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、徐飞虎

2024.3~ 2024.4

课程安排

- 绪论 量子信息概念，历史和展望
- 第一章 量子体系 量子态， Schmidt分解，混合态， 密度矩阵，量子测量，量子不可克隆定理等。
- 第二章 量子纠缠 纠缠和可分型，纠缠判据 ，纠缠量化，多粒子推广等
- 第三章 量子关联表现 局域实在论，Bell不等式，多体推广，纠缠与非定域性的关系等
- 第四章 量子通信 量子通信方案，通信基本形式包括量子隐形传态、稠密编码，量子密钥分发等；非理想条件下量子保密通信方案和实验，数据处理方法，安全性分析；与纠缠关系
- 第五章 量子纠错 量子纠错码，原理、构造、应用
- 第六章 量子计算 量子算法、应用
- 新进展：量子成像等 （徐飞虎老师）

第四章 量子通信

徐飞虎：量子通信方案，量子密钥分发QKD；非理想条件下量子保密通信方案和实验，数据处理方法；QKD安全性分析等

陈凯：量子隐形传态理论和实验，与纠缠关系，纠缠交换等

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 à MDI-QKD
   - ② 设备无关的 à 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

REVIEWS OF MODERN PHYSICS

Recent Accepted Authors Referees Search Press About Staff

Secure quantum key distribution with realistic devices

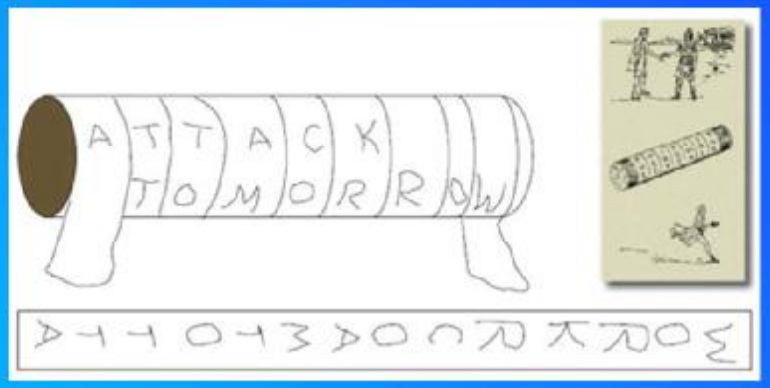
Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan

Rev. Mod. Phys. **92**, 025002 – Published 26 May 2020

https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.92.025002

保密通信

加密是一种古老的艺术



古希腊斯巴达人使用的加密术
(约公元前7世纪)

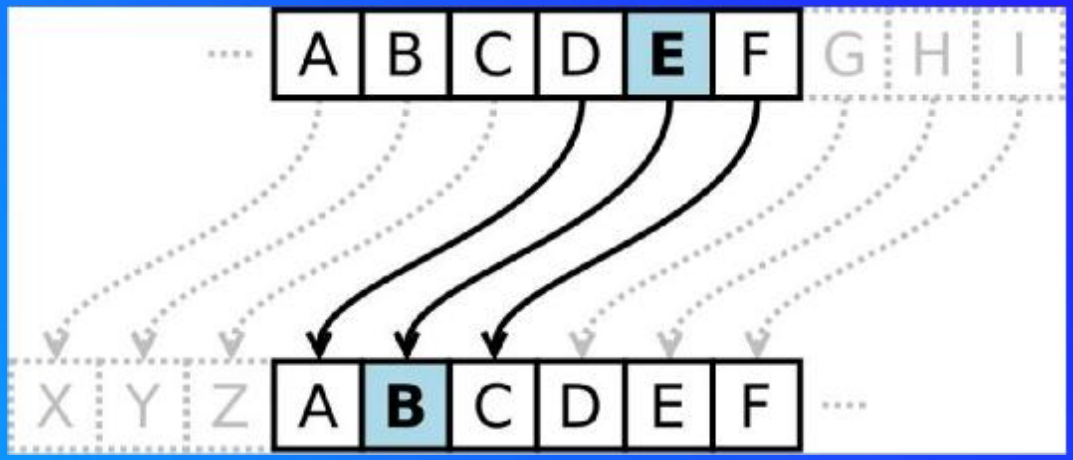
凯撒加密（变换）法
(约公元前1世纪)

- 恺撒大帝曾用此方法对重要的军事信息进行加密
  - 使用暗号，即改变字母顺序，使局外人无法组成一个单词
  - 想读懂意思，得用第4个字母置换第一个字母，即以D代A，以此类推

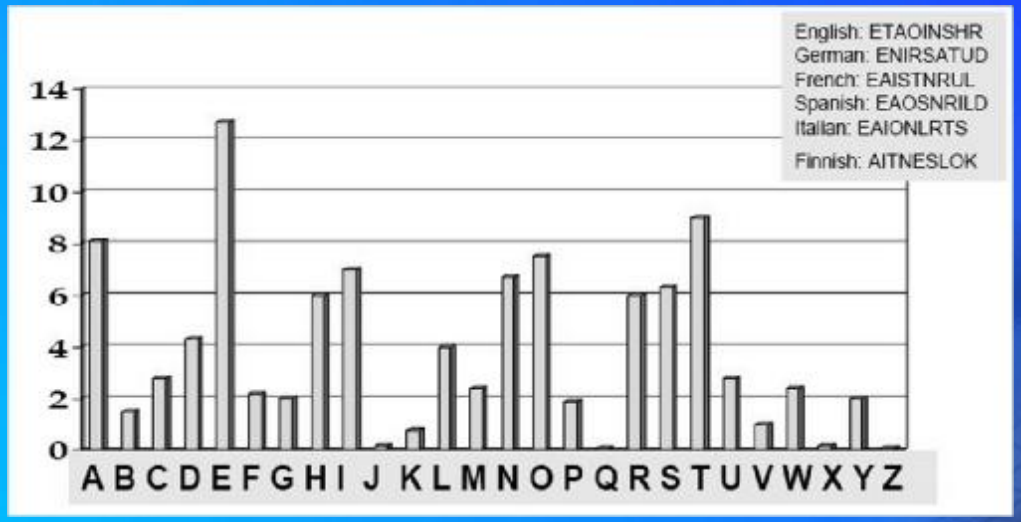
密文：GRJ　　明文：DOG

加密是一种古老的艺术

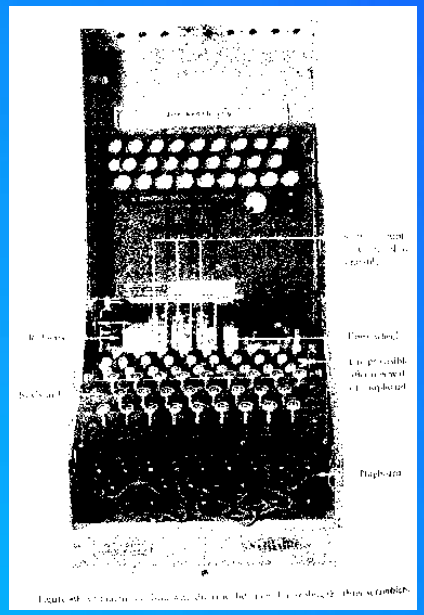
- 知道替换规则，就可以破解



- 阿拉伯数学家Al-Kindi发现利用字母出现的频率可以破译密码



近代加密技术



1920s German Enigma Machine
10 million billion possible combinations!
Looked unbreakable.

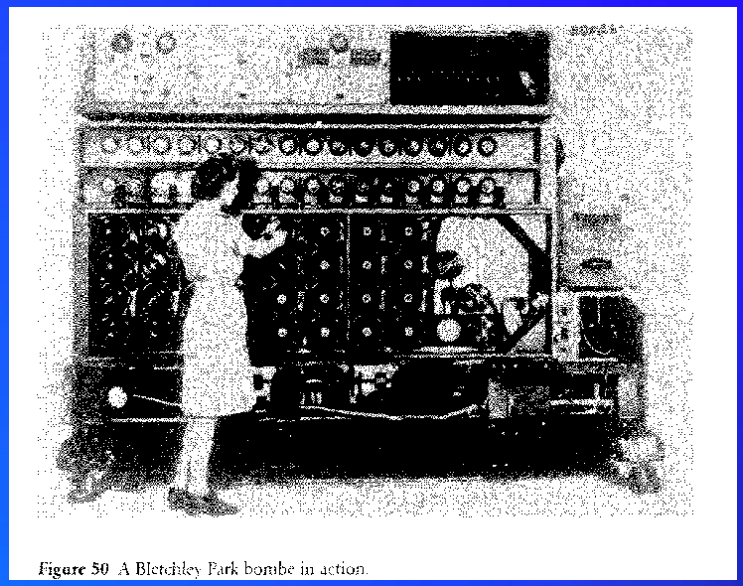
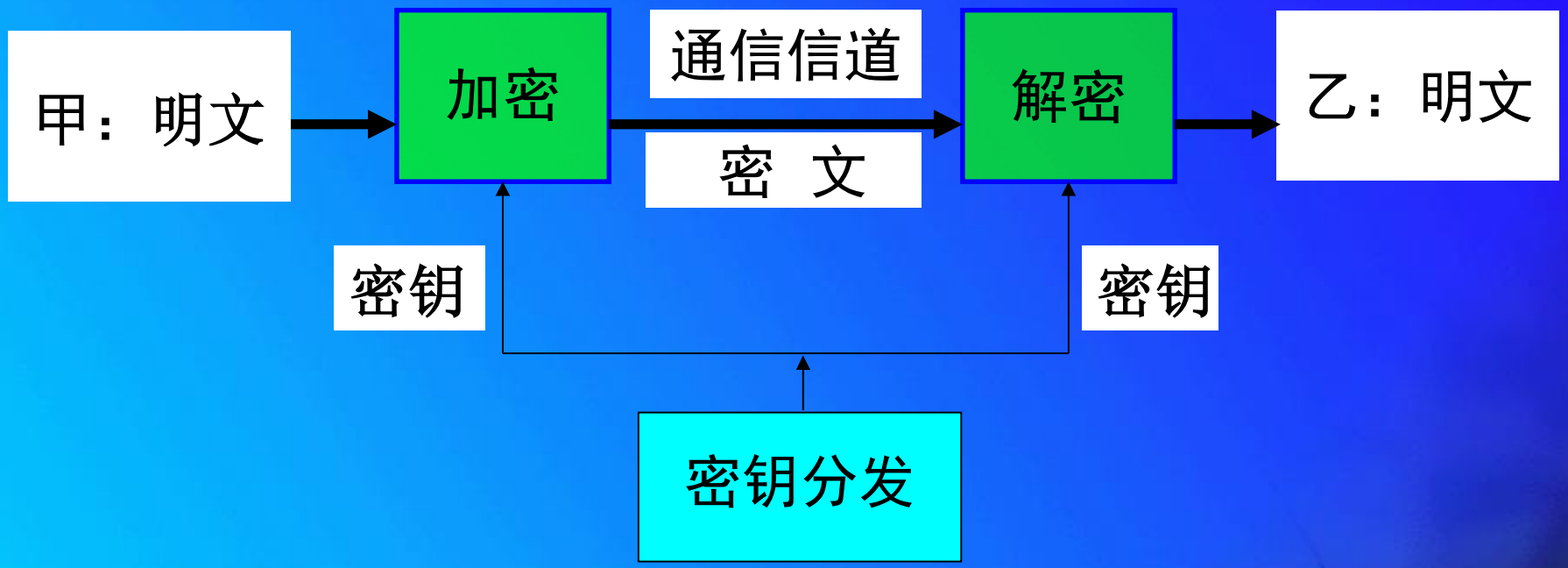


Figure 50 A Bletchley Park bombe in action.

1940 Allied code-breaking machine
“bombe”
Enigma Broken!

Enigma代码的破解成为了现代计算机研制的先驱！

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、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

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

分配和使用密钥常规体制及安全性

- 基于计算复杂度的非对称加密
- 例如 RSA，基于素数乘法与质因数分解的计算需求不同

3 × 5 = ☐　　21 = ☐ × ☐

53 × 79 = ☐　　4183 = ☐ × ☐

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3 = ☐ × ☐

Q RSA 512：1999年被破解

RSA 768：2009年被破解

RSA 1024??

Q 2017年2月，谷歌破解了广泛应用于文件数字证书中的SHA-1算法……

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
- 例：基于Hash函数的世界通行密码标准系列算法MD5等被王小云院士等人破解
- 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）

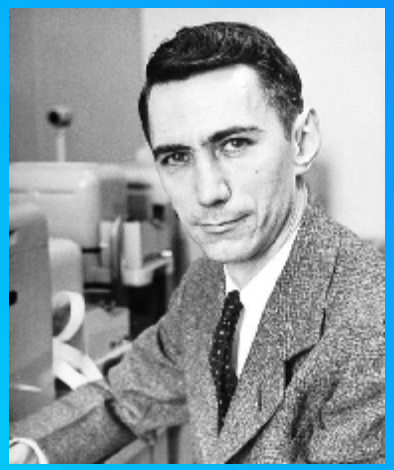
传统的保密通信体系已经无法保证通信的安全性要求！

一次一密的加密方式

- 遥远两地分发共享密钥
- 生成的密钥，通过一次一密（OTP）的方式加密信息

二进制加法	
$0 \oplus 0 = 0$	$0 \oplus 1 = 1$
$1 \oplus 0 = 1$	$1 \oplus 1 = 0$

明文	“a”							
明文-ASCII	0	1	1	0	0	0	0	1
密码	0	0	1	1	1	0	0	1
密文-ASCII	0	1	0	1	1	0	0	0
密文	“X”							



Claude E. Shannon

一次一密的安全性是可证明的!

信息论安全!

常规密钥安全性分析总结

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

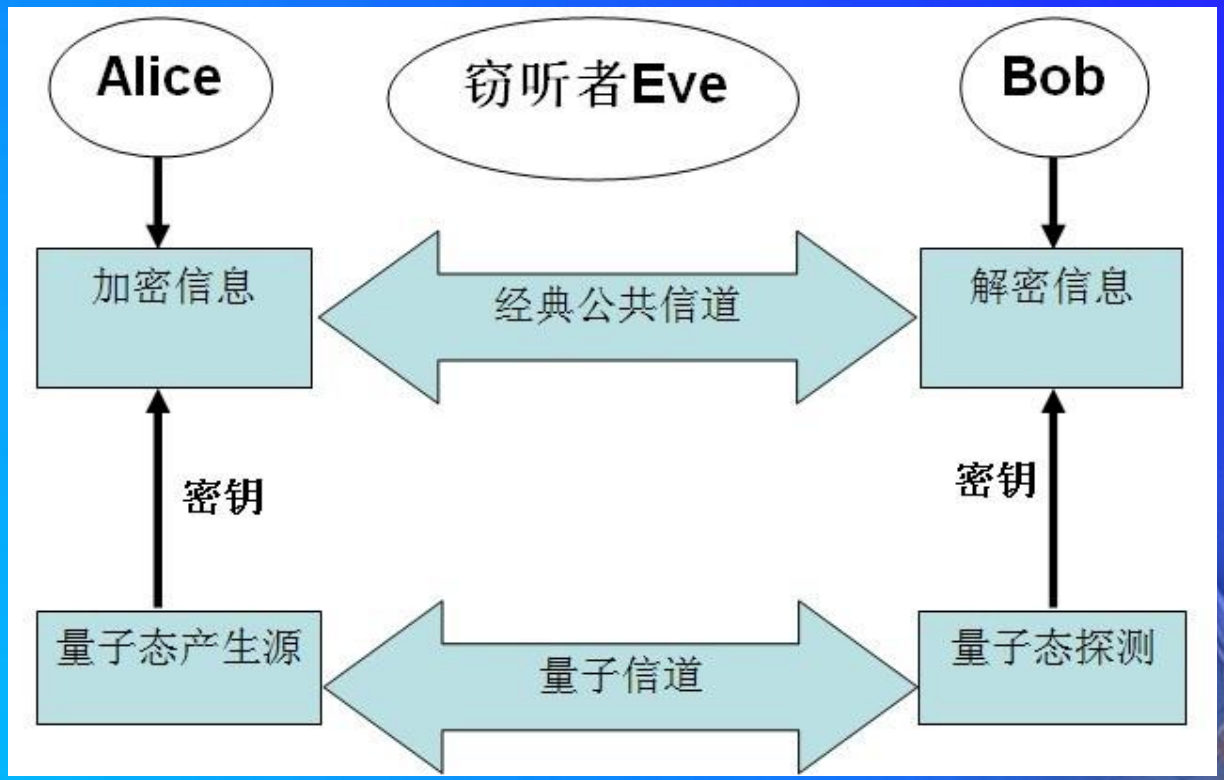
密钥的分配过程安全性无法保证

↓

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（QKD）

基于量子力学基本原理，Bennett和Brassard在1984年印度举行的一个IEEE会议上提出了世界上第一个量子密钥分发协议（Quantum Key Distribution, QKD），俗称BB84协议



BB84协议示意图

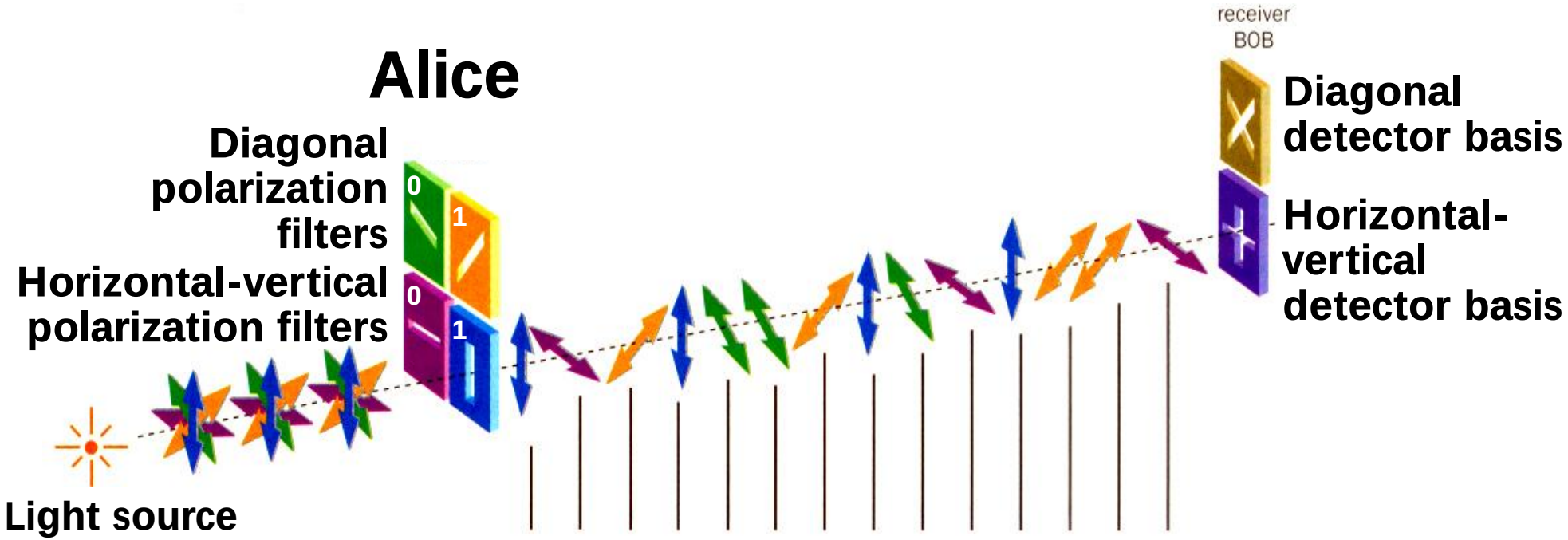
QKD基本原理

What is QKD?

