



上海交通大学·学术报告会  
2008年6月6日·东上院206教室

# 量子信息技术研究

报告人：何广强博士

上海交通大学电子工程系  
区域光纤通信网与新型光通信系统国家重点实验室

[gqhe@sjtu.edu.cn](mailto:gqhe@sjtu.edu.cn) or [laser\\_gqhe@hotmail.com](mailto:laser_gqhe@hotmail.com)



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 1 页 共 40 页

返回

全屏显示

关闭

退出



# 量子信息技术研究

-  第一部分 量子信息物理基础
-  第二部分 量子密码术
-  第三部分 量子隐形传态
-  第四部分 量子密集编码
-  第五部分 量子通信网络
-  第六部分 量子计算技术
-  第七部分 上海交通大学相关研究
-  问题讨论

量子信息理论基础

量子密码

量子隐形传态

量子纠缠交换

量子中继

量子密集编码

量子远程克隆

量子计算

量子物理世界版图

上海交通大学量子信息...

诚邀加盟

访问主页

标题页



第 2 页 共 40 页

返回

全屏显示

关闭

退出



# 1 量子信息理论基础

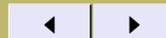
## 1.1. 物理学家全明星队



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 3 页 共 40 页

返回

全屏显示

关闭

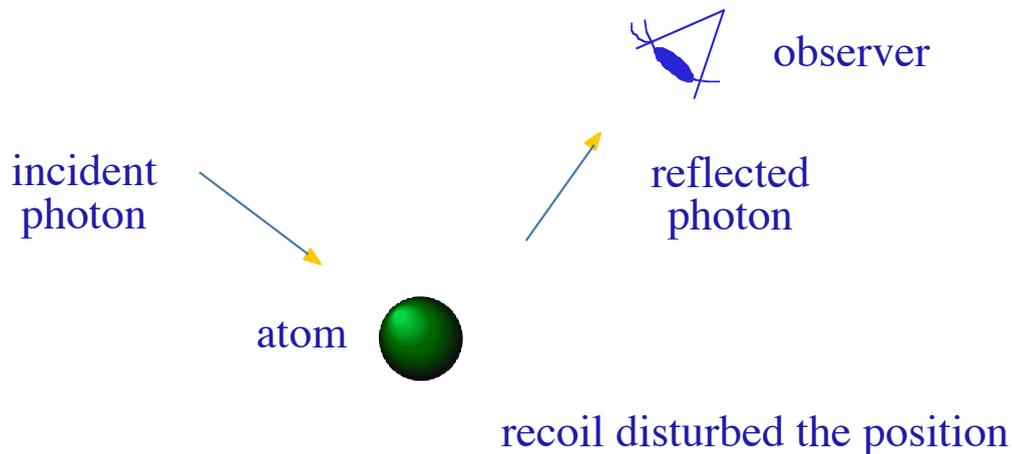
退出

## 1.2. 量子测不准原理

# The Heisenberg Uncertainty Principle

- It is impossible to make simultaneous *precise* measurements of a pair of canonically conjugate observables of an object.
  - Position and momentum
  - Energy and time
  - Amplitude and phase

## The Heisenberg Microscope



量子信息理论基础

量子密码

量子隐形传态

量子纠缠交换

量子中继

量子密集编码

量子远程克隆

量子计算

量子物理世界版图

上海交通大学量子信息...

诚邀加盟

访问主页

标题页



第 4 页 共 40 页

返回

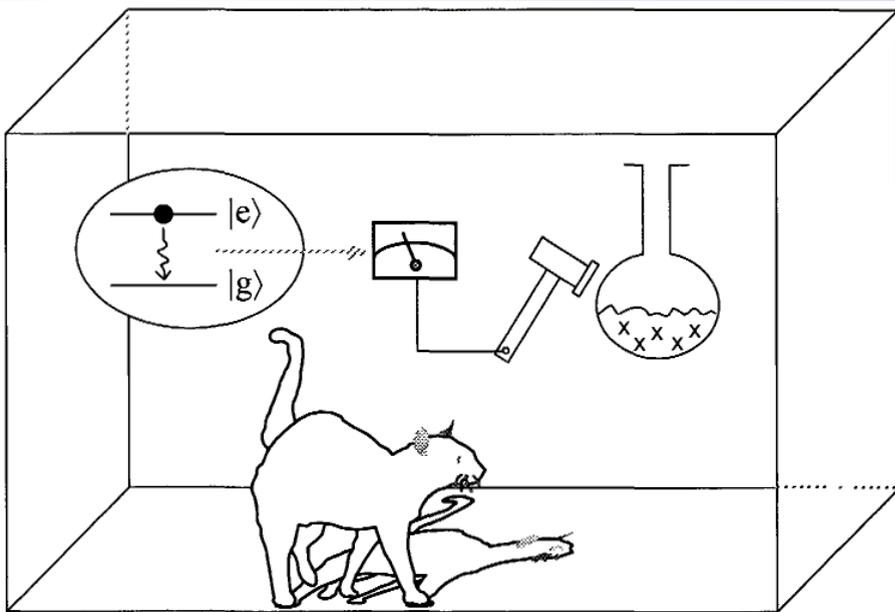
全屏显示

关闭

退出



### 1.3. 量子叠加原理



薛定谔的猫

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (1)$$

- 霍金：一想到薛定谔的猫，我就去拿手枪！

量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页

◀ ▶

◀ ▶

第 5 页 共 40 页

返回

全屏显示

关闭

退出



## 1.4. 量子不可克隆定理

**Classical Physics:**  
"bit"



**Quantum Physics:**  
"qubit"

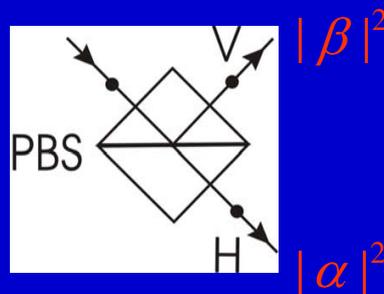


One bit of information per photon  
(encoded in polarization)

$$\begin{aligned} |H\rangle &= |"0"> \\ |V\rangle &= |"1"> \end{aligned}$$

$$|\Phi\rangle = \alpha |H\rangle + \beta |V\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

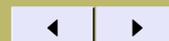
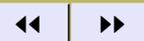


**Non-cloning theorem:**

**An unknown quantum state can not be copied precisely!**

访问主页

标题页



第 6 页 共 40 页

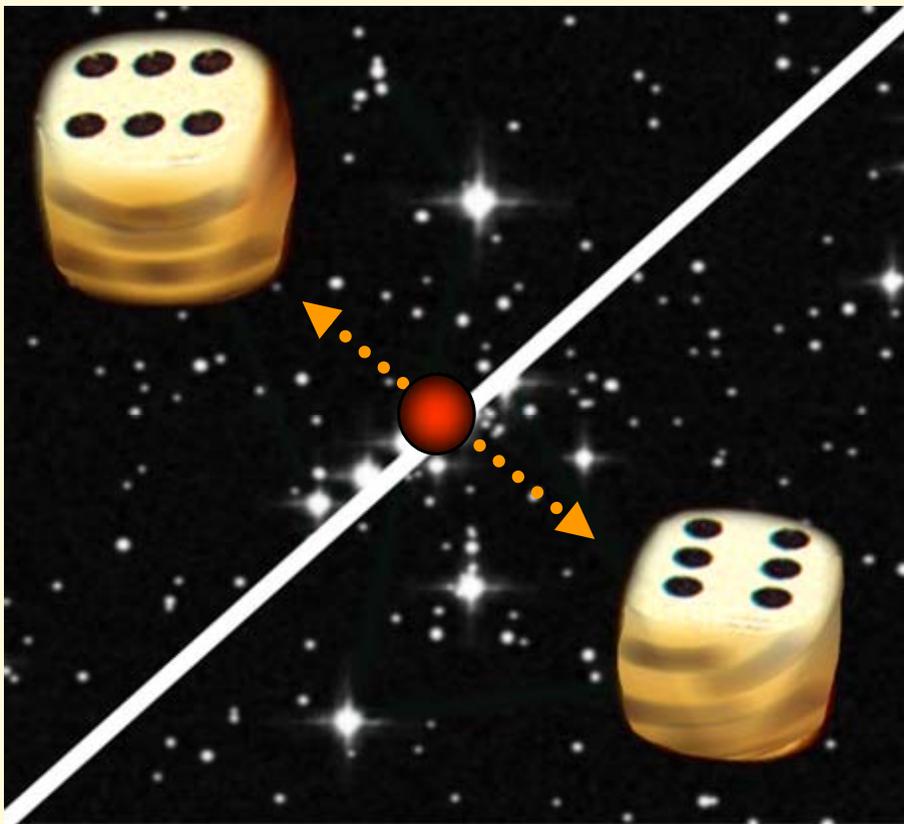
返回

全屏显示

关闭

退出

## 1.5. 神奇的量子纠缠



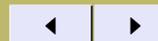
- 爱因斯坦：玻尔，亲爱的上帝不掷骰子！
- 玻尔：爱因斯坦，别去指挥上帝应该怎么做！
- 霍金：亲爱的上帝不但掷骰子，还把它掷到你看不见的地方！



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

[访问主页](#)

[标题页](#)



第 7 页 共 40 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)



## 2 量子密码

### 2.1. 量子密码意义

# Seeking absolute security

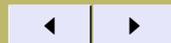
Quantum cryptography is theoretically unbreakable, yet a handful of physicists are finding ways to hack into its secrets. **Geoff Brumfiel** finds out how.



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 8 页 共 40 页

返回

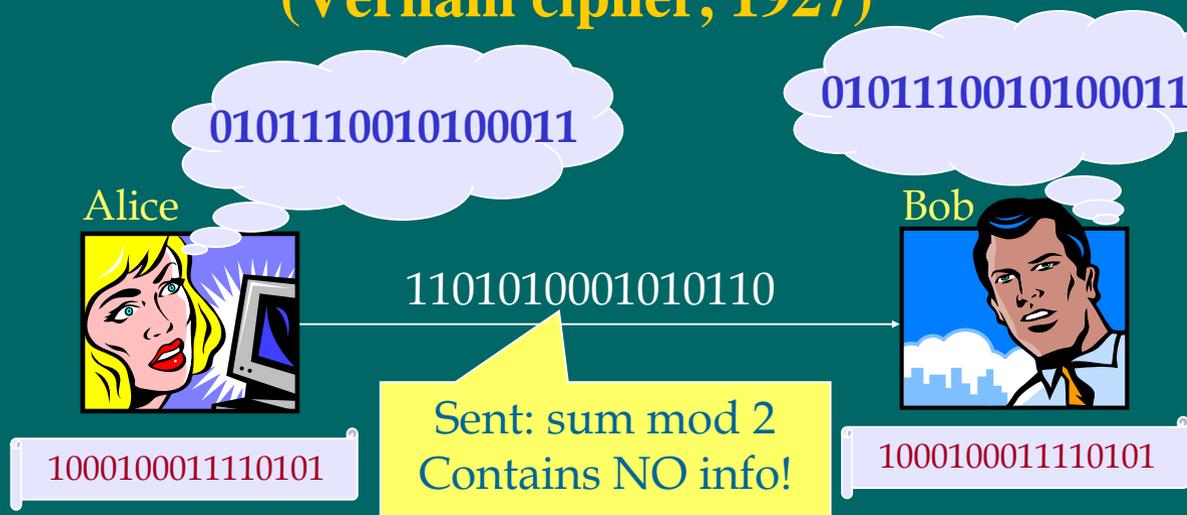
全屏显示

关闭

退出



# Secret key cryptography (Vernam cipher, 1927)



Unbreakable... unless the eavesdropper knows the key!!!

