

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（徐飞虎、陈凯老师）
- ◆ 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

REVIEWS OF MODERN PHYSICS

[Recent](#) [Accepted](#) [Authors](#) [Referees](#) [Search](#) [Press](#) [About](#) [Staff](#) 

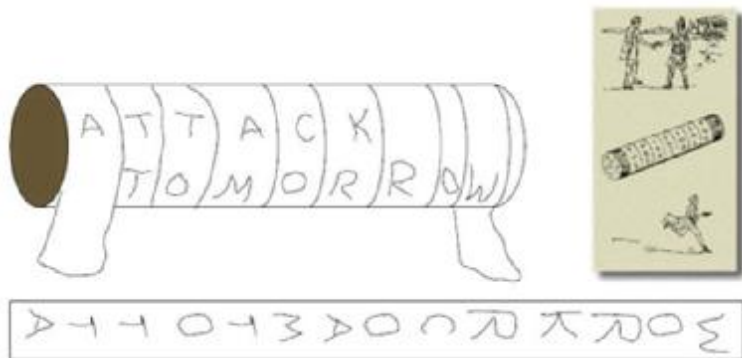
Secure quantum key distribution with realistic devices

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)

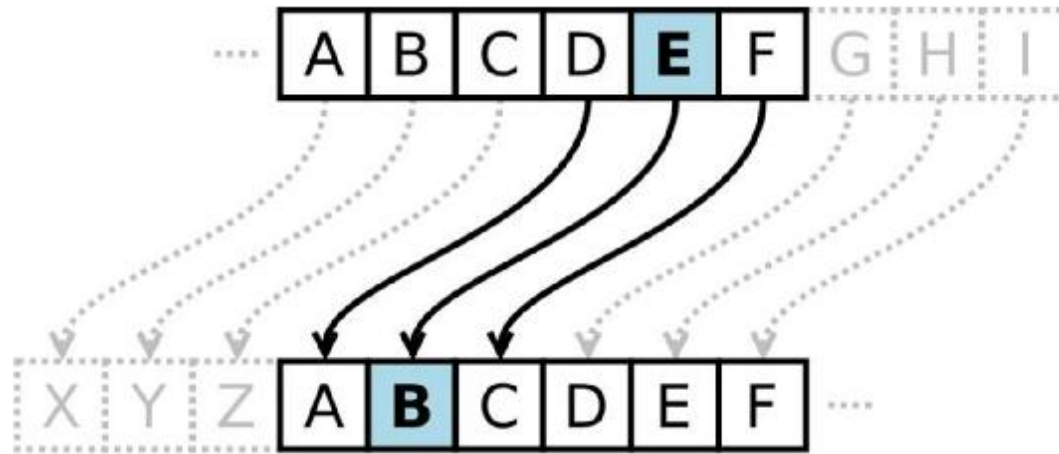
- 恺撒大帝曾用此方法对重要的军事信息进行加密
 - 使用暗号, 即改变字母顺序, 使局外人无法组成一个单词
 - 想读懂意思, 得用第4个字母置换第一个字母, 即以D代A, 以此类推

密文: GRJ

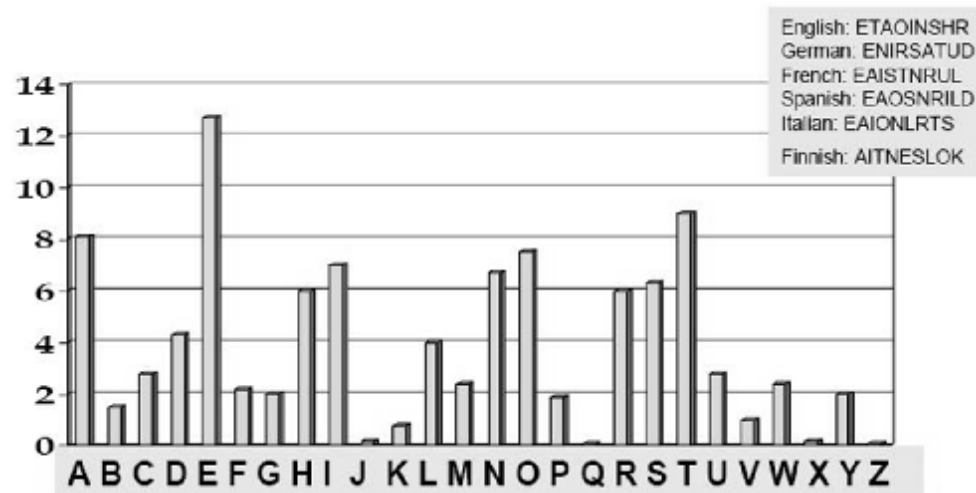
明文: DOG

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

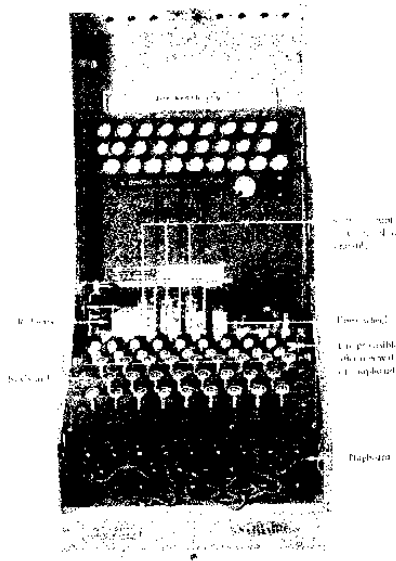


Figure 49 A German Enigma Machine from the 1920s. Photo courtesy of the British Library.

