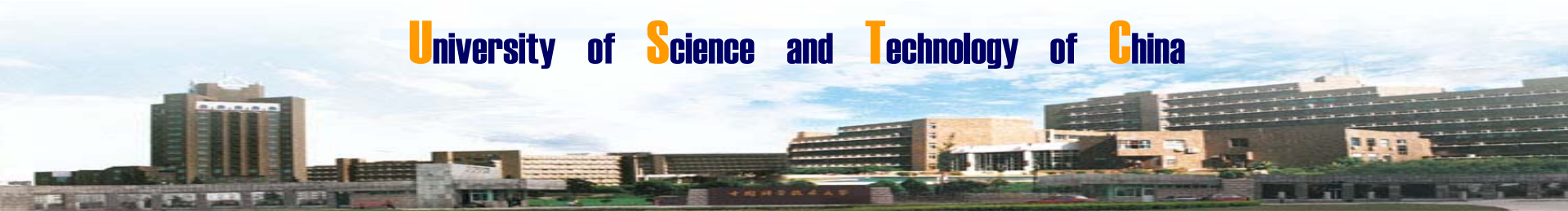
量子密码的原理和应用

蔡文奇

中国科学技术大学量子物理与量子信息研究部



传统密码术

- 私钥密码系统

  通信双方Alice和Bob共享同一个私钥，通过私钥实现加密解密，但密钥分配和原始密钥的保密通信存在严重问题，易被窃听，并不安全

- 公钥密码系统

  接收方Bob向所有人公布“公钥”，发送方Alice用此公钥将消息加密 后传给Bob，第三方使用公钥逆向解密非常困难，而Bob可以用与 该公钥匹配的私钥轻松解密，并且私钥只有Bob一人拥有

QPQI Quantum Physics and Quantum Information

传统密码术的危机

- 著名的RSA密码系统

  目前最广泛被采用的公钥密码系统，其安全性建立在经典计算机分解大数因数的十分困难的基础之上.

- 量子Shor算法

  利用量子计算机的特点，将大数因子分解的计算复杂度从指数关系转为多项式关系，一旦量子计算机出现，RSA公钥加密术将不再安全.

- 幸运的是，虽然量子力学剥夺了一方面，但它在另一方面也给出了补偿

- 被称作量子密码术或量子密钥分配的过程，利用了量子力学原理来保证秘密信息的可证明的安全分配

量子密码术

- 利用了量子力学原理，通过公开信道在异地用户之间实现密钥的分配，并严格保证了密钥分配过程中的安全性

QPQI

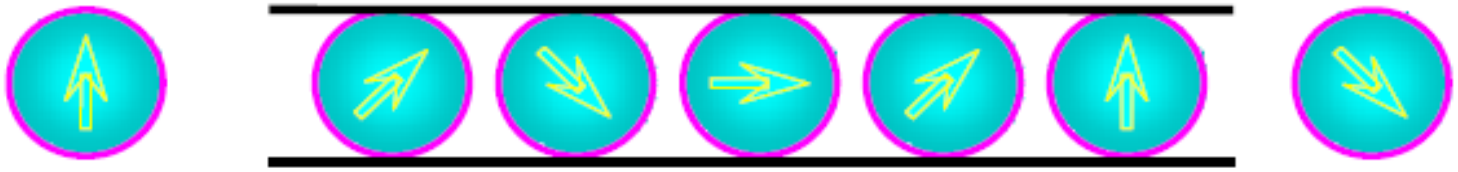
Quantum Physics and Quantum Information

安全保障

- 量子（随机，叠加）性——不可分取,不可预测
- 不可克隆定理：不可能构造这样的量子设备，它对任意的 $|\psi\rangle$，在给定 $|\psi\rangle$ 的条件下，输出 $|\psi\rangle\,|\psi\rangle$ ——不可拷贝
- 量子测量塌缩——一旦测量将破坏原量子态