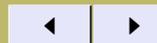
⇒ How to distribute the key among the partners?

**Q-crypto is a protocol for secure key distribution!**

**i.e., purpose: establish two identical lists of secret bits.**

访问主页

标题页



第 9 页 共 40 页

返回

全屏显示

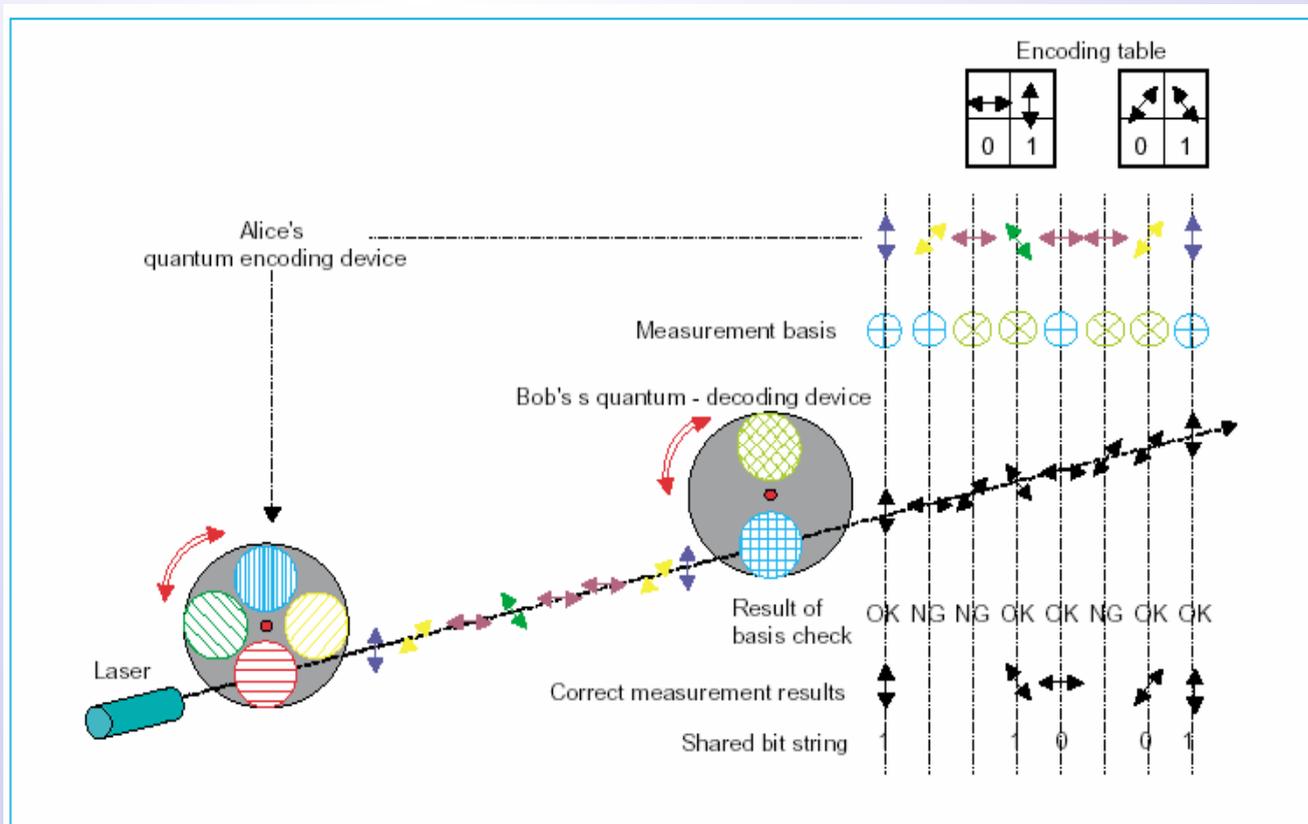
关闭

退出



## 2.2. 量子密码协议

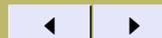
### 2.2.1. BB84协议



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 10 页 共 40 页

返回

全屏显示

关闭

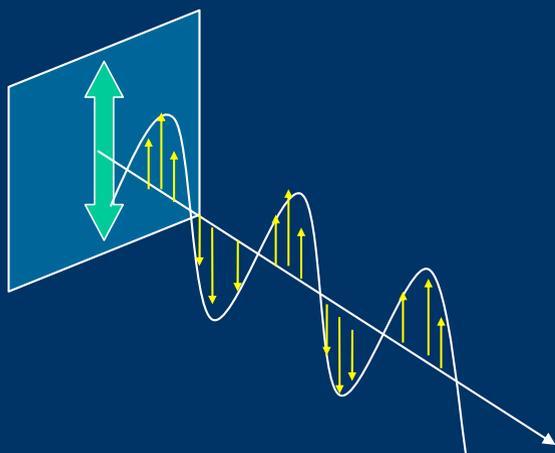
退出



# Physics: Polarization of Light

## Classical light field

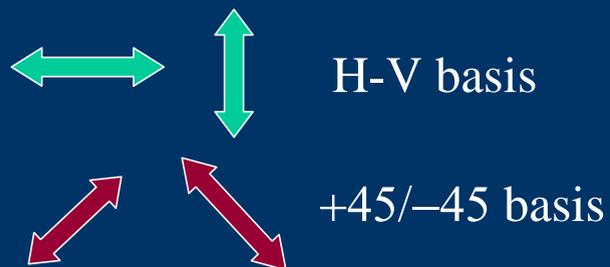
Light = Electric field propagating as a transverse wave



**Polarization** =  
direction of oscillation  
of the electric field

## Quantum light field

- light is « made » of photons
- polarization is a property of each photon
- the state of polarization of the photon determines the direction of oscillation of the macroscopic field.



[访问主页](#)

[标题页](#)



第 11 页 共 40 页

[返回](#)

[全屏显示](#)

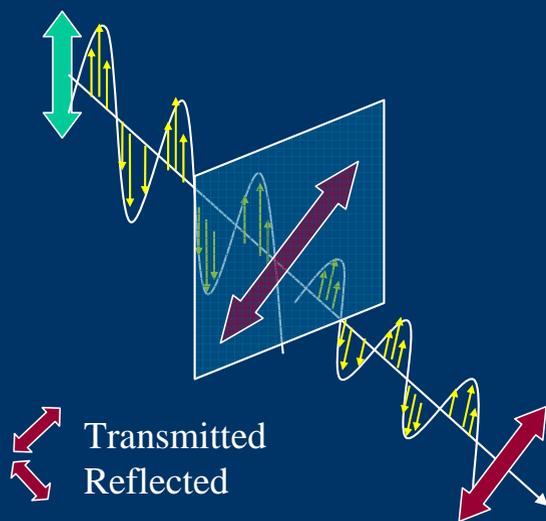
[关闭](#)

[退出](#)

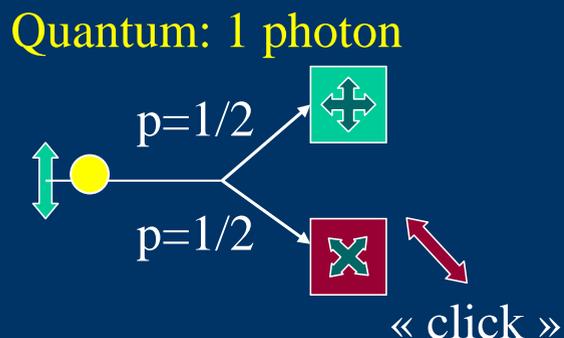
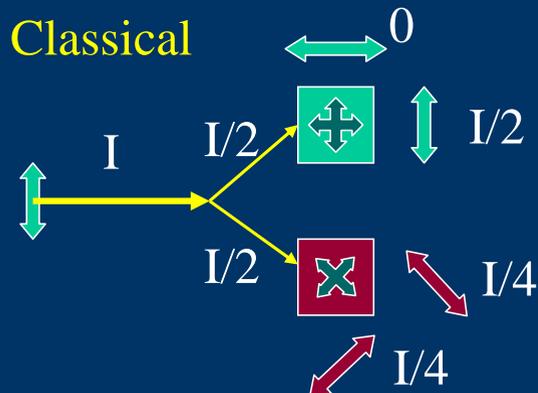


# Physics: Measuring Polarization

Polarizers = Filters



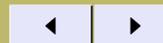
- Half intensity
- New polarization state



The polarization of a single photon cannot be learnt with certainty!

访问主页

标题页



第 12 页 共 40 页

返回

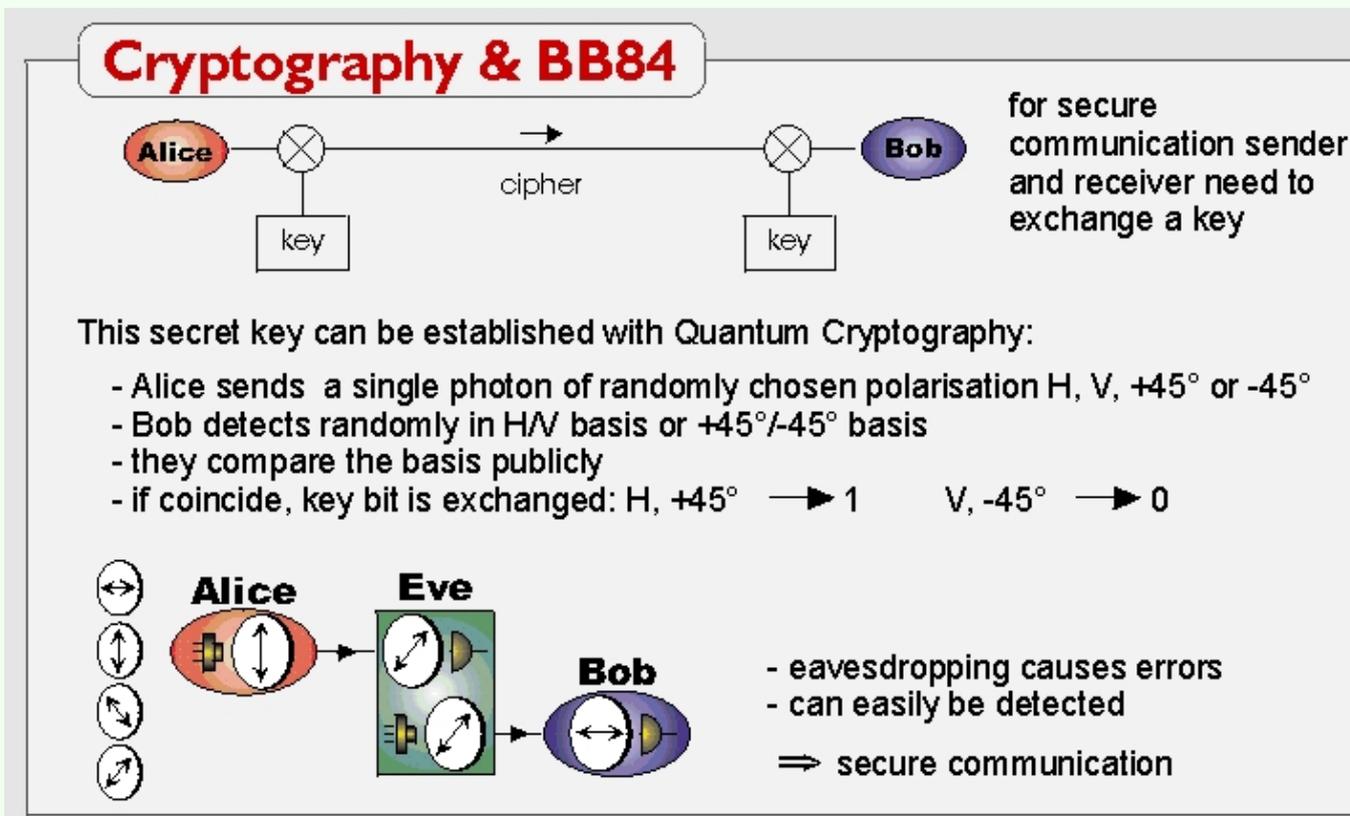
全屏显示

关闭

退出

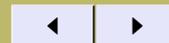


## • BB84协议工作原理



[访问主页](#)