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

量子密码基本原理

BB84协议



Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0	
Bob's detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+	
Bob's measurement	1	0	0	1	0	0	1	1	0	0	0	1	0	0	
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0	

Image reprinted from article: W. Tittel, G. Ribordy & N. Gisin, "Quantum cryptography," Physics World, March 1998

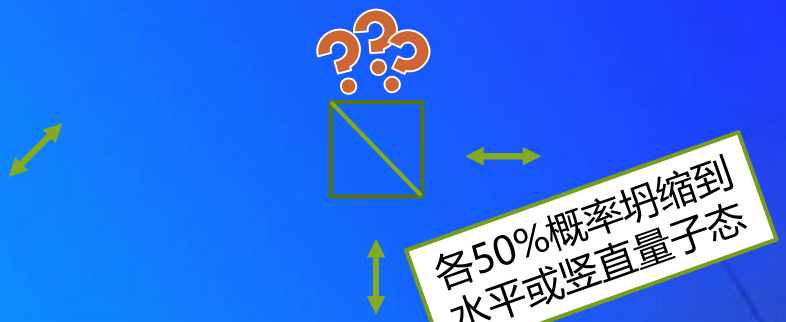
QKD保密原理举例

- 偏振态与偏振检测

水平、竖直偏振

+45°、-45°偏振

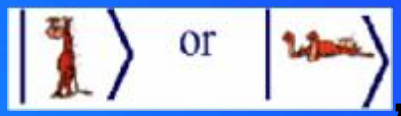
+45°偏振经过水平检偏?

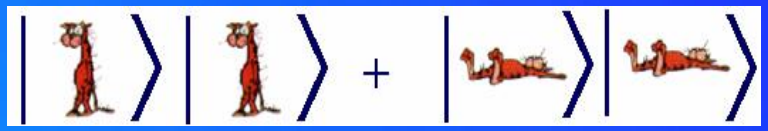


- 单个未知量子态不可克隆
- 在错误基矢测量会随机坍缩到该基矢对应的量子态

QKD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

$|y\rangle$

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！

QKD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协议过程

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

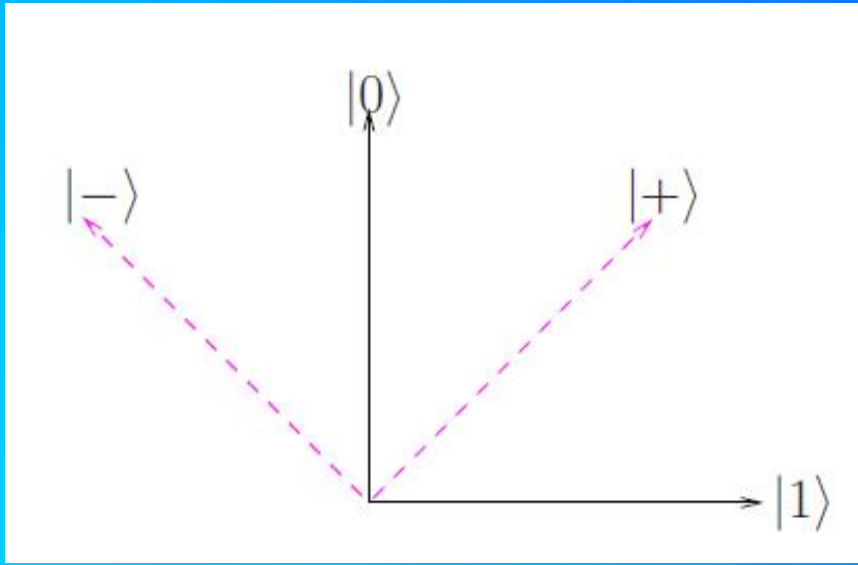
In order to prevent an eavesdropper from reading the bits, Alice randomly chooses to write each bit x_i as a qubit $|\psi_i\rangle$ in either the **rectilinear basis** as $|0\rangle$ or $|1\rangle$ or in the **diagonal basis** as $|+\rangle$ or $|-\rangle$

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

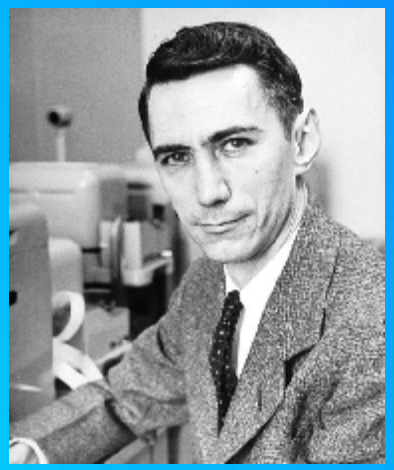
1: Alice chooses $(4+\delta)n$ random data bits.
2: Alice chooses a random $(4+\delta)n$-bit string b. She encodes each data bit as $\{|0\rangle, |1\rangle\}$ if the corresponding bit of b is 0 or $\{|+\rangle, |-\rangle\}$ if b is 1.
3: Alice sends the resulting state to Bob.
4: Bob receives the $(4+\delta)n$ 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.

QKD+OPT

- Alice和Bob通过QKD共享密钥
- 生成的密钥，通过一次一密的方式加密信息

二进制加法	
$0 \oplus 0 = 0$	$0 \oplus 1 = 1$
$1 \oplus 0 = 1$	$1 \oplus 1 = 0$

明文	“a”							
明文-ASCII	0	1	1	0	0	0	0	1
密码	0	0	1	1	1	0	0	1
密文-ASCII	0	1	0	1	1	0	0	0
密文	“X”							



Claude E. Shannon

一次一密的安全性是可证明的!

信息论安全!

QKD安全性

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.

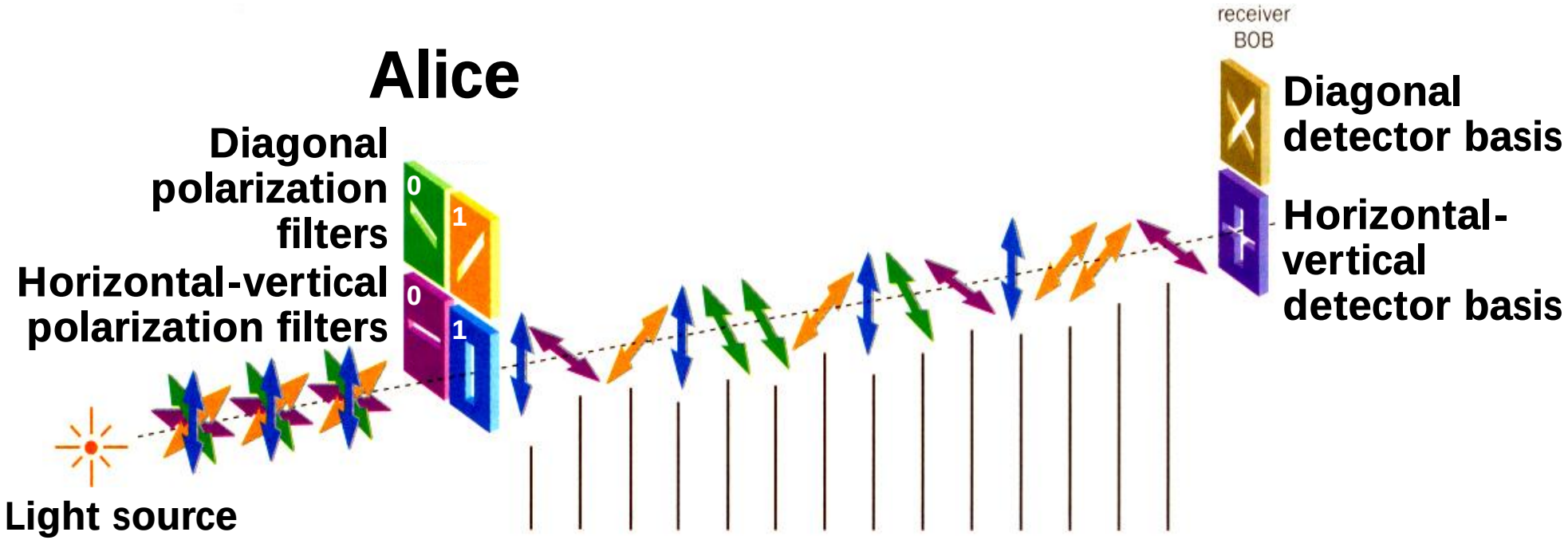
Is QKD secure?

- Dominic Mayers and subsequently by others, including Eli Biham and collaborators and Michael Ben-Or prove that the standard BB84 protocol is secure (1995).

- 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 (1995).

- 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.

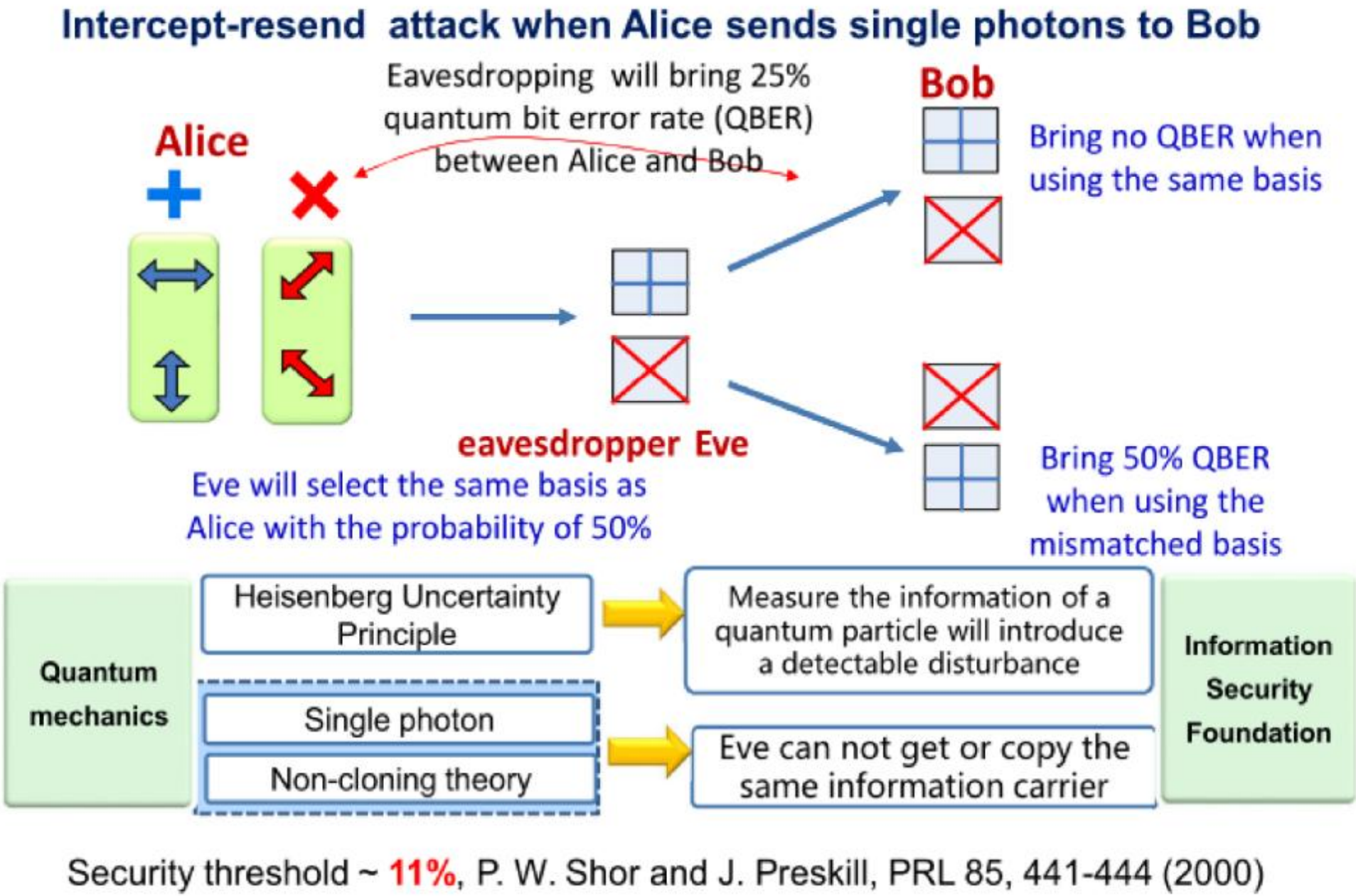
BB84协议



Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0	
Bob's detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+	
Bob's measurement	1	0	0	1	0	0	1	1	0	0	0	1	0	0	
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0	

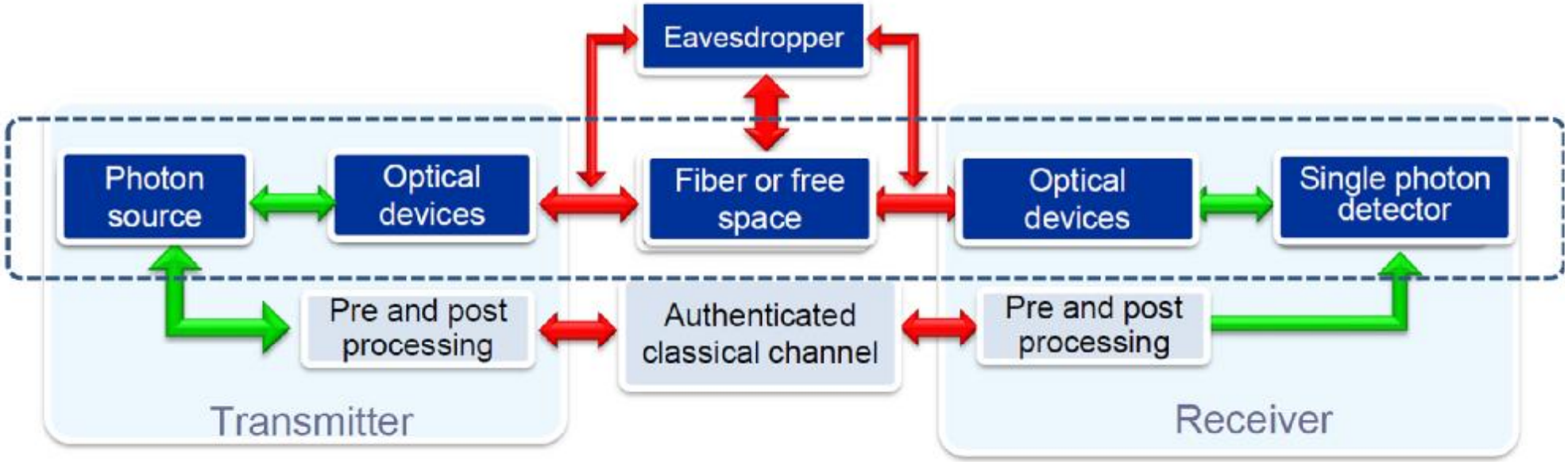
Image reprinted from article: W. Tittel, G. Ribordy & N. Gisin, "Quantum cryptography," Physics World, March 1998

QKD安全性-QBER



Security threshold ~ **11%**, P. W. Shor and J. Preskill, PRL 85, 441-444 (2000)

现实QKD系统



Photons are a natural carrier for quantum information

- Long coherence time
- Easy to manipulate
- Multi-degree of freedom
- Plenty of off-the-shelf devices

- Transmission loss
- Hard to be restored
- Need specific transmission channel
- A little expense

现实QKD系统

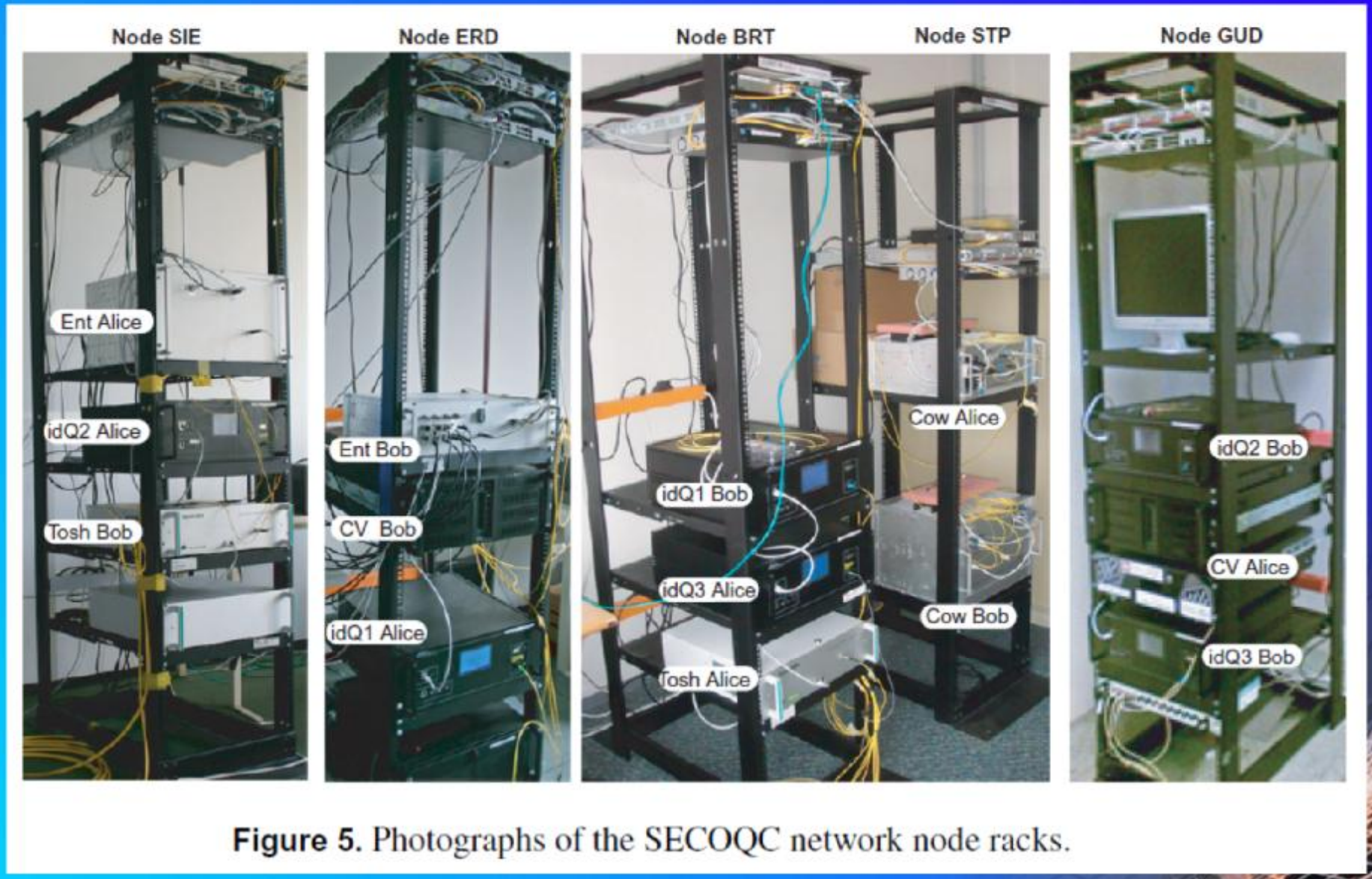


Figure 5. Photographs of the SECOQC network node racks.

