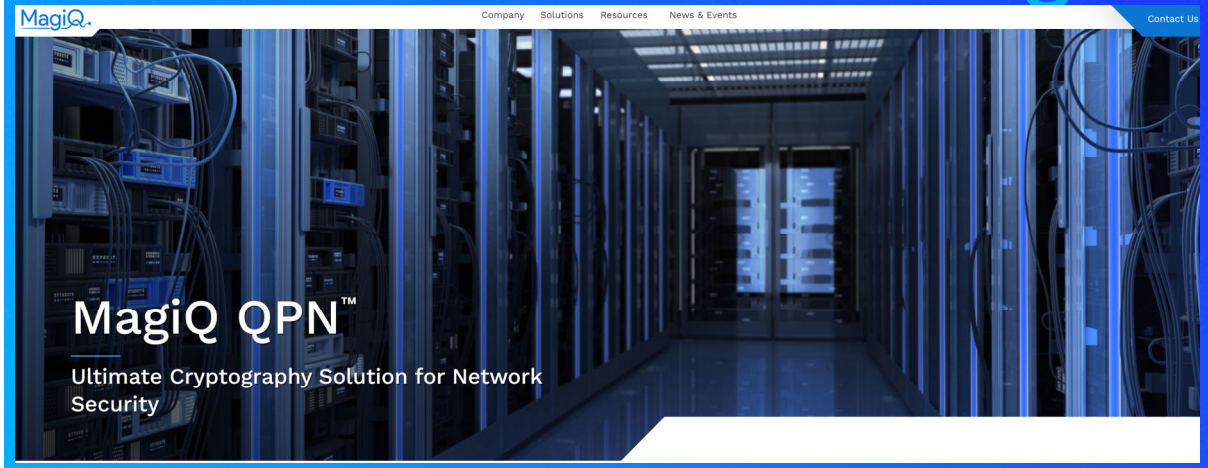
- 1999建立于美国，目前设有Boston总部和纽约Office。
- 大致从2008年起建立了MagiQ Research Labs，与US Army, DARPA, NASA以及与包括世界500强的多个公司进行联合研究。

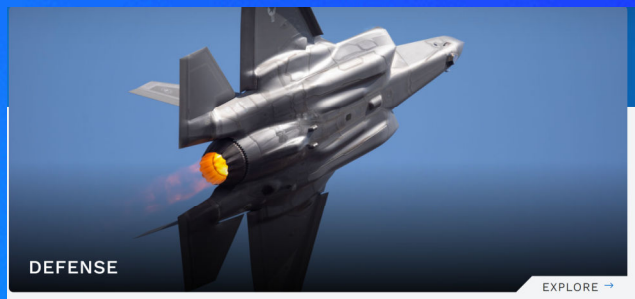


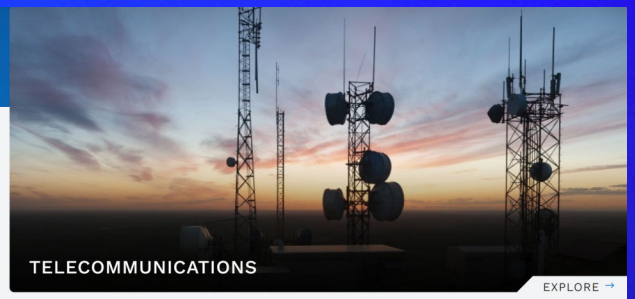
MAGIQ QPN™ 8505

Army DARPA JTRS NASA Navy

MagiQ







Army DARPA JTRS NASA Navy

中国科学技术大学 陈凯

MagiQ

MagiQ QPN™: State of the Art Quantum Cryptography

MagiQ QPN is a market leading Quantum Cryptography solution that delivers advanced network security and fool-proof defense against the numerous cryptographic key distribution and management challenges.

Keys generated and disseminated using QPN quantum cryptography consist of truly random characters that are distributed based upon the laws of quantum mechanics, which guarantees that **keys cannot be intercepted during the key exchange session.** Therefore, MagiQ QPN provides security that will remain secure against future advances in algorithms, computational power, hardware design, and even quantum computing.

How it Works | **Who Needs It?** | **Features & Benefits**

Protecting **financial information** is one of the highest priorities of corporations and entities involved in financial management and securities exchange. With MagiQ QPN, financial organizations can secure their most critical communication links to prevent intrusion and data theft. MagiQ QPN supports a variety of network architectures and provides the cryptographic key exchange infrastructure to protect the information channels.

Storage area networks offer the promise of protecting corporate assets offsite by creating electronic copies of critical information for future retrieval. Encryption is used to protect the data link to the storage site (data in transit) and to protect the data at the site (data at rest). QPN guarantees high-security in storage area network applications to better meet customer security requirements now and for the future.

Military and Government

Hostile forces are a real and a continuous threat to government and military network security. QPN can safeguard against hackers and unwanted network security breaches by "trusted" insiders attempting to access highly-classified government and military information.

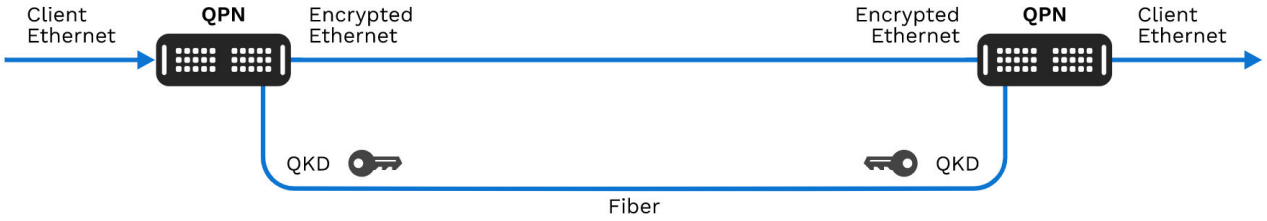
MagiQ QPN enables future-proof quantum security for other industries as well:

- R&D companies looking to protect trade secrets, intellectual properties, patents and business plans
- Voice and data service providers who need to secure confidential customer data and/or access to the network command channel
- Large Power Grid Providers open to terrorist or malicious hacking into the command and control channel interfaces

中国科学技术大学 陈凯

How it Works | **Who Needs It?** | **Features & Benefits**

The security of quantum cryptography lies in its ability to exchange the encryption keys with absolute security – Quantum Key Distribution. By sending the key bits encoded at the single photon level on a photon-by-photon basis, quantum mechanics guarantees that the act of an eavesdropper observing a photon irretrievably changes the information encoded on that photon. Therefore, the eavesdropper can neither copy nor clone, nor read the information encoded on the photon without modifying it; eavesdropping is instantly detected making this key exchange uncompromisingly secure.



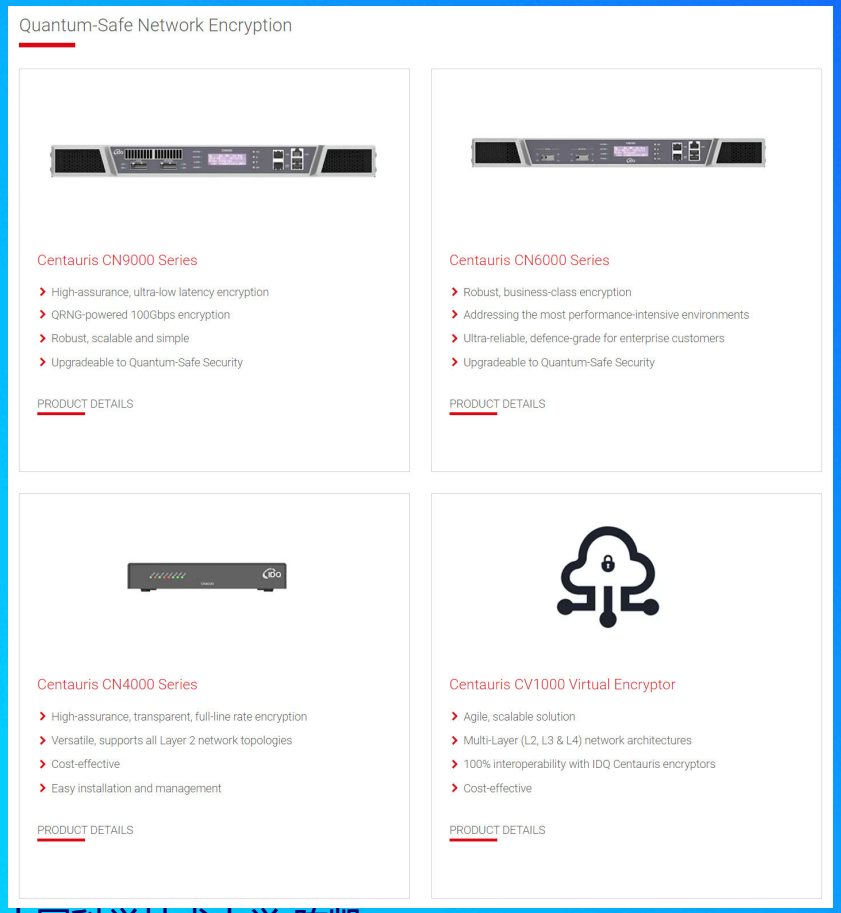
QPN implements the BB84 protocol, invented by Bennet and Brassard in 1984. This protocol assumes that the sender and recipient share an optical link (fiber) and a classical (non-quantum) unsecured communication channel, for example, a standard internet link.