[标题页](#)



第 13 页 共 40 页

[返回](#)

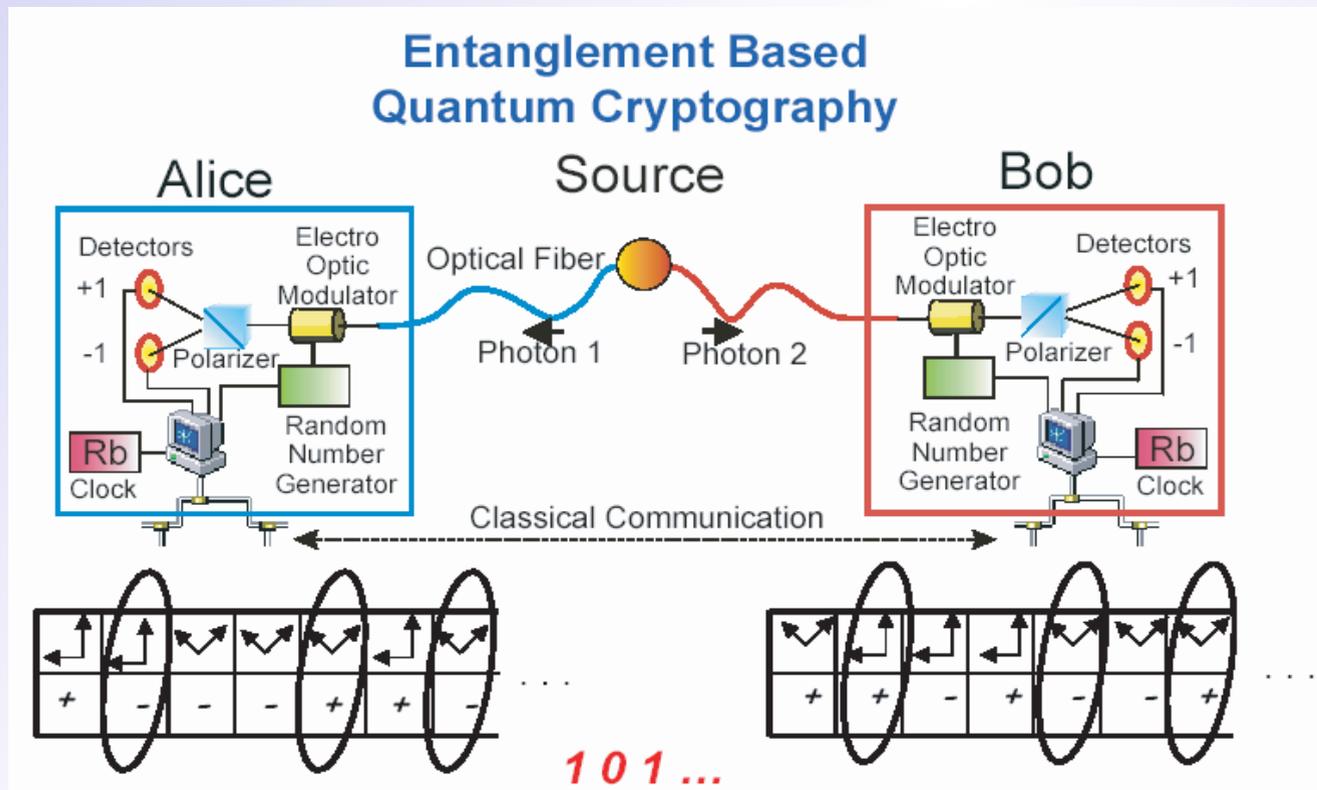
[全屏显示](#)

[关闭](#)

[退出](#)



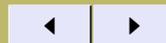
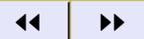
## 2.2.2. EPR协议



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 14 页 共 40 页

返回

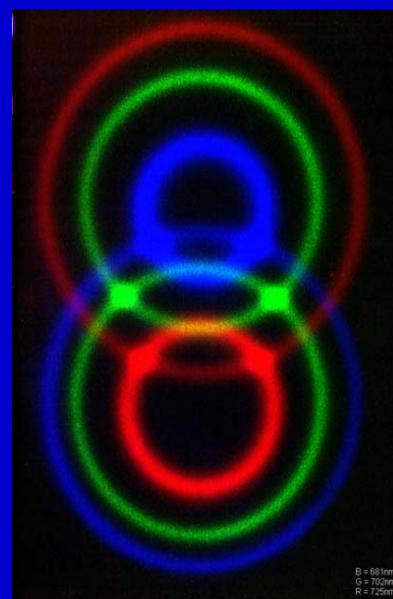
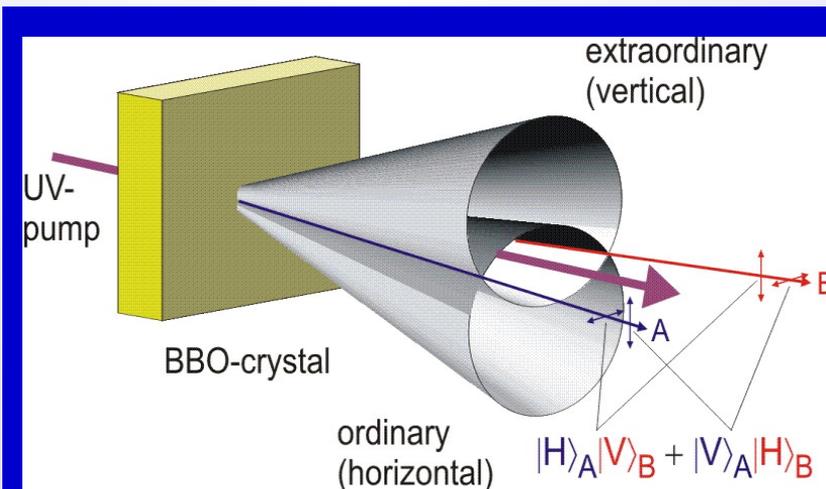
全屏显示

关闭

退出



量子信息理论基础  
 量子密码  
 量子隐形传态  
 量子纠缠交换  
 量子中继  
 量子密集编码  
 量子远程克隆  
 量子计算  
 量子物理世界版图  
 上海交通大学量子信息...  
 诚邀加盟



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

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

访问主页

标题页



第 15 页 共 40 页

返回

全屏显示

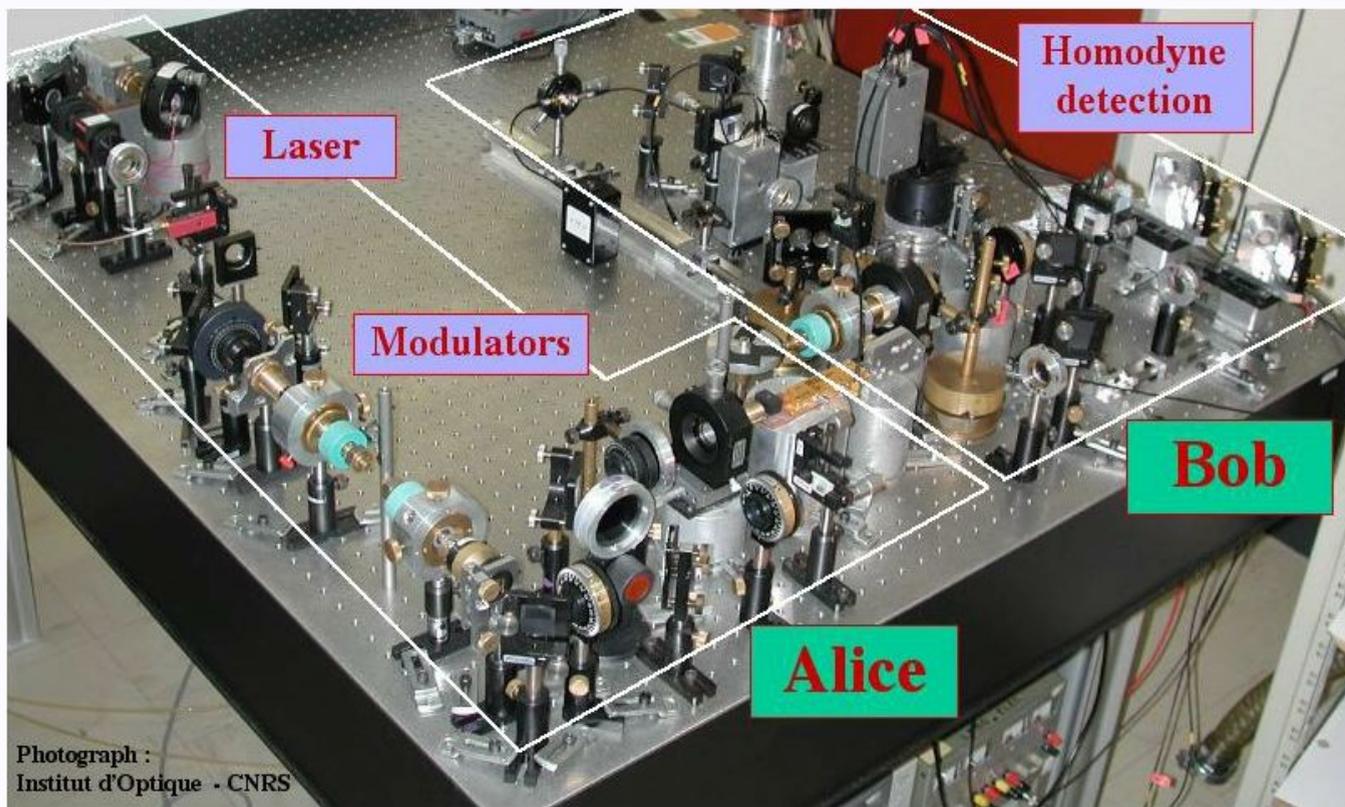
关闭

退出



## 2.3. 实验实现

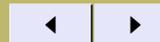
### 2.3.1. 自由空间 (1)



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 16 页 共 40 页

返回

全屏显示

关闭

退出



## 2.3.2. 自由空间 (2)

### Alice Setup

- 4 laser diodes are sending faint pulses in H, V, +45° and -45° polarisation
- intrinsic polarisation of the laser diodes requires no further optics
- spatial mode of light is indistinguishable from 4 diodes
- emission spectra of laser diodes overlap ⇒ indistinguishable

### Location

Advantages of height: - low absorption  
- less turbulences  
- less ambient light

Disadvantages: - extreme working conditions  
- dependency on weather  
- distance to workshop