现实QKD系统

The resources required in QKD systems

Photon source	Photon manipulation	Photon detector	Interface and auxiliary
• WCS source • Entanglement source • Quantum dot, NV center, et al.	• Polarization • Phase • Time-bin • Frequency • Orbital angular momentum • Amplitude • Intensity	• InGaAs • Si • Ge • Superconducting materials • PMT • Homodyne/Heterodyne	• Narrow band filter • WDM • Circulator • Isolator • Faraday rotator • Clocksync

Sources

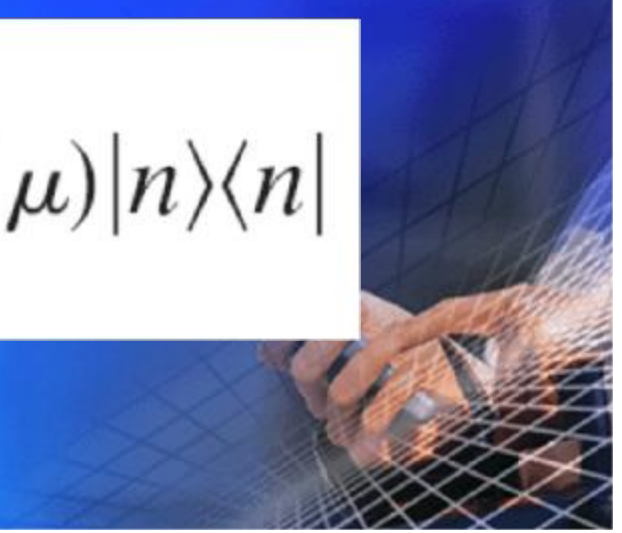
The output of a laser in a given mode is described by a coherent state of the field,

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

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

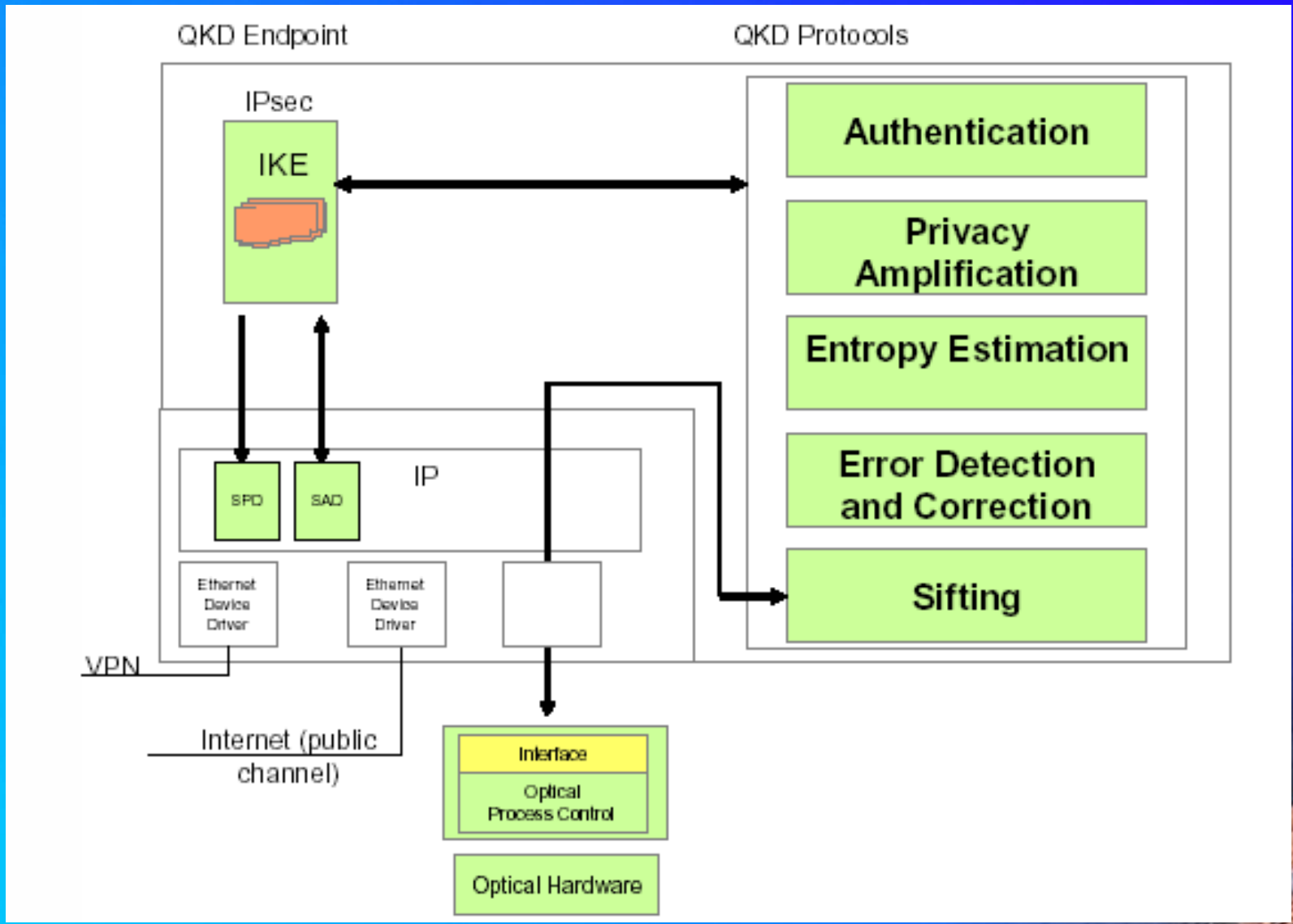
TABLE I. Typical parameters of single-photon detectors: detected wavelength λ, quantum efficiency η, fraction of dark counts p_d, repetition rate, maximum count rate, jitter, and temperature of operation T; the last column refers to the possibility of distinguishing the photon numbers. For acronyms and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

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

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.

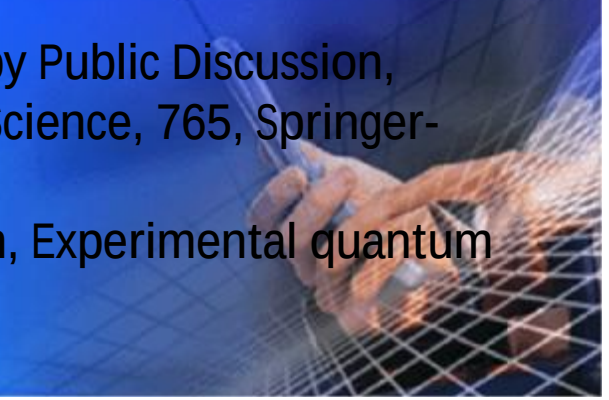
e_1 is the bit error rate for single photon state.

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 .



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

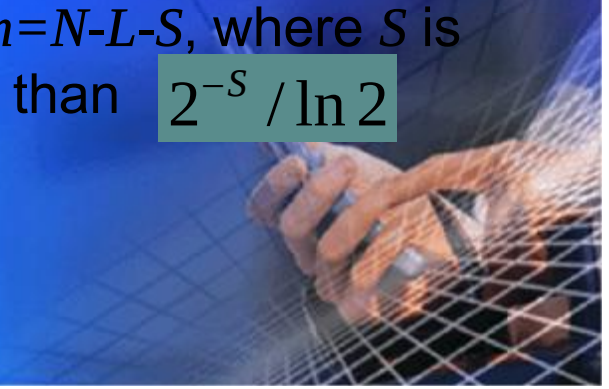
Applying a 0-1 $m*N$ matrix to k, Alice and Bob obtain a final m-bit key k' about which Eve has an exponentially small amount of information.

Use good hashing function

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

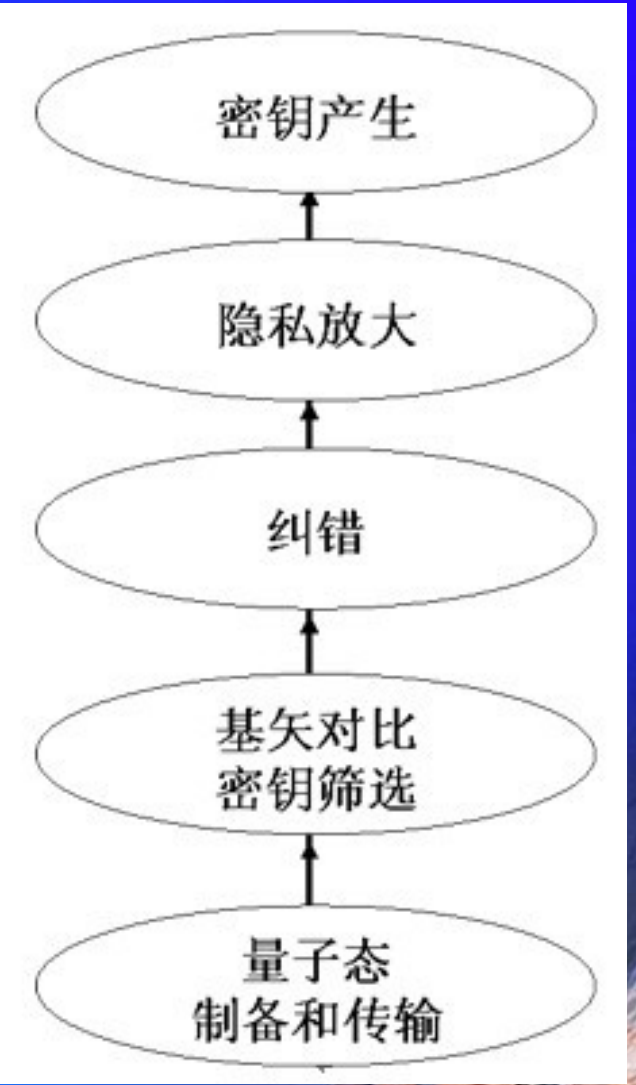
$$f : \{0,1\}^N \rightarrow \{0,1\}^{N-L-S}$$

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.



总结：QKD process

- 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



- **QKD只是用来传递密码，并非明文**
- **QKD需要经典通信的辅助**

诱骗态量子密钥分发

Decoy-state QKD

Decoy QKD Outline

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

1. Motivation and Introduction

What? Why?

Commercial Quantum Crypto products available on the market Today!

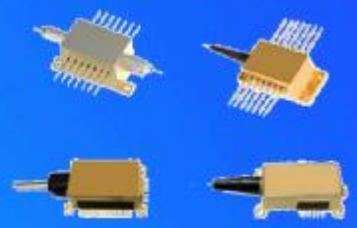
MAGIQ TECH.

- Distance over 100 km of commercial Telecom fibers.

ID QUANTIQUE

Commercial Quantum Crypto products available on the market Today!

第四代终端
（**4U19**英寸标准机箱）



- 通过核心器件的芯片化，未来可将终端的体积缩小到手机大小
- 核心器件的全国产化

国盾量子商用QKD产品

Laser sources

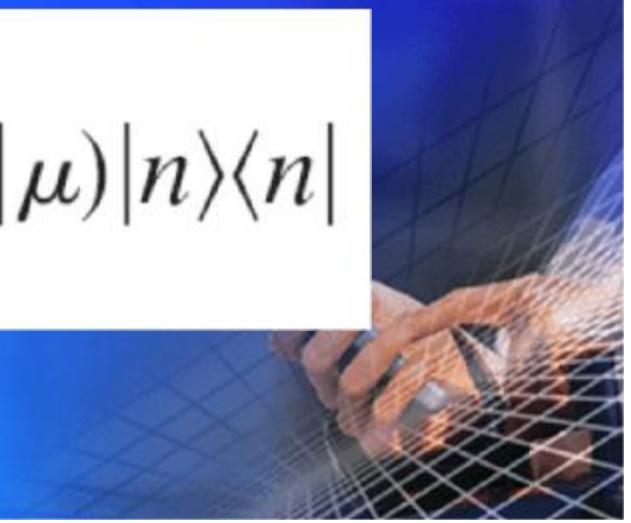
The output of a laser in a given mode is described by a coherent state of the field,

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

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

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

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



Security proof of BB84 protocol

ASSSUMPTIONS:

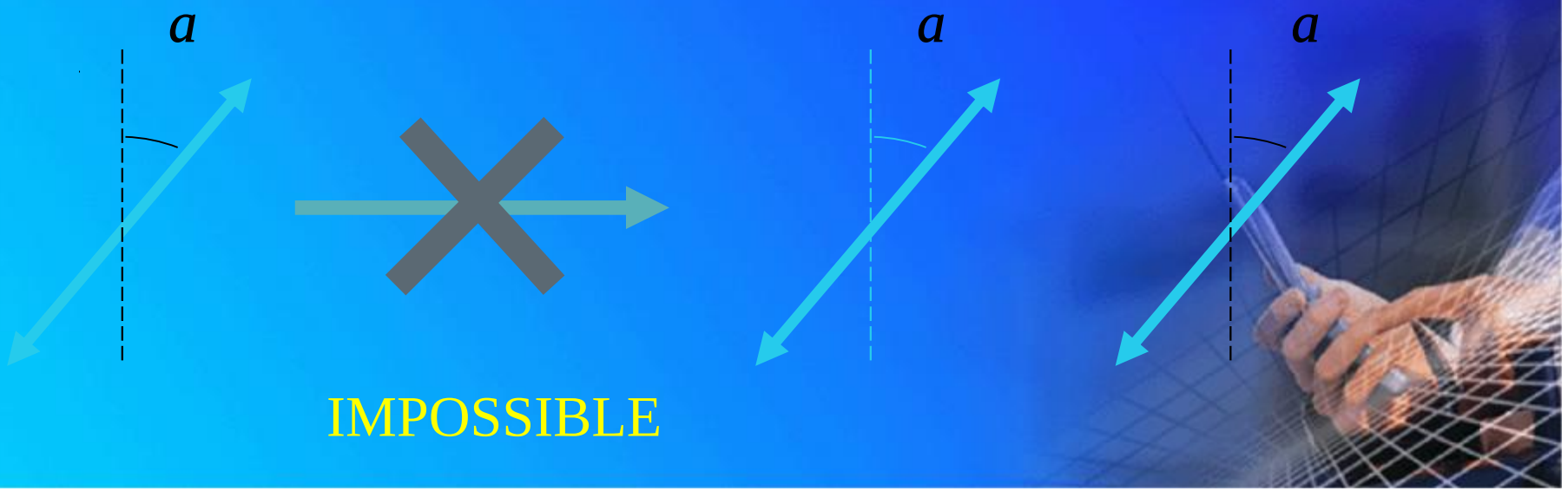
1. Source: Emits perfect single photons. (No multi-photons)
2. Channel: noisy but lossless. (No absorption in channel)
3. Detectors: a) Perfect detection efficiency. (100 %)
4. Basis Alignment: Perfect. (Angle between X and Z basis is exactly 45 degrees.)

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

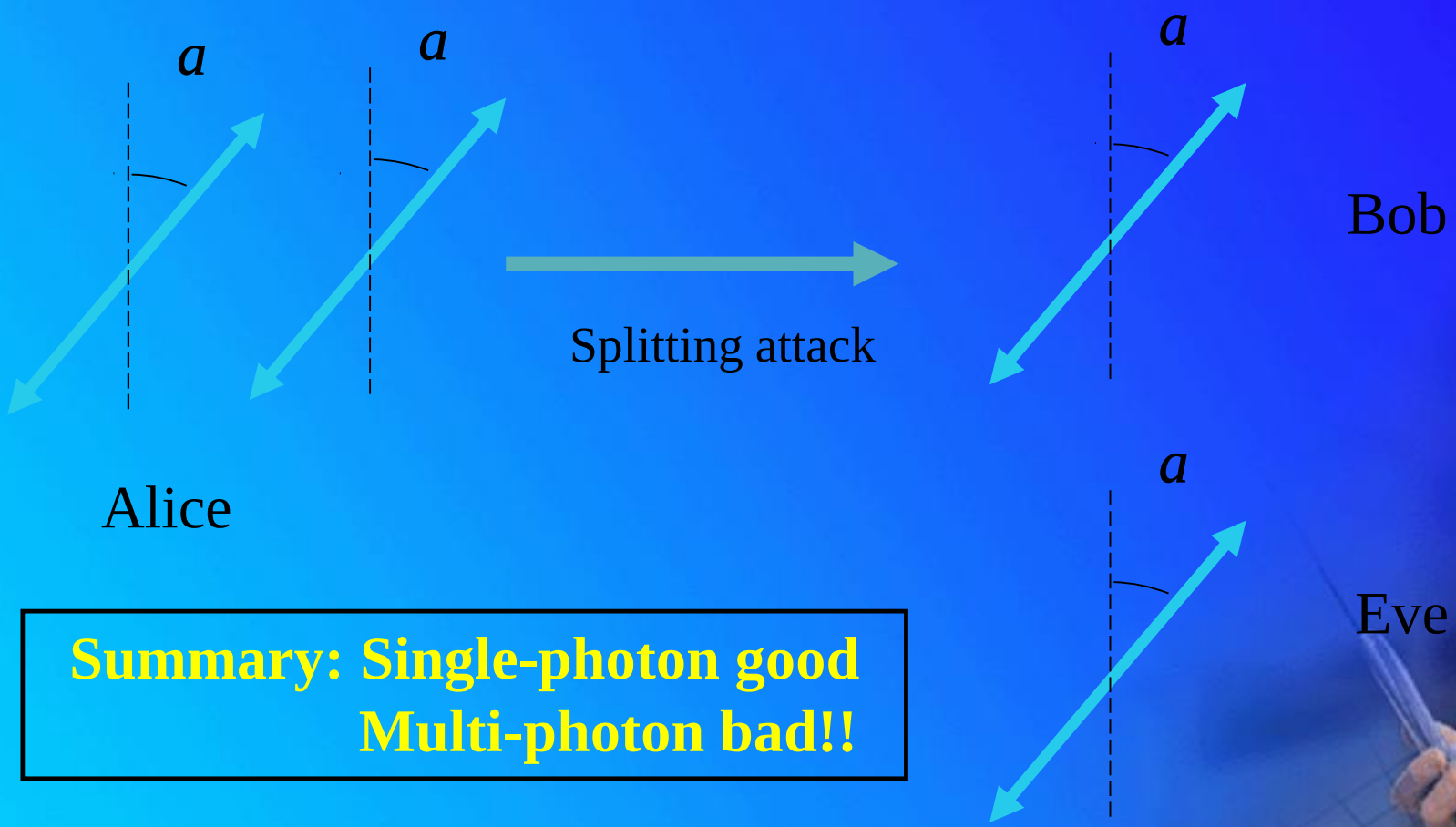
Reminder: Quantum No-cloning Theorem

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



Problem: Photon-Number Splitting (PNS) attack

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



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

G Brassard, N Lütkenhaus, T Mor, B Sanders, Physical review letters 85, 1330 (2000)

