量子密码学

1901210635 龚彦韬
1901210593 张宇驰

目录

01 *Part One*

量子密码学概论

量子密码学概论

什么是量子密码学

传统密码技术：存在缺陷

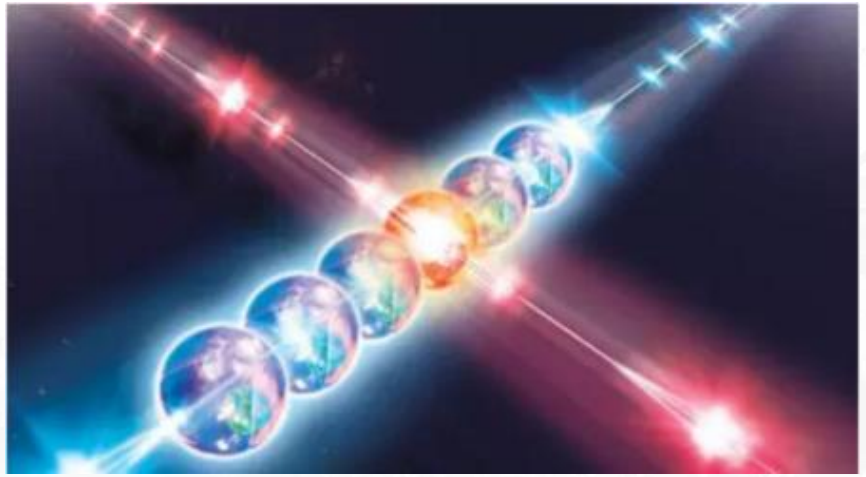
- 基于数学的密码体制
- 密钥安全性

量子密码体制：更为可靠且安全

- 海森堡测不准原理
- 量子不可克隆原理

量子测量

- 量子力学假定封闭量子系统演变是么正演化。
  - 么正性是物理学名词，
  - 微观过程物质不灭的原理
  - 量子测量
- 在不知道量子状态的情况下，复制单个量子是不可能的。因为要复制单个量子就必须先要做测量，而测量就必然会改变量子的状态。