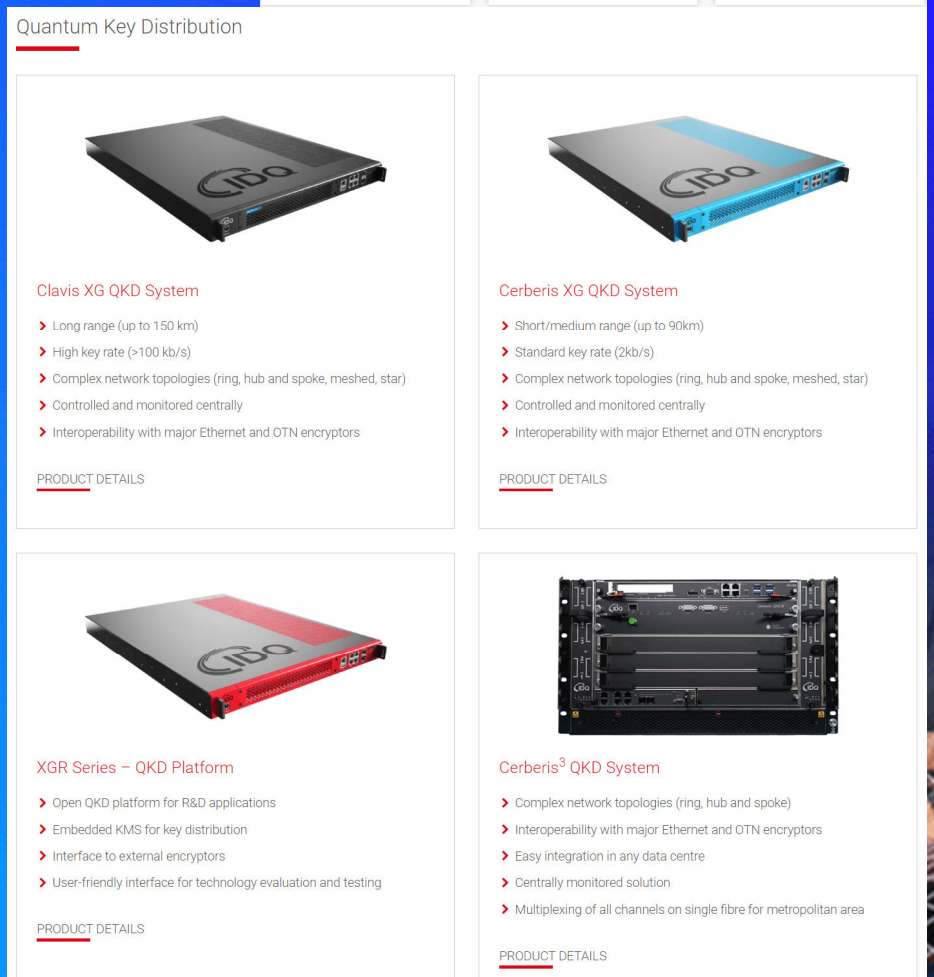
QPN sends photons over the fiber to create the secure keys between two QPN stations. A photon is an elementary light particle that has measurable properties, like polarization, which can be 'up' or 'down'. These can be used to encode and transmit a value of a bit from one QPN station to the other. The transmitting QPN station uses a truly random number generator to come up with the value of the bit encoded on the photon.

The security of the BB84 protocol is based on the fundamental Heisenberg Uncertainty Principle, that states that observing a photon (eavesdropping) does change its properties, i.e., in the presence of eavesdropping, the values of the received bits will differ from the values of the bits sent. This fundamental principal eliminates the ability of any eavesdropper to hide his/her 'footprints on the photon.

ID Quantique 产品

- id Quantique (IDQ) 在2001年建于Geneva
- 公司产品
  - Centauris Layer 2 Encryptors: High speed multi-protocol encryptors
  - Cerberis: A fast and secure solution of high speed encryption combined with quantum key distribution。典型的基于AES应用
  - Clavis^2: QKD for R&D Applications
  - 探测器，随机数发生器，短脉冲激光源等

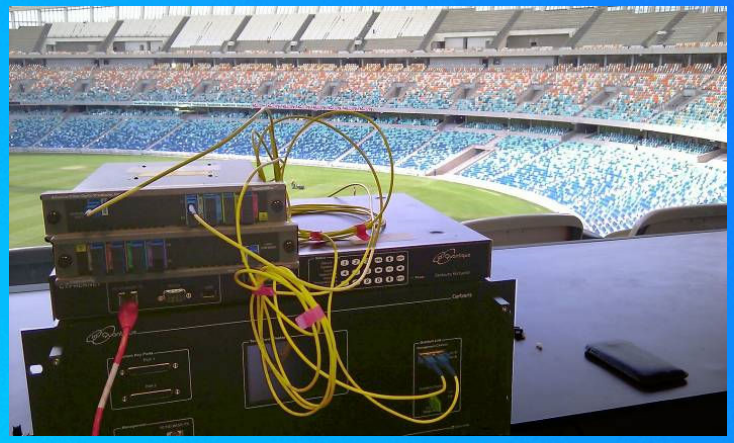




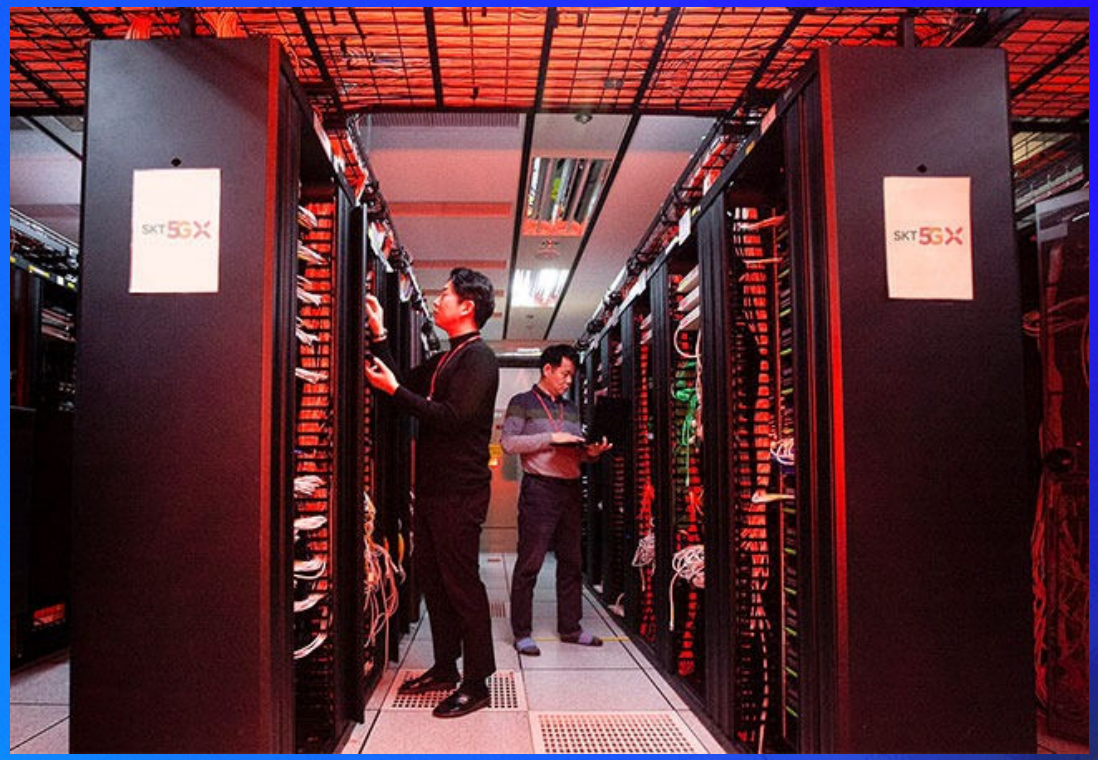
ID Quantique

2010 FIFA 世界杯

Durban, South Africa – The first use of ultra secure quantum encryption at a world public event，基于AES 256



2019 SK Telecom Continues to Protect its 5G Network with Quantum Cryptography Technologies



SK Telecom Continues to Protect its 5G Network with Quantum Cryptography Technologies

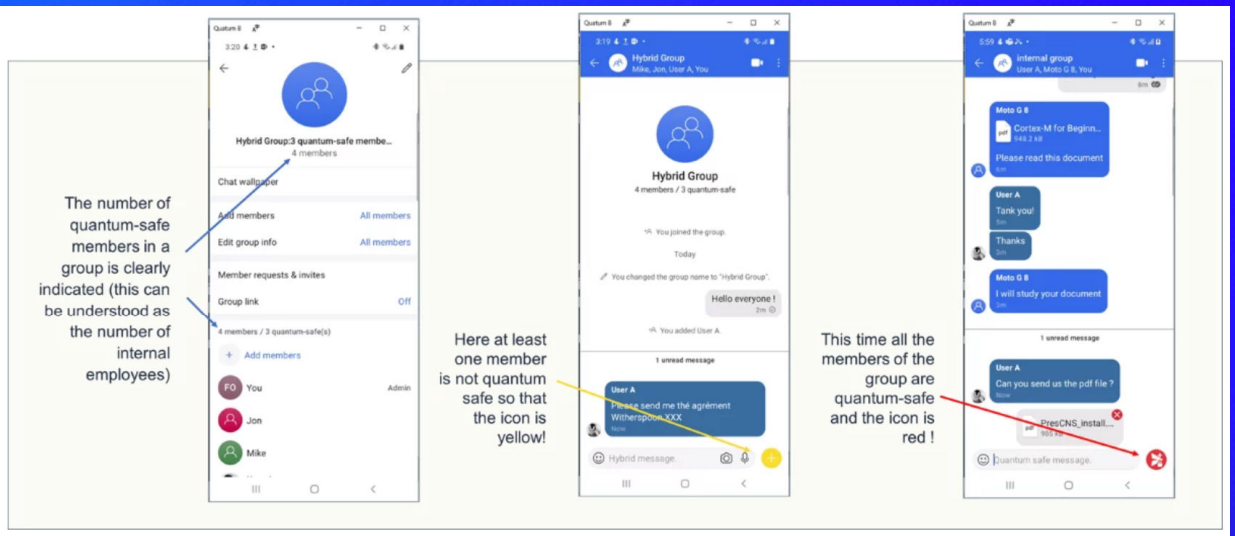
- SK Telecom applied Quantum Random Number Generator (QRNG) to the subscriber authentication center of its 5G network

- SK Telecom plans to apply Quantum Key Distribution (QKD) technology to the Seoul-Daejeon section of its LTE and 5G networks to prevent hacking and eavesdropping

- SK Telecom is playing a pivotal role in global standardization of QKD and QRNG technologies at ITU-T.

ID Quantique

Quantique and CryptoNext partner to deliver next-gen, quantum-safe messaging



The solution aims at enabling governments, enterprises and organizations of all types to manage sensitive communications for specific groups of people, such as executive teams, and/or specific projects.