QKD: Practice

Reality:

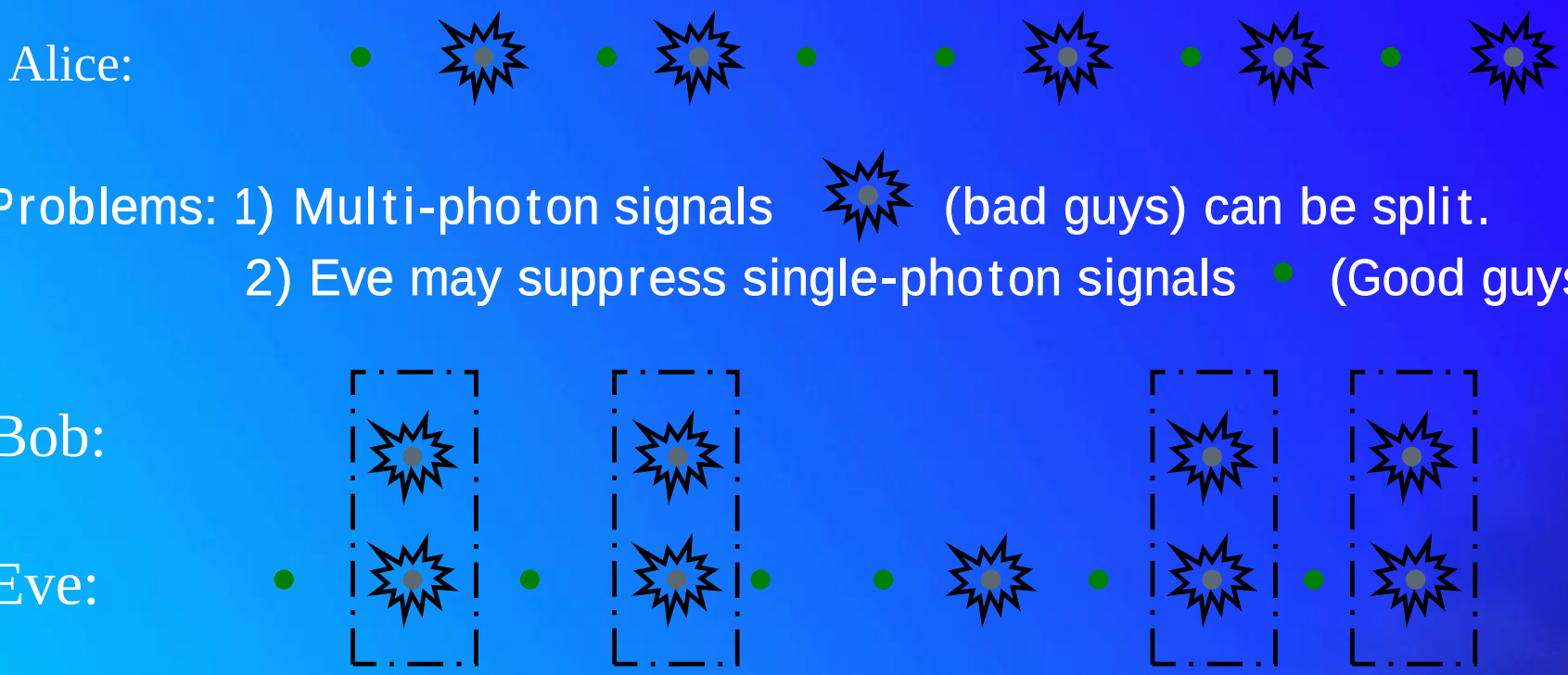
1. Source: (**Poisson photon number distribution**)
   Mixture. Photon number = k with probability: $\frac{a^k}{k!}e^{-a}$
   Some signals are, in fact, **double photons!**
2. Channel: Absorption inevitable. (e.g. 0.2 dB/km)
3. Detectors:
   (a) Efficiency ~30% for Telecom wavelengths
   (b) "Dark counts": 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?

2. Define the problem

Help!

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)

Figures of merits in QKD

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

  How many final key that Alice and Bob can generate?

- (Maximal) distance of secure QKD.

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

GLLP Formula for key generation rate

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

Error correction Privacy amplification

Q_μ is total # of detection events of signals.

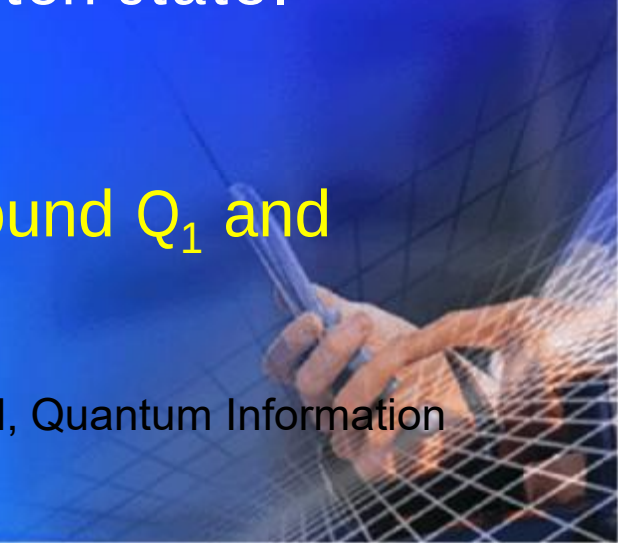
E_μ is overall bit error rate of signals.

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**, 325-360, quant-ph/0212066 (2004)

Prior Art Result

Consider the worst case scenario where all signals received by Bob are bad guys (Insecure, Multi-photon signal)

To prevent this from happening, we need:

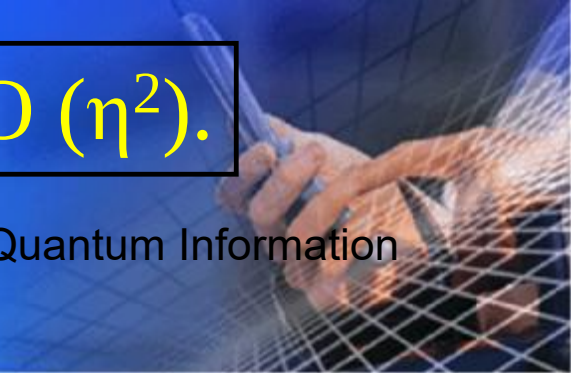
# of signals received by Bob

> # 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 $S = O(\eta^2)$.



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

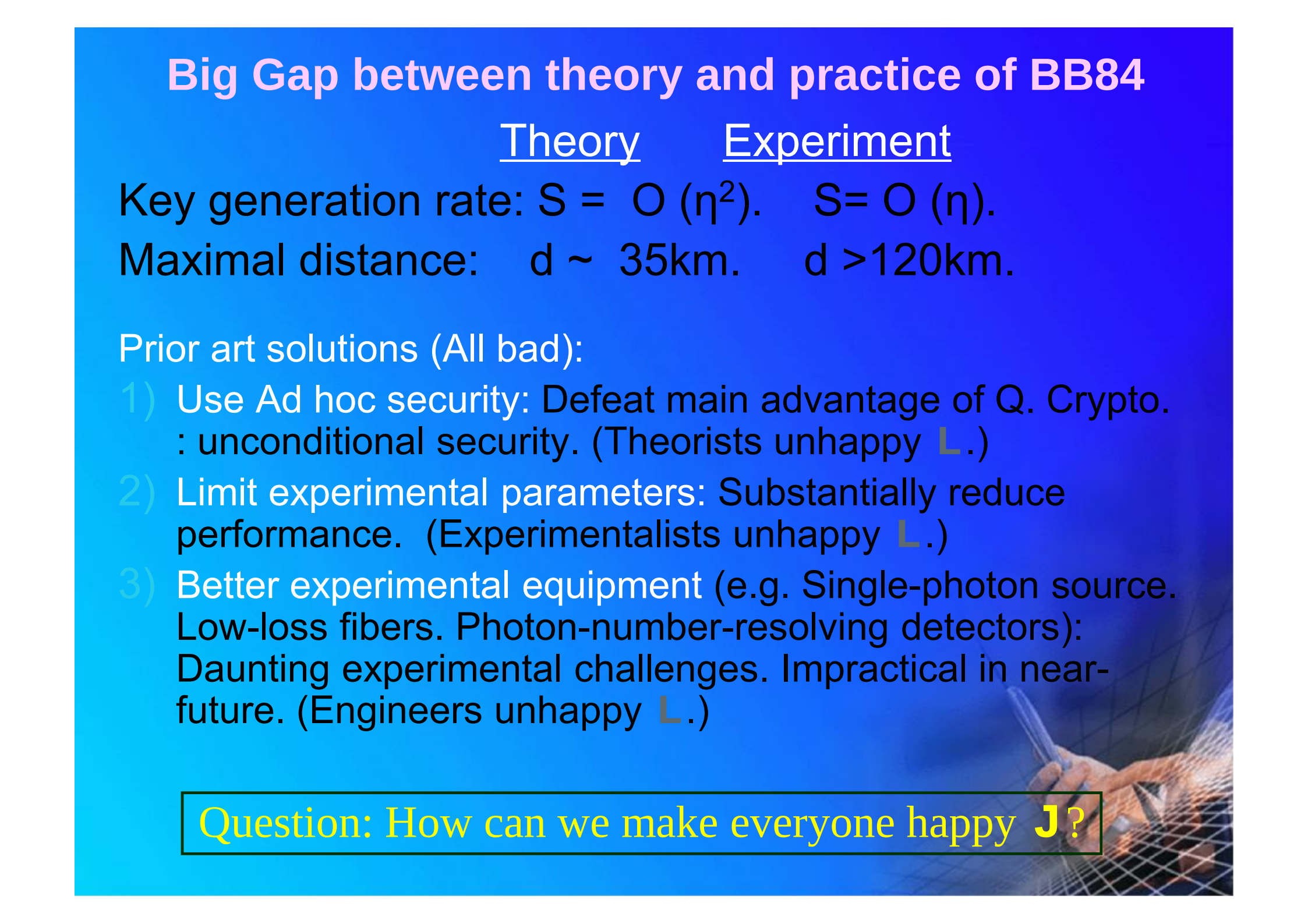
Big Gap between theory and practice of BB84

	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 L.)
2) Limit experimental parameters: Substantially reduce performance. (Experimentalists unhappy L.)
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 L.)

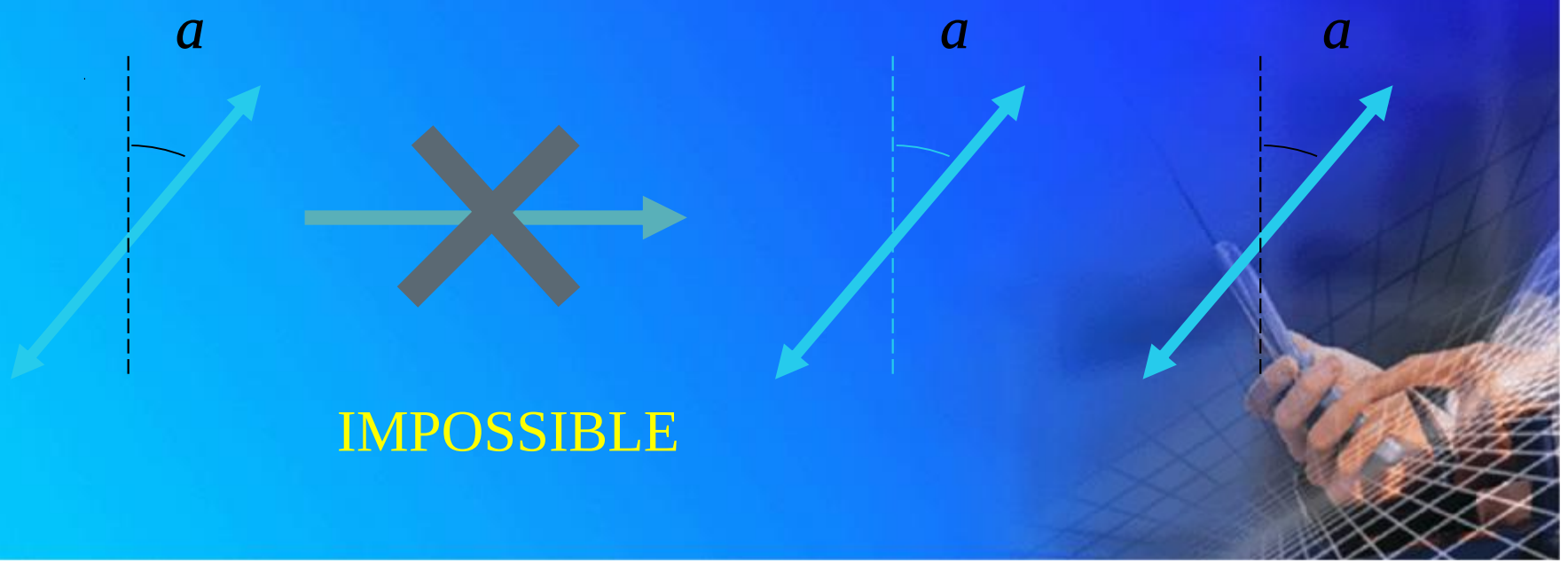
Question: How can we make everyone happy J?



Security: Quantum No-Cloning Theorem

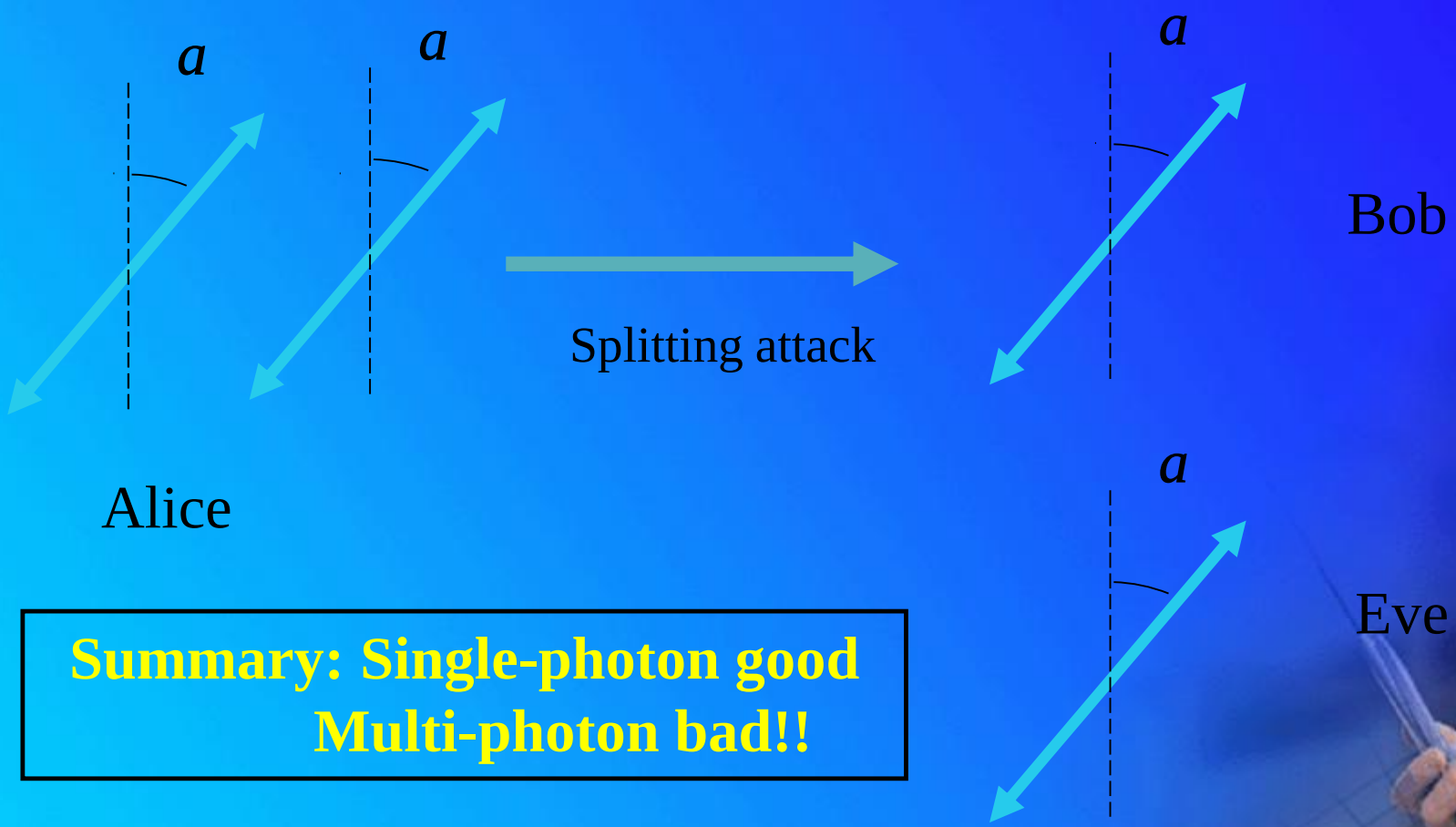
- An unknown quantum state **CANNOT** be cloned. Therefore, Eve cannot have the same information as Bob.

- Single-photon signals are secure.



Problem: Photon-Number Splitting (PNS) attack

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

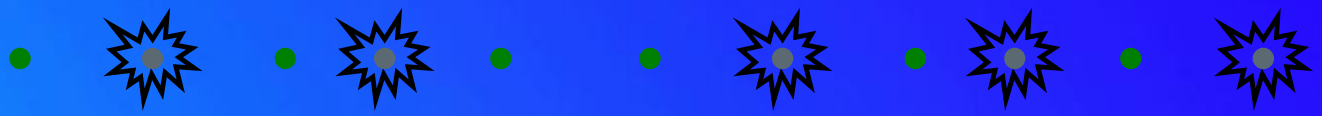


Summary: Single-photon good
Multi-photon bad!!