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

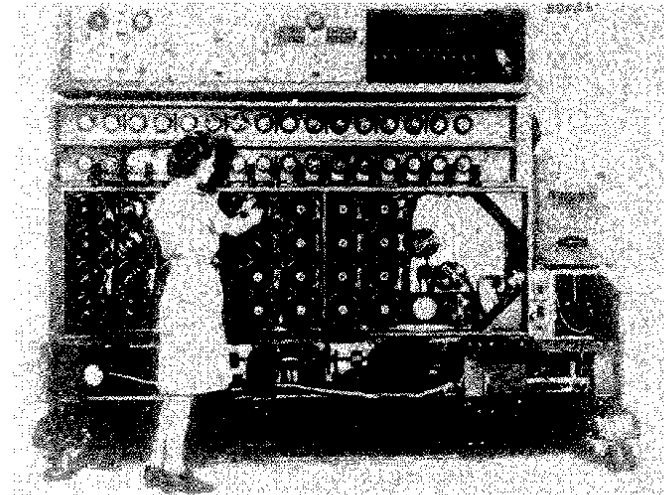


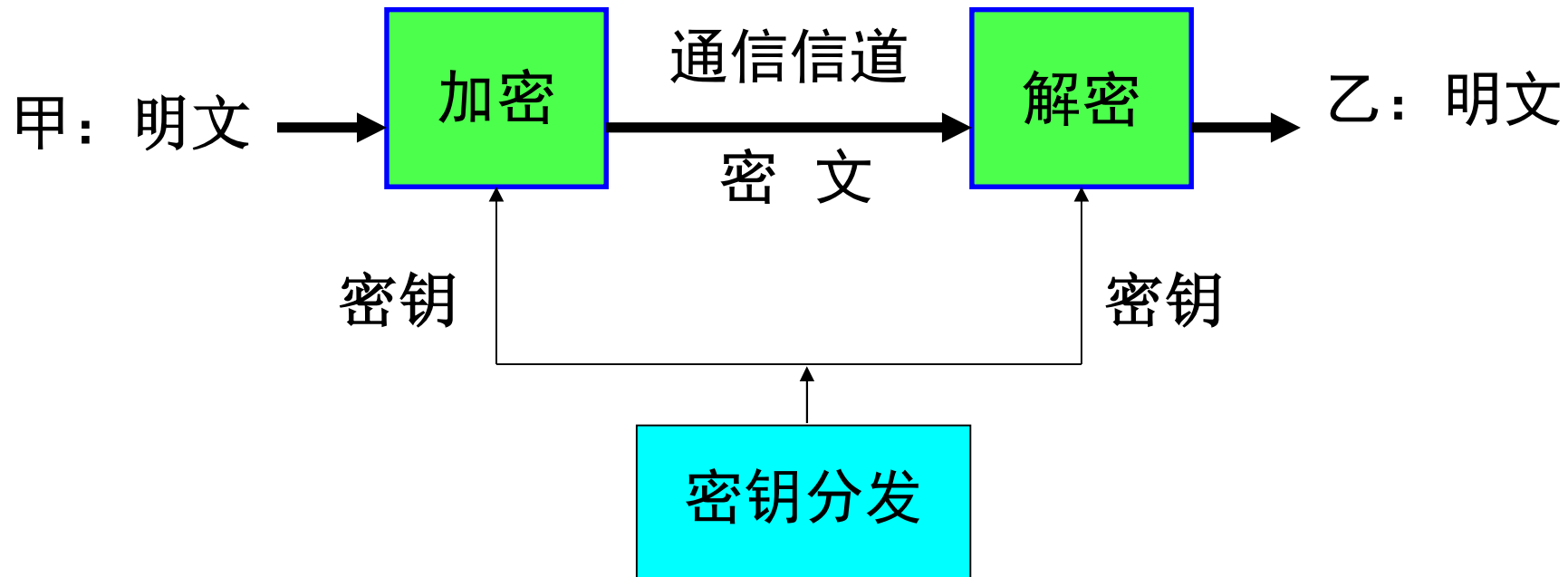
Figure 50 A Bletchley Park bombe in action.

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

$$3 \times 5 = \square$$

$$21 = \square \times \square$$

$$53 \times 79 = \square$$

$$4183 = \square \times \square$$

$$\begin{array}{l} 12301866845301177551304949583 \\ 84962720772853569595334792197 \\ 32245215172640050726365751874 \\ 52021997864693899564749427740 \\ 63845925192557326303453731548 \\ 26850791702612214291346167042 \\ 92143116022212404792747377940 \\ 80665351419597459856902143413 \end{array} = \square \times \square$$