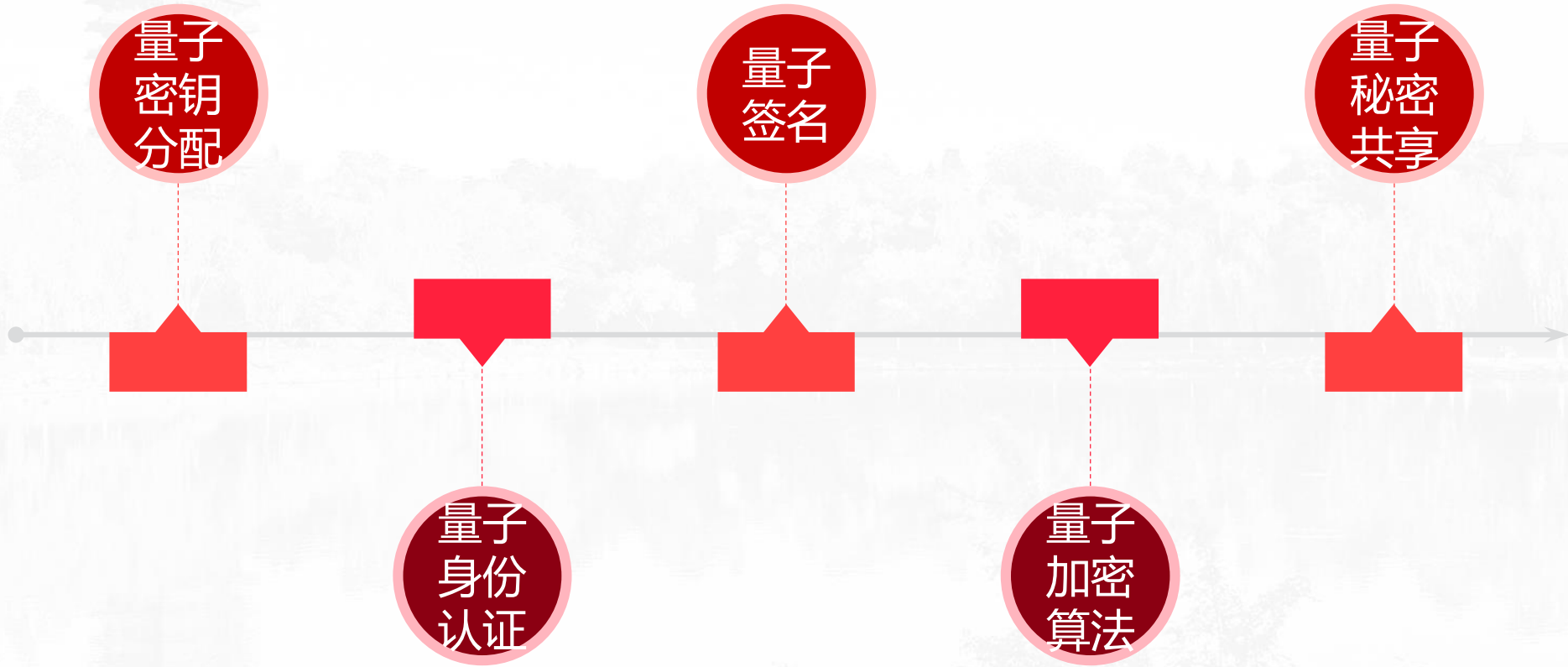


量子叠加原理

- 量子态叠加原理，又称叠加态原理，是量子力学中的一个基本原理，广泛应用于量子力学各个方面。
- 若ψ_1和ψ_2是体系的两个可能的态，则它们的线性叠加 $\psi = c_1\psi_1 + c_2\psi_2$ 也是体系可能的态。相叠加的态可以扩展为n个甚至无穷个，而且叠加是线性的，叠加系数是复常数。量子态的叠加，是几率幅的叠加，而不是物理量的叠加。由ψ_1和ψ_2两种态叠加起来的态ψ是一个新的状态，它既不是ψ_1态也不是ψ_2态，它可以具有原来两个态都没有的新的性质。

量子密码学概论

量子密码学的研究领域



02 *Part Two*

经典量子密钥分发协议

经典量子密钥分发协议

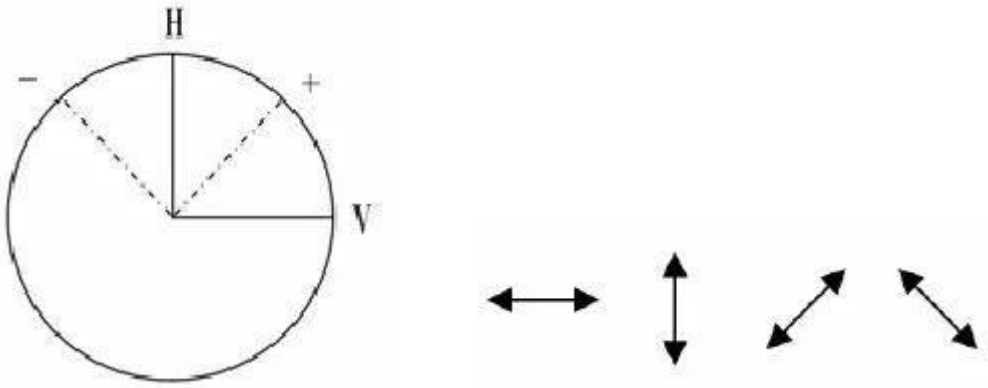
量子密钥分发及其威胁

- 量子密钥分发的基本思想。
- 通信中的窃听主要有两类：
  - 第一类是窃听者Eve对传输的量子态做一系列测量,并从测量结果中获取所需信息。由量子力学原理可知，Eve的任何测量都会使单光子的量子态或纠缠光子的关联性遭到破坏。在公开信道通信过程中，这种窃听方式很容易被察觉。
  - 第二类是Eve不进行直接量子测量而是采用量子复制机来拷贝传送的量子态，并将原来的量子态传送给Bob，留下复制的量子态进行测量，这样就可以在不被发现的情况下获取信息。

经典量子密钥分发协议

BB84协议

- BB84协议是量子密码学中第一个密钥分发协议，由Bennett和Brassard在1984年提出，也是使用和实验最多的量子密钥分发方案之一。BB84协议通过光子的4种偏振态来进行编码，如图所示。其中，线偏振光子和圆偏振光子的两个状态各自正交，但是线偏振光子和圆偏振光子之间的状态互不正交。