G Brassard, N Lütkenhaus, T Mor, B Sanders, Physical review letters 85, 1330 (2000)

Problem: Photon-Number Splitting (PNS) attack

Alice:

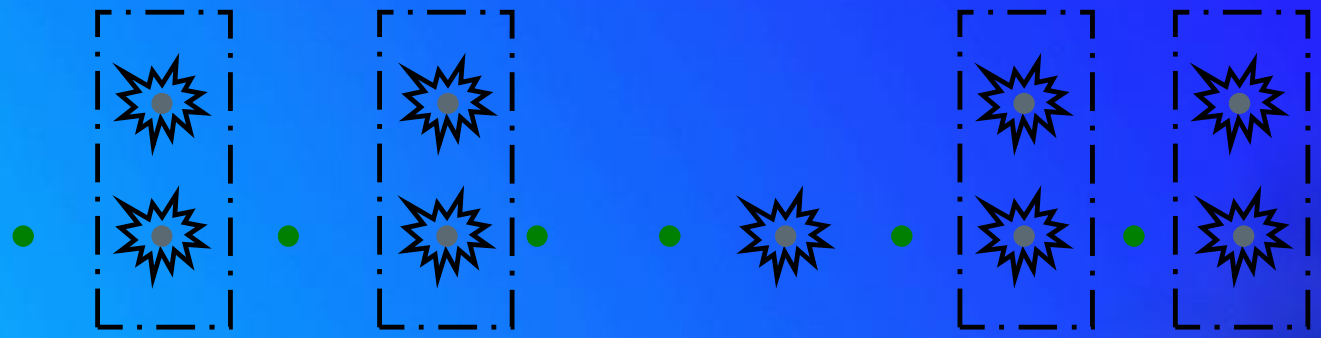


Problems: 1) Multi-photon signals (bad guys) can be split.

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

Bob:

Eve:



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)

GLLP Formula for key generation rate

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

Error correction — Privacy amplification

Q_μ is total # of detection events of signals.

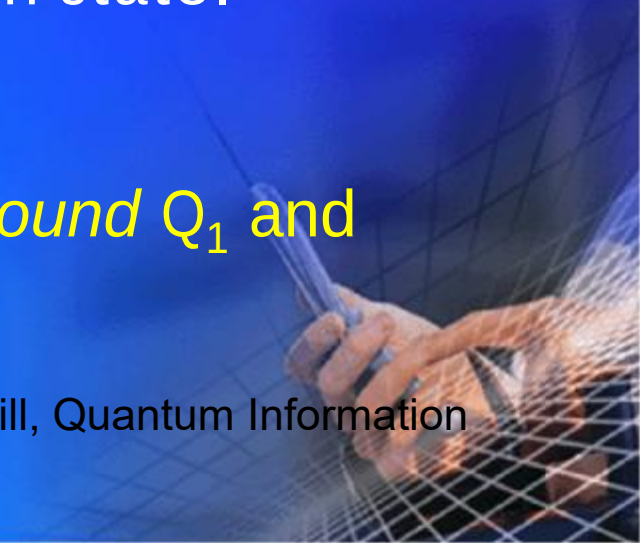
E_μ is overall bit error rate of signals.

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**, 325-360, quant-ph/0212066 (2004)

GLLP Formula for key generation rate

Consider the worst case scenario where **all** signals received by Bob are Multi-photon signal

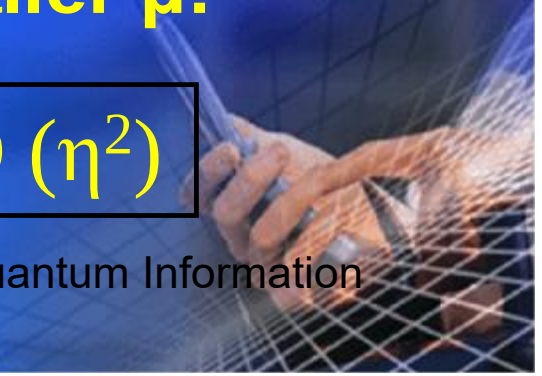
To prevent this from happening, we need:

# 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: **μ = O (η)**

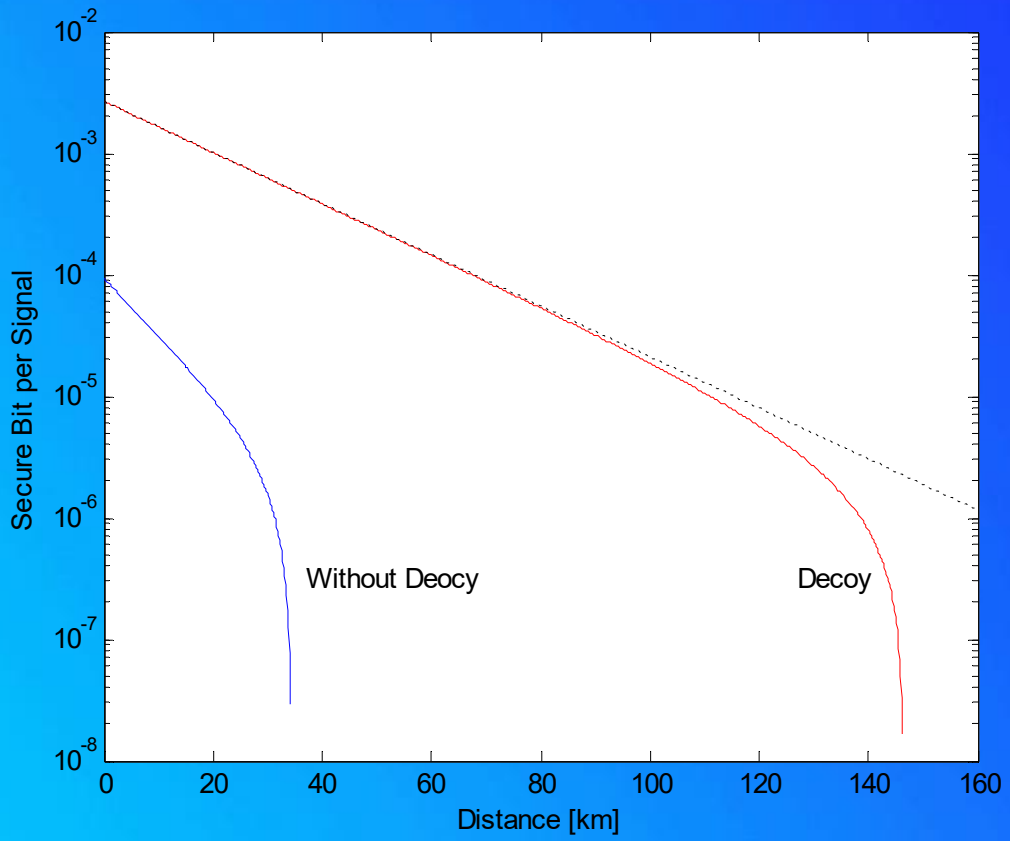
Longer distance needs much smaller μ!

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



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

Simulation results



Key parameter:

Wavelength: 1550nm

Channel loss: 0.2 dB/km

Signal error rate: **3.3%**

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

Receiver loss and detection efficiency: **4.5%**

QKD is ONLY practical within 35 km fiber!!

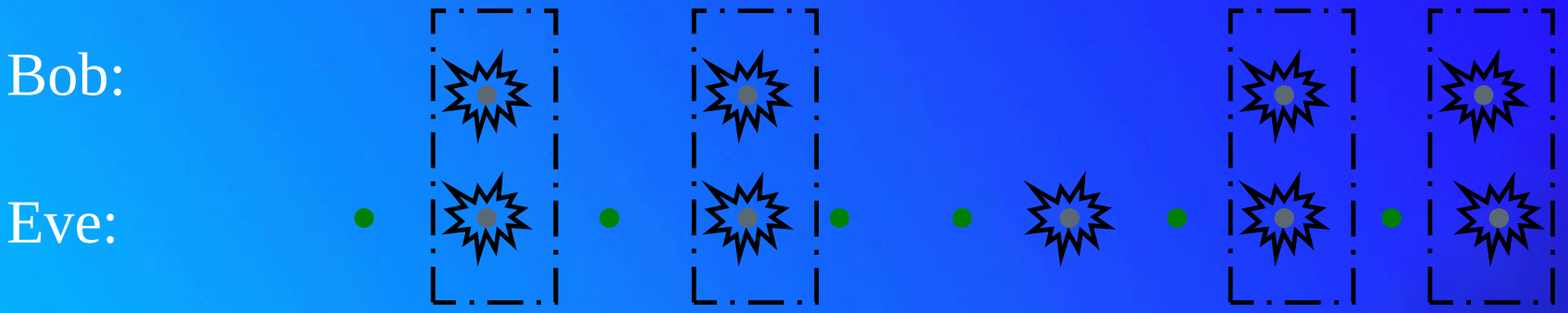
The experiment data for the simulation come from the paper:
C. Gobby, Z. L. Yuan, and A. J. Shields, Applied Physics Letters, (2004)

Decoy-state 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)*

Photon-Number Splitting (PNS) 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 PNS attack:

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

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

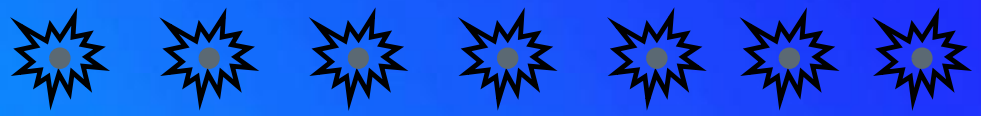
Yield for multi-photons may be much higher than single-photon

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. Then, Eve will be caught!

Procedure of Decoy State QKD (Toy Model)

A) Signal state: Poisson photon number distribution, coherent state 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: **μ~ 1** (at Alice). Mixture 1.

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

Hwang's **heuristic** idea (PRL-2003):

- If Eve lets an abnormally high fraction of multi-photons go to Bob, then decoy states will have an abnormally high transmission probability.

- Therefore, Alice and Bob can catch Eve!

W.-Y. Hwang, *Phys. Rev. Lett. 91, 057901 (2003)*

Can we make things rigorous and practical?

YES!

H.-K. Lo, X.-F. Ma, and K. Chen, *Phys. Rev. Lett. 94, 230504 (2005)*
X.-B. Wang, *Phys. Rev. Lett. 94, 230503 (2005)*

Experimental observation

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

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

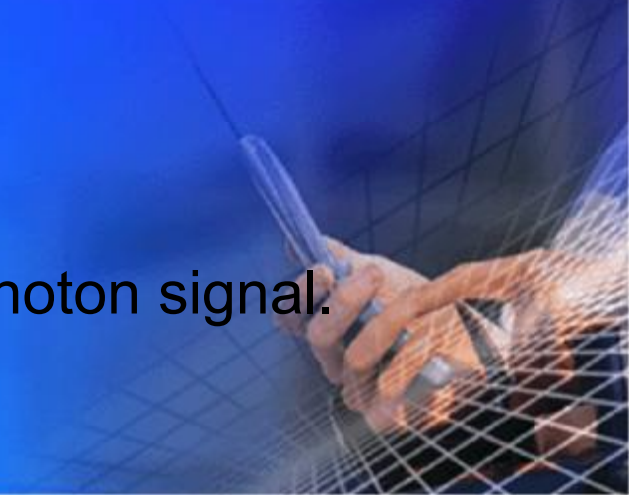
If Eve cannot treat the decoy state any differently from a signal state

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

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

Y_n: yield of an n-photon signal

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



Decoy-state ideas

Try **every** Poisson distribution μ_i!

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:

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

Decoy-state ideas

Conclusion: We severely limit Eve's eavesdropping strategies.

Any attempt by Eve to change *any* of (Y_n, e_n)'s will, in principle be caught.

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

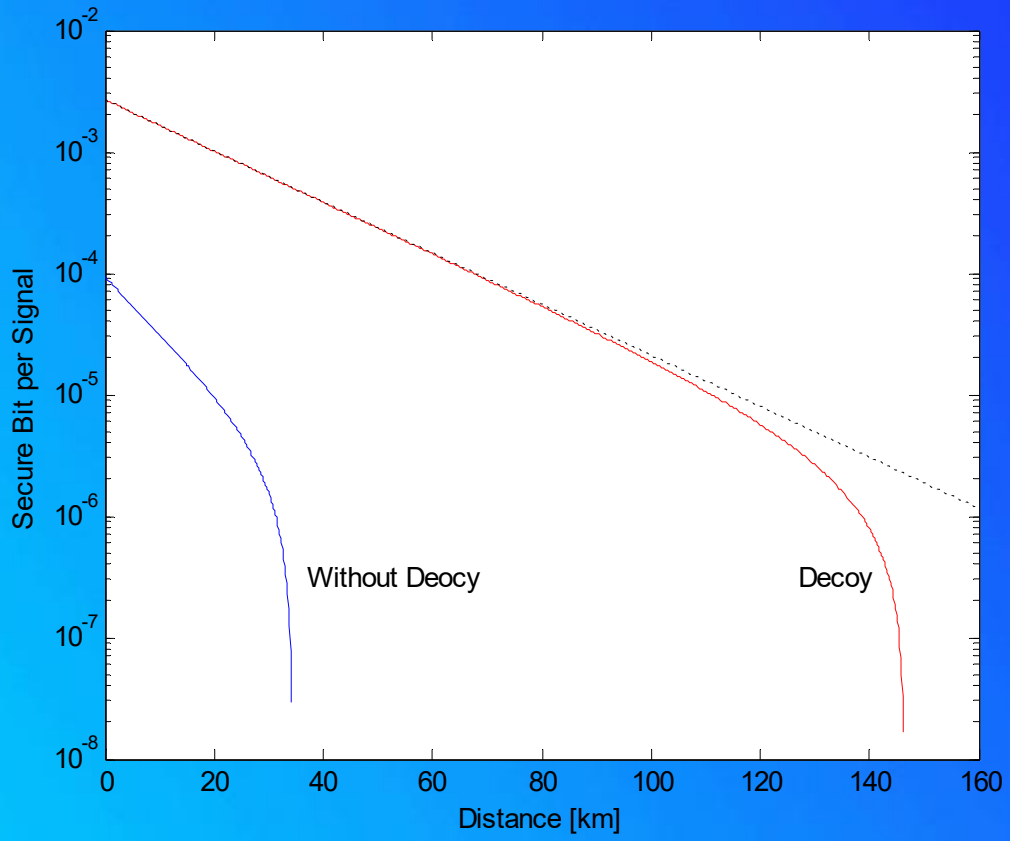
Decoy QKD

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)*

Compare the results with and without decoy states



Key parameter:

Wavelength: 1550nm

Channel loss: 0.2 dB/km

Signal error rate: 3.3%

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

Receiver loss and detection efficiency: 4.5%

Even with imperfect photon source, one gets much higher performance possible without compromising security.

The experiment data for the simulation come from the paper:
C. Gobby, Z. L. Yuan, and A. J. Shields, Applied Physics Letters, (2004)

Practical decoy-state ideas

1. *Making things rigorous* (Combine with GLLP security 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)
3. *Constructing a general theory with a finite number of decoy states* (bound Y_1 & e_1)

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

H.-K. Lo, X.-F. Ma, and K. Chen, *Phys. Rev. Lett. 94, 230504 (2005)*
X.-B. Wang, *Phys. Rev. Lett. 94, 230503 (2005)*

实用Decoy QKD

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, Decoy-state protocol for quantum cryptography with four different intensities of coherent light. Phys. Rev. A, 72, 012322 (2005)

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

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

其中 m 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 $\mathbf{Y_n}$，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。

$$R \geq = q\{-Q_m f(Q_m) H_2(E_m) + Q_1[1 - H_2(e_1)]\}$$

实用Decoy QKD

Bob端总的接收率为

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

同时总的量子误码率QBER满足

$$E_m Q_m = \sum_{i=0}^{\infty} e_i Q_i = \sum_{i=0}^{\infty} e_i Y_i \frac{m^i}{i!} e^{-m}$$

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。

- **How to calculate lower bound Q_1 and upper bound e_1?**
- **What are minimum number of decoy states?**

实用Decoy QKD

以一个信号态(平均光子数密度为m)和2个诱骗态（平均光子数密度分别为n_1,n_2）为例，假设 $n_1 \geq n_2 \geq 0, m > n_1 + n_2$

则有

$$Q_{n_1} e^{n_1} - Q_{n_2} e^{n_2} = Y_1(n_1 - n_2) + \sum_{i=2}^{\infty} \frac{Y^i}{i!}(n_1^i - n_2^i) \leq Y_1(n_1 - n_2) + \frac{(n_1^2 - n_2^2)}{m^2} \sum_{i=2}^{\infty} Y^i \frac{m^i}{i!}$$

$$= Y_1(n_1 - n_2) + \frac{(n_1^2 - n_2^2)}{m^2}(Q_m e^m - Y_0 - Y_1 m)$$

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 $a^i - b^i \leq a^2 - b^2$

实用Decoy QKD

可得单光子态的接收率的下限

$$Q_1 \geq Q_1^L = me^{-m}Y_1^L = \frac{m^2 e^{-m}}{mn_1 - mn_2 - n_1^2 + n_2^2}[Q_{n_1}e^{n_1} - Q_{n_2}e^{n_2} - \frac{n_1^2 - n_2^2}{m^2}(Q_m e^m - Y_0)]$$

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 $E_m Q_m$ 的公式,两式相减可得单光子态的QBER的上限，

$$e_1 \leq e_1^U = \frac{E_{n_1}Q_{n_1}e^{n_1} - E_{n_2}Q_{n_2}e^{n_2}}{(n_1 - n_2)Y_1^L}$$

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

$$R \geq = q\{-Q_m f(Q_m) H_2(E_m) + Q_1[1 - H_2(e_1)]\}$$

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

m 为光源的平均光子数密度；

Q_m 为光源信号态接收率；

E_m 是接收到的信号态误码率；

$H_2(x)$ 为二元熵函数；

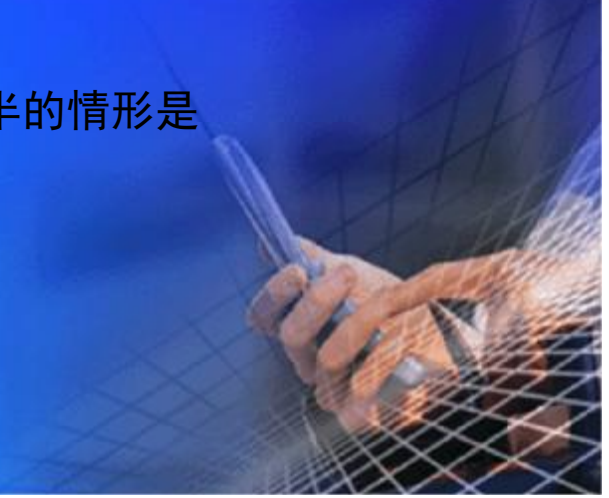
q 为系统效率，对于BB84协议来说为1/2，这是因为只有一半的情形是Alice和Bob选定了相同的基矢；

$f(Q_m)$ 为双边纠错效率，大于1；

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



Combining Decoy with GLLP

$$R \geq= q\{-Q_m f(Q_m) H_2(E_m) + Q_1[1 - H_2(e_1)]\}$$

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

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.
4. A useful tool for other quantum protocols!!