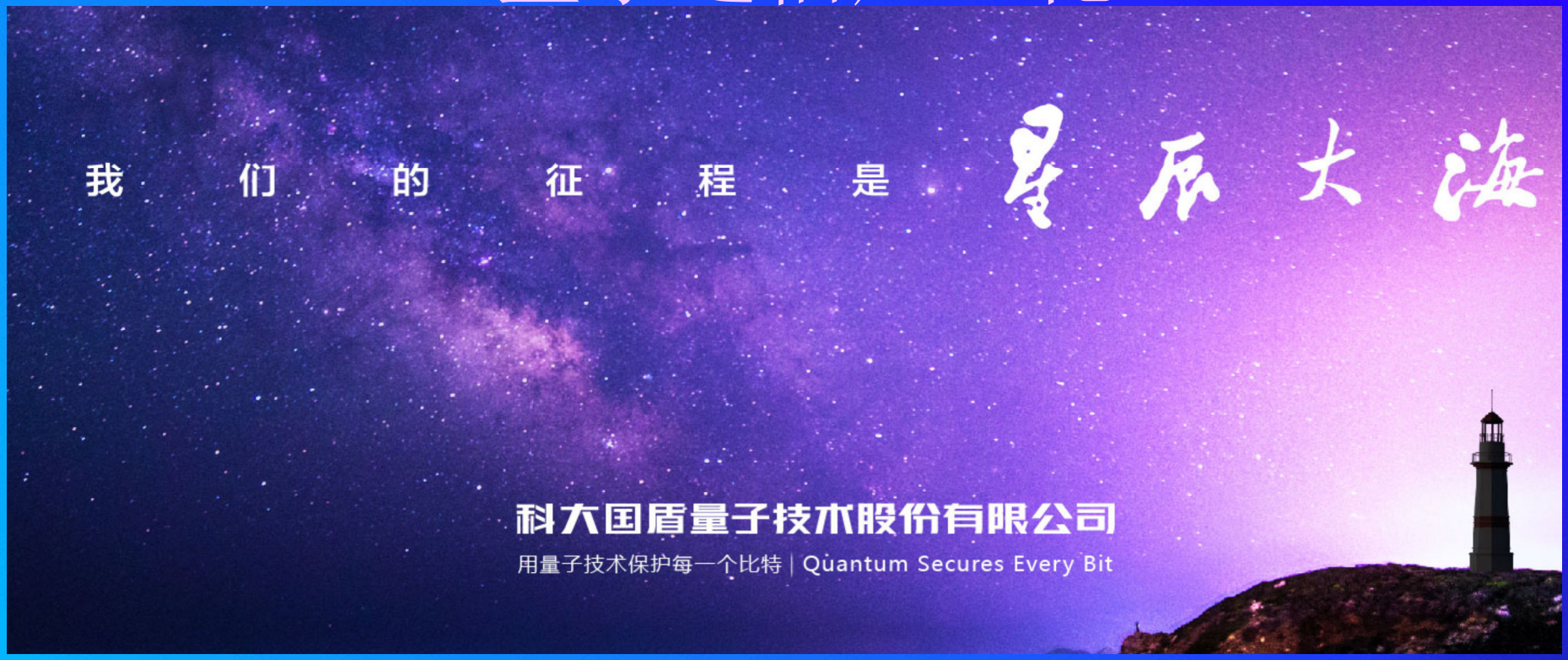
Telefonica, Fortinet & IDQ demonstrate the first Quantum-Safe IPVPN connection suitable for managed datacentre interconnect

7th October 2021

Telefonica, Fortinet and IDQ have jointly demonstrated the first Quantum-Safe IPVPN connection suitable for offering a fully managed datacenter interconnection service.

DISCOVER MORE

量子通信产业化



中国科学技术大学 陈凯

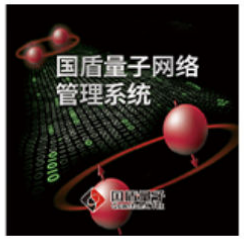
科大国盾量子技术股份有限公司
（QuantumCTek Co., Ltd.）

科大国盾量子技术股份有限公司
（QuantumCTek Co., Ltd.）

量子保密通信网络核心设备

量子安全应用产品

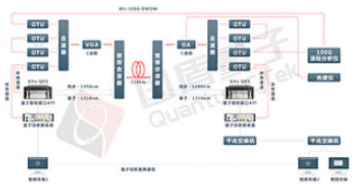
管控软件



核心组件

科学与科研仪器

大容量商用化超长距量子共纤传输应用



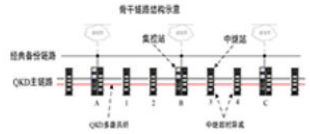
北京农商银行城域环网量子技术应用

交通银行企业网银用例建设

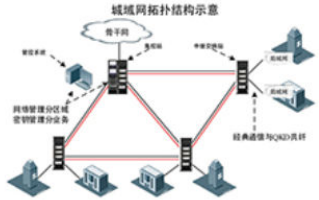
网商银行云上量子加密通信案例

工商银行异地数据千公里级量子加密传输应用

骨干网应用



城域网应用



局域网应用

政务应用

金融应用

中国科学技术大学 陈凯

国盾量子


国盾量子
QuantumCTek
首页
量子产品
解决方案
典型案例
旗下企业
QuantumCTek
用量子技术保护每一个比特
Quantum Secures Every Bit
开拓者 实践者 引领者
国盾量子
QuantumCTek
股票简称：国盾量子
股票代码：688027
不忘初心 光量未来
科大国盾量子技术股份有限公司首次公开发行股票并在科创板上市仪式
保荐机构（主承销商）：国元证券股份有限公司
二〇二〇年七月九日

科大国盾量子技术股份有限公司

易科腾 EQTINFO　国盾量子 QuantumCTek

EQR 2000-2　EQR 2000-4　EQR 3000-8　EQR 3000-12

量子安全加密路由器

量子安全加密路由器是结合量子保密通信技术与经典通信技术的高保密量子安全产品。该产品采用量子保密通信技术，结合设计理念和模块化可扩展的平台，凭借“安全可靠、性能强劲、一机多能、弹性扩展、轻松易维、绿色节能”六大特性，满足用户当前和未来各种业务部署的需求，为实现信息高安全传送提供智能而有弹性的设备平台。

国盾量子 QuantumCTek | SANGFOR 深信服科技

联合打造

量子安全SSL VPN

量子安全SSL VPN产品是结合量子保密通信技术与SSL VPN技术的一款高保密量子安全产品，该产品为科大国盾量子携手深信服科技推出的量子安全SSL VPN产品，具备量子密钥保护、全面安全、快速接入等特性。

国盾安全手机A2021H

国盾安全手机（A2021H）将量子保密通信技术融入到新一代智能5G终端，产品基于全隔离异构双系统和量子安全服务系统实现，与传统加密手机相比，其量子安全加密功能和安全操作系统在注重隐私保护的信息时代更具有应用价值。