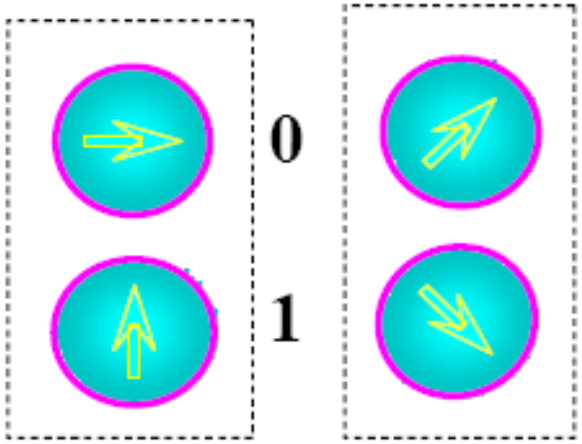
QPQI Quantum Physics and Quantum Information

光子的偏振态



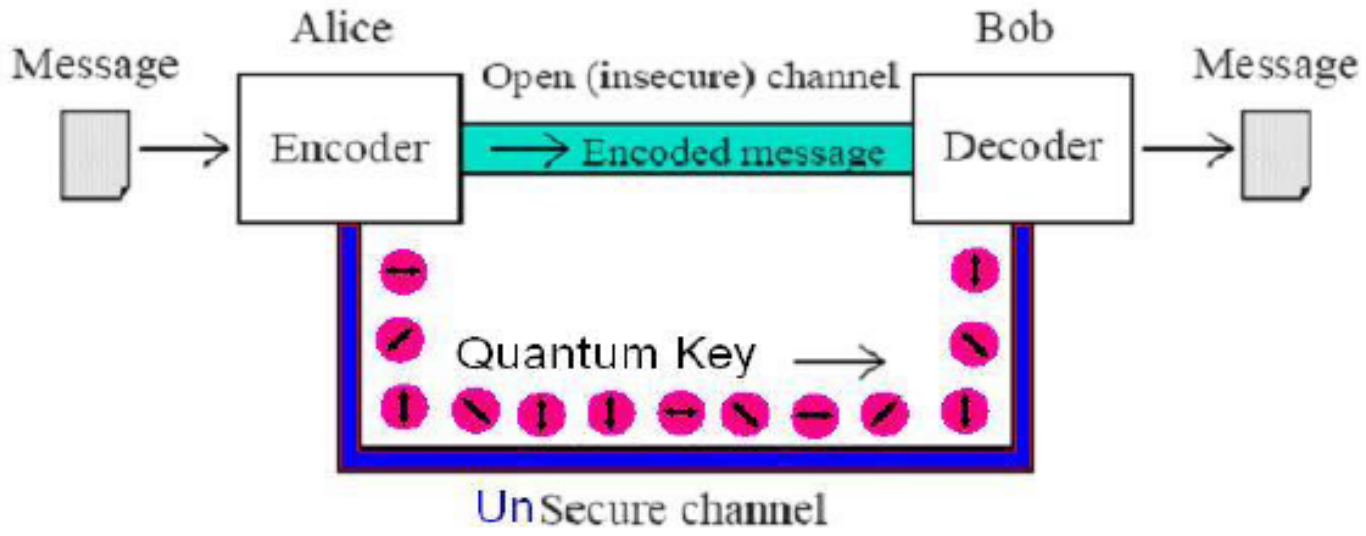
Alice

Bob



量子密码原理

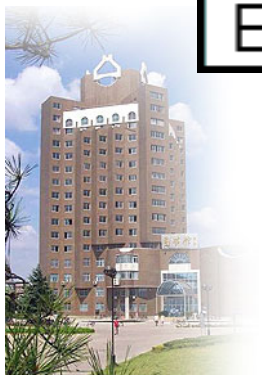
量子密钥分配技术



量子密码原理

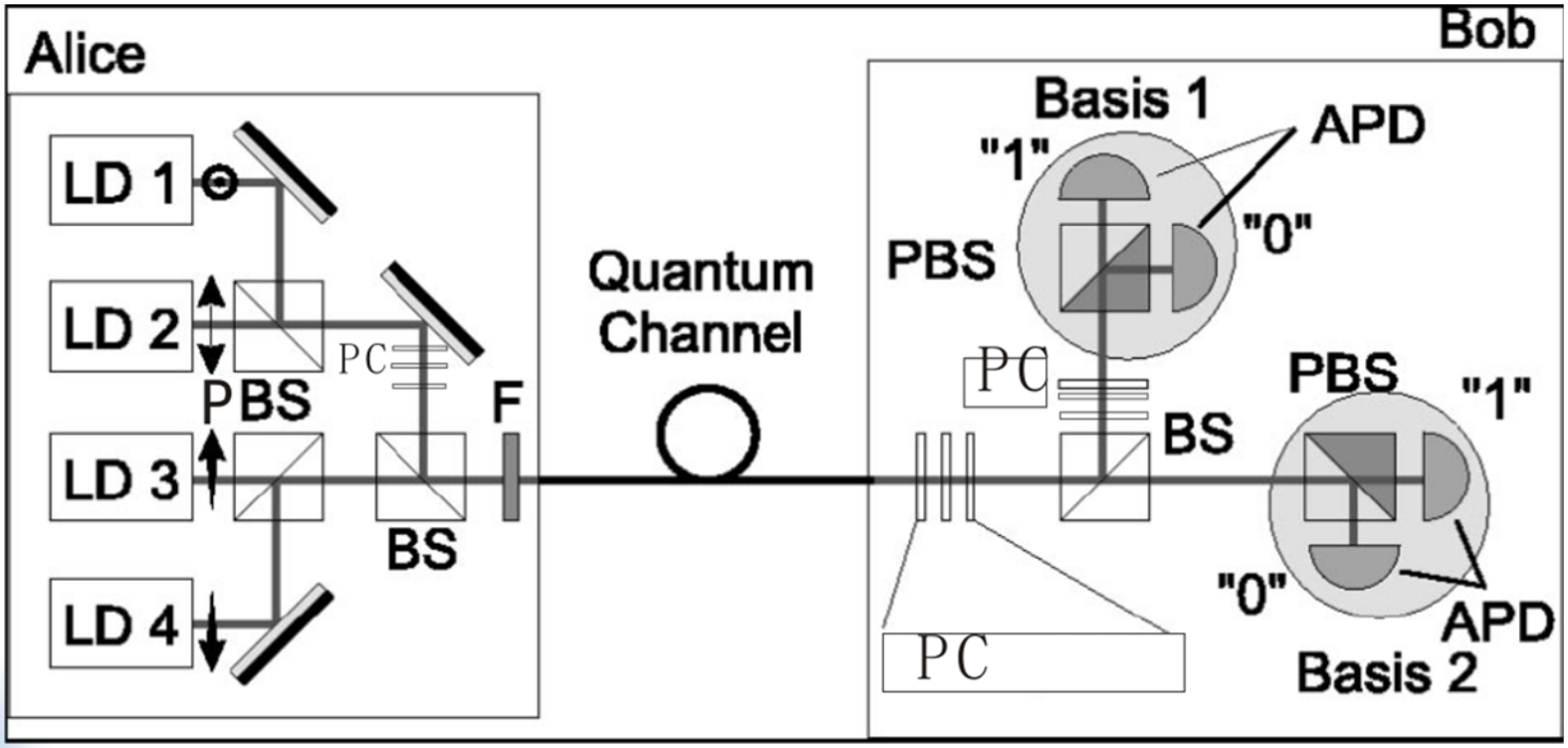
- BB84协议

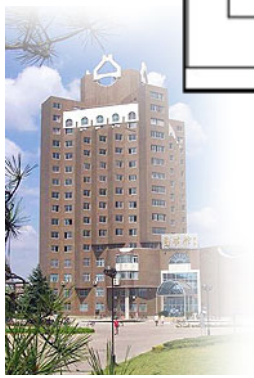
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
A	↘	↘	→	↑	→	↗	→	↑	↑	↘	↗	→	↘	↑
B	+	×	×	+	×	×	+	×	×	×	+	+	+	+
C	→	↘		↑	↗	↗	→		↗	↘	↑		↑	↑
D		↘		↑		↗	→			↘				↑
E		1		1		0	0			1				1