### Bob Setup

- randomness of basis due to randomness of detection behind a 50/50 beam splitter
- 4 SPAD are detecting the polarisations
- temperature controlled with peltiers (-30°C)

### 欧盟正在建设的空间量子密码系统



### Pictures

Alice pointing to karwendel

sender telescope

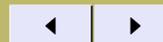
bob module connected to the receiver telescope

looking onto bobs laser

量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 17 页 共 40 页

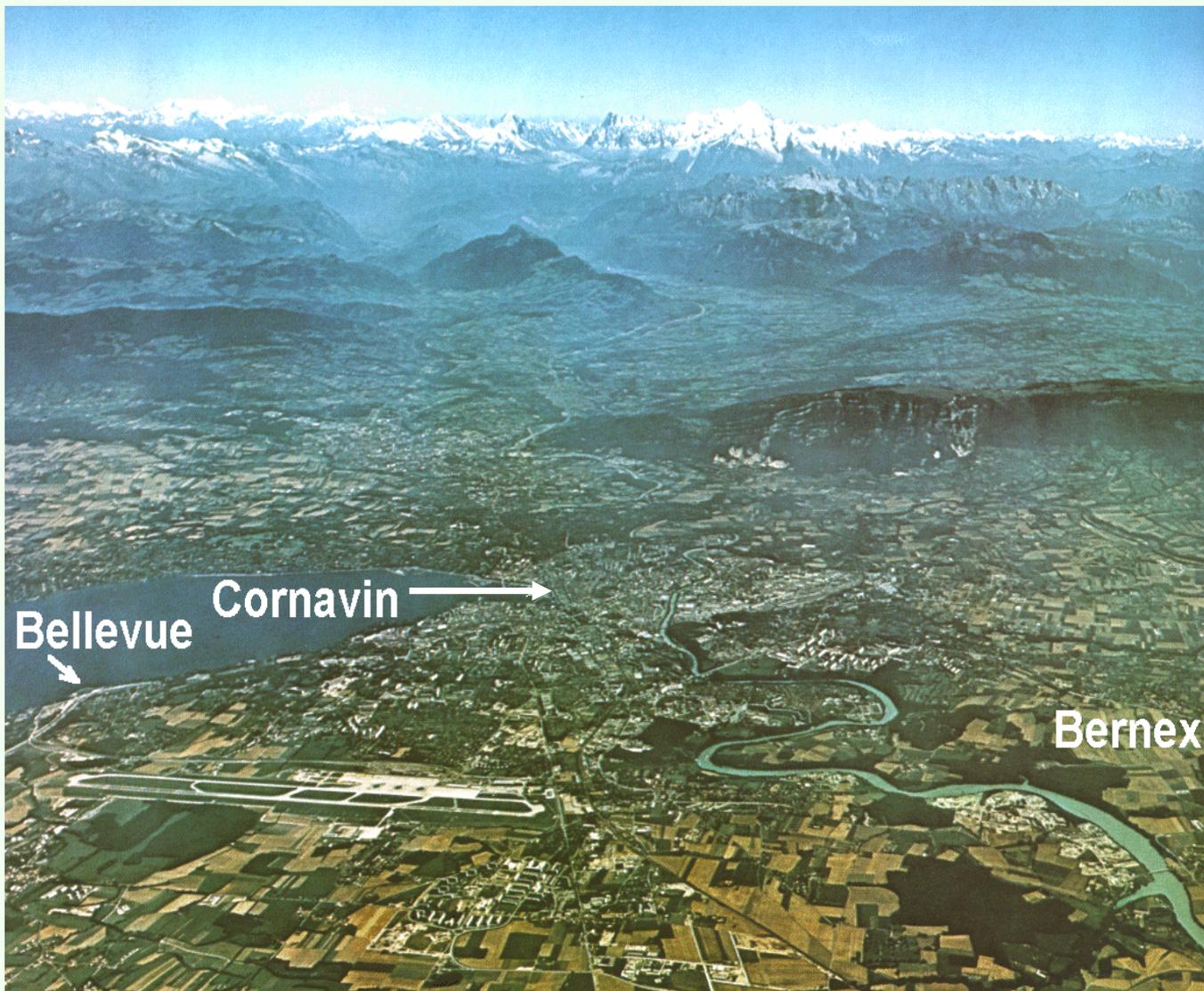
返回

全屏显示

关闭

退出

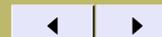
### 2.3.3. 光纤信道（1）：瑞士日内瓦湖下光缆



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 18 页 共 40 页

返回

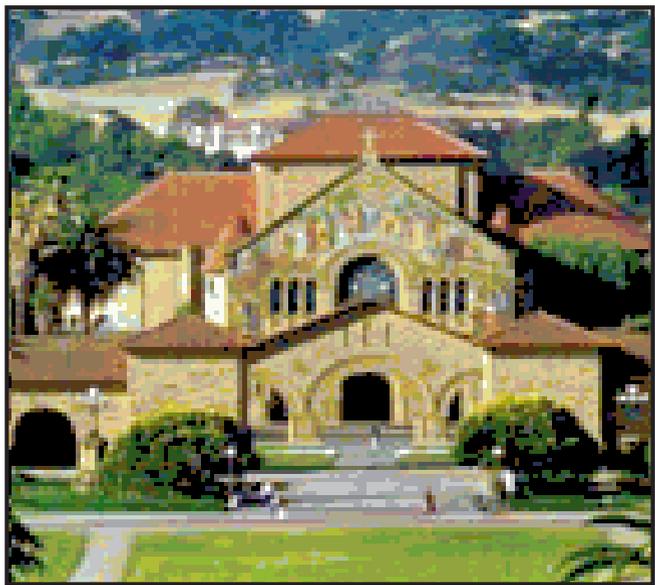
全屏显示

关闭

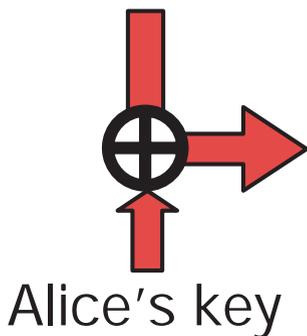
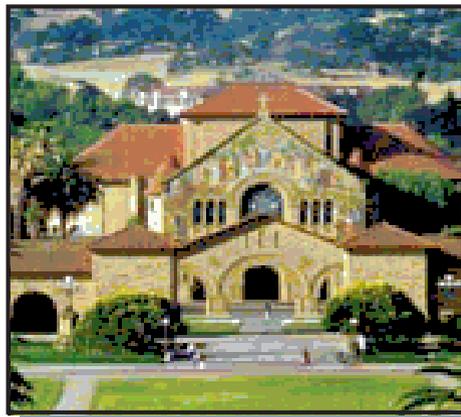
退出

## 2.3.4. 光纤信道 (2) : 美国斯坦福大学

Original message



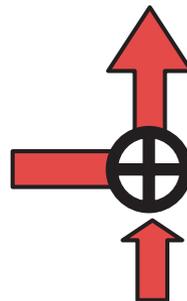
Decoded message



Alice's key



Encoded message



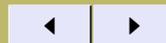
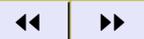
Bob's key



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 19 页 共 40 页

返回

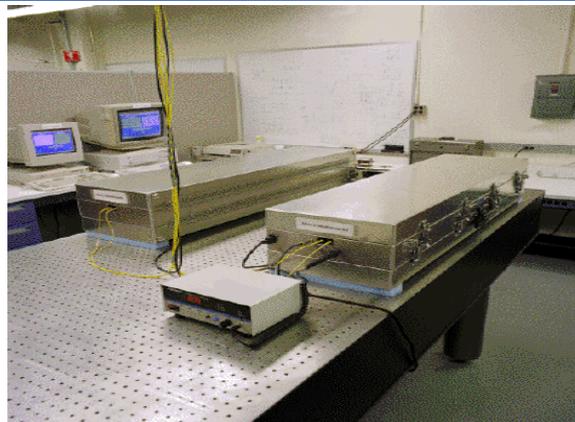
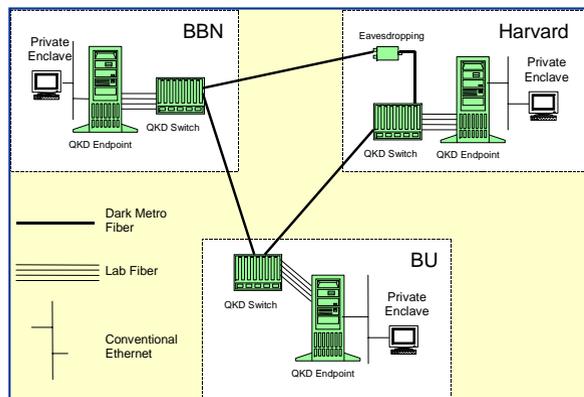
全屏显示

关闭

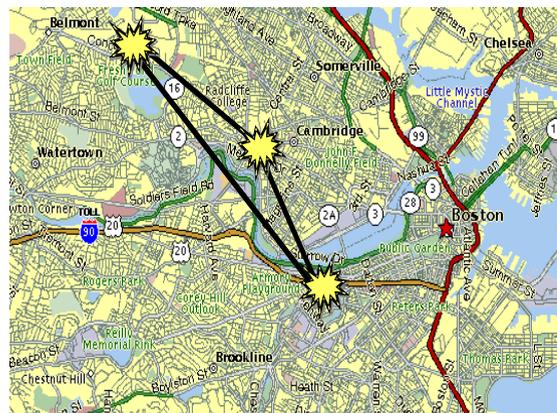
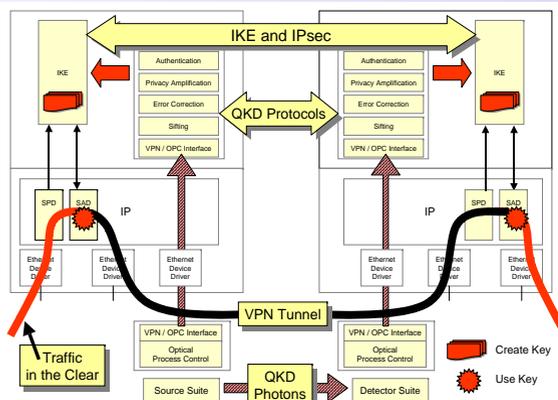
退出



## 2.3.5. DARPA:QKD网络



美国国防部正在建设的基于互联网的量子密码系统



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 20 页 共 40 页

返回

全屏显示

关闭

退出



## 2.4. 量子密码产品

### 量子密钥分配系统



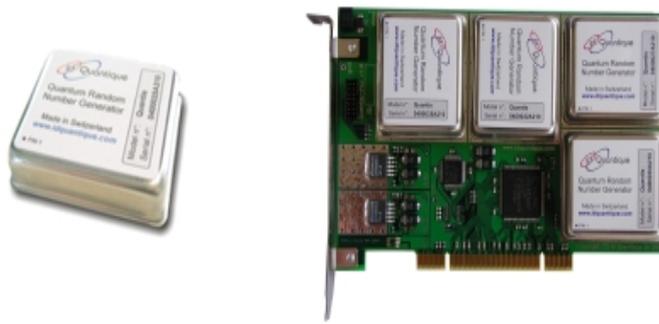
### 量子随机数发生器



### 量子信号检测仪



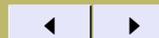
### 真随机数发生器PCI版本



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

[访问主页](#)

[标题页](#)



第 21 页 共 40 页

[返回](#)

[全屏显示](#)

[关闭](#)