关键特性

- 量子密钥高安全保护
- 自主安全操作系统
- 防盗无隐患
- 方便易用
- 5G先锋
- AI智能系统引擎

典型应用

- 移动通话
- 移动办公/作业
- 移动电子政务
- 物联网
- 移动支付

60+比特层叠版 •

8比特减重版 •

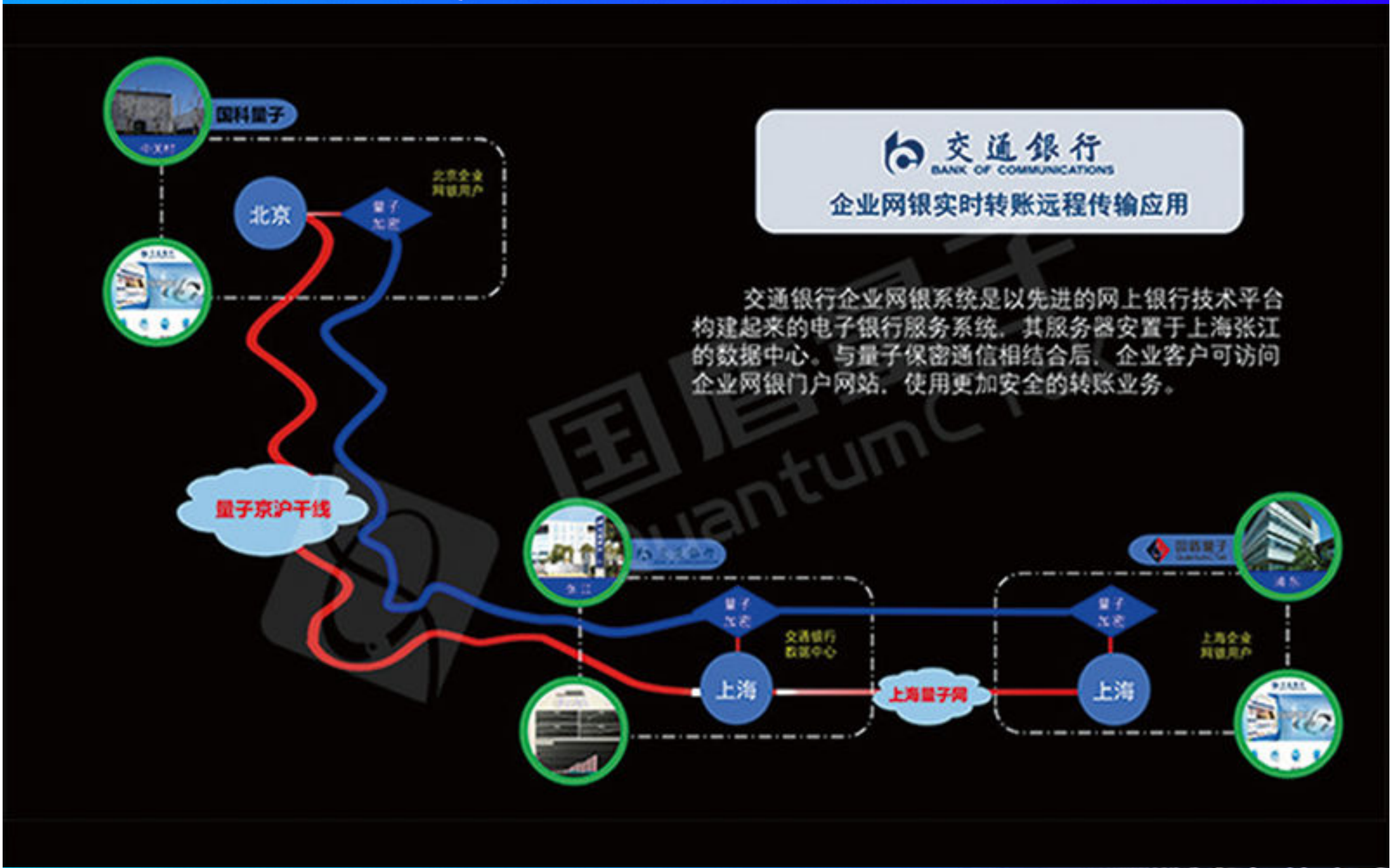
中国科学技术大学 陈凯

ez-Q™ Engine超导量子计算操控系统

科大国盾量子技术股份有限公司
（QuantumCTek Co., Ltd.）

中国科学技术大学 陈凯

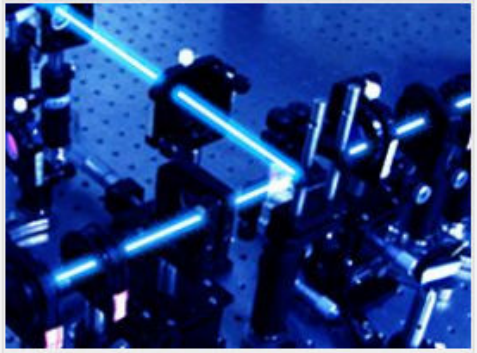
科大国盾量子技术股份有限公司
（QuantumCTek Co., Ltd.）



安徽问天量子科技股份有限公司

量子密钥分配终端

量子密码通信应用设备



量子密钥分配实验系统

激光器

中国科学技术大学 陈凯

第四章 量子通信

1. 保密通信
2. QKD基本原理
3. BB84协议过程
4. QKD安全性
5. 诱骗态(Decoy-state QKD)
   - ① Decoy QKD原理
   - ② 实用Decoy QKD
   - ③ Decoy QKD实验
6. QKD的现实安全性
   - ① 探测端的安全性→MDI-QKD
   - ② 设备无关的→ DI-QKD
7. 量子隐形传态(Quantum Teleportation) [原理、实验]
8. 量子纠缠交换(Entanglement Swapping)
9. 量子通信网络
10. 量子通信商用公司
11. **量子通信发展与实用化QKD之路**

量子通信的发展

地面量子通信实验在几百公里以上存在技术障碍

光纤量子信道

最小损耗：0.2dB/km

地面自由空间信道

地球曲率和大气衰减

空间量子通信

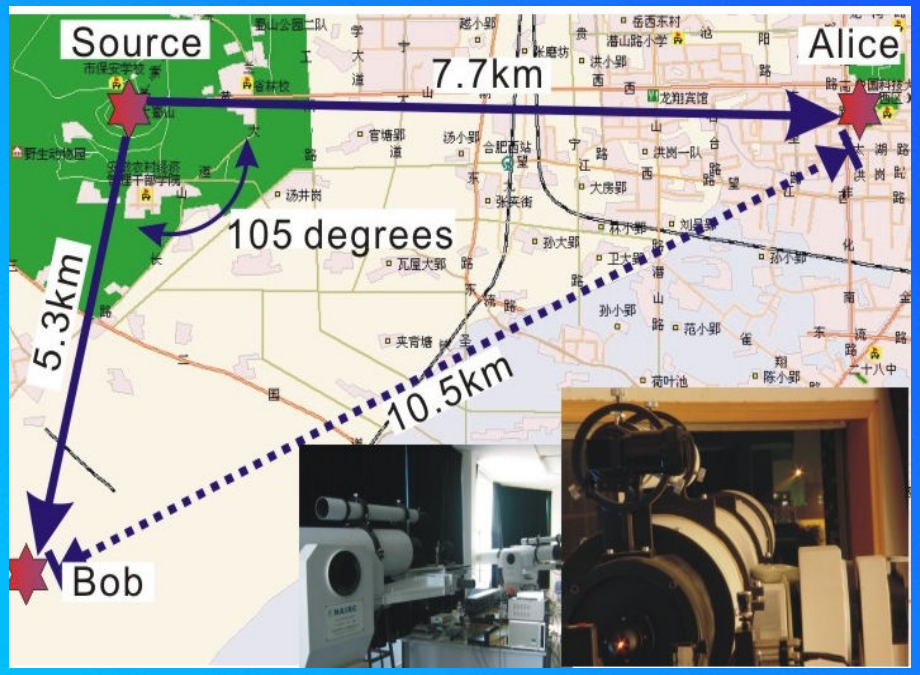
1、全球量子密钥分发网络

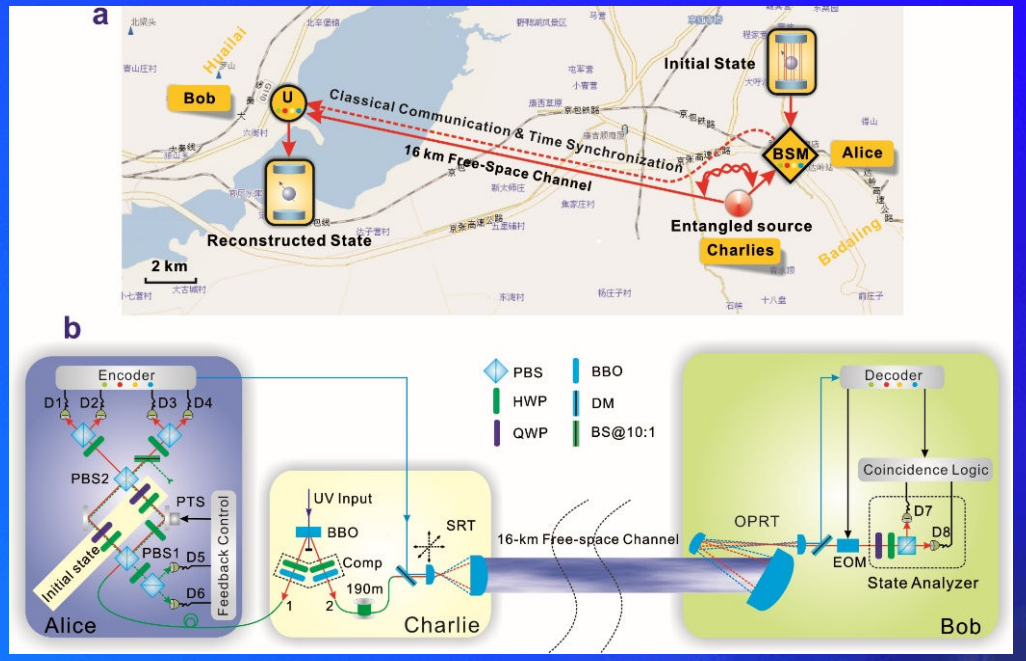
2. 在空间大尺度下的量子通信实现

Free-Space Quantum Communication

Phase 1:

Test the possibility of single photon and entangled photons passing through atmosphere





- Free-space quantum entanglement distribution ~13km

  Peng *et al.*, PRL 94, 150501 (2005)

- Free-space quantum teleportation (16km)
  - Scheme: Boschi *et al.*, PRL 80, 1121(1998)
  - Experiment: Jin *et al.*, Nature Photonics 4, 376 (2010)

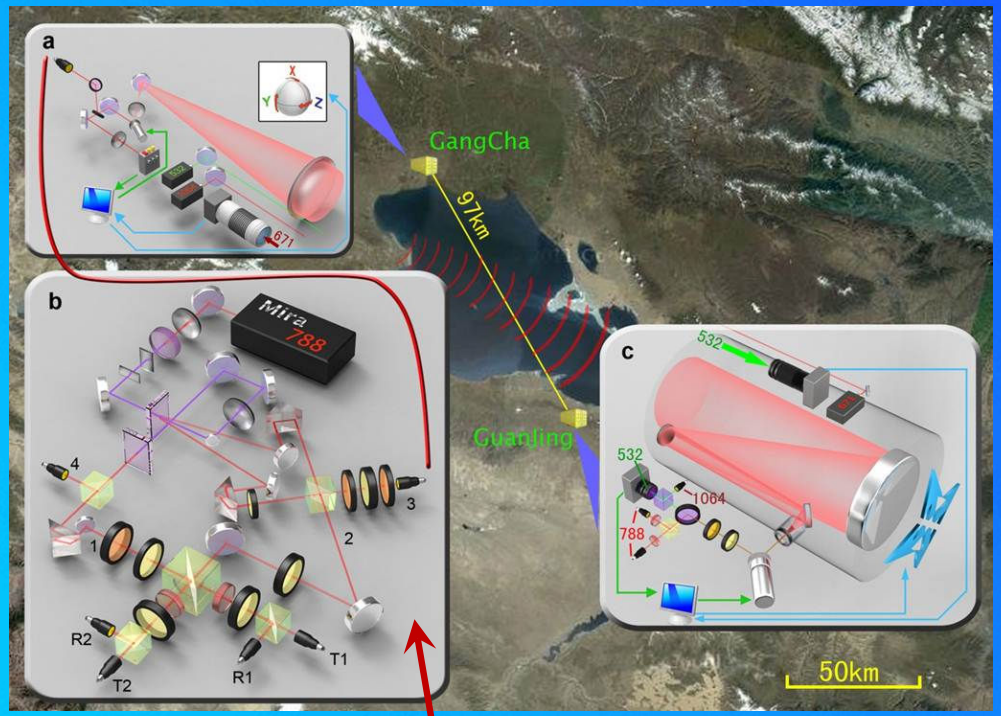
Well beyond the effective thickness of the aerosphere!