Quantum Physics and Quantum Information

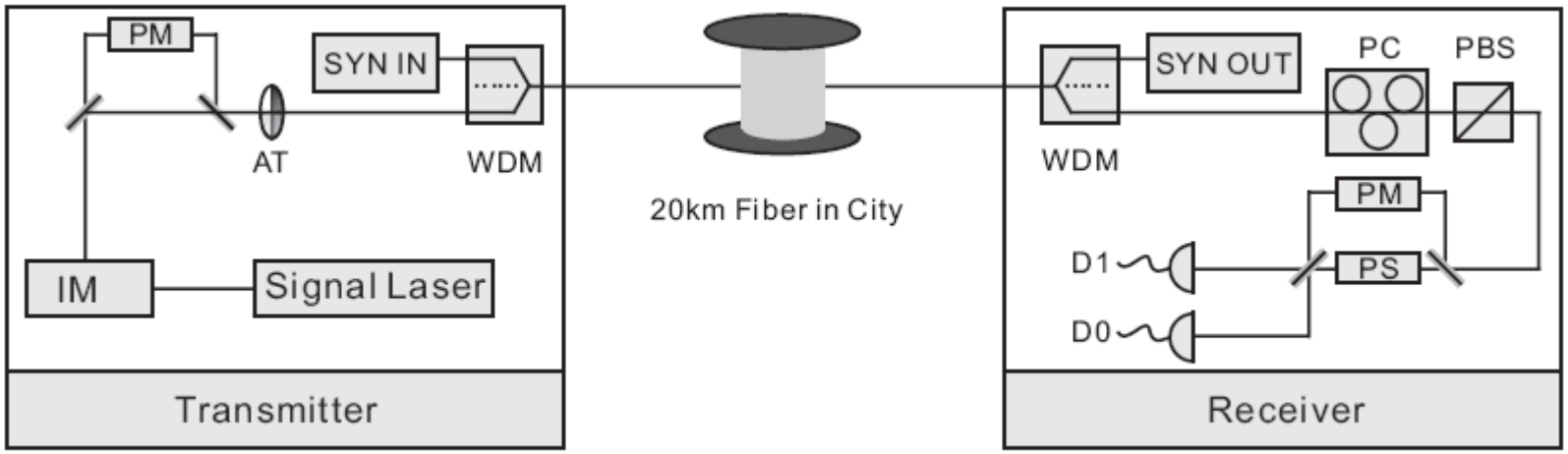
极化编码的光路设置图





Quantum Physics and Quantum Information

相位编码光路图



Quantum Physics and Quantum Information

安全漏洞与解决方案

- 真正意义上的单光子源还无法实现,有一定机率（虽然机率很小）一个脉冲会发射多个光子,如果窃听方将多光子态分出一个光子,而将其余的光子仍发给Bob,从而窃听到信息并且不被通信双方发现.