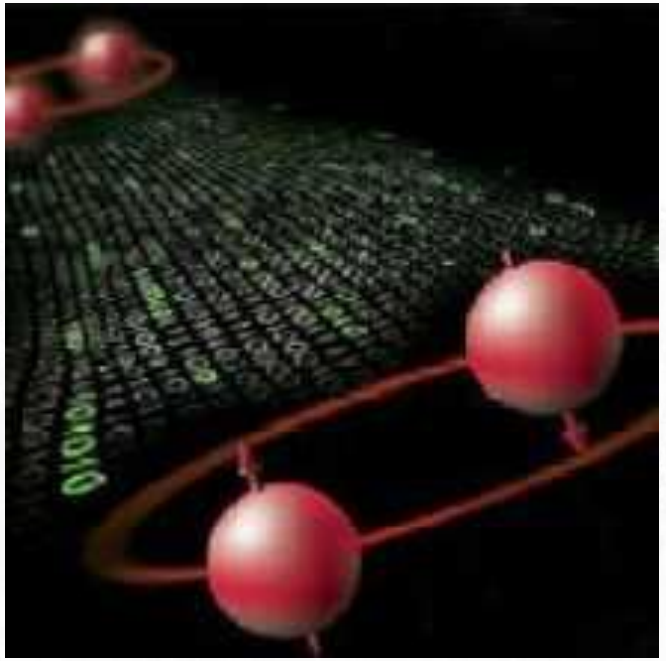


- BB84协议的实现需要两个信道：经典信道和量子信道。经典信道要确保收发双方Alice和Bob之间能进行一些必要信息的交换，而量子信道用于传输携带信息的或者随机的量子态。

经典量子密钥分发协议

BB84协议的安全性

在BB84 协议中，所采用的线偏振和圆偏振是共扼态，满足测不准原理。根据测不准原理，线偏振光子的测量结果越精确意味着对圆偏振光子的测量结果越不精确。因此，任何攻击者的测量必定会对原来量子状态产生改变，而合法通信双方可以根据测不准原理检测出该扰动，从而检测出与否存在窃听。另外，线偏振态和圆偏振态是非正交的，因此它们是不可区分的，攻击者不可能精确地测量所截获的每一个量子态，也就不可能制造出相同的光子来冒充。测不准原理和量子不可克隆定理保证了 BB84 协议量子通信的无条件安全性。



经典量子密钥分发协议

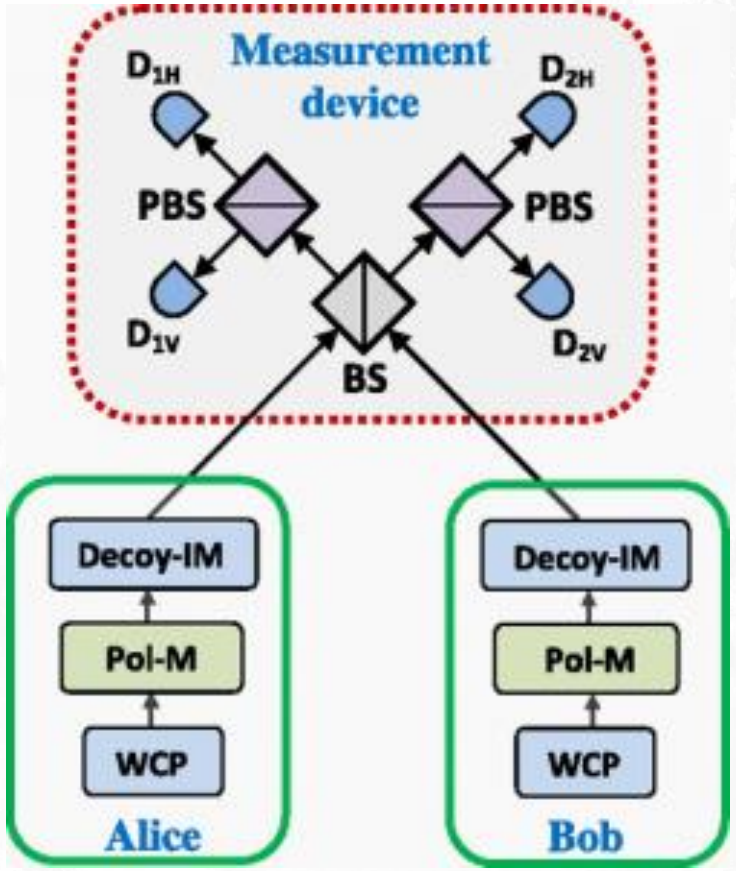
MDI-QKD协议

尽管 QKD 具有理论上的无条件安全性，然而实际 QKD 系统中因为器件的不完美性仍然存在一些安全性漏洞，针对这些安全漏洞存在多种攻击方案。2012 年多伦多大学的 Lo 等人提出的测量设备无关的量子密钥分发协议（measurement-device-independent quantum key distribution，MDI-QKD）彻底地关闭了 QKD 系统所有测量端的漏洞。在 MDI-QKD 中通信双方 Alice 和 Bob 分别随机制备 BB84 弱相干态，然后发送给一个不可信的第三方 Charlie 进行贝尔态测量，根据 Charlie 公布的贝尔态测量结果 Alice 和 Bob 建立安全的密钥。MDI-QKD 可以等价为一个时间反演的 BBM92 协议，Alice 和 Bob 根据后选择纠缠态建立安全的密钥，因此即使贝尔态测量设备完全为 Eve 所控制也不影响安全性，该协议天然地免疫所有探测器端的攻击