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！

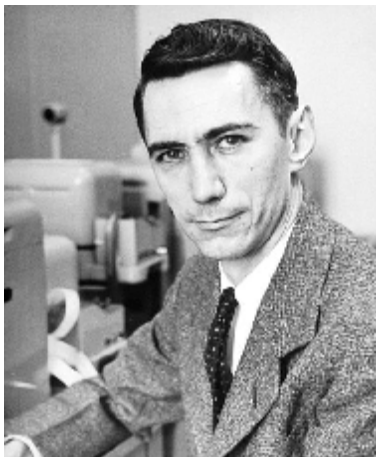
一次一密的加密方式

- ◆ 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

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

明文-ASCII	0	1	1	0	0	0	0	1
密文-ASCII	0	1	0	1	1	0	0	0



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

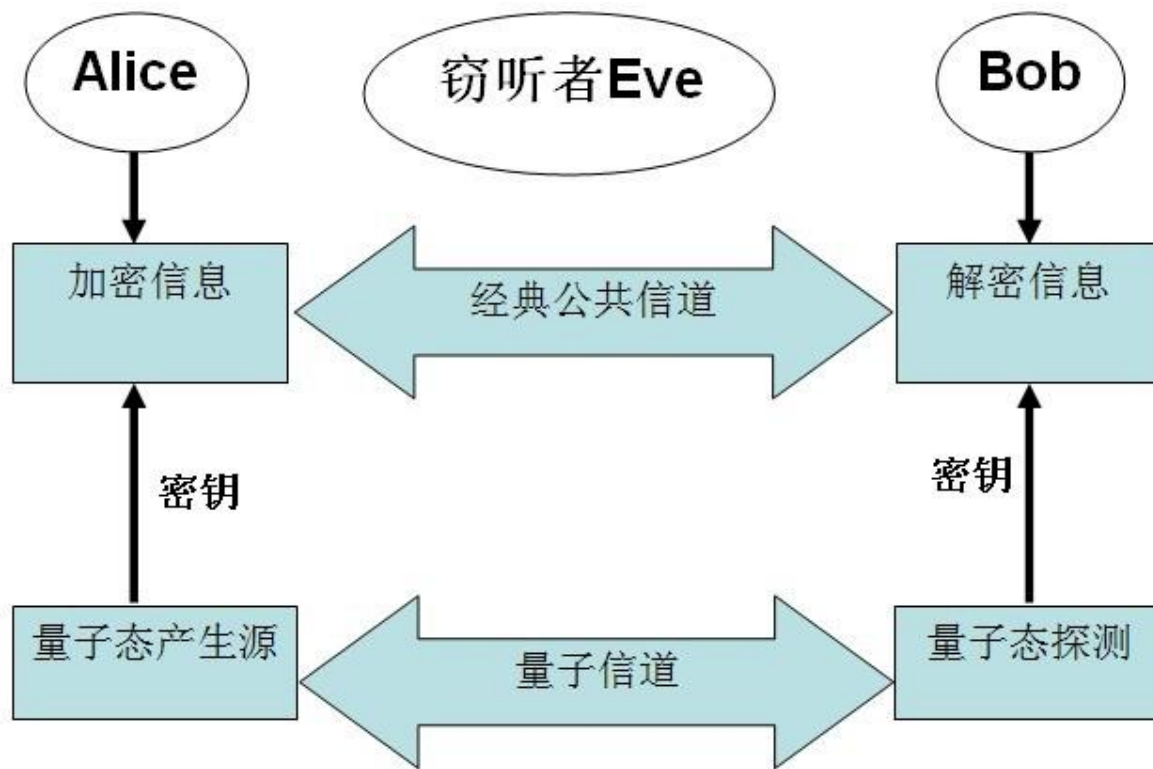
密钥的分配过程安全性无法保证



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

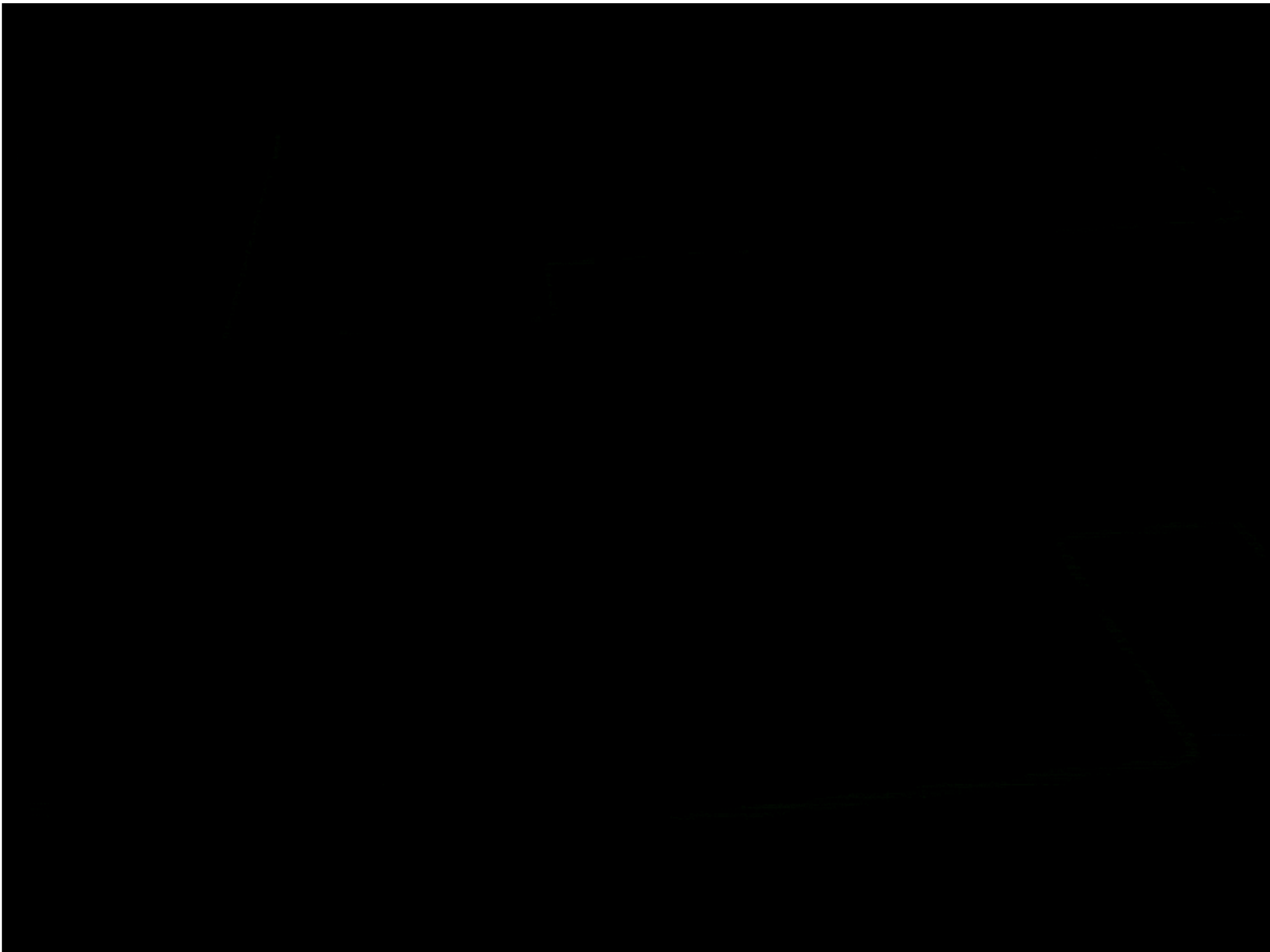


BB84协议示意图

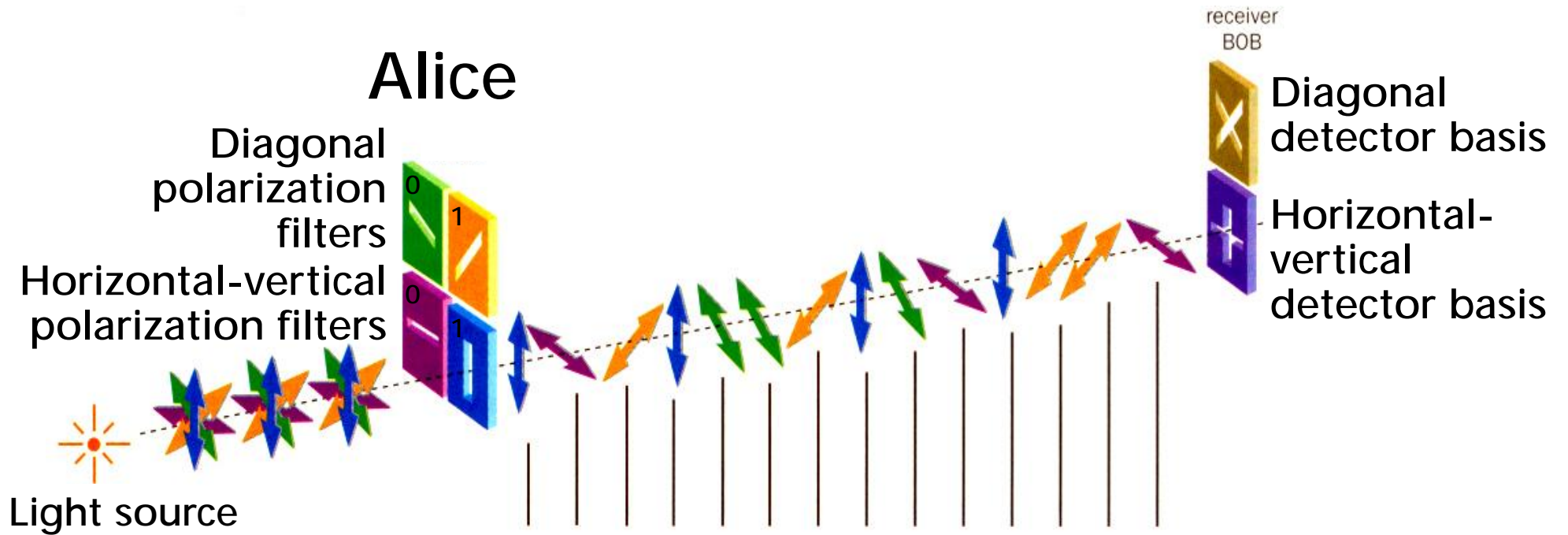
QKD基本原理

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



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	+	x	+	+	x	x	+	+	x	+	x	x	+	+
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

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?



各50%概率坍缩到
水平或竖直量子态

- 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

$$| \text{standing} \rangle \text{ or } | \text{lying} \rangle, | \text{standing} \rangle + | \text{lying} \rangle$$
$$| \text{standing} \rangle | \text{standing} \rangle + | \text{lying} \rangle | \text{lying} \rangle$$