诱骗态QKD实验

量子通信国际动态

- 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

欧洲

美国

Ü “保持国家竞争力”计划中，量子信息为重点支持课题

Ü 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

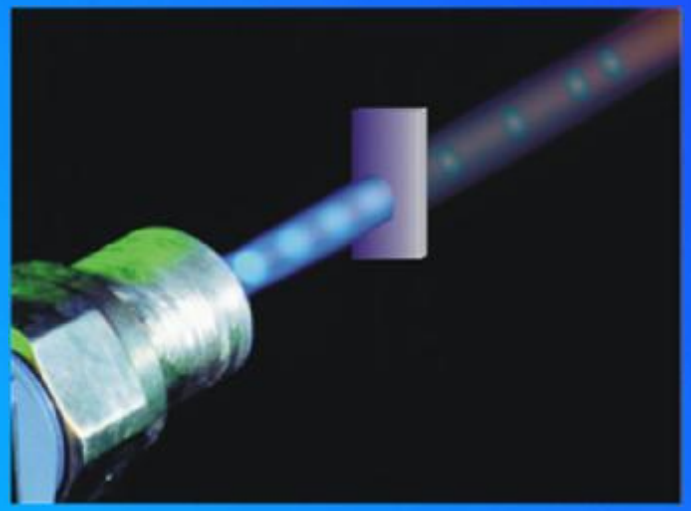
Ü 09年，美国军方完成了飞机与地面间的自由空间量子通信演示实验

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

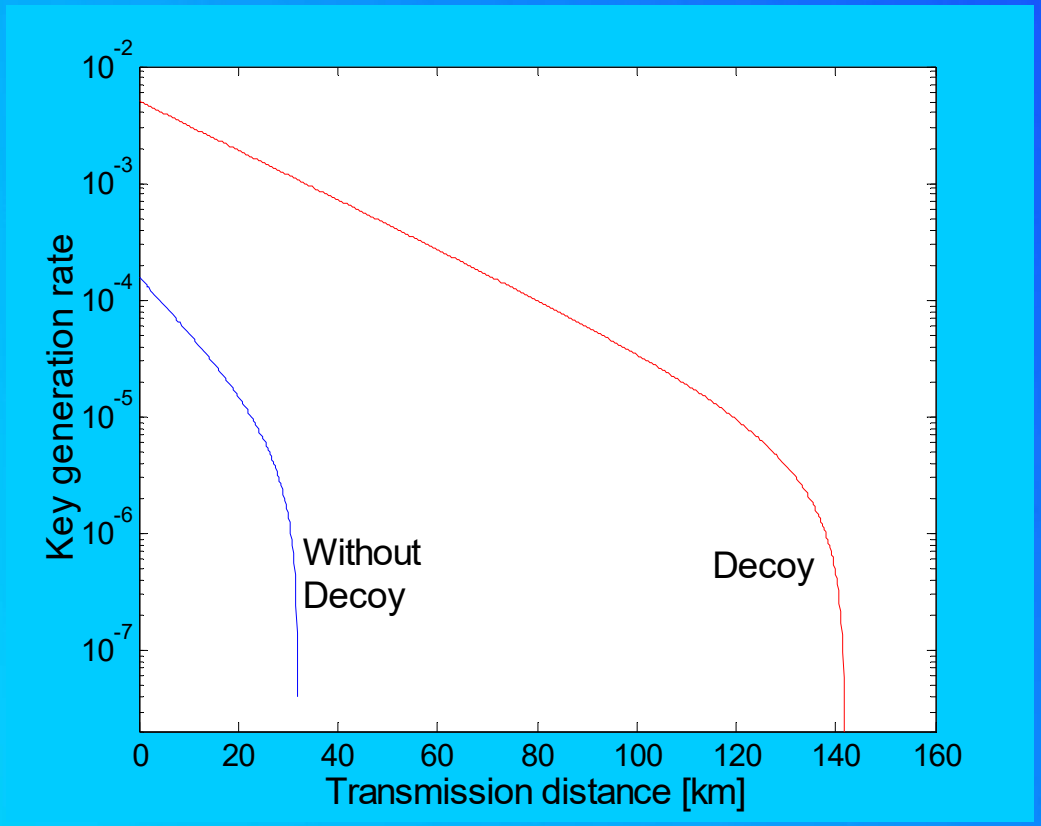
  B. Huttner et al, PRA 51, 1863 (1985)
  G. Brassard et al., PRL 85, 1330 (2000)

- 即使在理想情况下，
  信息安全传输的最远距离也只有30公里，且成码率极低

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/彭承志教授研究组(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)

- **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

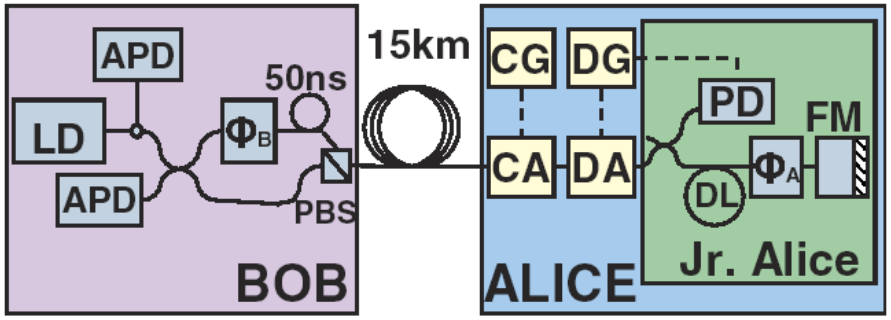


FIG. 1 (color online). Schematic of the experimental setup in our system. Inside Bob (Jr. Alice): Components in Bob's (Alice's) package of id Quantique QKD system. Our modifications: CA, compensating AOM; CG, compensating generator; DA, decoy AOM; DG, decoy generator. Original QKD system: LD, laser diode; 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(15km)

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

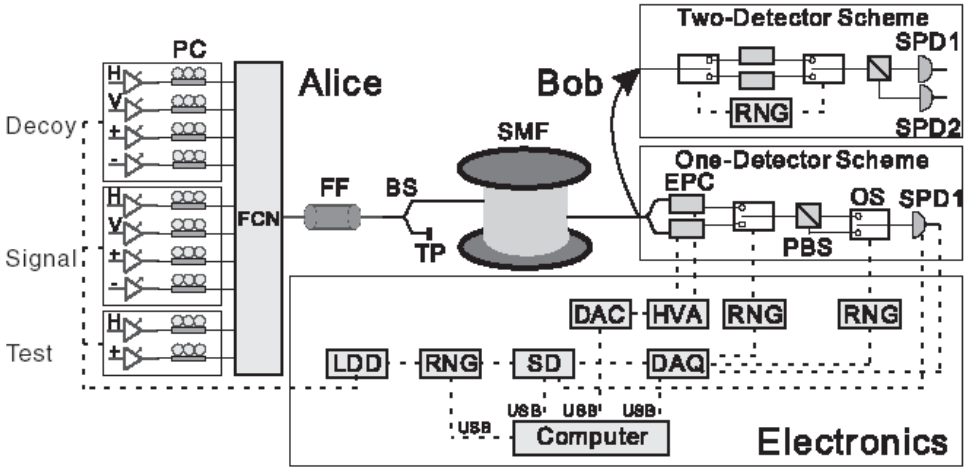


FIG. 1. Schematic diagram of the experimental setup. Solid lines and dashed lines represent the optical fiber and electric cable, respectively. See the text for the abbreviations.

基于诱骗态量子通信的实验

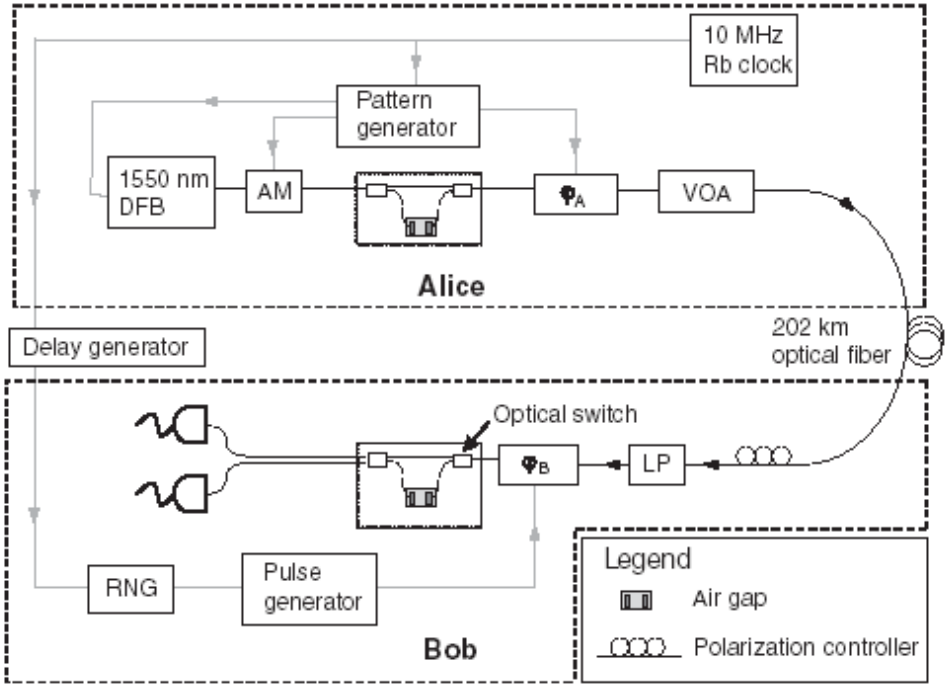


FIG. 1. QKD system used in this work. DFB, distributed feedback laser; VOA, variable optical attenuator; AM, amplitude modulator; LP, linear polarizer; RNG, random number generator.

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

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

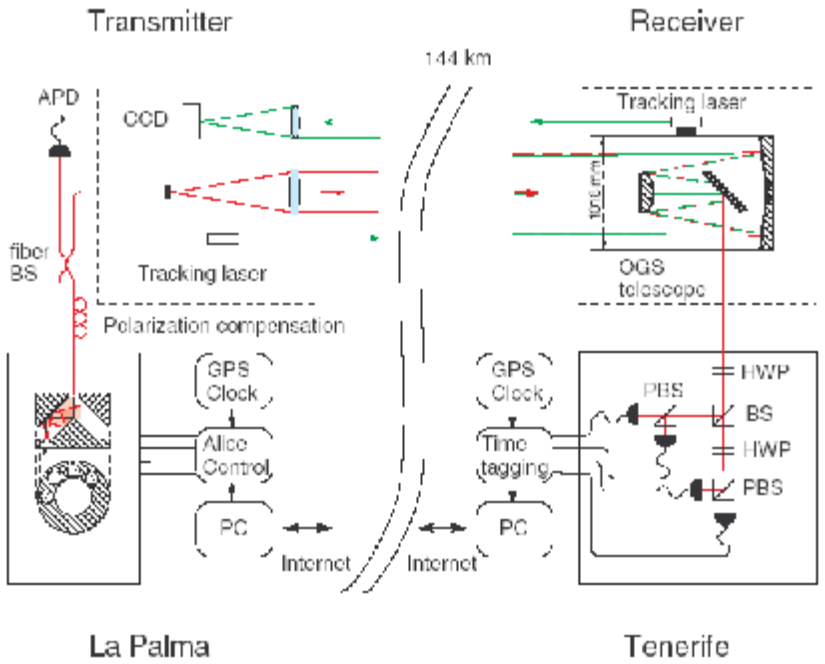


FIG. 2 (color online). Schematics of the experimental setup on the two canary islands. BS, beam splitter; PBS, polarizing beam splitter; HWP, half-wave plate; APD, avalanche photo diode.

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

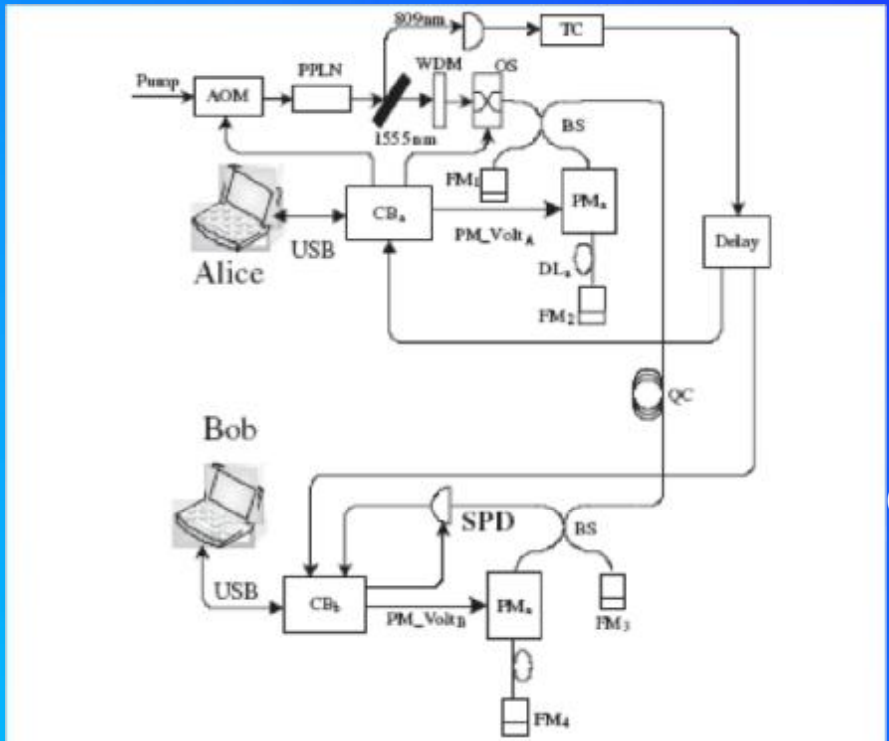


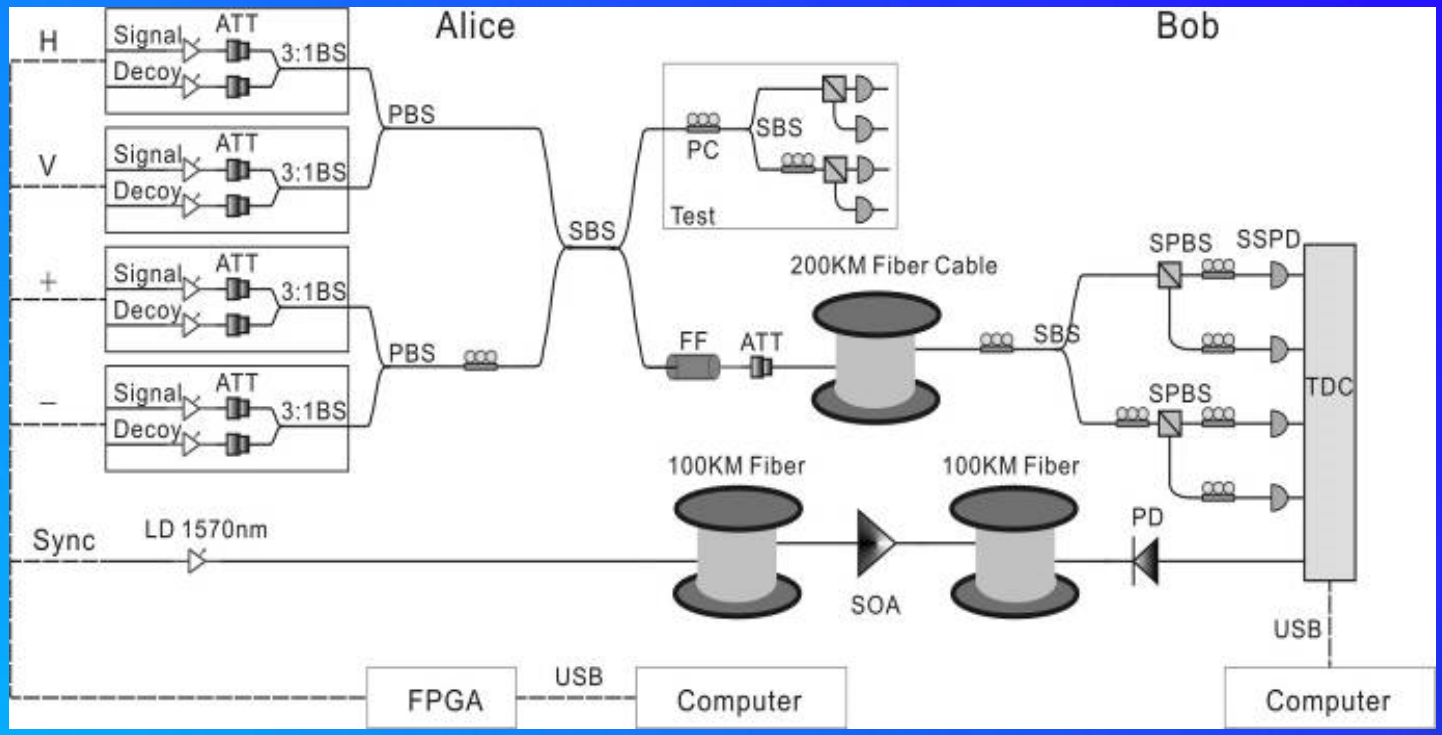
FIG. 2. The experimental setup of our quantum key transmission system. PPLN: periodically-poled $LiNbO_3$, AOM: acousto-optical-modulator, WDM: wavelength-division multiplexing, OS: optical switch, TC: time chopper, BS: beam-splitter, FM: Faraday Mirror, PM: phase modulator, DL: delay line, QC: quantum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

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).