Free-Space Quantum Communication

Phase 2: Test the feasibility of quantum communication via high-loss ground-to-satellite channel

- Free-Space Quantum Teleportation (97km)

State	Fidelity
H	0.814±0.031
V	0.886±0.024
$+$	0.773±0.031
$-$	0.781±0.031
R	0.808±0.026
L	0.760±0.027



Four-photon quantum teleportation experiment

☑Entanglement source: 450000/s

☑Four-photon coincidence rate: 1500/s

high-brightness entangled photon source technology used in our 8-photon entanglement experiment

Channel loss: 35-53dB

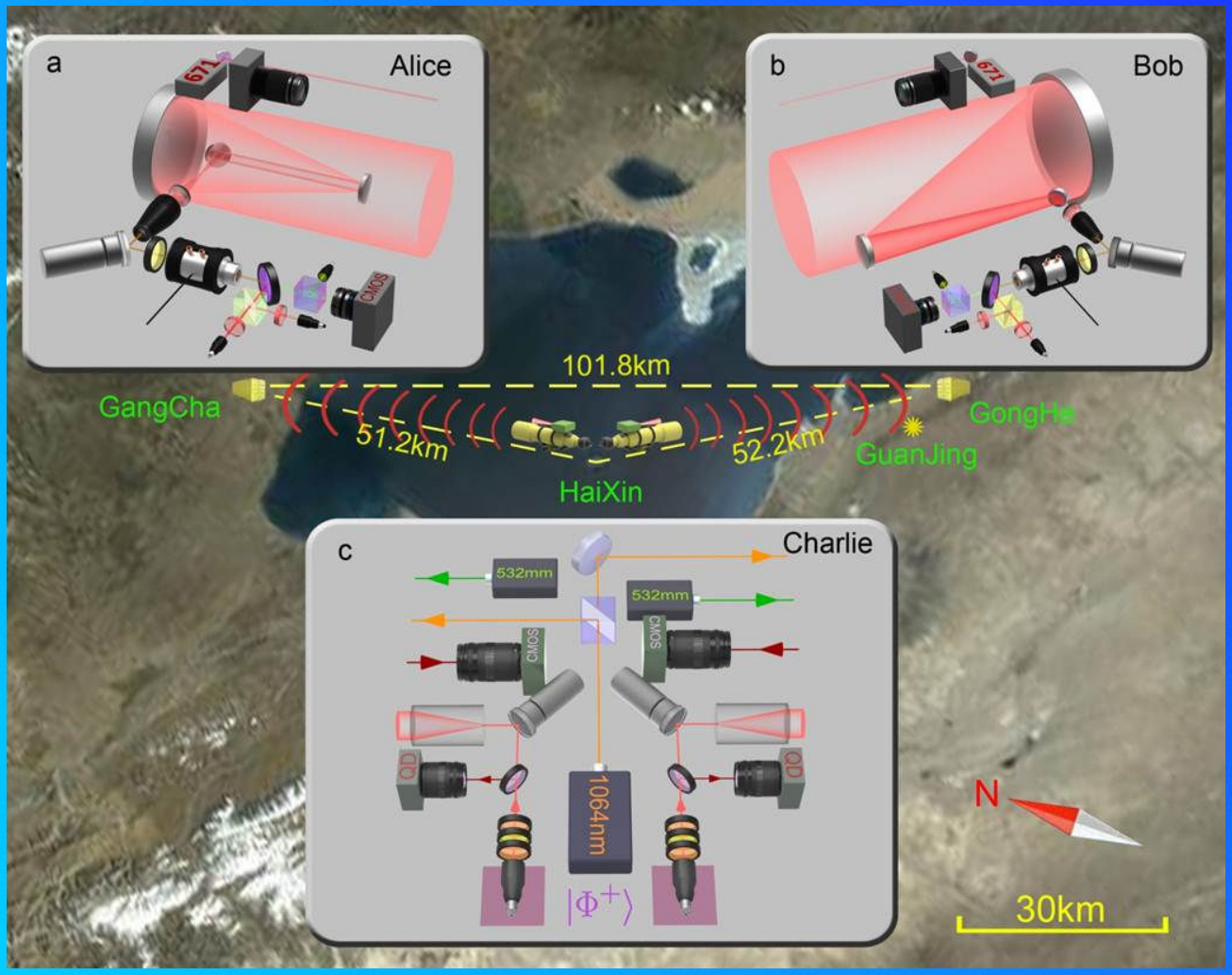
V. S.

Loss for an uplink of ground to satellite: 45dB

Free-Space Quantum Communication

- and Free-space quantum entanglement distribution (over 100km)

  Yin *et al.*, **Nature** 488, 185 (2012)



Violation of CHSH inequality:

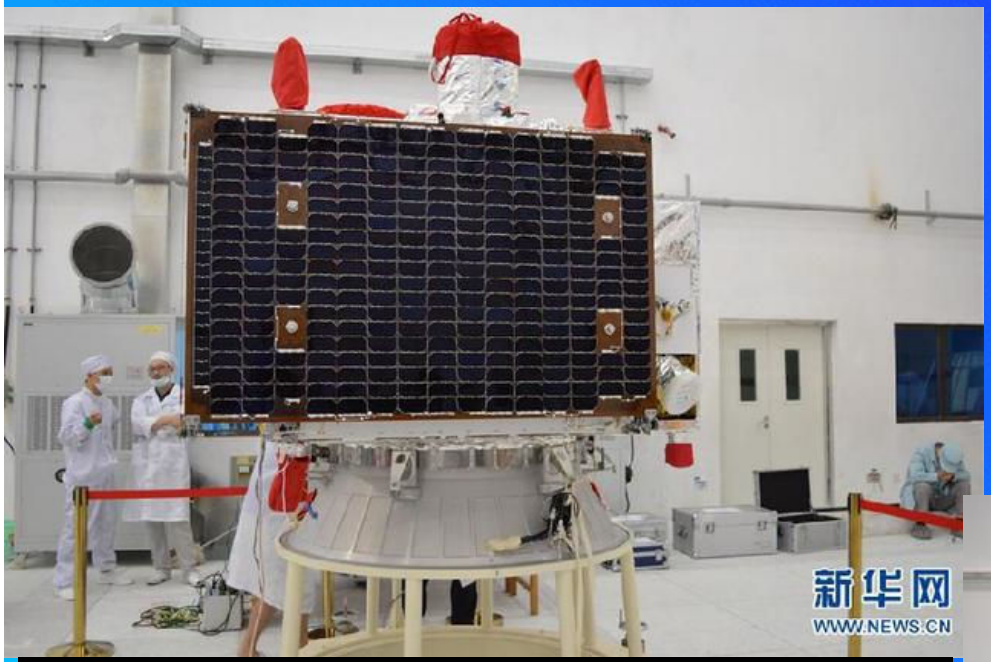
2.51 ± 0.21

Channel loss:
66-85dB

V. S.

Loss for two-downlink between satellite and two ground stations:
75dB

世界首颗量子卫星



“墨子号”量子卫星与地面站通信试验照片公布

“墨子号”量子卫星与地面站量子通信

世界首颗量子科学实验卫星“墨子号”成功发射

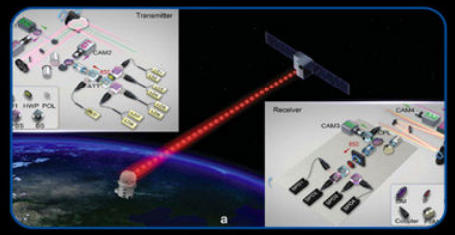
2017-08-10

热烈祝贺“墨子号”顺利完成
三大科学实验任务

中国率先掌握星地一体广域量子通信网络技术

01 千公里级星地双向量子纠缠分发及空间尺度量子力学非定域性检验

02 1200公里星地量子密钥分发

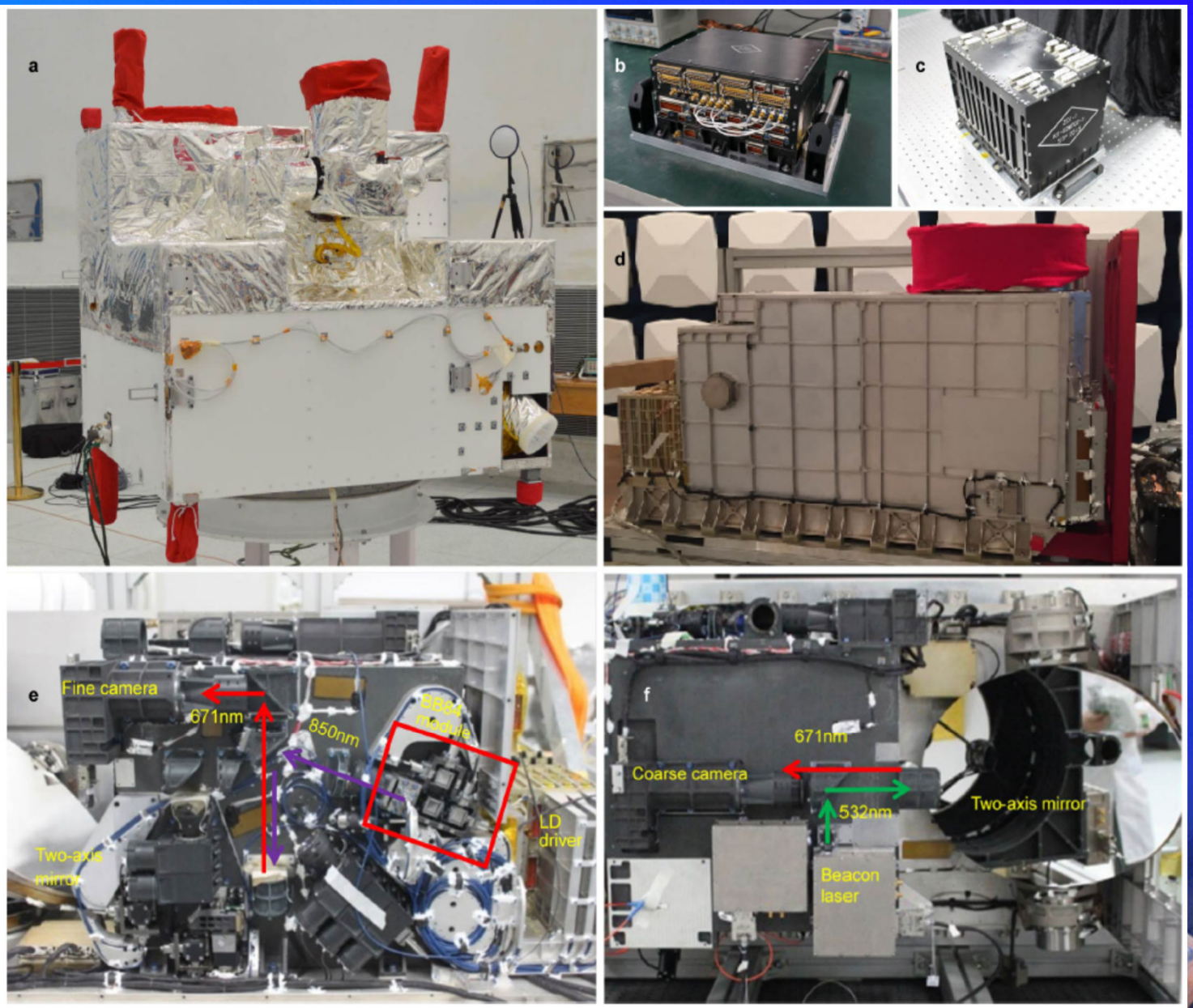


03 1400公里地星量子隐形传态

摘自国盾量子新闻

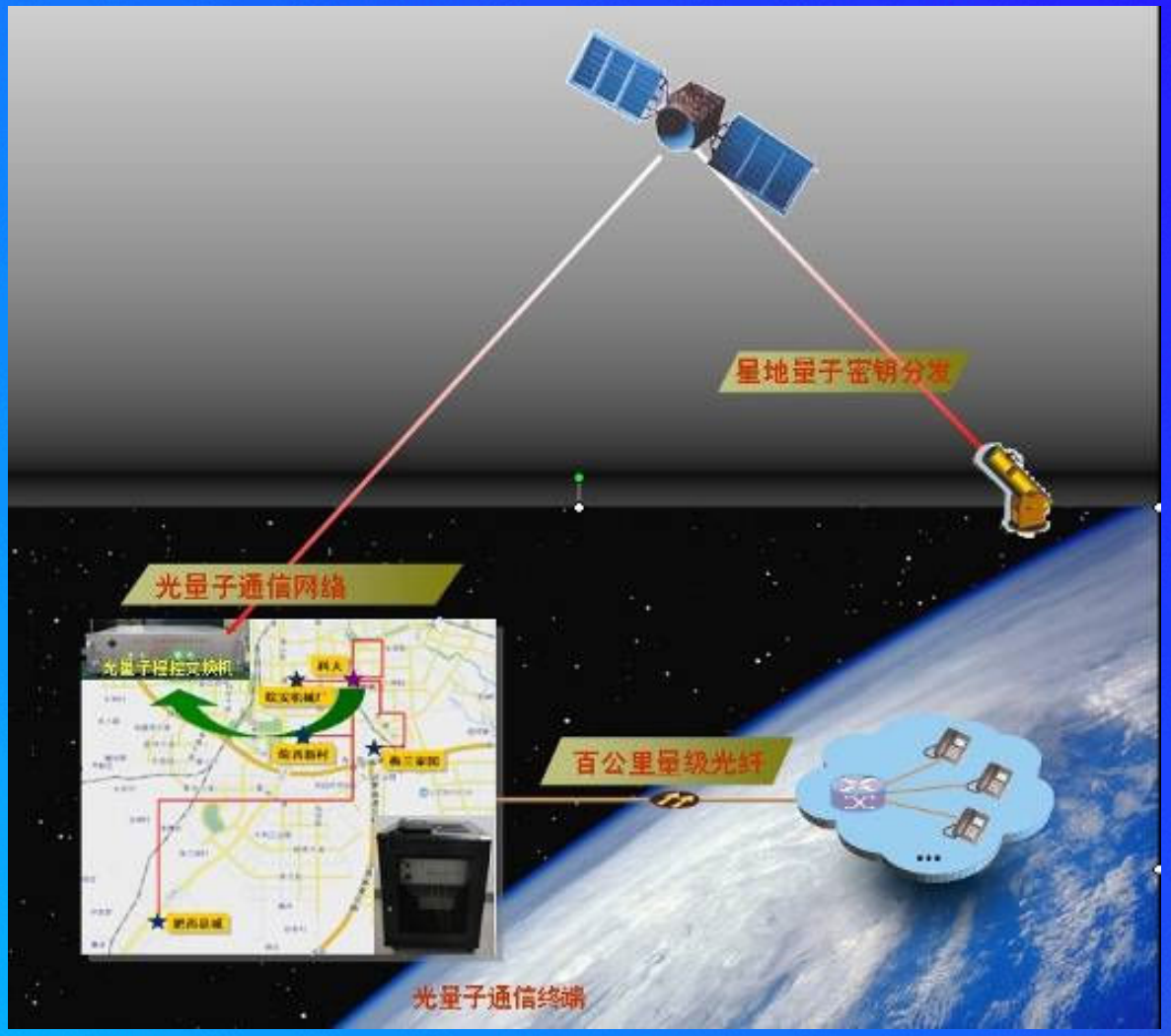
中国科学技术大学 陈凯

“墨子号”量子卫星与地面站装置图



Extended Data Figure 2 | The Micius satellite and the payloads. **a**, A full view of the Micius satellite before being assembled into the rocket. **b**, The experimental control box. **c**, The APT control box. **d**, The optical transmitter. **e**, Left side view of the optical transmitter optics head. **f**, Top side view of the optical transmitter optics head.

广域量子通信



城域量子通信网络的规模化＋

可信中继和量子中继器的城际量子网络＋

星地量子通信

→ 广域量子通信网络

实用化QKD之路

TABLE I. List of quantum hacking strategies.

Attack	Source or detection	Target component	Manner	Year
Photon number splitting (Brassard *et al.*, 2000; Lütkenhaus, 2000)	Source	WCP (multiphotons)	Theory	2000
Detector fluorescence (Kurtsiefer *et al.*, 2001)	Detection	Detector	Theory	2001
Faked state (Makarov and Hjelme, 2005; Makarov, Anisimov, and Skaar, 2006)	Detection	Detector	Theory	2005
Trojan horse (Vakhitov, Makarov, and Hjelme, 2001; Gisin *et al.*, 2006)	Source and detection	Backreflection light	Theory	2006
Time shift (Qi, Fung *et al.*, 2007; Zhao *et al.*, 2008)	Detection	Detector	Experiment[a]	2007
Time side channel (Lamas-Linares and Kurtsiefer, 2007)	Detection	Timing information	Experiment	2007
Phase remapping (Fung *et al.*, 2007; Xu, Qi, and Lo, 2010)	Source	Phase modulator	Experiment[a]	2010
Detector blinding (Makarov, 2009; Lydersen *et al.*, 2010)	Detection	Detector	Experiment[a]	2010
Detector blinding (Gerhardt *et al.*, 2011a; Gerhardt *et al.*, 2011b)	Detection	Detector	Experiment	2011
Detector control (Lydersen, Akhlaghi *et al.*, 2011; Wiechers *et al.*, 2011)	Detection	Detector	Experiment	2011
Faraday mirror (Sun, Jiang, and Liang, 2011)	Source	Faraday mirror	Theory	2011
Wavelength (Li *et al.*, 2011; Huang *et al.*, 2013)	Detection	Beam splitter	Experiment	2011
Dead time (Henning *et al.*, 2011)	Detection	Detector	Experiment	2011
Channel calibration (Jain *et al.*, 2011)	Detection	Detector	Experiment[a]	2011
Intensity (Jiang *et al.*, 2012; Sajeed, Radchenko *et al.*, 2015)	Source	Intensity modulator	Experiment	2012
Phase information (Sun *et al.*, 2012, 2015; Tang *et al.*, 2013)	Source	Phase randomization	Experiment	2012
Memory attacks (Barrett, Colbeck, and Kent, 2013)	Detection	Classical memory	Theory	2013
Local oscillator (Jouguet, Kunz-Jacques, and Diamanti, 2013; Ma *et al.*, 2013a)[b]	Detection	Local oscillator	Experiment	2013
Trojan horse (Jain *et al.*, 2014, 2015)	Source and detection	Backreflection light	Experiment	2014
Laser damage (Bugge *et al.*, 2014; Makarov *et al.*, 2016)	Detection	Detector	Experiment	2014
Laser seeding (Sun *et al.*, 2015)	Source	Laser phase or intensity	Experiment	2015
Spatial mismatch (Sajeed, Chaiwongkhot *et al.*, 2015; Chaiwongkhot *et al.*, 2019)	Detection	Detector	Experiment	2015
Detector saturation (Qin, Kumar, and Alléaume, 2016)[b]	Detection	Homodyne detector	Experiment	2016
Covert channels (Curty and Lo, 2019)	Detection	Classical memory	Theory	2017
Pattern effect (Yoshino *et al.*, 2018)	Source	Intensity modulator	Experiment	2018
Detector control (Qian *et al.*, 2018)	Detection	Detector	Experiment	2018
Laser seeding (Sun *et al.*, 2015; Huang *et al.*, 2019; Pang *et al.*, 2019)	Source	Laser	Experiment	2019
Polarization shift (Wei, Zhang *et al.*, 2019)	Detection	SNSPD	Experiment	2019

[a]Demonstration on a commercial QKD system.
[b]Continuous-variable QKD.

Feihu Xu *et al.*, Secure quantum key distribution with realistic devices
Rev. Mod. Phys. 92, 025002 (2020).

实用化QKD之路

TABLE II. List of decoy-state QKD experiments and their performance.

Reference	Clock rate	Encoding	Channel	Maximal distance	Key rate (bits/s)	Year
Zhao *et al.* (2006a, 2006b)	5 MHz	Phase	Fiber	60 km	422.5	2006
Peng *et al.* (2007)	2.5 MHz	Polarization	Fiber	102 km	8.1	2007
Rosenberg *et al.* (2007)	2.5 MHz	Phase	Fiber	107 km	14.5	2007
Schmitt-Manderbach *et al.* (2007)	10 MHz	Polarization	Free space	144 km	12.8[a]	2007
Yuan, Sharpe, and Shields (2007)	7.1 MHz	Phase	Fiber	25.3 km	5.5 K	2007
Yin *et al.* (2008)	1 MHz	Phase	Fiber	123.6 km	1.0	2008
Wang *et al.* (2008)[b]	0.65 MHz	Phase	Fiber	25 km	0.9	2008
Dixon *et al.* (2008)	1 GHz	Phase	Fiber	100.8 km	10.1 K	2008
Peev *et al.* (2009)	7 MHz	Phase	Fiber network	33 km	3.1 K	2009
Rosenberg *et al.* (2009)	10 MHz	Phase	Fiber	135 km	0.2	2009
Yuan *et al.* (2009)	1.036 GHz	Phase	Fiber	100 km	10.1 K	2009
Chen *et al.* (2009)	4 MHz	Phase	Fiber network	20 km	1.5 K	2009
Liu *et al.* (2010)	320 MHz	Polarization	Fiber	200 km	15.0	2010
Chen *et al.* (2010)	320 MHz	Polarization	Fiber network	130 km	0.2 K	2010
Sasaki *et al.* (2011)	1 GHz	Phase	Fiber network	45 km	304.0 K	2011
Wang *et al.* (2013)	100 MHz	Polarization	Free space	96 km	48.0	2013
Fröhlich *et al.* (2013)	125 MHz	Phase	Fiber network	19.9 km	43.1 K	2013
Lucamarini *et al.* (2013)	1 GHz	Phase	Fiber	80 km	120.0 K	2013
Fröhlich *et al.* (2017)	1 GHz	Phase	Fiber	240 km[c]	8.4	2017
Liao *et al.* (2017a)	100 MHz	Polarization	Free space	1200 km	1.1 K	2017
Yuan *et al.* (2018)	1 GHz	Phase	Fiber	2 dB	13.7 M	2018
Boaron *et al.* (2018)	2.5 GHz	Time bin	Fiber	421 km[c]	6.5	2018

[a]Asymptotic key rate.
[b]Heralded single-photon source.
[c]Ultra-low-loss fiber.