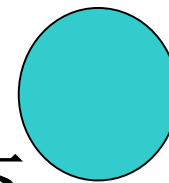
单光子量子态不可克隆原理

未知量子态



X 不可能的

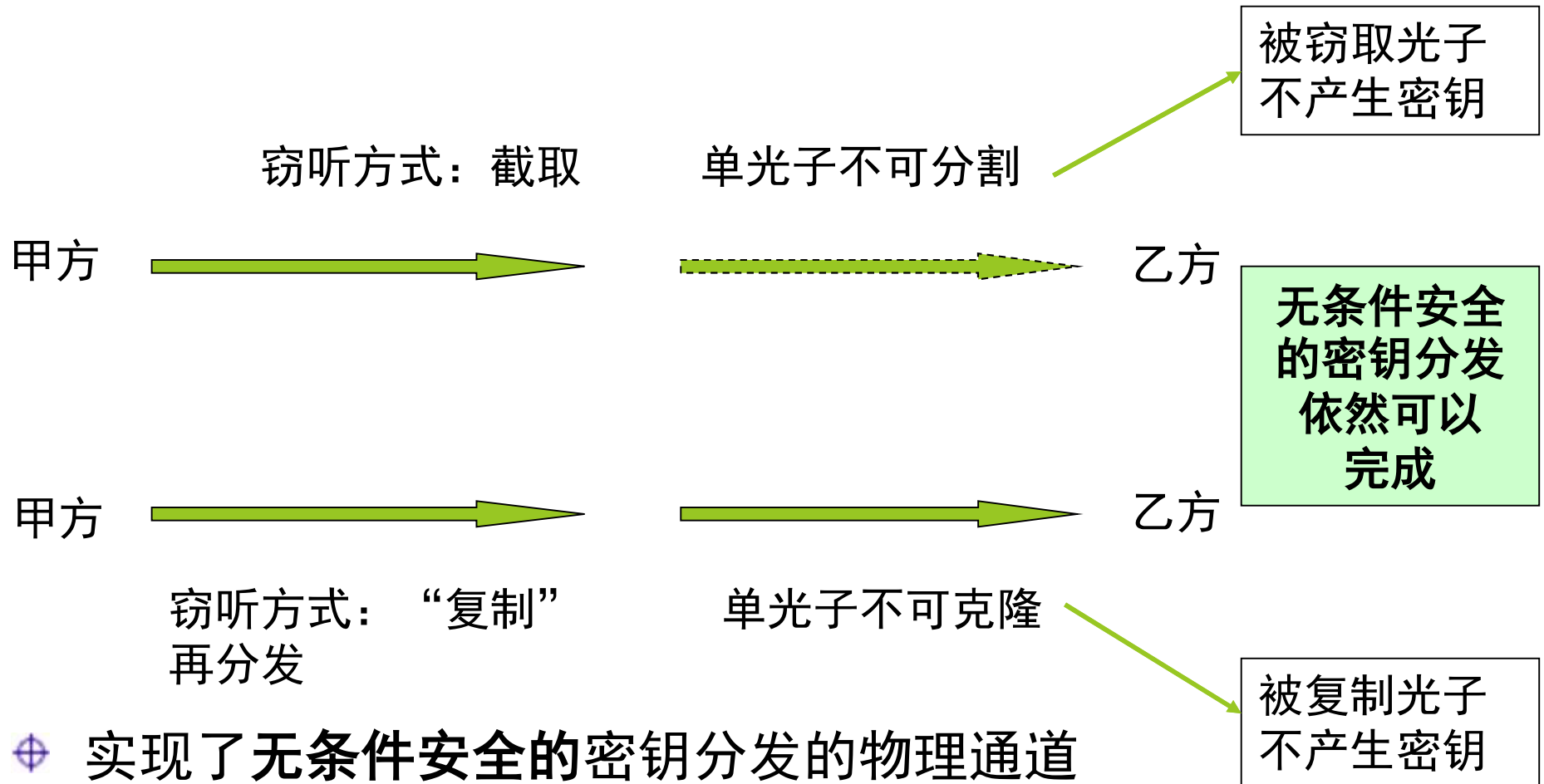
复制到
另一量子体系



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



- ⊕ 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 $x_1 \dots x_4$ of bits to send to Bob.

Bit	x_1	x_2	x_3	x_4
Value	0	1	1	0

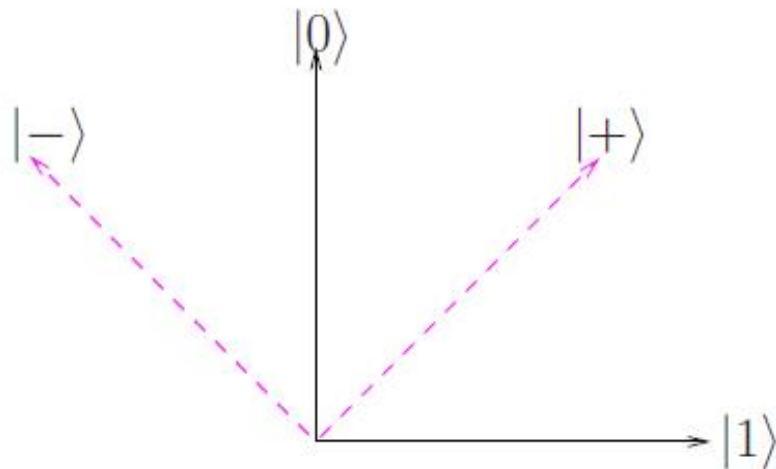
In order to prevent an eavesdropper from reading the bits, Alice randomly chooses to write each bit x_i as a qubit $|\psi_i\rangle$ in either the rectilinear basis as $|0\rangle$ or $|1\rangle$ or in the diagonal basis as $|+\rangle$ or $|-\rangle$

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 $0_×$,

$|-45\rangle$, codes for $1_×$.

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

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 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

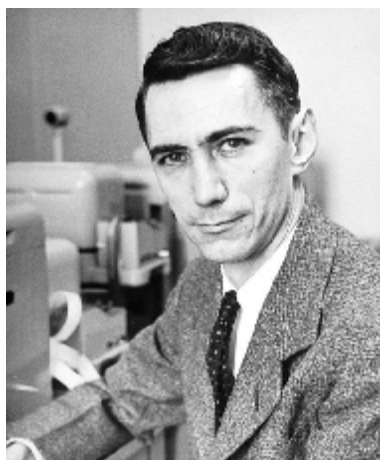
$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

明文-ASCII	0	1	1	0	0	0	0	1
密文-ASCII	0	1	0	1	1	0	0	0



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

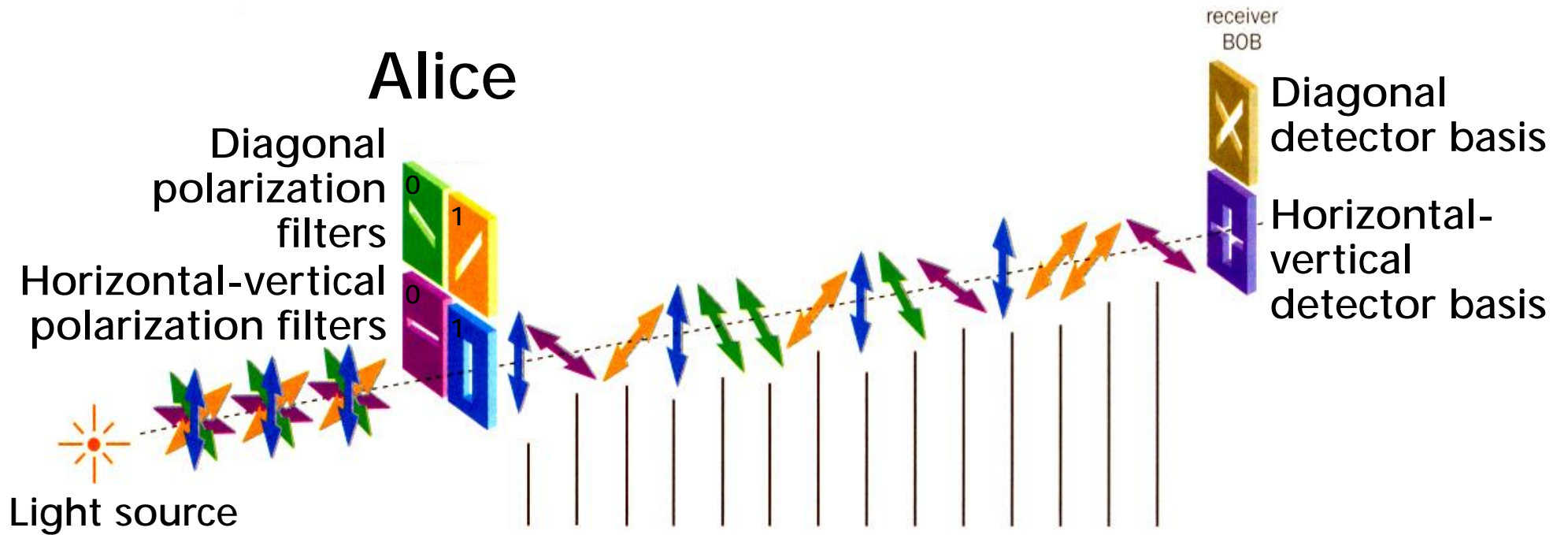
To serve as a secure key in cryptographic uses, there are two criteria:

- (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.