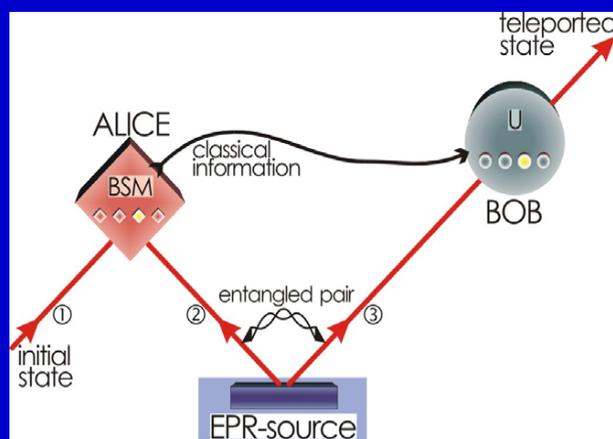
[退出](#)

# 3 量子隐形传态

## 3.1. 量子隐形传态 (1)



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟



$$\begin{aligned}
 |\Psi\rangle_{123} &= |\Phi\rangle_1 \otimes |\Phi^+\rangle_{23} \\
 &= |\Phi^+\rangle_{12} \otimes (\alpha|H\rangle_3 + \beta|V\rangle_3) + \\
 &\quad |\Phi^-\rangle_{12} \otimes (\alpha|H\rangle_3 - \beta|V\rangle_3) + \\
 &\quad |\Psi^+\rangle_{12} \otimes (\alpha|V\rangle_3 + \beta|H\rangle_3) + \\
 &\quad |\Psi^-\rangle_{12} \otimes (\alpha|V\rangle_3 - \beta|H\rangle_3),
 \end{aligned}$$

Initial state

$$|\Phi\rangle_1 = \alpha|H\rangle_1 + \beta|V\rangle_1$$

The shared entangled pair

$$|\Phi^+\rangle_{23} = \frac{1}{\sqrt{2}} (|H\rangle_2|H\rangle_3 + |V\rangle_2|V\rangle_3)$$

where

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

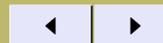
$$|\Psi^\pm\rangle_{12} = \frac{1}{\sqrt{2}} (|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2)$$

图11. 量子隐形传态

★ C. H. Bennett et al, Phys. Rev. Lett, 73, 3801(1993).

访问主页

标题页



第22页共40页

返回

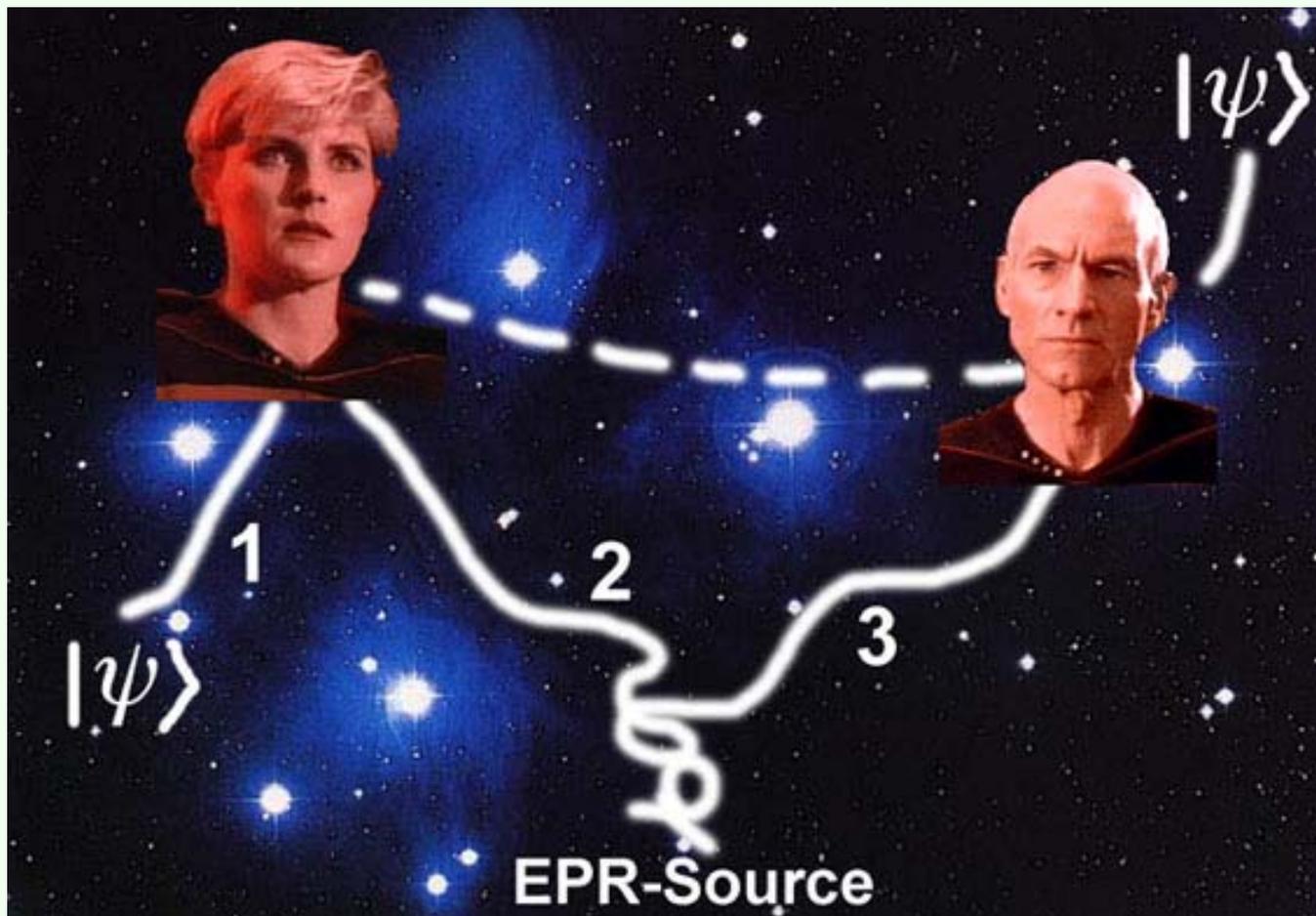
全屏显示

关闭

退出



## 3.2. 量子隐形传态 (2)



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 23 页 共 40 页

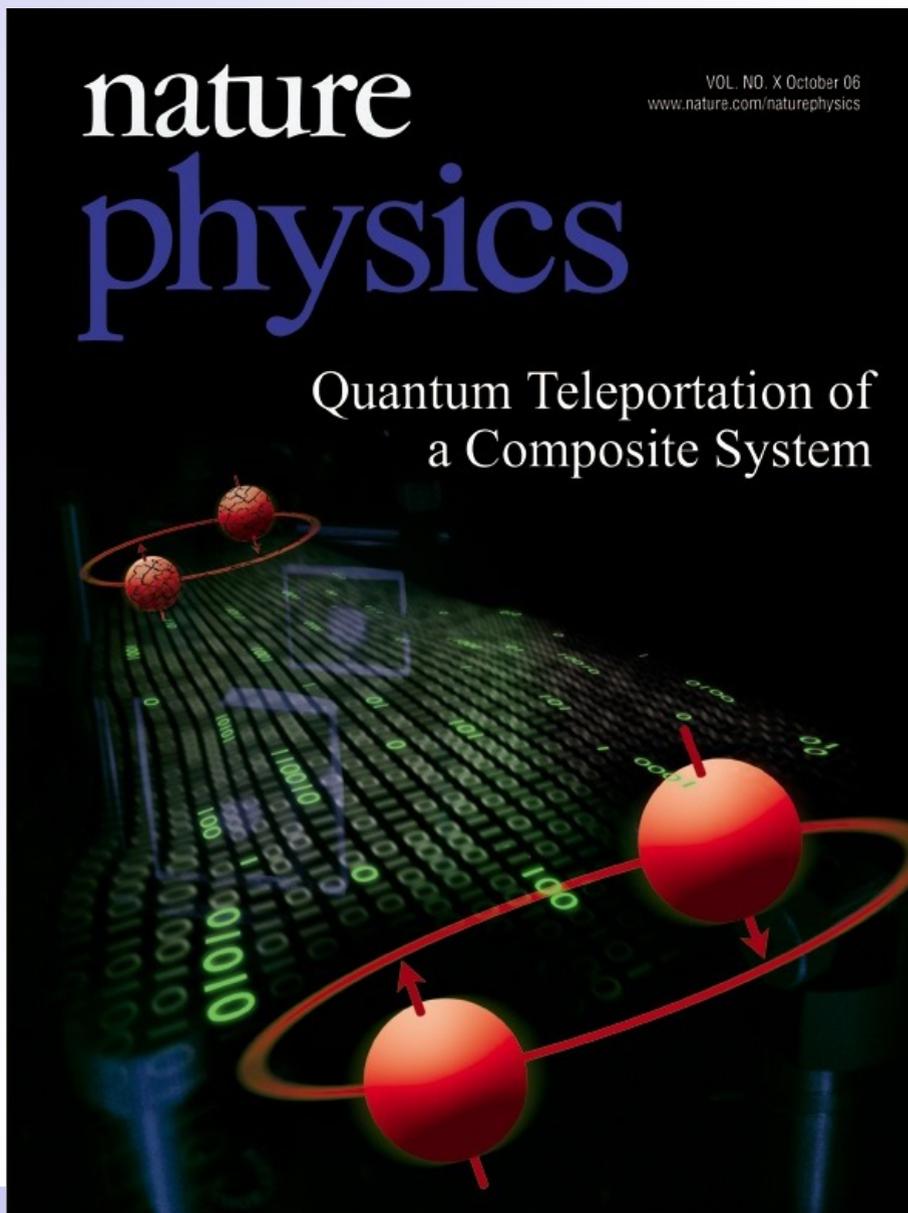
返回

全屏显示

关闭

退出

### 3.3. 量子隐形传态 (3)



量子信息理论基础

量子密码

量子隐形传态

量子纠缠交换

量子中继

量子密集编码

量子远程克隆

量子计算

量子物理世界版图

上海交通大学量子信息...