Feihu Xu *et al.*, Secure quantum key distribution with realistic devices
Rev. Mod. Phys. 92, 025002 (2020).

实用化QKD之路

TABLE III. List of MDI-QKD experiments and their performance.

Reference	Clock rate	Encoding	Distance or loss	Key rate (bits/s)	Year	Notes
Rubenok *et al.* (2013)[a]	2 MHz	Time bin	81.6 km	0.24[b]	2013	Field-installed fiber
Liu *et al.* (2013)	1 MHz	Time bin	50 km	0.12	2013	First complete demonstration
Ferreira da Silva *et al.* (2013)[a]	1 MHz	Polarization	17 km	1.04[b]	2013	Multiplexed synchronization
Z. Tang *et al.* (2014)	0.5 MHz	Polarization	10 km	4.7×10^{-3}	2014	Active phase randomization
Y.-L. Tang *et al.* (2014)	75 MHz	Time bin	200 km	0.02	2014	Fully automatic system
Tang *et al.* (2015)	75 MHz	Time bin	30 km	16.9	2015	Field-installed fiber
C. Wang *et al.* (2015)	1 MHz	Time bin	20 km	8.3[b]	2015	Phase reference free
Valivarthi *et al.* (2015)	250 MHz	Time bin	60 dB	5×10^{-2}	2015	Test in various configurations
Pirandola *et al.* (2015)[a]	10.5 MHz	Phase	4 dB	0.1	2015	Continuous variable
Y.-L. Tang *et al.* (2016)	75 MHz	Time bin	55 km	16.5	2016	First fiber network
Yin *et al.* (2016)	75 MHz	Time bin	404 km	3.2×10^{-4}	2016	Longest distance
G.-Z. Tang *et al.* (2016)	10 MHz	Polarization	40 km	10	2016	Include modulation errors
Comandar *et al.* (2016)[a]	1 GHz	Polarization	102 km	4.6 K	2016	High repetition rate
Kaneda *et al.* (2017)[a]	1 MHz	Time bin	14 dB	0.85	2017	Heralded single-photon source
C. Wang *et al.* (2017)	1 MHz	Time bin	20 km	6.3×10^{-3}	2017	Stable against polarization change
Valivarthi *et al.* (2017)	20 MHz	Time bin	80 km	100	2017	Cost-effective implementation
H. Liu *et al.* (2018)	50 MHz	Time bin	160 km	2.6[b]	2018	Phase reference free
H. Liu *et al.* (2019)	75 MHz	Time bin	100 km	14.5	2019	Asymmetric channels
Wei *et al.* (2019)	1.25 GHz	Polarization	20.4 dB	6.2 K	2019	Highest repetition or key rate

[a]No random modulations.
[b]Asymptotic key rate.

Feihu Xu *et al.*, Secure quantum key distribution with realistic devices
Rev. Mod. Phys. 92, 025002 (2020).

实用化QKD之路

TABLE IV. List of TF-QKD experiments.

Reference	Distance or loss	Key rate (bits/s)	Year
Minder *et al.* (2019)	90.8 dB	0.045[a]	2019
Wang, He *et al.* (2019)	300 km	2.01×10^3 [a]	2019
Y. Liu *et al.* (2019)	300 km	39.2	2019
Zhong *et al.* (2019)	55.1 dB	25.6[a]	2019
Fang *et al.* (2019)	502 km[b]	0.118	2019
J.-P. Chen *et al.* (2020)	509 km[b]	0.269	2019

[a]Asymptotic key rate.
[b]Ultra-low-loss fiber.

Feihu Xu *et al.*, Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* 92, 025002 (2020).

实用化QKD之路

TABLE V. List of some recent CV-QKD experiments and their performance.

Reference	Clock rate	Distance or loss	Key rate (bits/s)	Year	Notes
Jouguet *et al.* (2013)	1 MHz	80.5 km	~250	2013	Full implementation
Qi *et al.* (2015)	25 MHz	...	...	2015	Local LO
Soh *et al.* (2015)	250 kHz	...	...	2015	Local LO
Huang, Huang *et al.* (2015)	100 MHz	25 km	100 K	2015	Local LO
Pirandola *et al.* (2015)	10.5 MHz	4 dB	0.1	2015	CV MDI-QKD
Huang, Lin *et al.* (2015)	50 MHz	25 km	~1 M	2015	High key rate
Kumar, Qin, and Alléaume (2015)	1 MHz	75 km	490	2015	Coexistence with classical
Zhang *et al.* (2020)	5 MHz	202.8 km[a]	6.2	2020	Long distance

[a]Ultra-low-loss fiber.

TABLE VI. List of chip-based QKD experiments.

Reference	Clock rate	Distance or loss	Key rate (bits/s)	Year	Notes
C. Ma *et al.* (2016)	10 MHz	5 km	0.95 K	2016	Silicon, decoy BB84
Sibson *et al.* (2017)	1.72 GHz	4 dB	565 K	2017	InP, DPS
Sibson, Kennard *et al.* (2017)	1.72 GHz	20 km	916 K	2017	Silicon, COW
Bunandar *et al.* (2018)	625 MHz	43 km	157 K	2018	Silicon, decoy BB84
Ding *et al.* (2017)	5 kHz	4 dB	~7.5	2018	Silicon, high dimension
G. Zhang *et al.* (2019)	1 MHz	16 dB	0.14 K	2019	Silicon, CV-QKD
Paraïso *et al.* (2019)	1 GHz	20 dB	270 K	2019	InP, modulator free
Wei *et al.* (2019)	1.25 GHz	140 km	497	2019	Silicon, MDI-QKD

Feihu Xu *et al.*, Secure quantum key distribution with realistic devices
Rev. Mod. Phys. 92, 025002 (2020).

其他QKD协议

TABLE VII. List of recent experiments of other QKD protocols.

Reference	Clock rate	Distance or loss	Key rate (bits/s)	Year
Quantum access network (Fröhlich *et al.*, 2013)	125 MHz	19.9 km	259	2013
Centric network (Hughes *et al.*, 2013)	10 MHz	50 km	...	2013
RRDPS (Guan *et al.*, 2015)	500 MHz	53 km	~118.0	2015
RRDPS (Takesue *et al.*, 2015)	2 GHz	20 km	2.0 K	2015
RRDPS (S. Wang *et al.*, 2015)	1 GHz	90 km	~800	2015
RRDPS (Li *et al.*, 2016)	10 kHz	18 dB	15.5	2016
High dimension (Lee *et al.*, 2014)	8.3 MHz	...	456	2014
High dimension (Zhong *et al.*, 2015)	cw	20 km	2.7 M	2015
High dimension (Mirhosseini *et al.*, 2015)	4 kHz	...	6.5	2015
High dimension (Sit *et al.*, 2017)	...	0.3 km	~30 K	2017
High-dimension (Islam *et al.*, 2017)	2.5 GHz	16.6 dB	1.07 M	2017
Coherent one way (Korzh *et al.*, 2015)	625 MHz	307 km	3.2	2015
Modulator free (Yuan *et al.*, 2016)	1 GHz	40 dB	~10	2016

Feihu Xu *et al.*, Secure quantum key distribution with realistic devices
Rev. Mod. Phys. 92, 025002 (2020).

其它量子安全协议

TABLE VIII. List of recent developments of other quantum-cryptographic protocols beyond QKD.

Protocol	Theory or experiment	Notes
Noisy quantum storage (Damgård *et al.*, 2008; Wehner, Schaffner, and Terhal, 2008; Konig, Wehner, and Wullschleger, 2012)	Theory	Unconditional security
Oblivious transfer (Erven *et al.*, 2014)	Experiment	Noisy-storage model
Bit commitment (Ng *et al.*, 2012)	Experiment	Noisy-storage model
Bit commitment (Kent, 2012)	Theory	Relativistic assumption
Bit commitment (Lunghi *et al.*, 2013; Liu *et al.*, 2014)	Experiment	Relativistic assumption
Bit commitment (Chakraborty, Chailloux, and Leverrier, 2015; Lunghi *et al.*, 2015; Verbanis *et al.*, 2016)	Experiment	Long commitment time
Digital signature (Clarke *et al.*, 2012)	Experiment	First demonstration
Digital signature (Collins *et al.*, 2014; Dunjko, Wallden, and Andersson, 2014)	Experiment	No quantum memory
Digital signature (Donaldson *et al.*, 2016; Yin *et al.*, 2017a)	Experiment	Insecure channel
Coin flipping (Berlín *et al.*, 2011; Pappa *et al.*, 2014)	Experiment	Loss tolerance
Data locking (Fawzi, Hayden, and Sen, 2013; Lloyd, 2013; Lupo, Wilde, and Lloyd, 2014)	Theory	Loss tolerance
Data locking (Liu *et al.*, 2016; Lum *et al.*, 2016)	Experiment	Loss tolerance
Blind quantum computing (Broadbent, Fitzsimons, and Kashefi, 2009; Barz *et al.*, 2012)	Theory and experiment	No quantum memory
Blind quantum computing (Reichardt, Unger, and Vazirani, 2013; Huang *et al.*, 2017)	Theory and experiment	Classical clients

Feihu Xu *et al.*, Secure quantum key distribution with realistic devices
Rev. Mod. Phys. 92, 025002 (2020).

QKD发展

TABLE IX. List of reviews related to QKD.

Reference	Subject
Gisin *et al.* (2002)	Experimental basics of QKD
Scarani *et al.* (2009)	Theoretical basics of QKD
Lo, Curty, and Tamaki (2014), Diamanti *et al.* (2016), and Zhang *et al.* (2018)	Practical challenges of QKD
Jain *et al.* (2016))	Quantum hacking attacks
Xu, Curty, Qi, and Lo *et al.* (2015)	Measurement-device-independent QKD
Hadfield (2009) and Zhang *et al.* (2015)	Single-photon detector
X. Ma *et al.* (2016) and Herrero-Collantes and Garcia-Escartin (2017)	Quantum random number generator
Coles *et al.* (2017)	Entropy uncertainty relation
Weedbrook *et al.* (2012), Diamanti and Leverrier (2015), and Laudenbach *et al.* (2018)	Continuous-variable QKD
Sangouard *et al.* (2011), Pan *et al.* (2012), and Munro *et al.* (2015)	Quantum repeaters
Kimble (2008) and Wehner, Elkouss, and Hanson (2018)	Quantum internet
Brunner *et al.* (2014)	Bell nonlocality or device-independent QKD
Fitzsimons (2017)	Blind quantum computing
Xavier and Lima (2020)	High-dimensional QKD

Feihu Xu *et al.*, Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* 92, 025002 (2020).