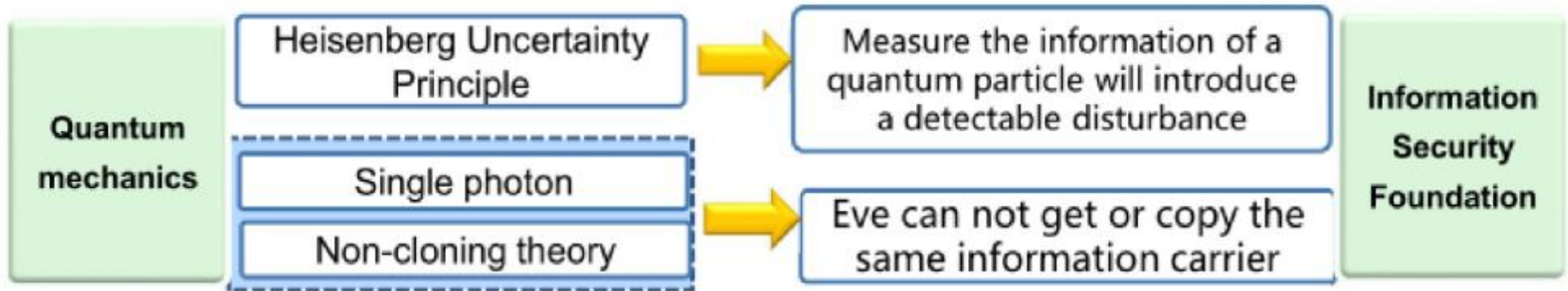
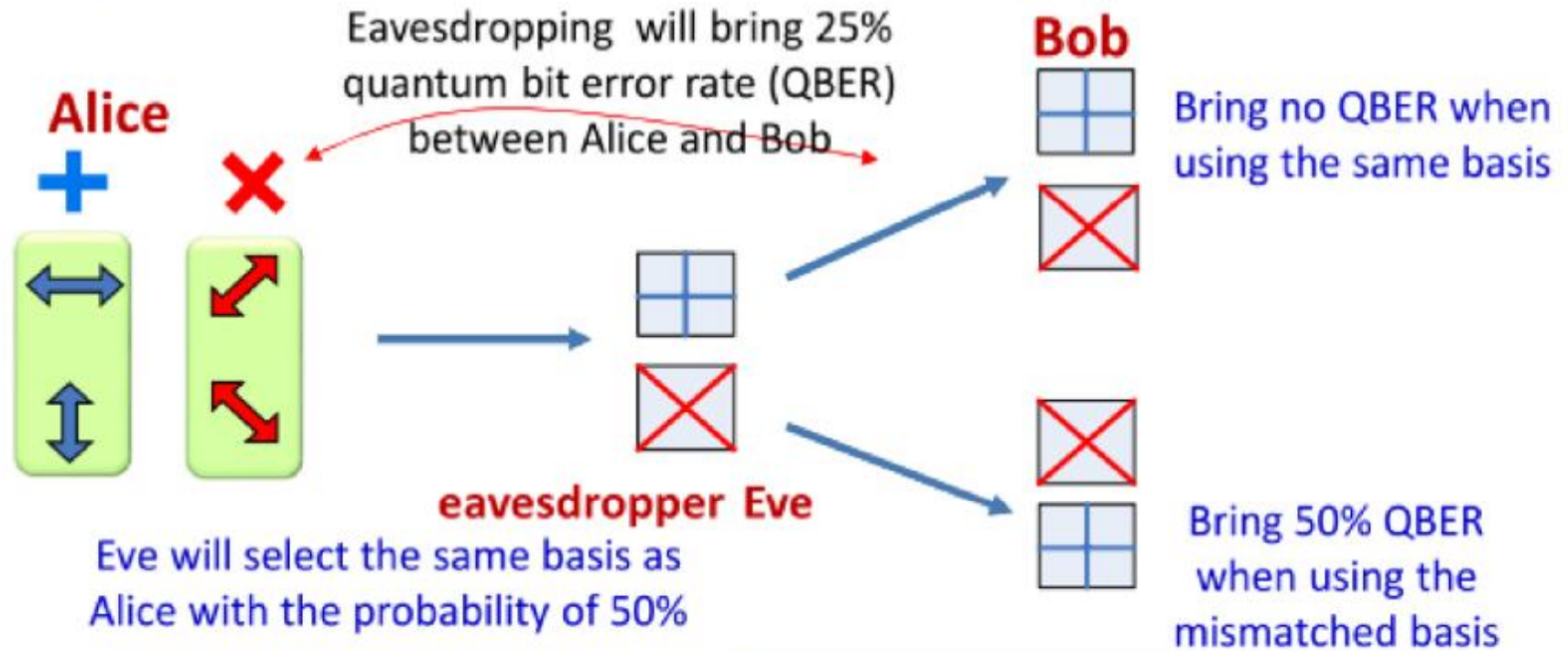
BB84协议



Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Bob's detection basis	+	x	+	+	x	x	+	+	x	+	x	x	+	+
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