诚邀加盟

访问主页

标题页

◀ ▶

◀ ▶

第 24 页 共 40 页

返回

全屏显示

关闭

退出

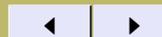
### 3.4. 量子隐形传态 (4)



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

[访问主页](#)

[标题页](#)



第 25 页 共 40 页

[返回](#)

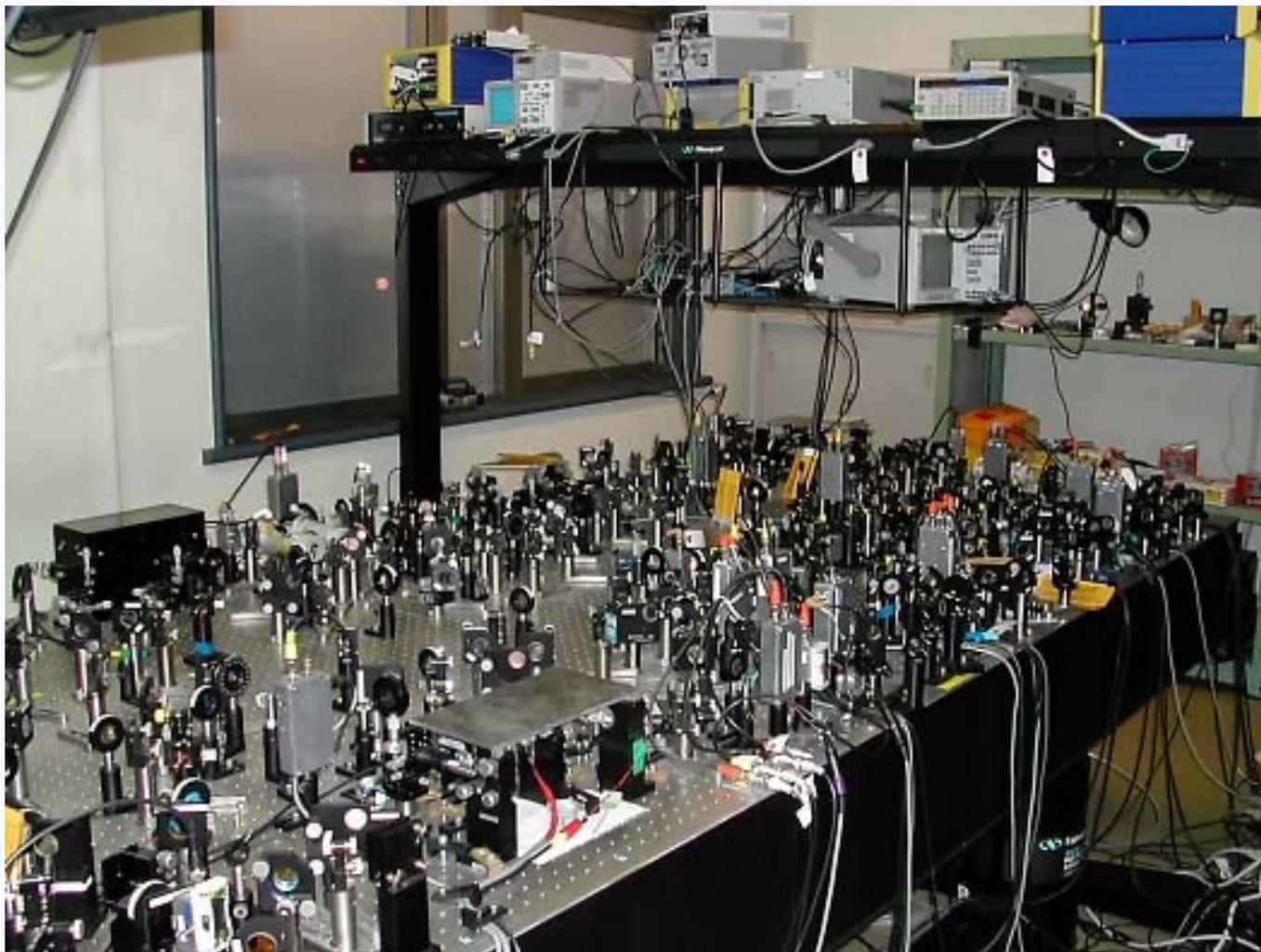
[全屏显示](#)

[关闭](#)

[退出](#)



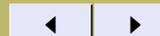
### 3.5. 量子隐形传态 (5)



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 26 页 共 40 页

返回

全屏显示

关闭

退出

# 4 量子纠缠交换

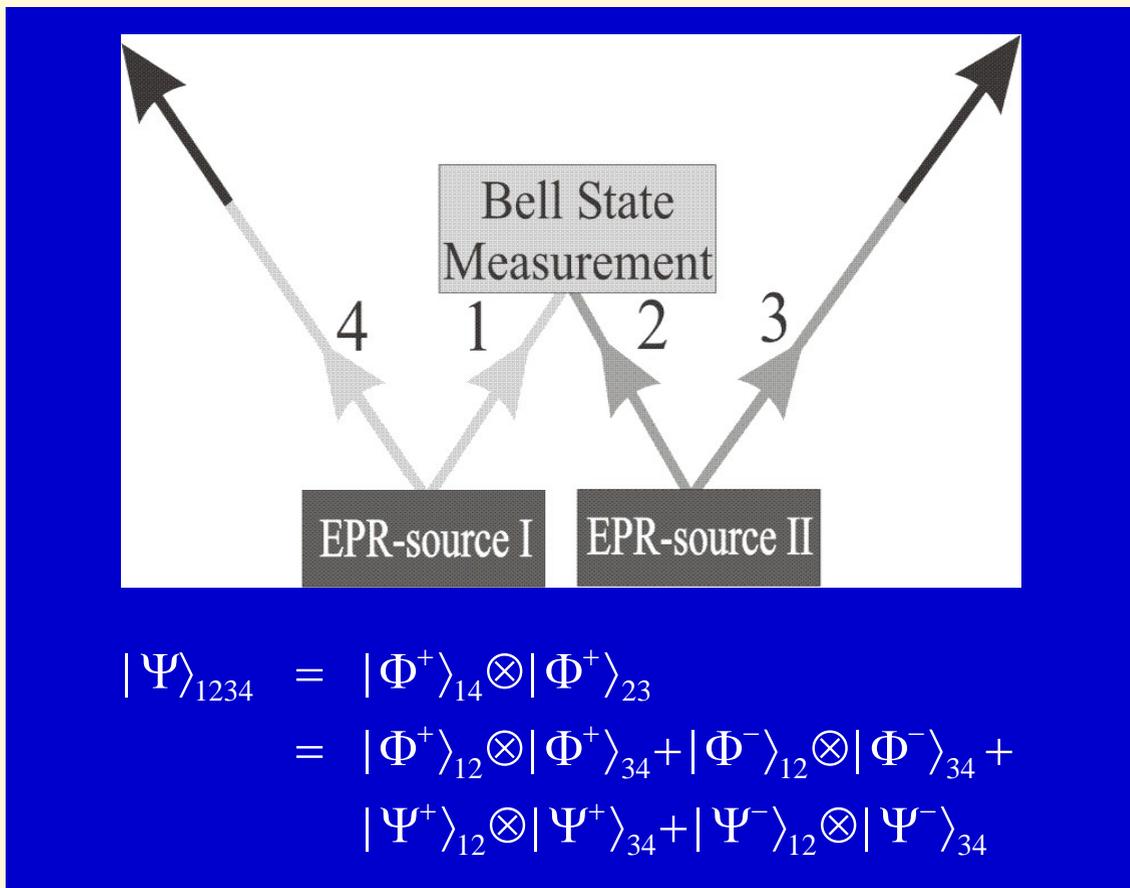


图12. 量子纠缠交换

★ J. W. Pan et al, Phys. Rev. Lett, 80, 3891 (1998).



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页

◀ ▶

◀ ▶

第 27 页 共 40 页

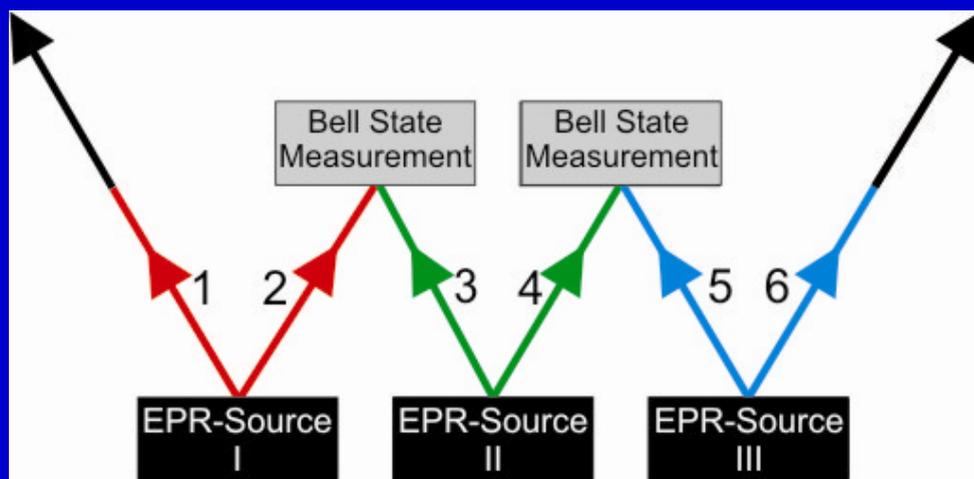
返回

全屏显示

关闭

退出

## 5 量子中继



Needed for  
realization of quantum repeaters  
speeding up distribution of entanglement

图13. 量子中继

★ J. W. Pan et al, Phys. Rev. Lett, 80, 3891 (1998).



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 28 页 共 40 页

返回

全屏显示

关闭

退出

## 6 量子密集编码

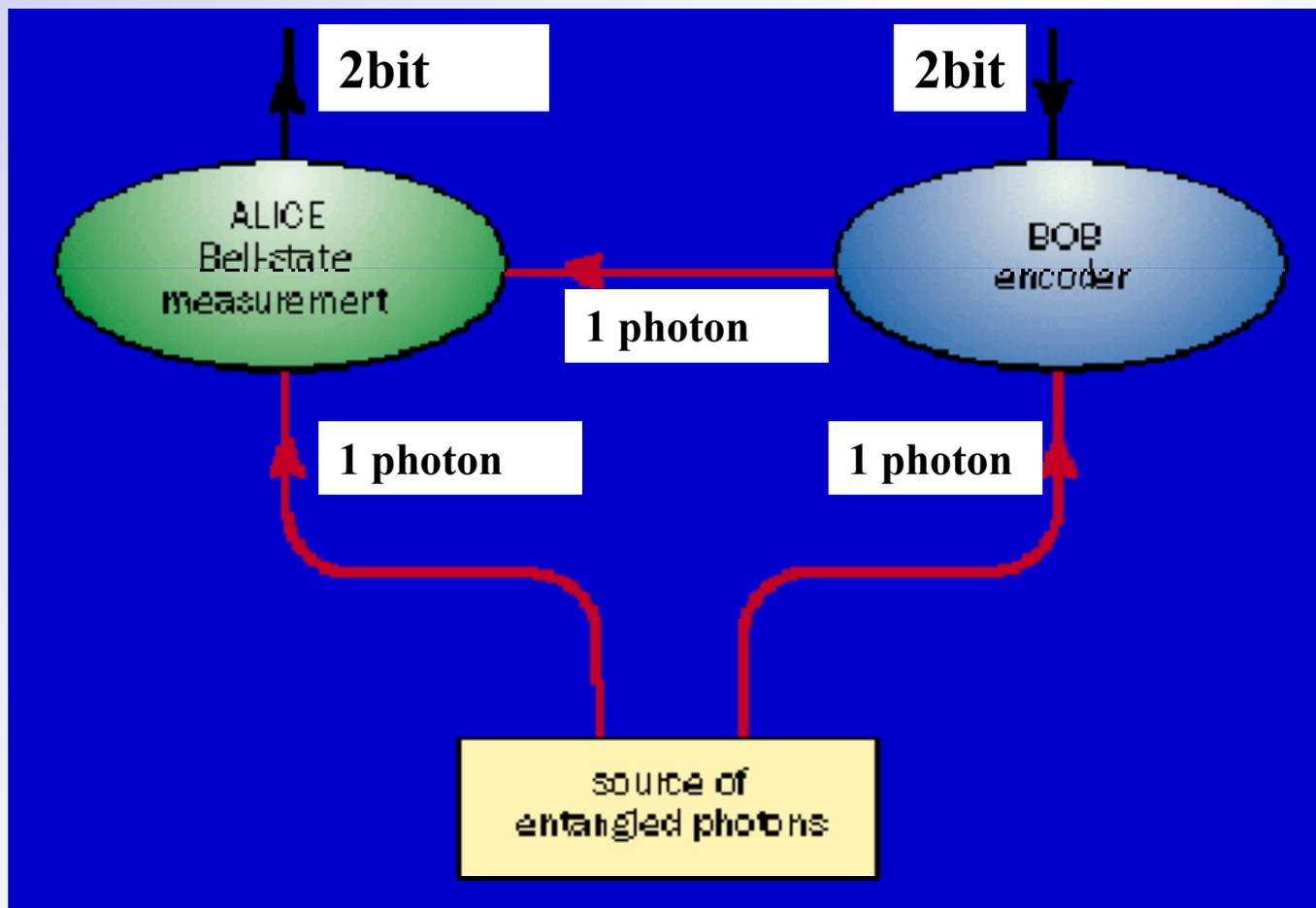


图14. 量子密集编码

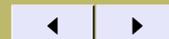
★ C. H. Bennett et al, Phys. Rev. Lett. 69, 2881 (1992)