QKD的现实安全性

现实安全性

1989年首个量子密码实验

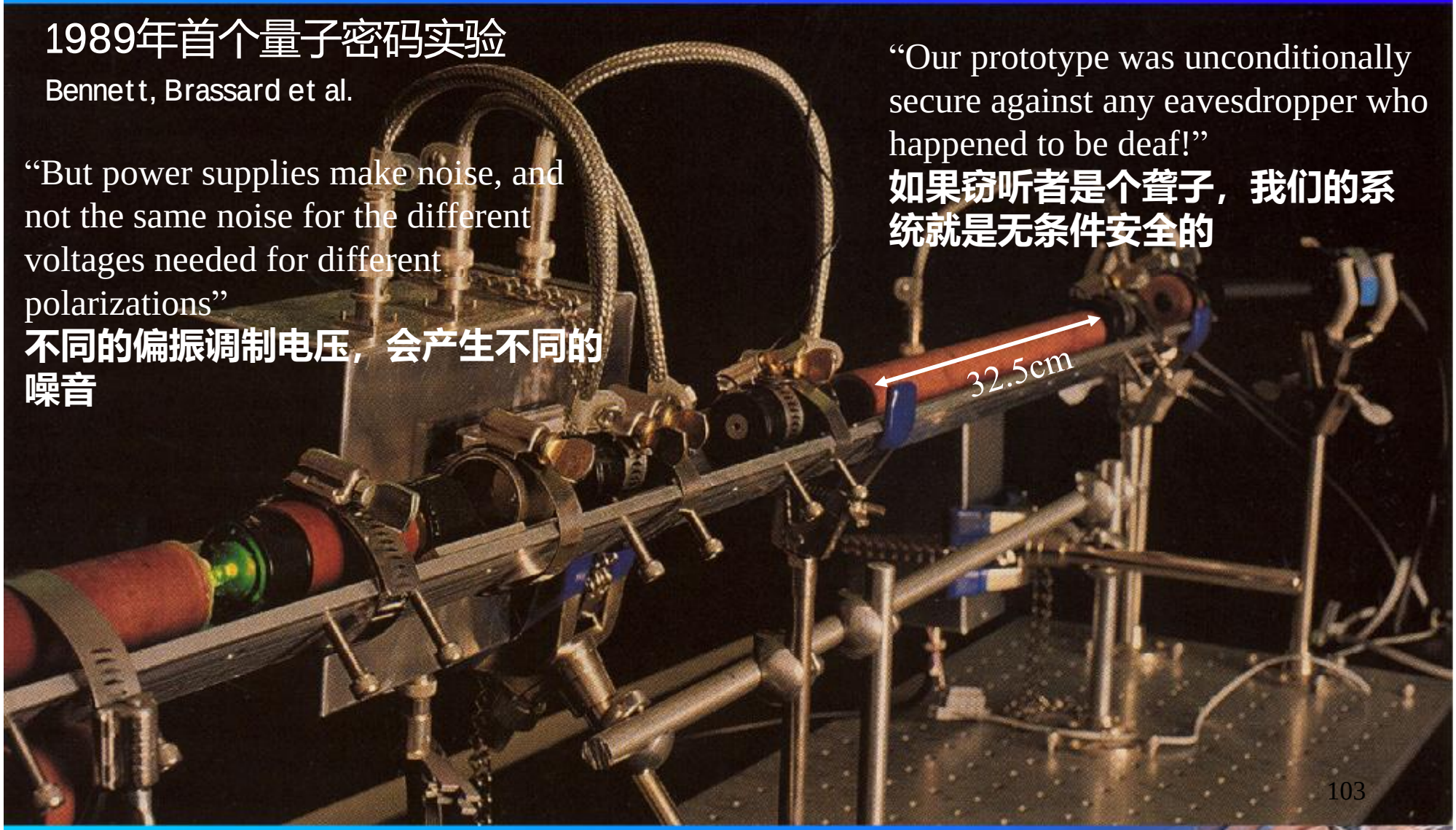
Bennett, Brassard et al.

“But power supplies make noise, and not the same noise for the different voltages needed for different polarizations”

不同的偏振调制电压，会产生不同的噪音

“Our prototype was unconditionally secure against any eavesdropper who happened to be deaf!”

如果窃听者是个聋子，我们的系统就是无条件安全的



G. Brassard, Brief History of Quantum Cryptography: A Personal Perspective, arXiv:quant-ph/0604072 (2006)

现实安全性

Attack	Source/Detection	Target component	Manner	Year
Photon-number-splitting (Brassard et al., 2000; Lütkenhaus, 2000)	Source	WCP (multi-photons)	Theory	2000
Detector fluorescence (Kurtsiefer et al., 2001)	Detection	Detector	Theory	2001
Faked-state (Makarov et al., 2006; Makarov and Hjelme, 2005)	Detection	Detector	Theory	2005
Trojan horse (Gisin et al., 2006; Vakhitov et al., 2001)	Source&Detection	Backflection light	Theory	2006
Time shift (Qi et al., 2007; Zhao et al., 2008)	Detection	Detector	Experiment	2007
Time side-channel (Lamas-Linares and Kurtsiefer, 2007)	Detection	Timing information	Experiment	2007
Phase remapping (Fung et al., 2007; Xu et al., 2010)	Source	Phase modulator	Experiment	2010
Detector blinding (Lydersen et al., 2010b; Makarov, 2009)	Detection	Detector	Experiment	2010
Detector blinding (Gerhardt et al., 2011a,b)	Detection	Detector	Experiment	2011
Detector blinding (Lydersen et al., 2011; Wiechers et al., 2011)	Detection	Detector	Experiments	2011
Faraday mirror (Sun et al., 2011)	Source	Faraday mirror	Theory	2011
Wavelength (Huang et al., 2013; Li et al., 2011)	Detection	Beam-splitter	Experiment	2011
Dead-time (Henning et al., 2011)	Detection	Detector	Experiment	2011
Channel calibration (Jain et al., 2011)	Detection	Detector	Experiment	2011
Intensity (Jiang et al., 2012; Sajeed et al., 2015b)	Source	Intensity modulator	Experiment	2012
Phase information (Sun et al., 2012, 2015; Tang et al., 2013)	Source	Phase randomization	Experiment	2012
Memory attacks (Barrett et al., 2013)	Detection	Classical memory	Theory	2013
Local oscillator (Jouguet et al., 2013; Ma et al., 2013)	Detection	Local oscillator	Experiment	2013
Trojan horse (Jain et al., 2014, 2015)	Source&Detection	Backflection light	Experiment	2014
Laser damage (Bugge et al., 2014; Makarov et al., 2016)	Detection	Detector	Experiment	2014
Detector saturation (Qin et al., 2016)	Detection	Homodyne detector	Experiment	2016
Pattern effect (Yoshino et al., 2018)	Source	Intensity modulator	Experiment	2018

F. Xu, X. Ma, Q. Zhang, H.-K. Lo, J.-W. Pan, *Review of Modern Physics*, 92, 025002 (2020)

量子密码的现实安全性

量子密码的现实安全性

Alice

Bob

系统安全 = 理论安全 & 系统模型

“量子攻击”

解决方案

探测端的安全性

MDI-QKD

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 J

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


单光子探测器

Photodiode (P-N junction)

- P-N junction; input photon creates e-h pair, pushing e into conduction band
- P-layer collects holes, N-layer collects electrons

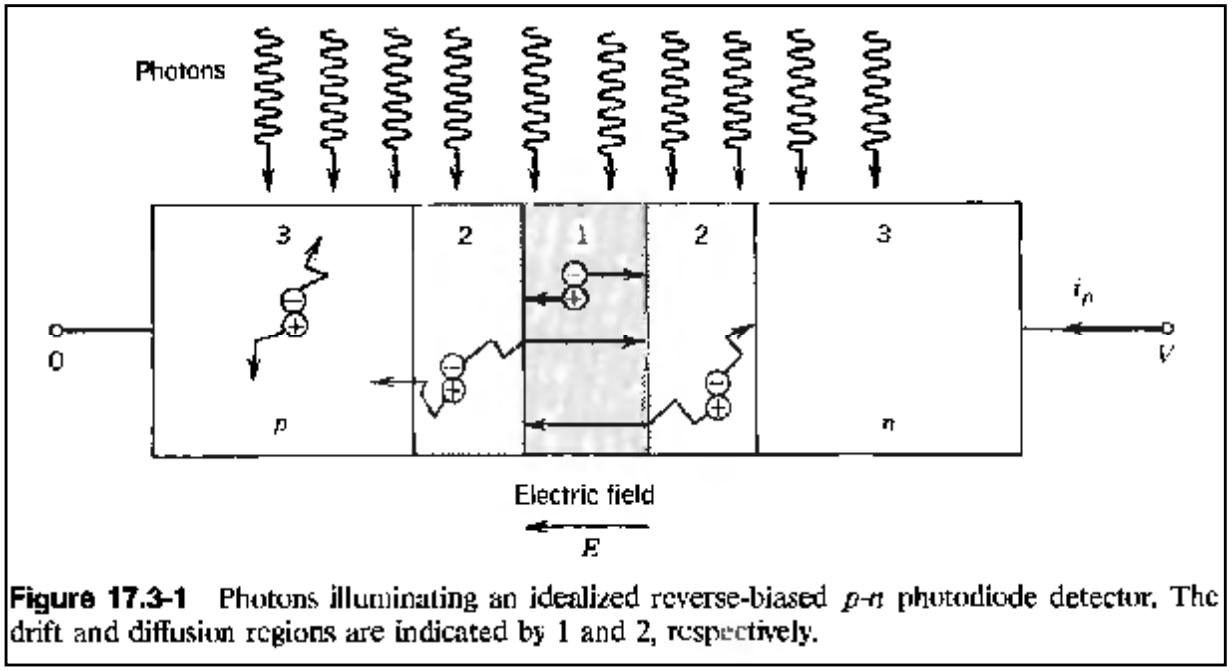
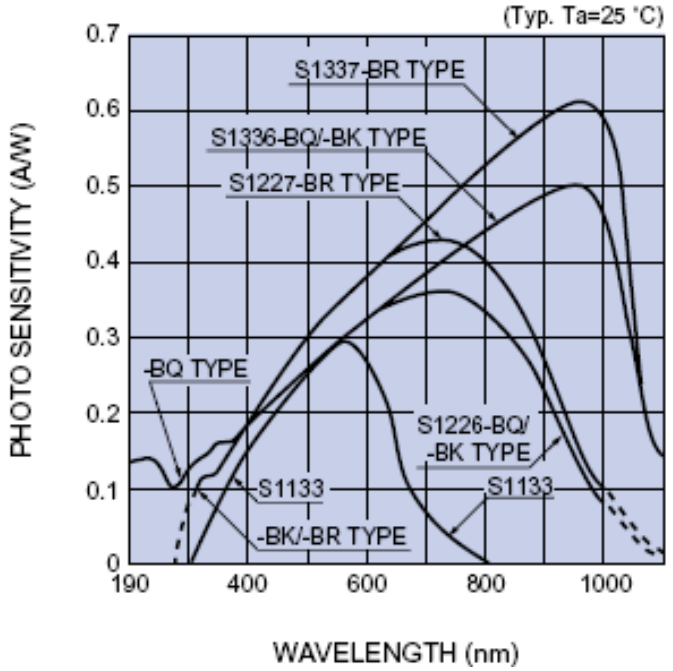


Figure 17.3-1 Photons illuminating an idealized reverse-biased *p-n* photodiode detector. The drift and diffusion regions are indicated by 1 and 2, respectively.



Avalanche photodiode (APD)

- High reverse-bias voltage enhances the E field
- Electrons and holes excited by the photons are accelerated in the strong E field
- Collisions causing impact-ionization of more electron-hole pairs

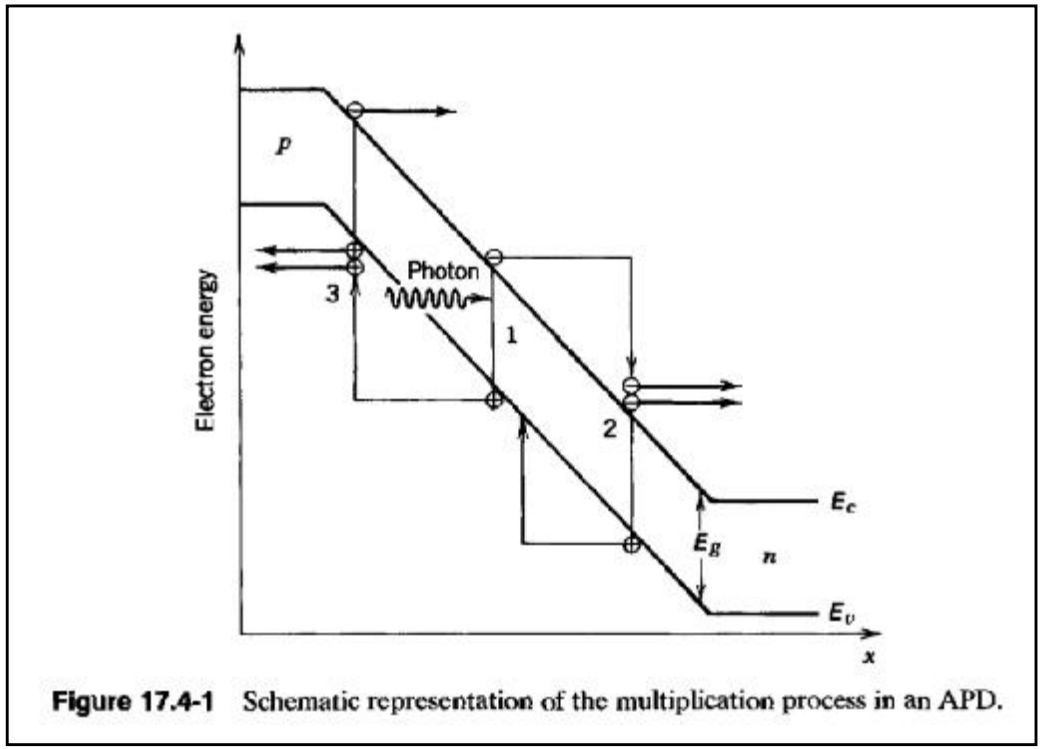
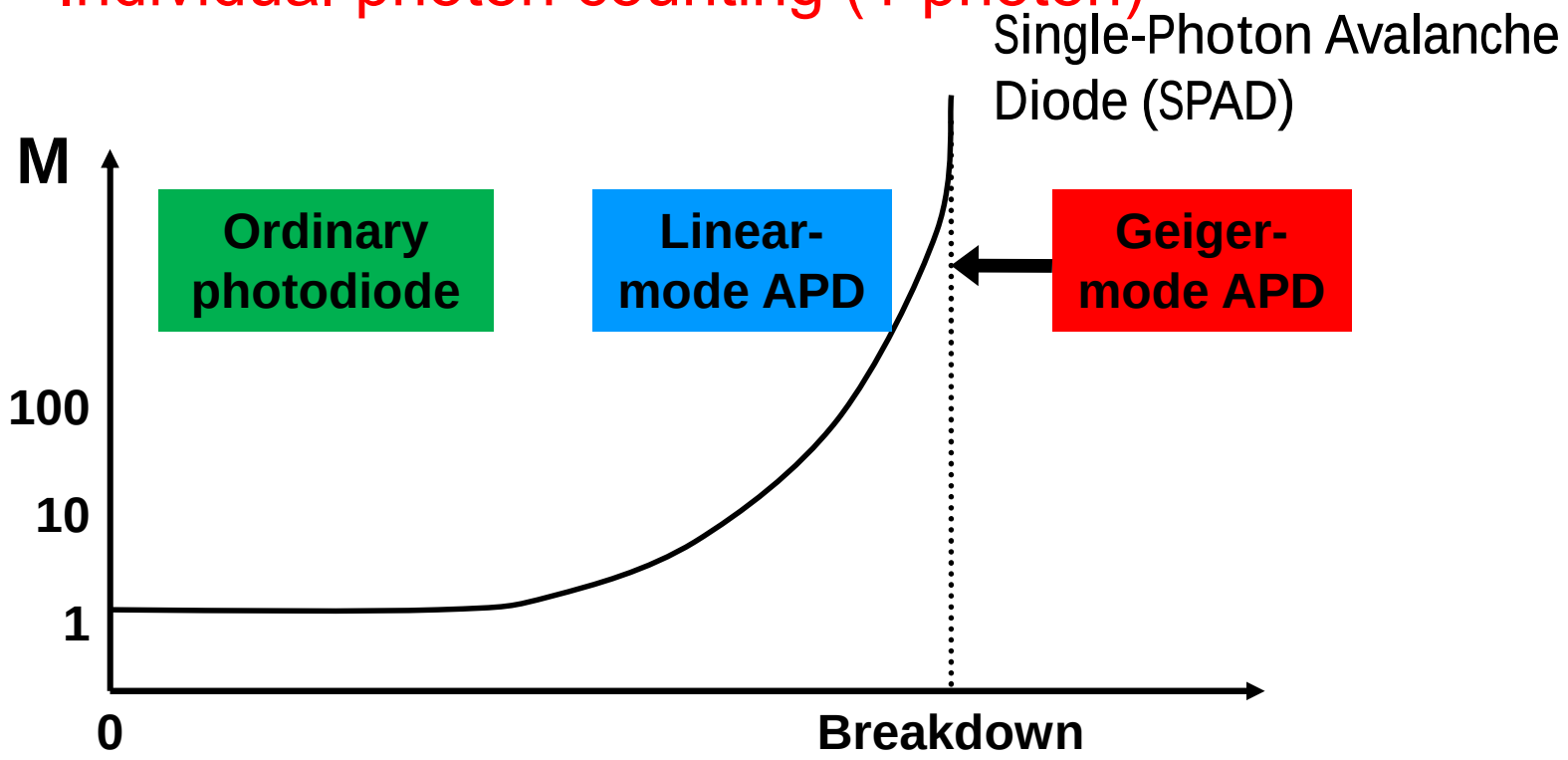


Figure 17.4-1 Schematic representation of the multiplication process in an APD.