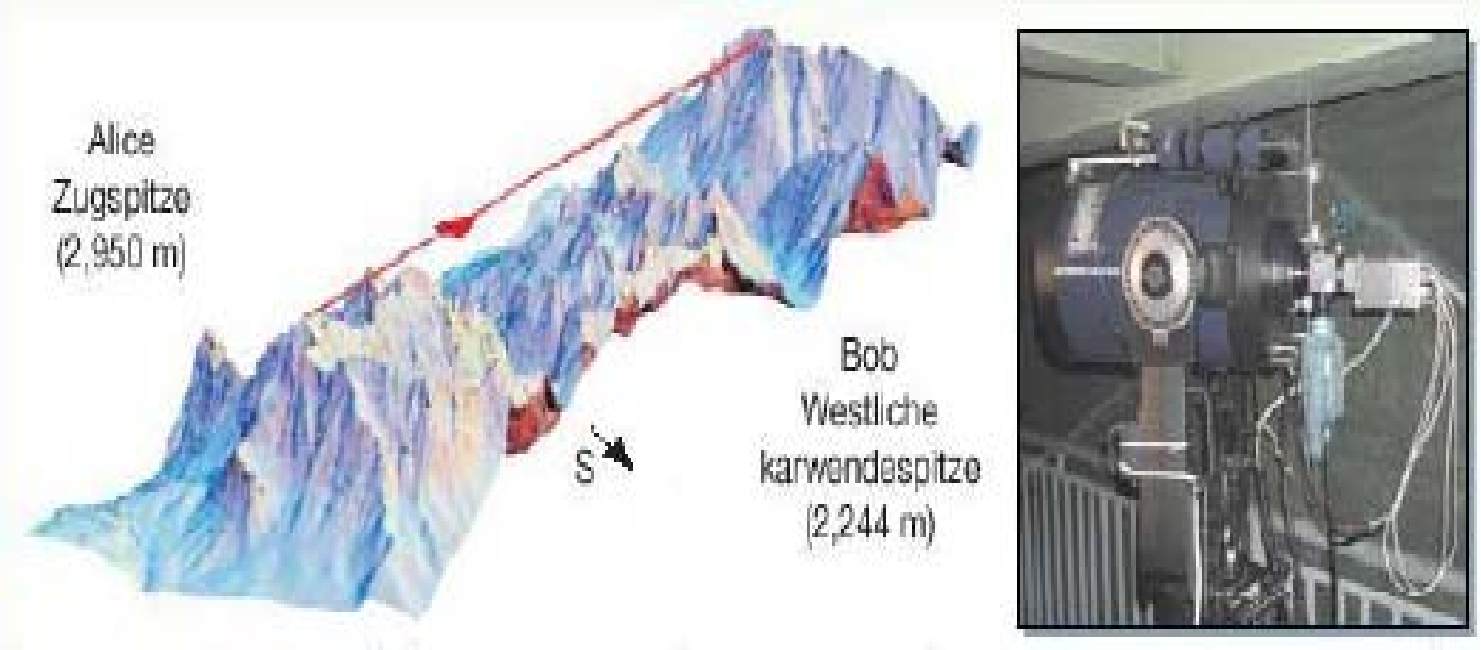
- Decoy(诱偏态)方案:在信号态中参杂一部分Decoy态，其光强与信号光成一定比率，因此Decoy态与信号态的多光子态机率不同，如果被第三方用分光子的方法窃听，将导致接收方的信号态与Decoy态比值不同。