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第29页共40页

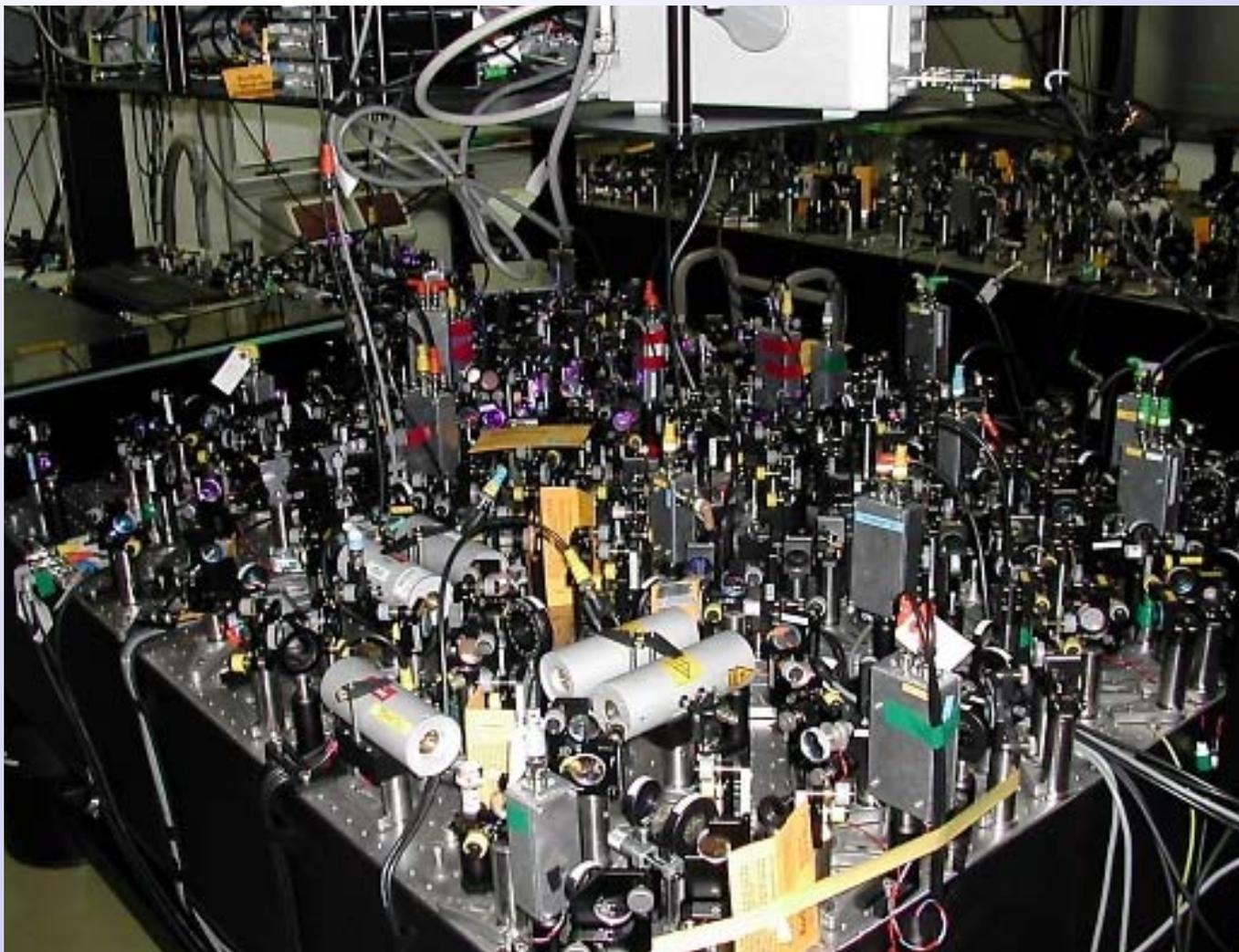
返回

全屏显示

关闭

退出

# 7 量子远程克隆



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

[访问主页](#)

[标题页](#)



第 30 页 共 40 页

[返回](#)

[全屏显示](#)

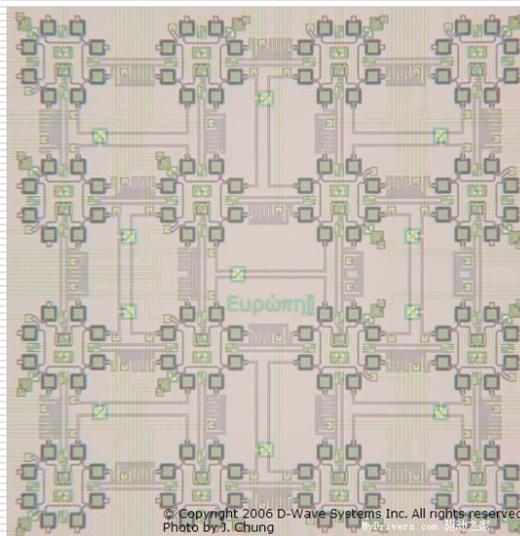
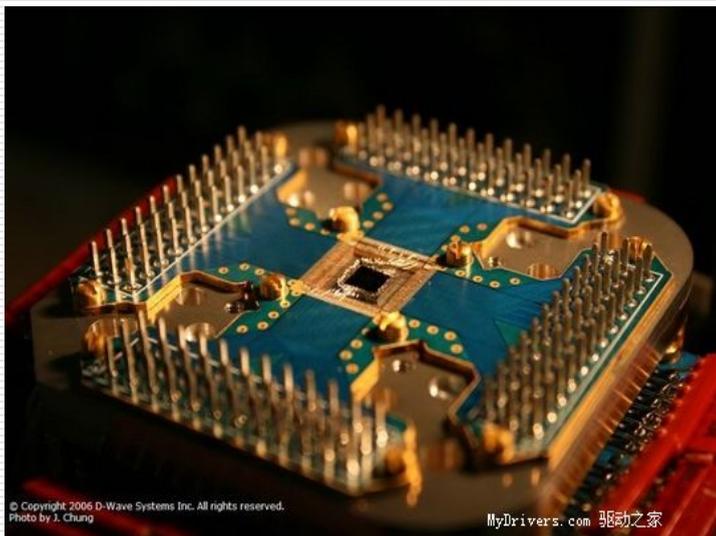
[关闭](#)

[退出](#)

## 8 量子计算

# A new model for quantum computer

A quantum computer by D-wave company in Canada in 2007



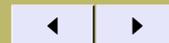
A Chip with 16 qubits for quantum computing



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

[访问主页](#)

[标题页](#)



第 31 页 共 40 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)



## 9 量子物理世界版图



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 32 页 共 40 页

返回

全屏显示

关闭

退出

# 10 上海交通大学量子信息研究成果

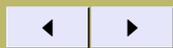
## 10.1. 量子密钥分配与验证系统



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

[访问主页](#)

[标题页](#)



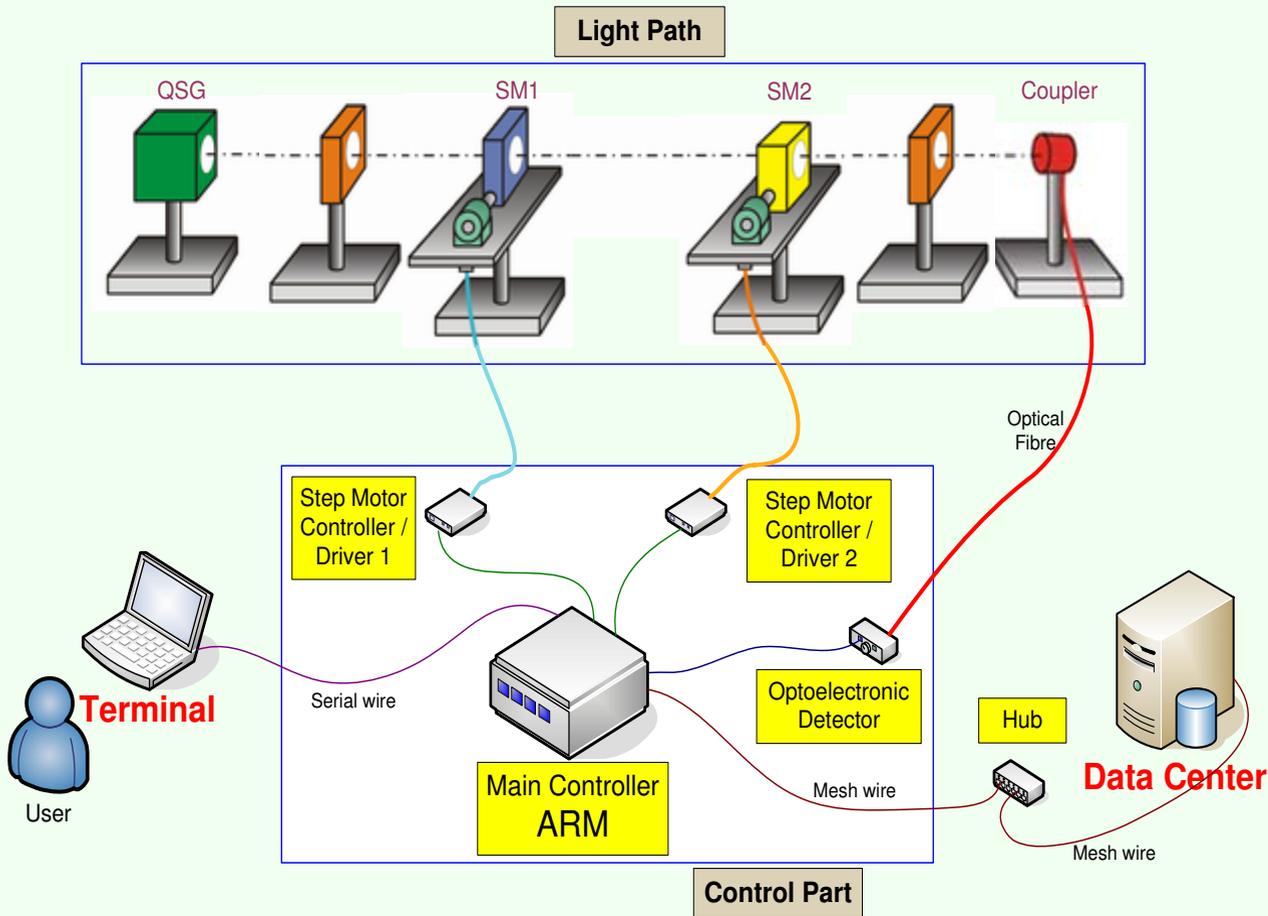
第 33 页 共 40 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)