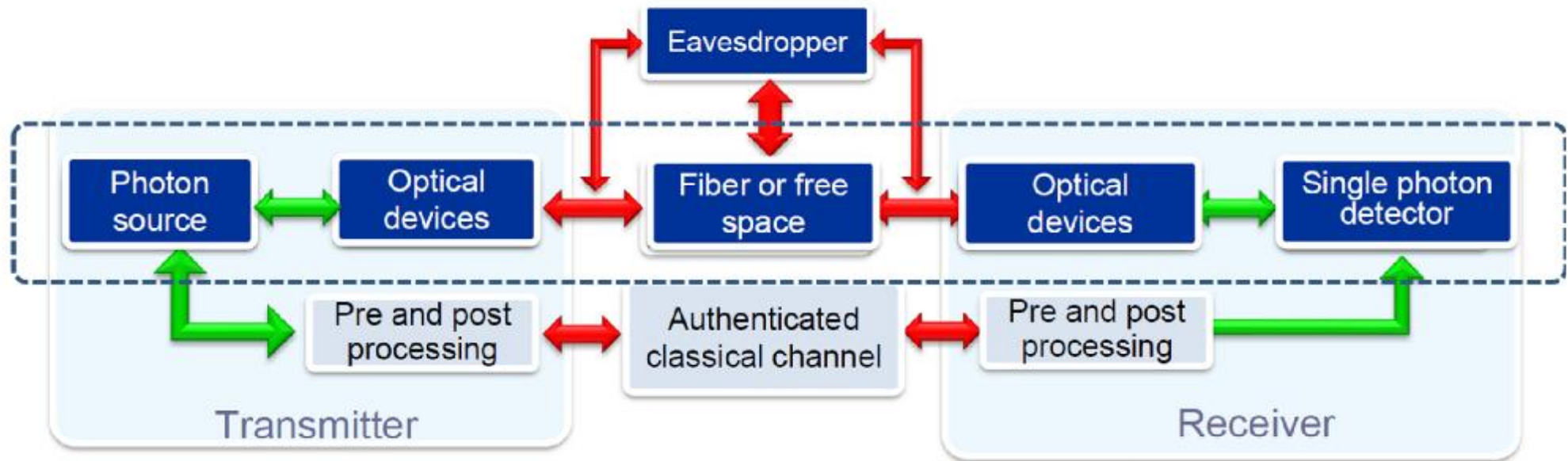
QKD安全性-QBER

Intercept-resend attack when Alice sends single photons to Bob



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

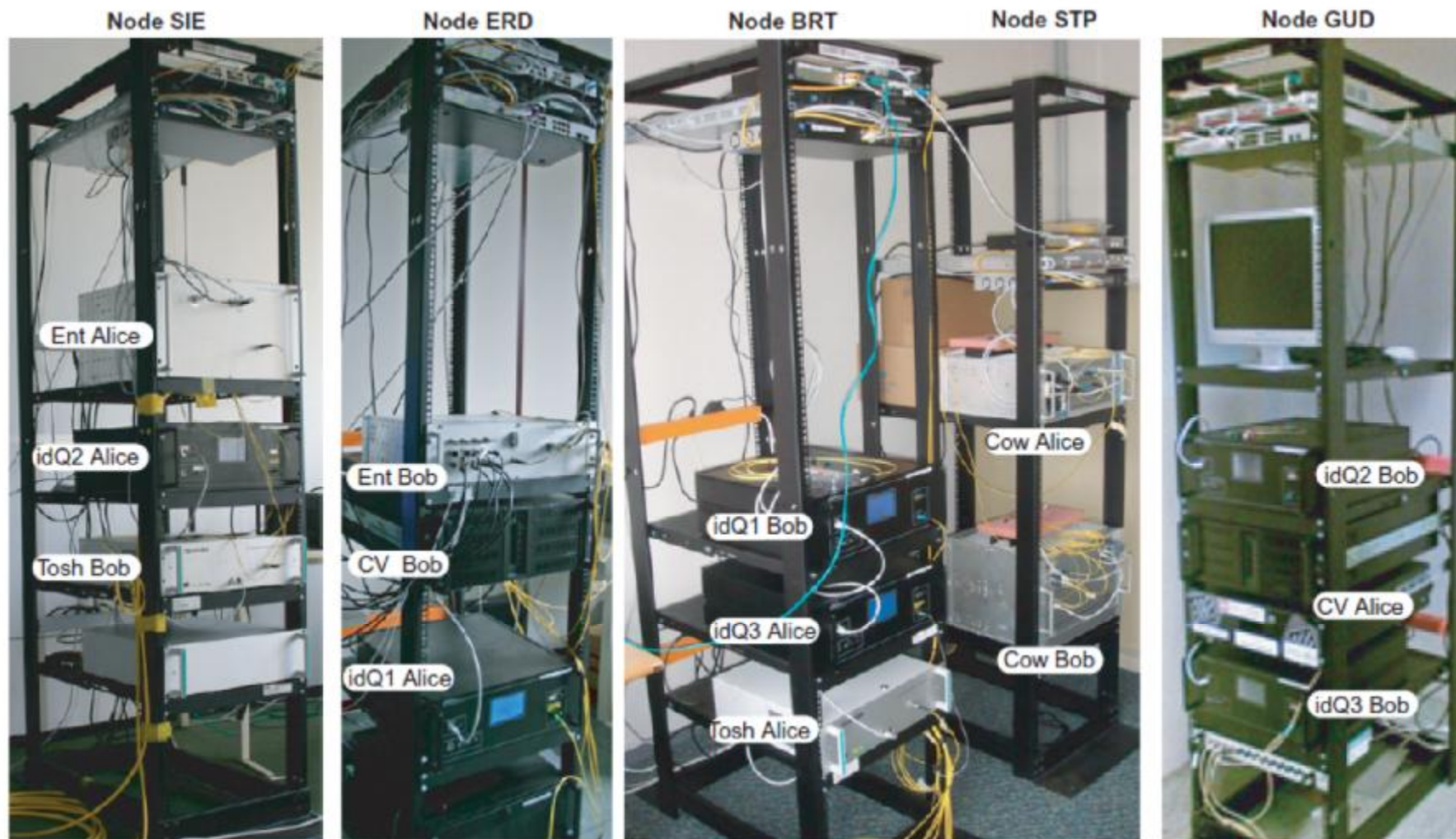


Figure 5. Photographs of the SECOQC network node racks.

现实QKD系统

The resources required in QKD systems

Photon source	Photon manipulation	Photon detector	Interface and auxiliary
<ul style="list-style-type: none">• WCS source• Entanglement source• Quantum dot, NV center, et al.	<ul style="list-style-type: none">• Polarization• Phase• Time-bin• Frequency• Orbital angular momentum• Amplitude• Intensity	<ul style="list-style-type: none">• InGaAs• Si• Ge• Superconducting materials• PMT• Homodyne/Hetrodyne	<ul style="list-style-type: none">• 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

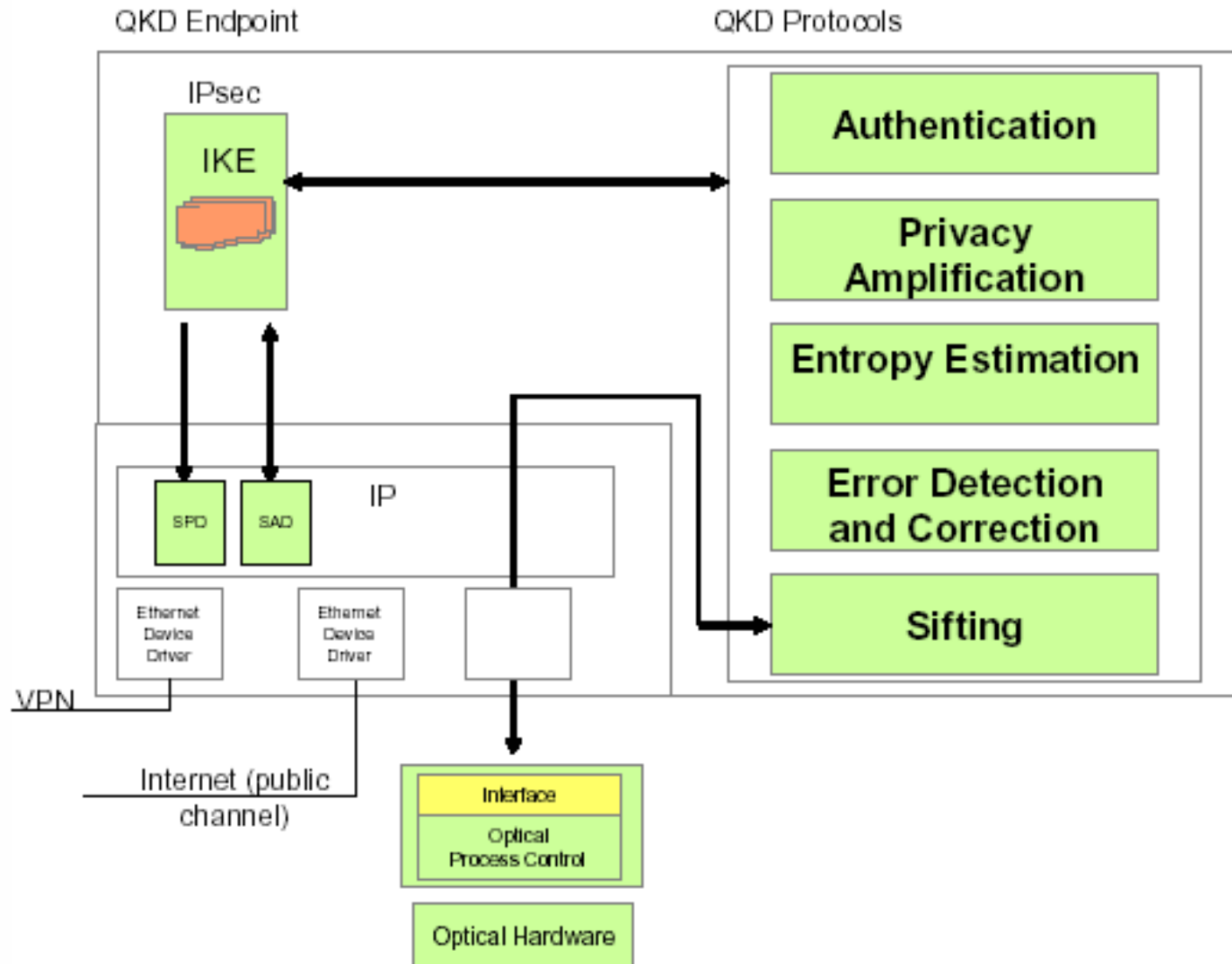
TABLE I. Typical parameters of single-photon detectors: detected wavelength λ , quantum efficiency η , fraction of dark counts p_d , repetition rate, maximum count rate, jitter, and temperature of operation T ; the last column refers to the possibility of distinguishing the photon numbers. For acronyms 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 universal₂

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

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 $m \times N$ 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