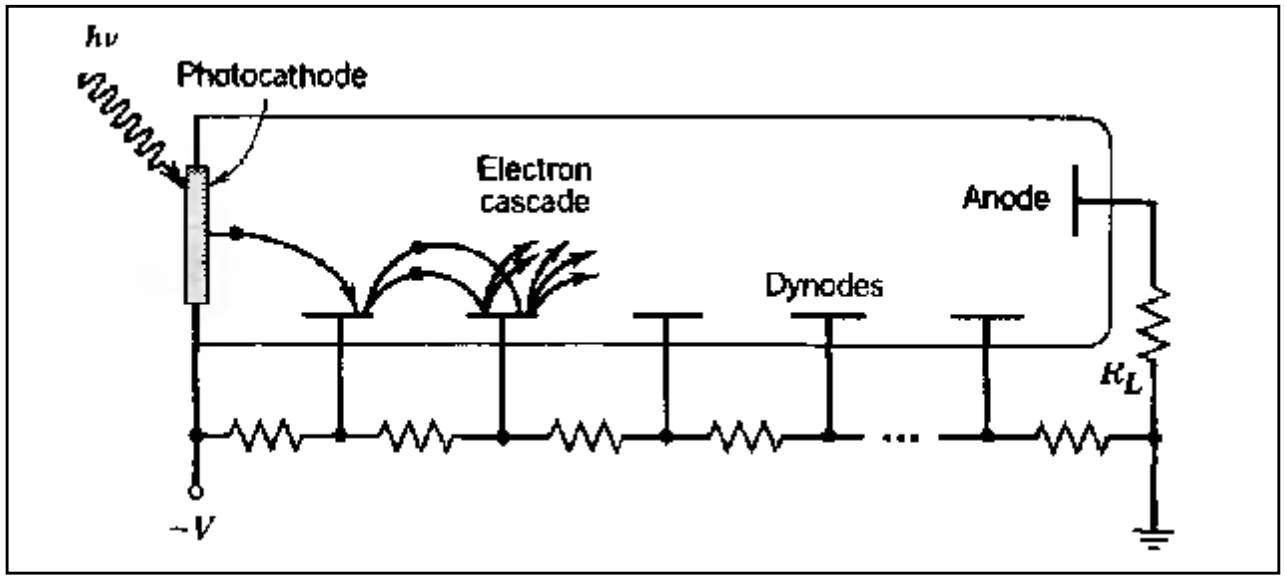
Operation modes of photodiode

- Ordinary mode
- Linear-mode APD
- Geiger-mode APD

Individual photon counting (1 photon)



Photomultiplier (PMT)



Superconducting Nano-wire (SNSPD)

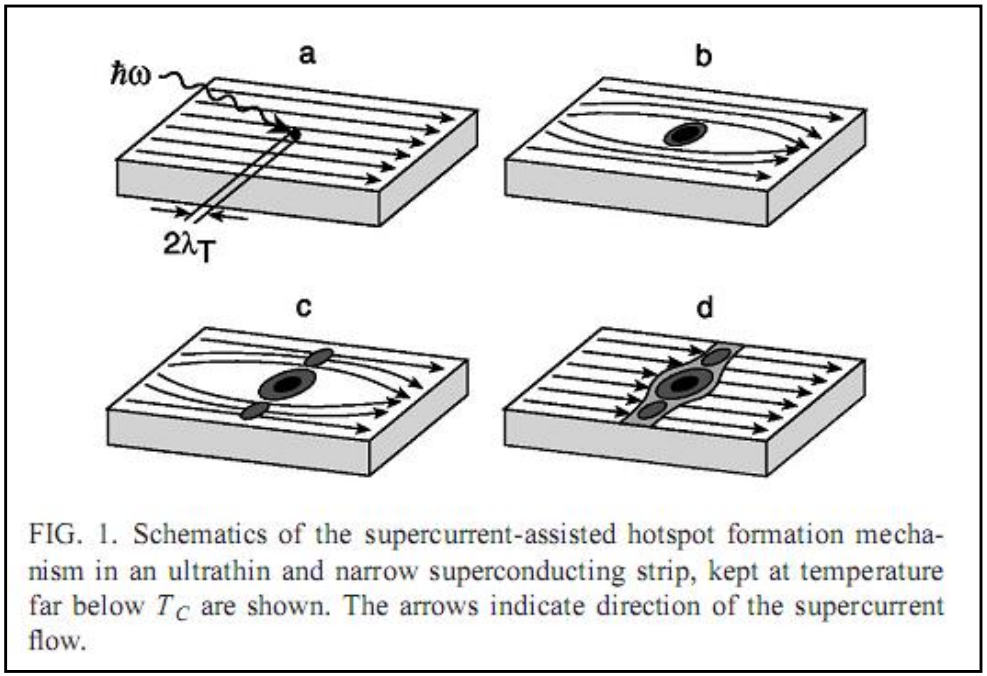
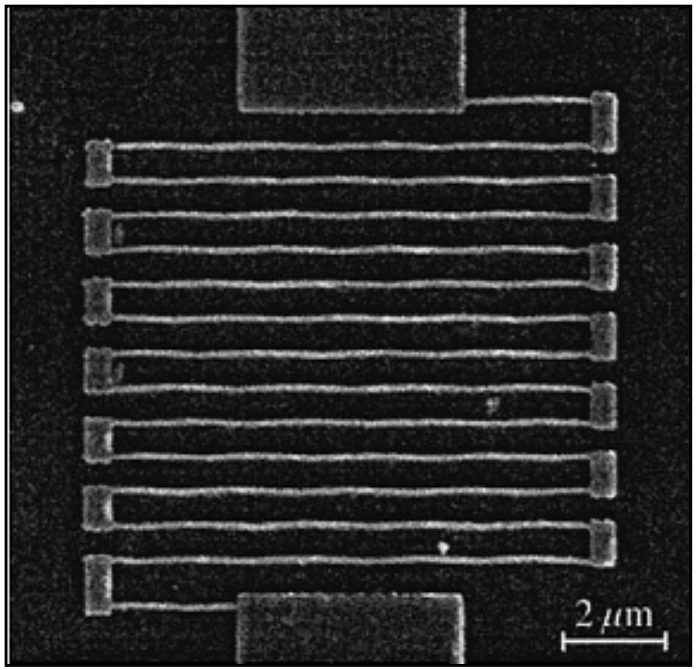


FIG. 1. Schematics of the supercurrent-assisted hotspot formation mechanism in an ultrathin and narrow superconducting strip, kept at temperature far below T_C are shown. The arrows indicate direction of the supercurrent flow.

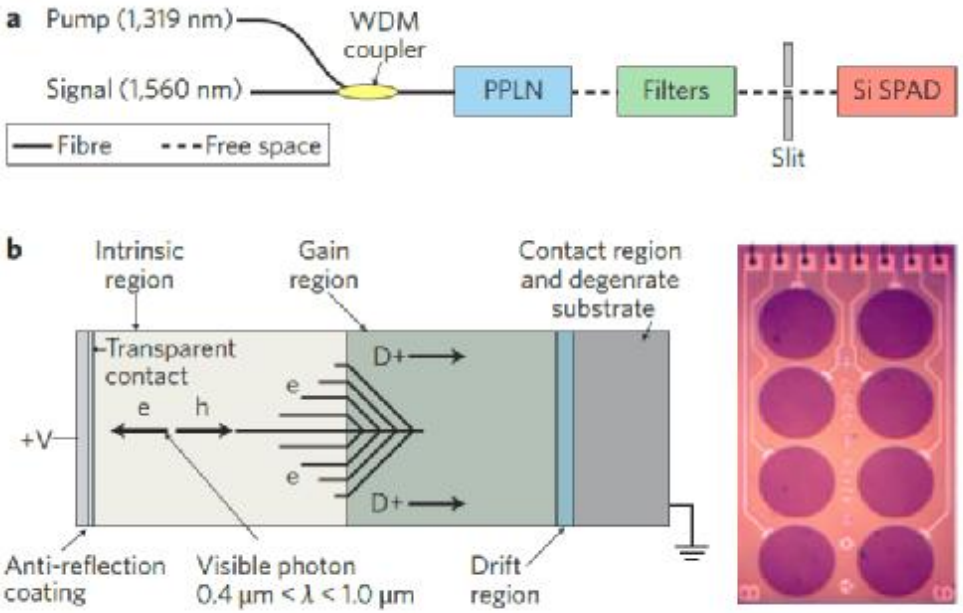


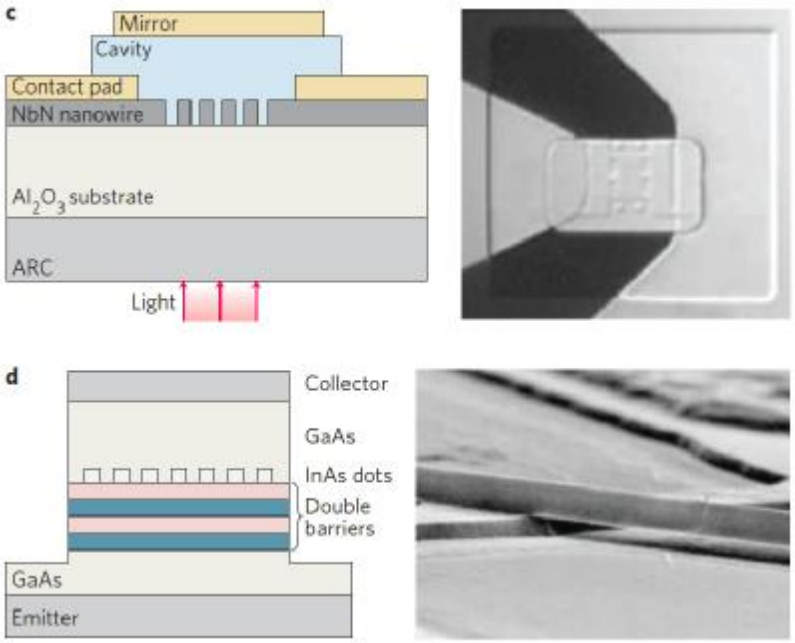
Nature Photonics 3, 696 (2009)

REVIEW ARTICLES | FOCUS
PUBLISHED ONLINE: 30 NOVEMBER 2009 | DOI: 10.1038/NPHOTON.2009.230
nature photonics

Single-photon detectors for optical quantum information applications

Robert H. Hadfield

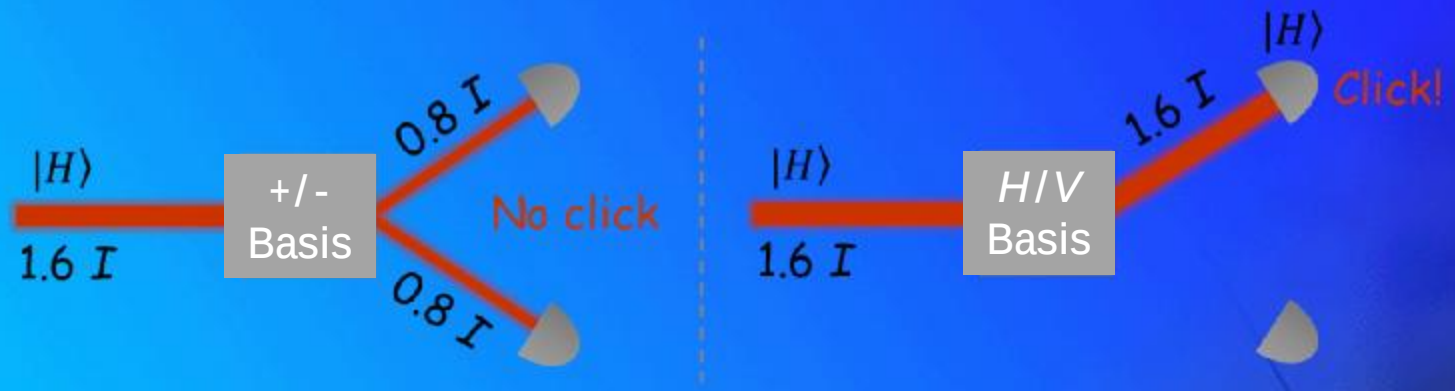




探测器的安全性

NEW found security loophole : imperfect single-photon detectors

Blinding attack: can fully control detectors by specially tailored strong light [Lydersen *et al.*, Nature Photonics 4, 686 (2010)]



Measurement Device Independent (MDI)-QKD

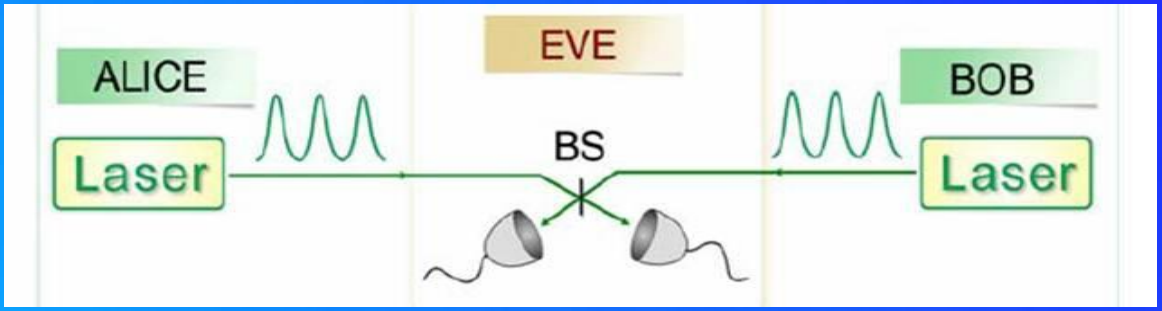
Immune to any attacks on detector

Scheme:

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

Experiment:

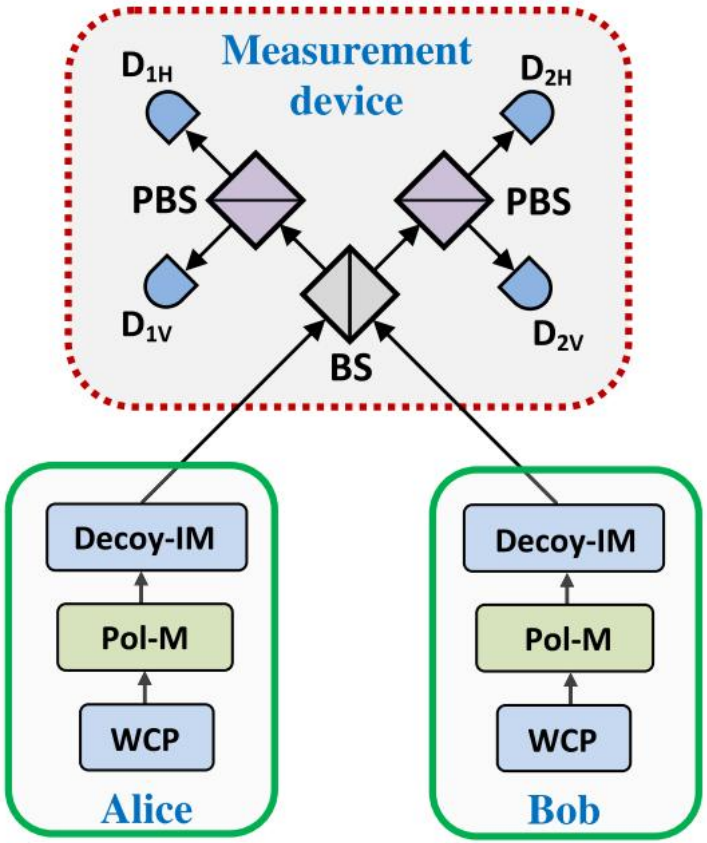
Liu *et al.*, PRL 111, 130502 (2013)



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



$$R = Q_{\text{rect}}^{1,1}[1 - H(e_{\text{diag}}^{1,1})] - Q_{\text{rect}} f(E_{\text{rect}}) H(E_{\text{rect}}), \quad (1)$$

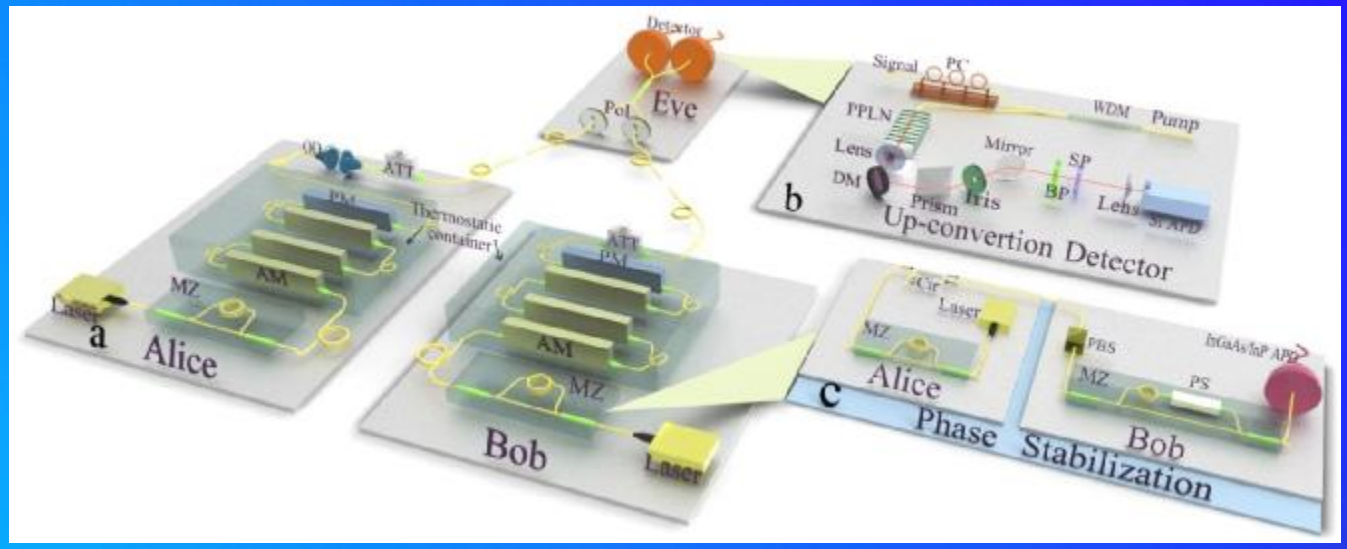
where Q_{rect} and E_{rect} denote, respectively, the gain and QBER in the rectilinear basis (i.e., $Q_{\text{rect}} = \sum_{n,m} Q_{\text{rect}}^{n,m}$, and $E_{\text{rect}} = \sum_{n,m} Q_{\text{rect}}^{n,m} e_{\text{rect}}^{n,m} / Q_{\text{rect}}$), $f(E_{\text{rect}}) > 1$ is an inefficiency function for the error correction process, and $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function.

First, we have implicitly assumed that the decoy-state method can be used to estimate the gain $Q_{\text{rect}}^{1,1}$ and the QBER $e_{\text{diag}}^{1,1}$. Second, we need to evaluate the secret key rate given by Eq. (1) for a realistic setup. Let us tighten up these loose ends here. Indeed, it can be shown that the technique to estimate the relevant parameters in the key rate formula is equivalent to that used in standard decoy-state QKD systems (see supplemental material for details

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

Measurement Device Independent (MDI)-QKD

Since coincidence detection is needed, the detection efficiency is important

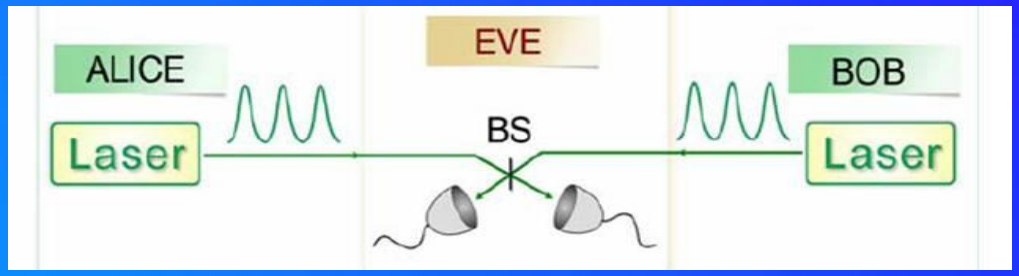


- Typical efficiency of single-photon InGaAs/InP APD at communication wavelength (1550nm): 10%
- Low noise up-conversion detector: 34%
  → increase coincidence probability for ~11 times

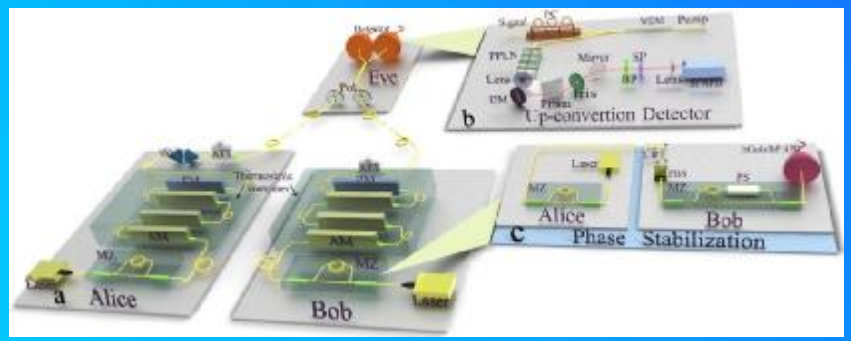
→

- MDI-QKD in 50km fiber
- Can achieve a transmission of more than 400km currently

Measurement Device Independent (MDI)-QKD



Requirement: high-precision interference between two remote independent lasers Æ relative timing jitter after hundreds km fiber < 10ps



First experiment (50km):

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

Extended distance:

- 200km: PRL 113, 190501 (2014)
- 404km: PRL 117, 190501 (2016)

Measurement Device Independent (MDI)-QKD

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).