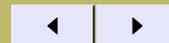
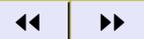
## 10.2. 基于量子身份认证“量子锁”



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

访问主页

标题页



第 34 页 共 40 页

返回

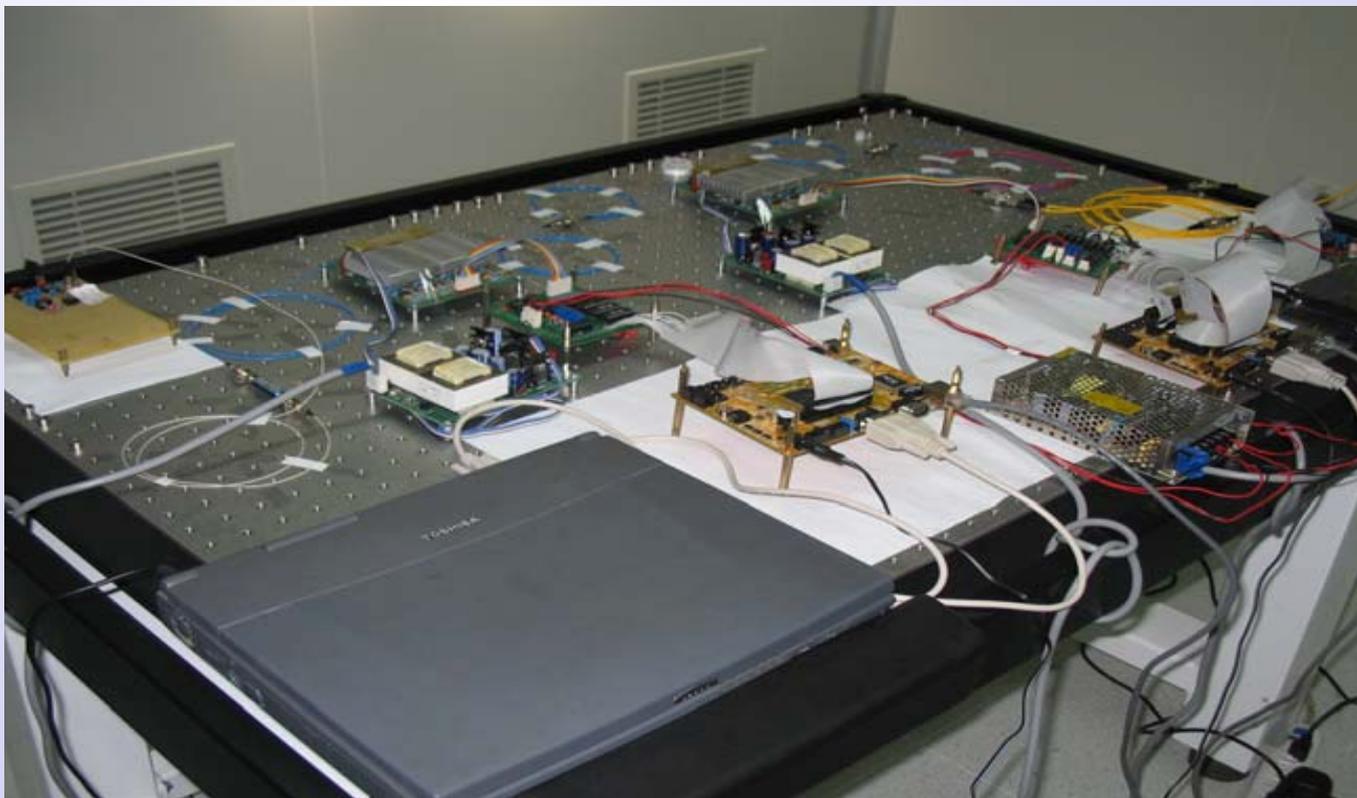
全屏显示

关闭

退出



## 10.3. 量子数据加密系统 (1)



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

[访问主页](#)

[标题页](#)

[◀](#) [▶](#)

[◀](#) [▶](#)

第 35 页 共 40 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)



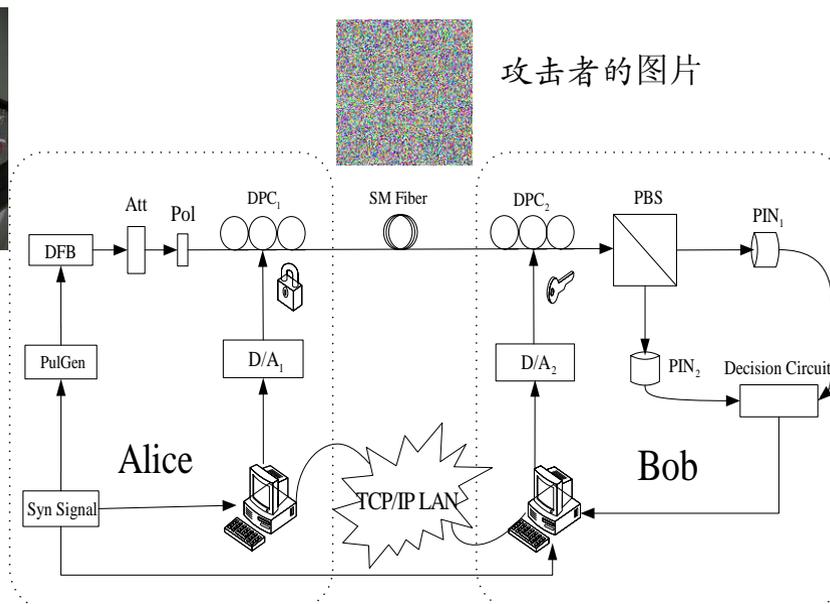
## 10.4. 量子数据加密系统 (2)



实验系统



发送者的图片



攻击者的图片

速率: 7kbit/s  
 误码率: 1/10000  
 光子数: 50000



访问主页

标题页



第 36 页 共 40 页

返回

全屏显示

关闭

退出

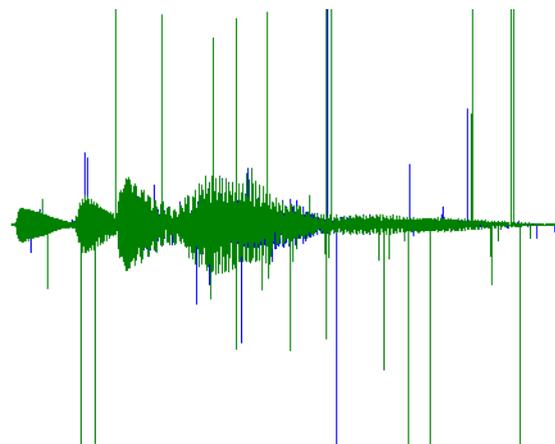


量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

## 10.5. 量子数据加密系统 (2)



(a) Alice发出的声音信号



(b) Bob接收到信号

访问主页

标题页



第 37 页 共 40 页

返回

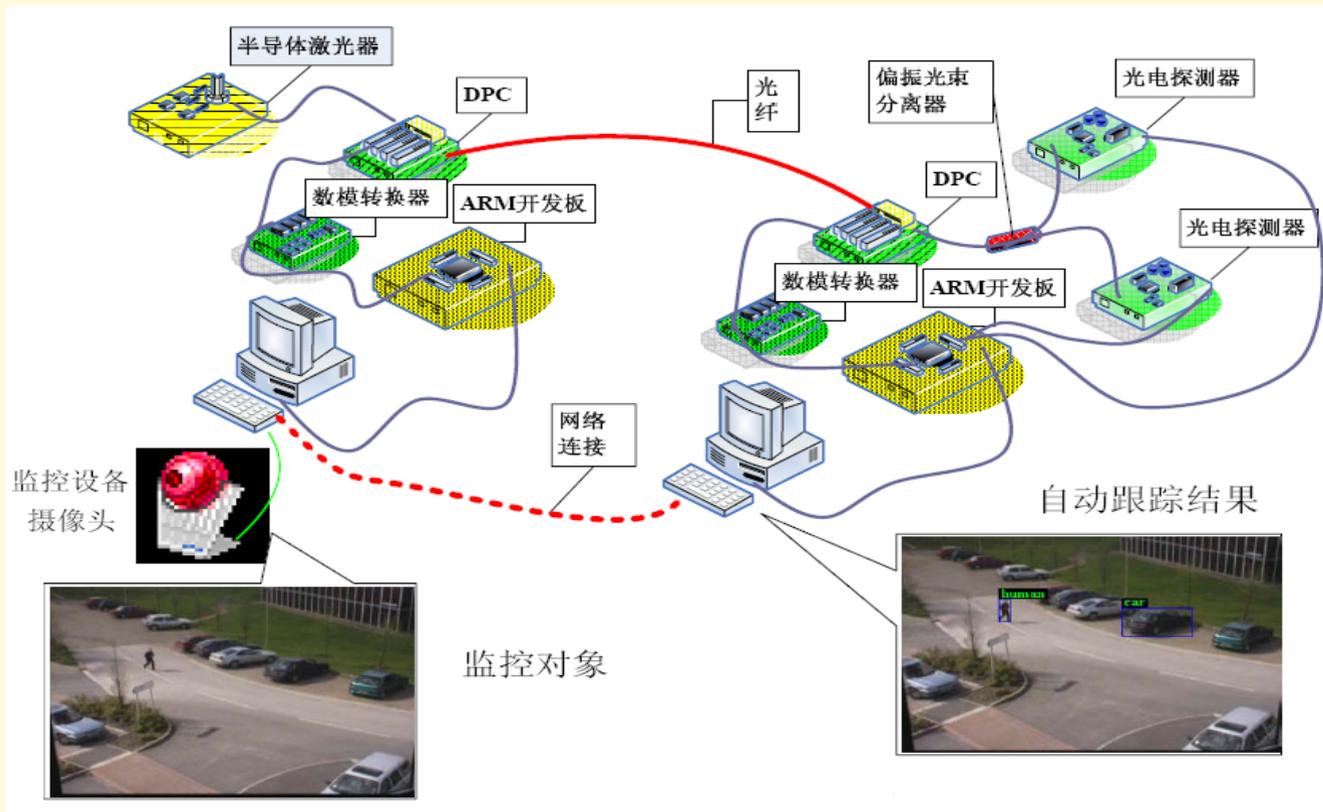
全屏显示

关闭

退出



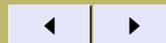
## 10.6. 量子安全监控系统



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

[访问主页](#)

[标题页](#)



第 38 页 共 40 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)



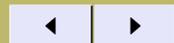
量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

# 11 诚邀加盟

- 浓厚的研究兴趣
- 量子物理基础
- 光通信基础或者电磁场基础
- 电路设计基础
- 程序设计能力

[访问主页](#)

[标题页](#)



第 39 页 共 40 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)



量子信息理论基础  
量子密码  
量子隐形传态  
量子纠缠交换  
量子中继  
量子密集编码  
量子远程克隆  
量子计算  
量子物理世界版图  
上海交通大学量子信息...  
诚邀加盟

# 谢谢

地址：上海市东川路 800 号交通大学电子工程系电信楼群 5  
号楼 205 房间 (200240)

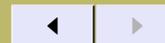
Email: [gqhc@sjtu.edu.cn](mailto:gqhc@sjtu.edu.cn) or [laser\\_gqhc@hotmail.com](mailto:laser_gqhc@hotmail.com)

电话： 021-34204362 (办公室)



访问主页

标题页



第 40 页 共 40 页

返回

全屏显示

关闭

退出