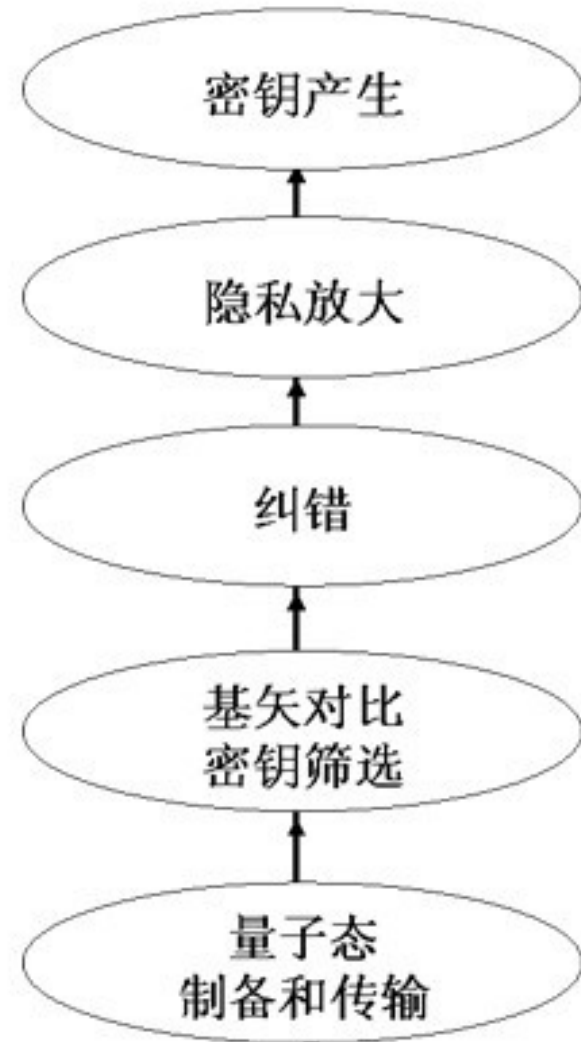
Alice chooses a randomly a hashing function f , from some class F which is **(strongly) universal₂**

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

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 & Eavesdropping 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!



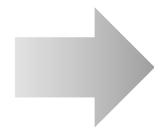
MAGIQ TECH.

- Distance over 100 km of commercial Telecom fibers.

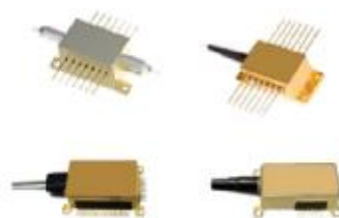


ID QUANTIQUE

Commercial Quantum Crypto products available on the market Today!



第四代终端
(4U19英寸标准机箱)



- R** 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
- R** 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,

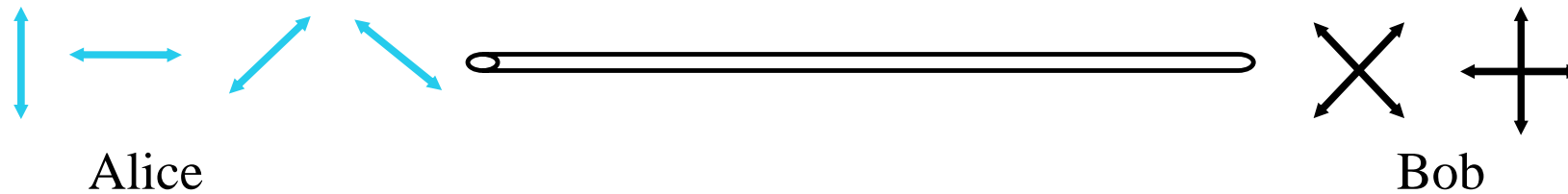
$$|\sqrt{\mu}e^{i\theta}\rangle \equiv |\alpha\rangle = e^{-\mu/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

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



ASSUMPTIONS:

Source: Emits perfect single photons. (No multi-photons)

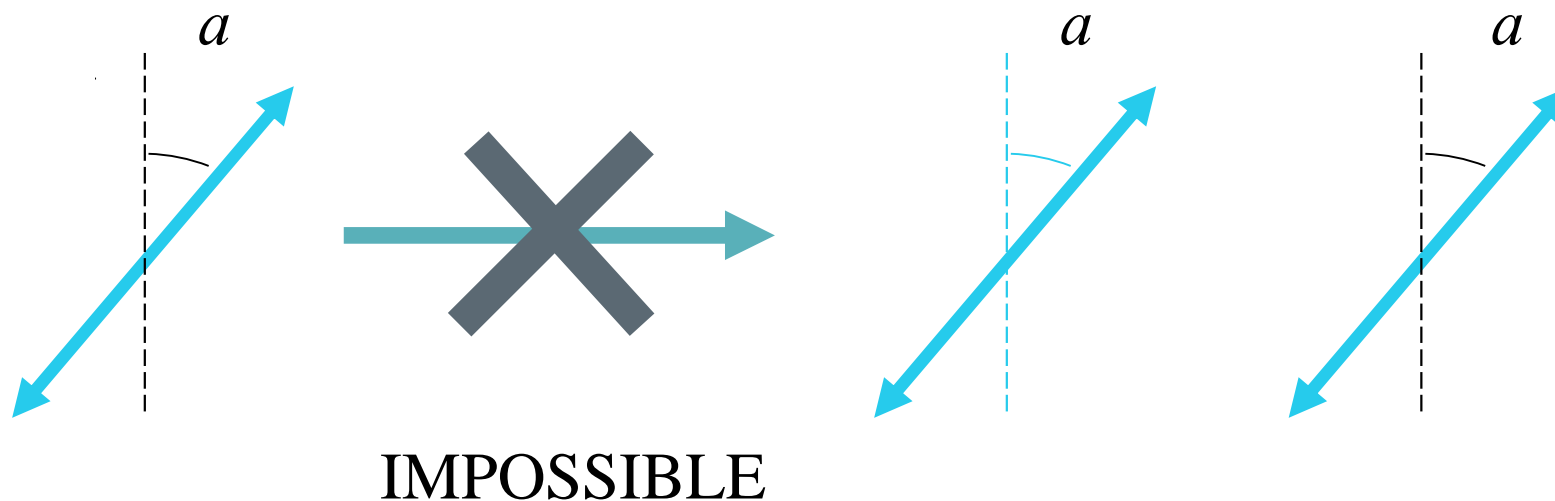
Channel: noisy but lossless. (No absorption in channel)

Detectors: ~~Assumptions lead to security proofs:~~ Perfect detection efficiency.
(100%)
Mayers (BB84), Lo and Chau (quantum-computing protocol),
Binnert et al. (BB84), Ben-Or (BB84), Shor-Preskill (BB84), ...

~~Basis Alignment: Perfect. (Angle between X and Z basis is exactly 45 degrees.)~~
Conclusion: QKD is secure in theory