QPQI Quantum Physics and Quantum Information

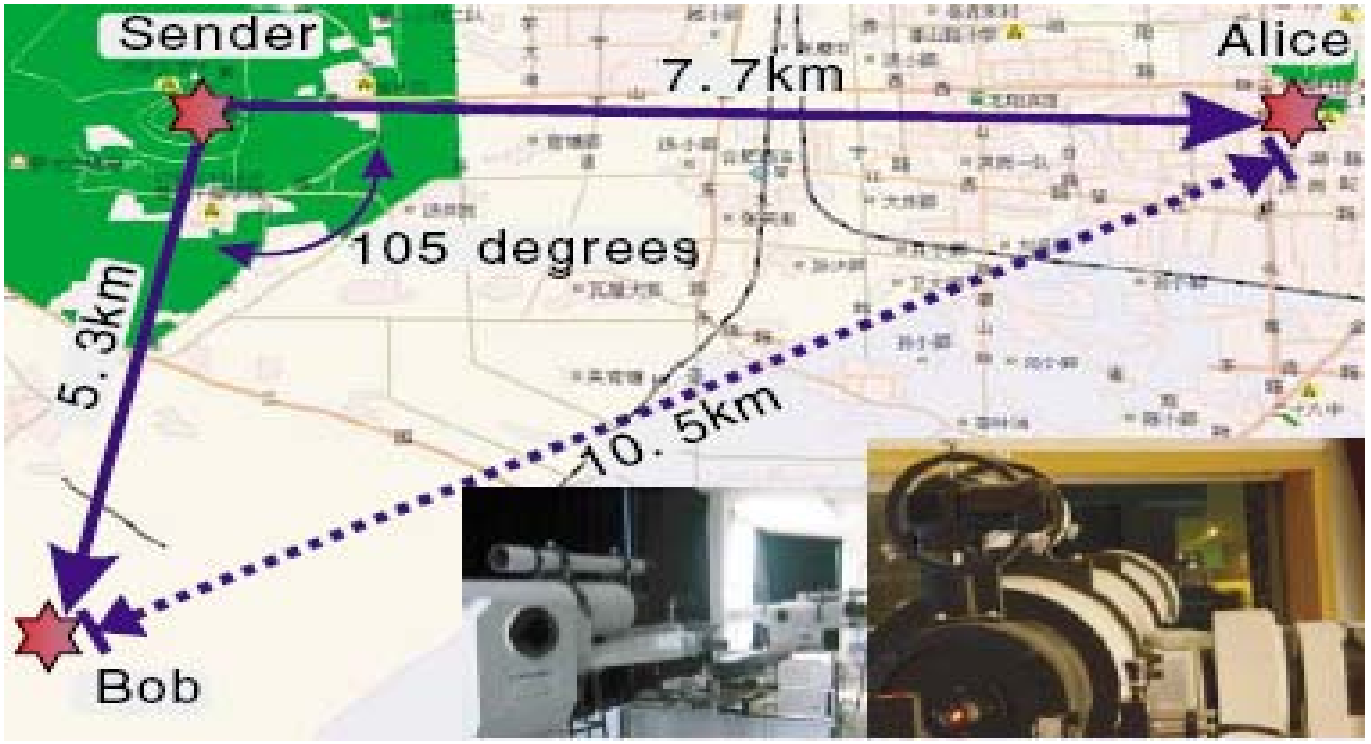
一些实验

美国Las Alamos Lab

德国Zugspitze



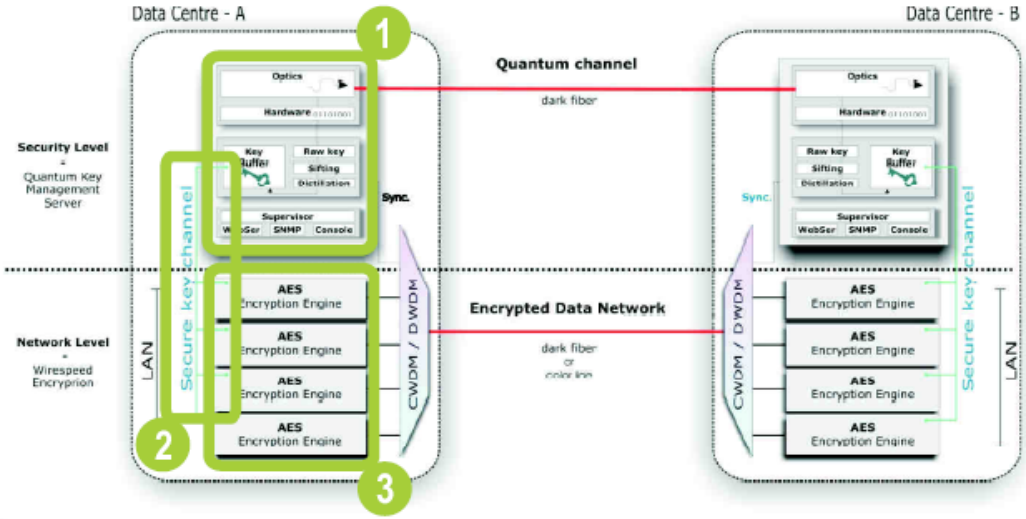
合肥 大蜀山



Quantum Physics and Quantum Information

应用实例

- id Quantique公司的产品



Quantum Physics and Quantum Information

QPQI

合肥三点光纤量子通讯系统

Quantum Physics and Quantum Information

Thanks!

Quantum Physics and Quantum Information