自由空间量子光学实验

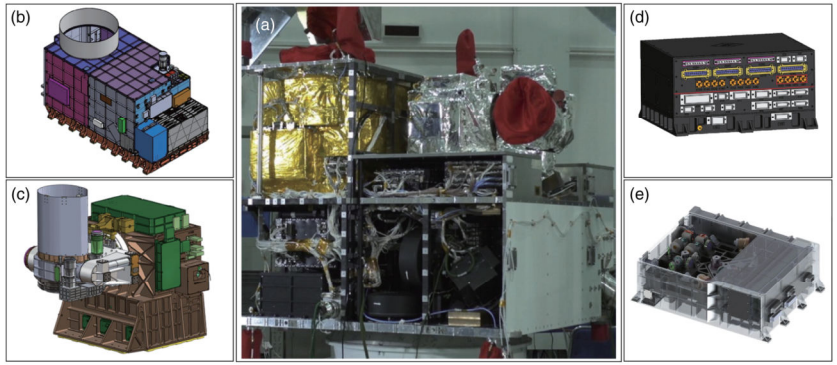


FIG. 18. Full view of the Micius satellite and the main payloads. (a) Photograph of the Micius satellite prior to launch. (b) Transmitter 1 for QKD, entanglement distribution, and teleportation. (c) Transmitter 2, especially designed for entanglement distribution. (d) Experimental control box. (e) Entangled-photon source.

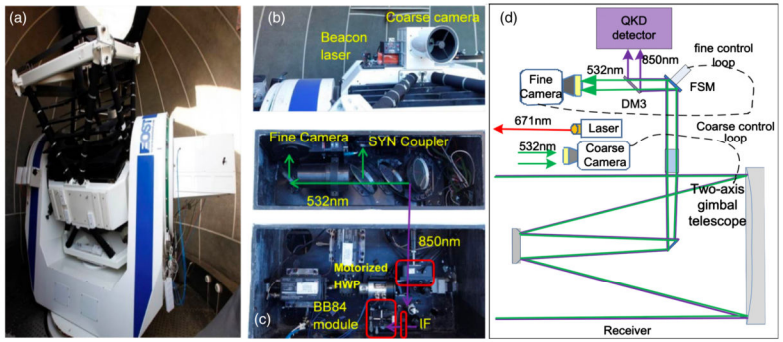


FIG. 23. Typical receiving ground station for the Micius satellite. (a) Two-axis gimbal telescope. (b) Beacon laser and coarse camera. (c) One of the two layers of the optical receiver box. (d) Typical optical design of the receiver including the receiving telescope, the ATP system, and the QKD-detection module. From Liao *et al.*, 2017a.

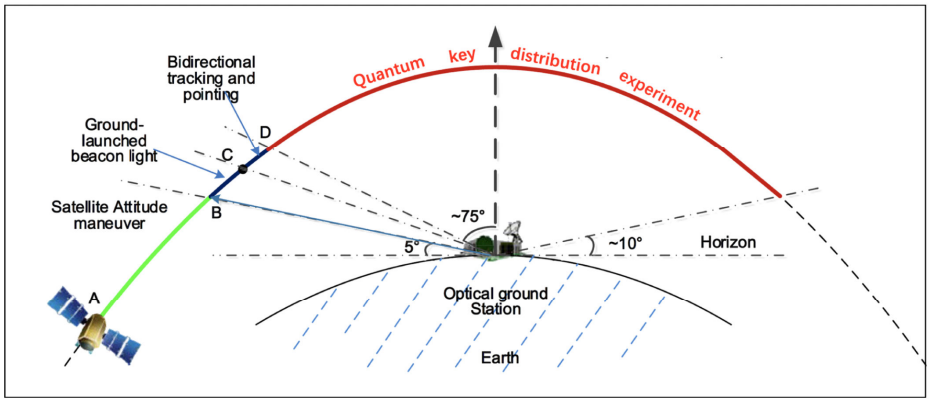


FIG. 27. Tracking and QKD processes during an orbit. From Liao *et al.*, 2017a.

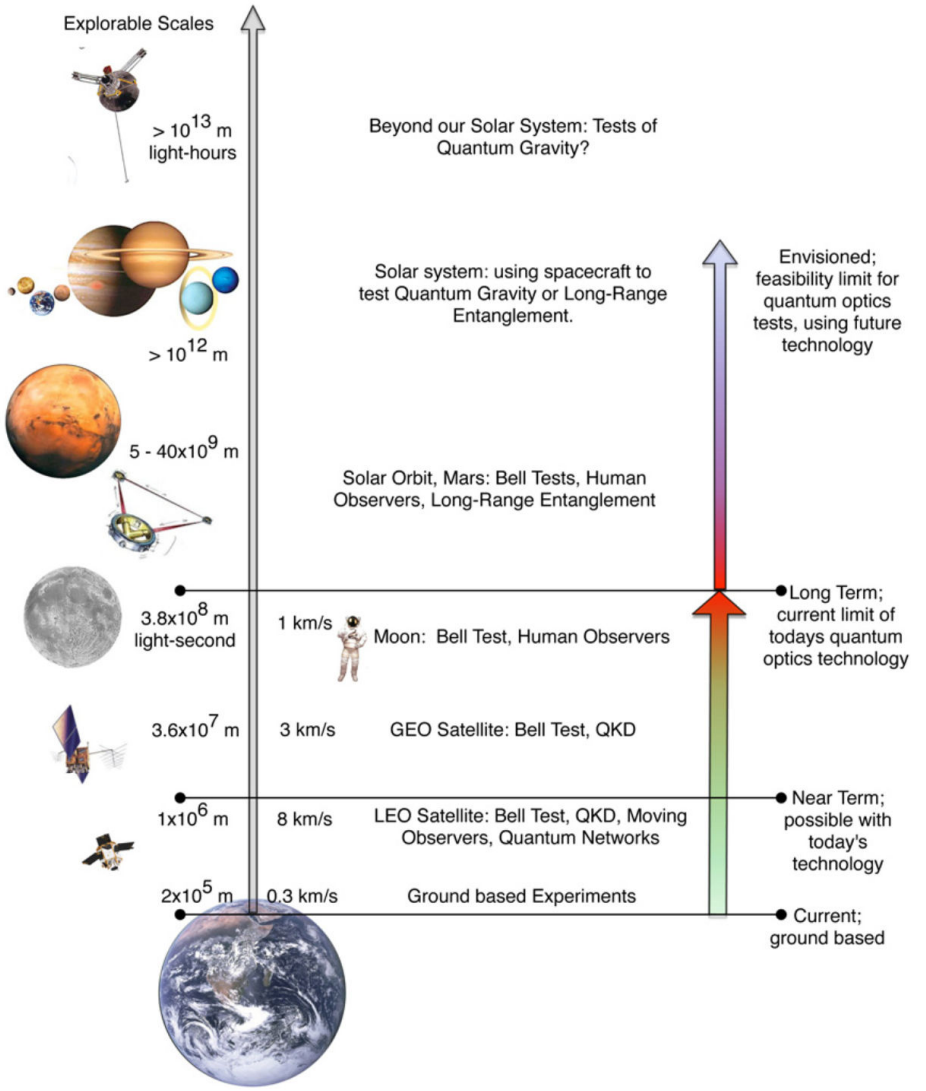


Figure 1. Overview of the distance and velocity scales achievable in a space environment explorable with man-made systems, with some possible quantum optics experiments at each given distance.

C.-Y. Lu *et al.*, Micius quantum experiments in space, Rev. Mod. Phys., 94 (2022) 035001.

中国科学技术大学 陈凯

Nicolas Gisin *et al.*, Quantum cryptography
Rev. Mod. Phys. 74, 145-195 (2002).

V. Scarani *et al.*, The security of practical quantum key distribution
Rev. Mod. Phys. 81, 1301-1350 (2009).

Jian-Wei Pan *et al.*, Multiphoton entanglement and interferometry
Rev. Mod. Phys. 84, 777-838 (2012).

Feihu Xu *et al.*, Secure quantum key distribution with realistic devices
Rev. Mod. Phys. 92, 025002 (2020).

C.-Y. Lu et al., Micius quantum experiments in space
Rev. Mod. Phys. 94, 035001 (2022).

Decoy QKD
W.-Y. Hwang, *Phys. Rev. Lett. 91, 057901 (2003);*
H.-K. Lo, X.-F. Ma, and K. Chen, *Phys. Rev. Lett. 94, 230504 (2005);*
X.-F. Ma, B. Qi, Y. Zhao and H.-K. Lo, Practical decoy state for quantum key distribution. *Phys. Rev. A, 72,012326 (2005).*
X.-B. Wang, *Phys. Rev. Lett. 94, 230503 (2005).*

MDI-QKD
H.-K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett. 108, 130503 (2012)*
Liu *et al.*, *Phys. Rev. Lett. 111, 130502 (2013);* Tang *et al.*, *Phys. Rev. Lett. 112, 190503 (2014)*
Tang *et al.*, *Phys. Rev. Lett. 113, 190501 (2014);* Yin *et al.*, *Phys. Rev. Lett. 117, 190501 (2016)*

TF-QKD
Lucamarini, M., Z. Yuan, J. Dynes, and A. Shields, *Nature 557, 400 (2018) .*
Ma, X., P. Zeng, and H. Zhou, *Phys. Rev. X 8, 031043 (2018).*

谢谢

中国科学技术大学 陈凯

乔布斯语录：
2005年斯坦福大学毕业典礼上的讲话

Your time is limited, so don't waste it living someone else's life. Don't be trapped by dogma, which is living with the results of other people's thinking. Don't let the noise of other's opinions drown out your own inner voice.

And most important, have the courage to follow your heart and intuition. They somehow already know what you truly want to become. Everything else is secondary.

乔布斯语录

Innovation distinguishes between a leader and a follower.

The only way to do great work is to love what you do. If you haven't found it yet, keep looking. Don't settle. As with all matters of the heart, you'll know when you find it.

Design is not just what it looks like and feels like. Design is how it works.