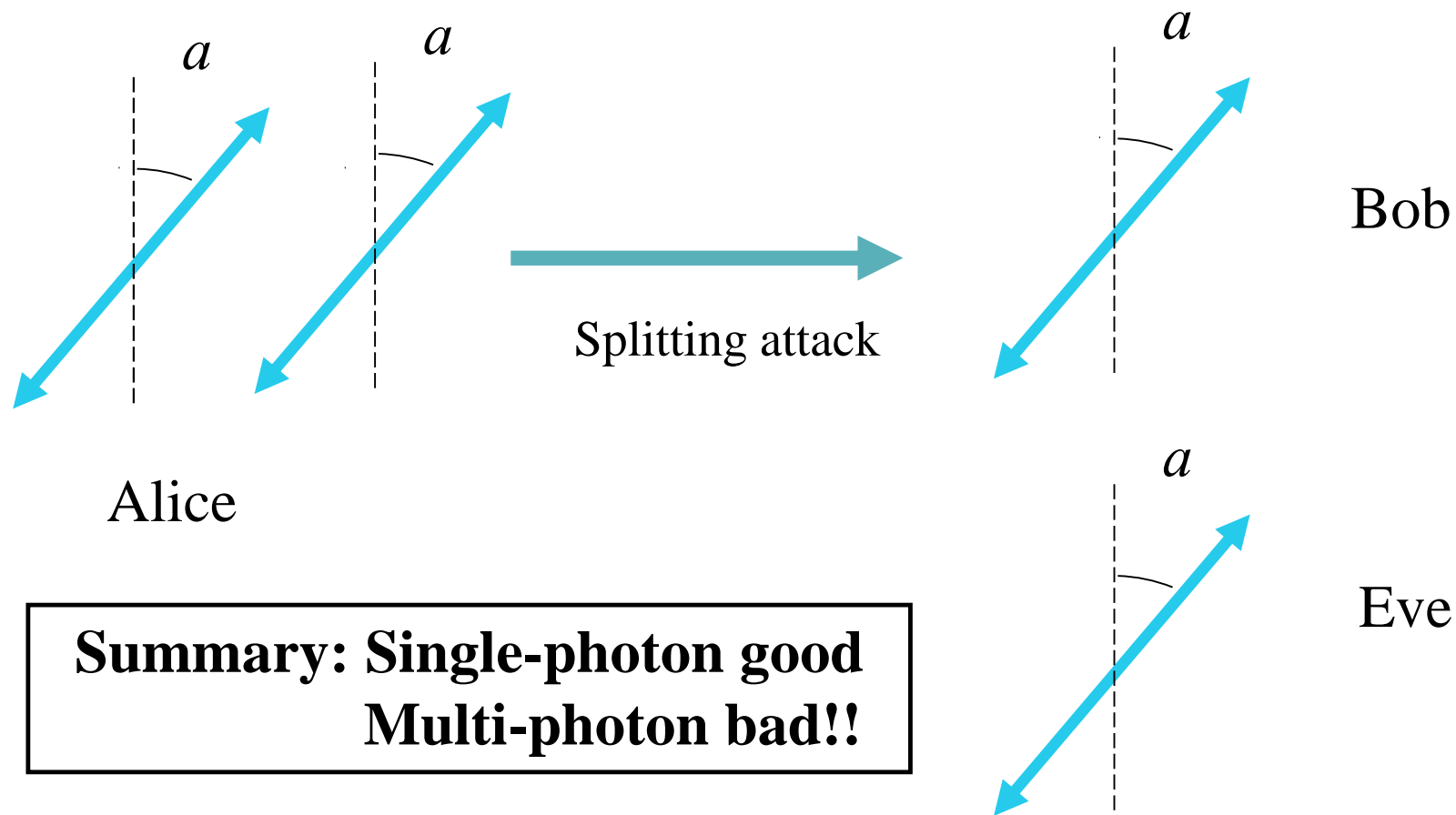
Reminder: Quantum No-cloning Theorem

- ◆ 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!!**

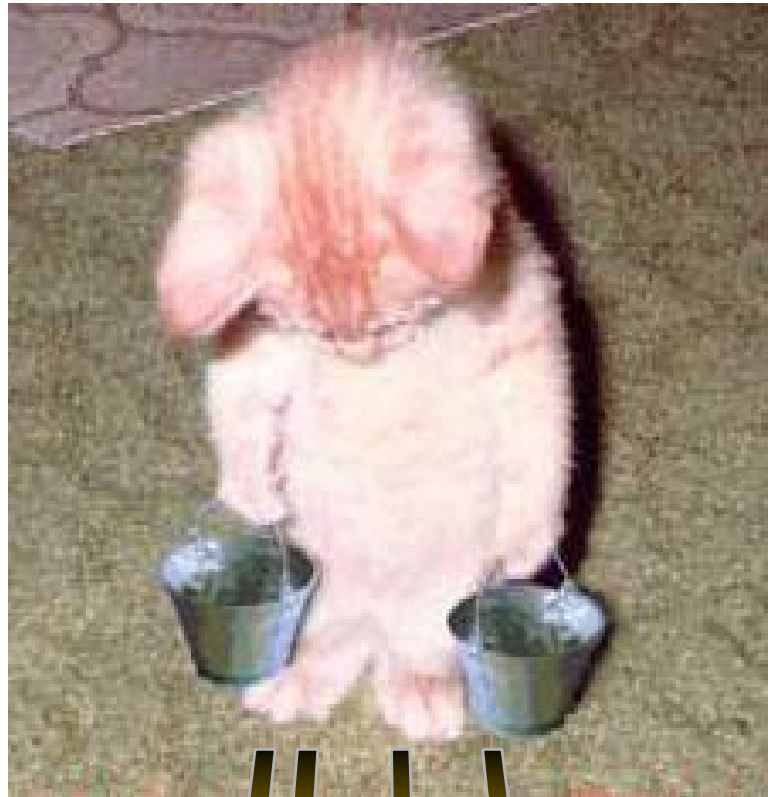
QKD: Practice

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 ~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

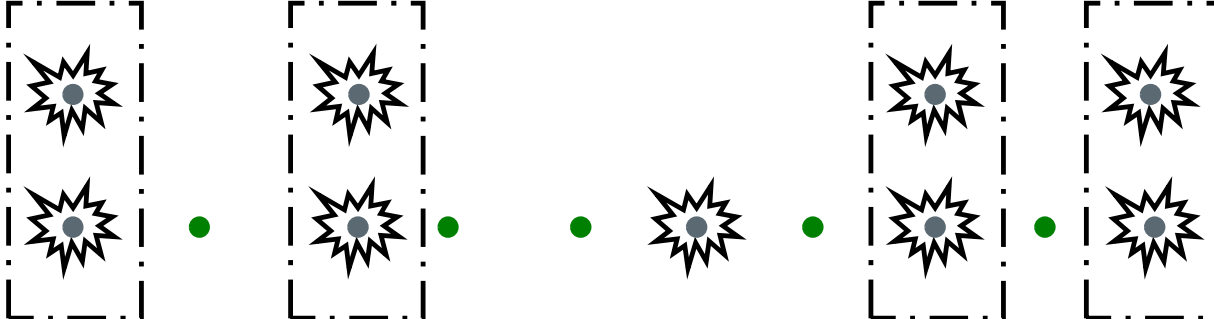
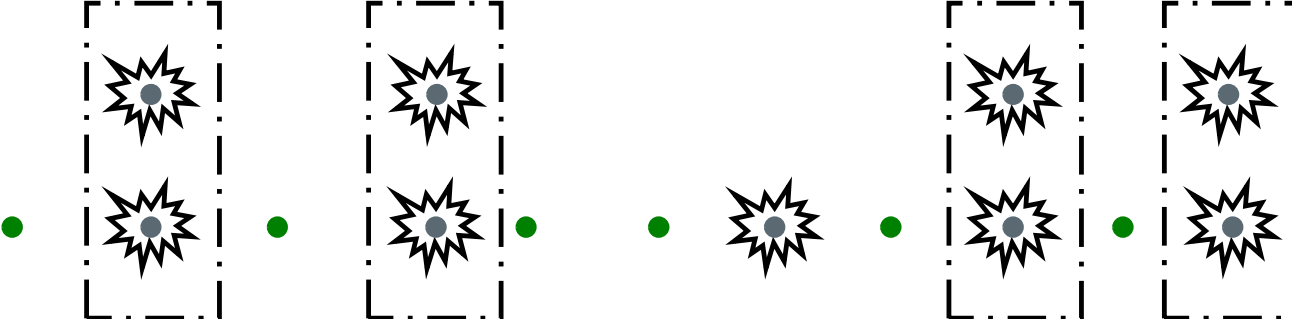


Help!

Big Problem: Nice guys come last

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)

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

$$S \geq \frac{1}{2} \left\{ \underbrace{-Q_\mu \cdot f(E_\mu) \cdot H_2(E_\mu)}_{\text{Error correction}} + \underbrace{Q_1 \cdot [1 - H_2(e_1)]}_{\text{Privacy amplification}} \right\}$$

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	$S = O(\eta^2).$
-------------------------------	------------------

Big Gap between theory and practice of BB84

<u>Theory</u>	<u>Experiment</u>
---------------	-------------------

Key generation rate: $S = O(\eta^2)$.	$S = O(\eta)$.
--	-----------------

Maximal distance: $d \sim 35\text{km}$.	$d > 120\text{km}$.
--	----------------------

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 ?