经典量子密钥分发协议

MDI-QKD协议

- Alice和Bob分别生成相干态脉冲并将其随机地编码为四个 BB84 态之一这里选取四个偏振态 |H⟩，|V⟩，|+⟩，|−⟩，其中 H/V 分别代表水平和竖直偏振，|±⟩=(|H⟩±|V⟩)/√2。
- 然后 Alice 和 Bob 通过一个量子信道把制备好的量子态发送给一个不可信的第三方 Charlie 进行贝尔态测量。
- Charlie 公布成功的贝尔态测量结果，Alice 和 Bob 公布他们编码使用的基矢。对于他们使用相同基矢的部分，根据 Charlie 的贝尔态测量结果，Alice 或 Bob 选择翻转或不翻转他们手中的比特以得到正关联的数据。
- 随后他们根据诱骗态方法得到单光子部分的增益和误码率，经过经典纠错和隐私放大过程得到最终的安全密钥。



MDI-QKD原理示意图

03 *Part Three*

两种新型量子密钥分发协议

两种新型量子密钥分发协议

TF-QKD协议和PM-QKD协议

QKD方案的局限性在于，它们永远不会超过具有损耗的光量子信道的秘密密钥容量(Secret Key Capacity，以下简称SKC)的限制。M. Lucamarini等于2018年提出了双场量子密钥分发协议(Twin-field Quantum Key Distribution，以下简称TF-QKD协议)，该协议在保证密钥安全的条件下突破了以前QKD协议的SKC界限，获得密钥生成率对通道透射率的平方根依赖性。然而在实际实现中，双场的相位锁定是非常具有挑战性的，马雄峰等人于2018年使用相位匹配量子密钥分发协议(Phase-matching Quantum Key Distribution，以下简称PM-QKD协议)结合相后补偿方法解决了该问题，使得锁相方法切实可行，进而在实际中提高了QKD的密钥生成率。

两种新型量子密钥分发协议

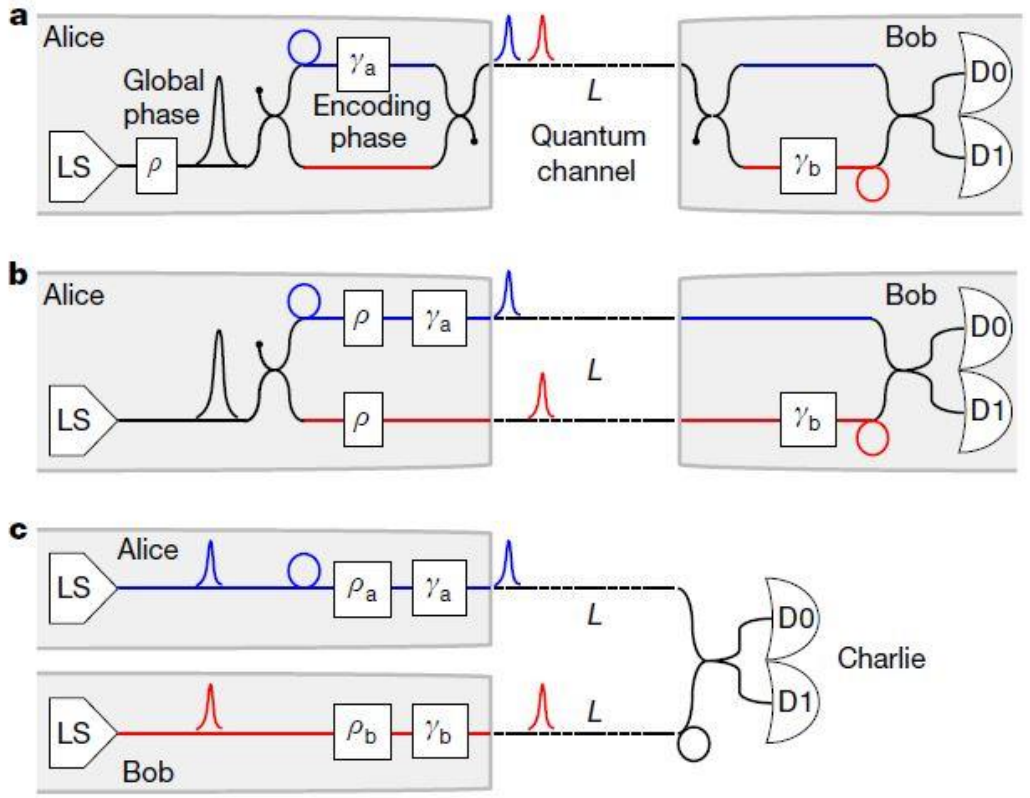
TF-QKD协议

- Step 1准备状态——Alice随机生成一个密钥比特 k_a，随机选择X基或Y基以确定密钥β_a（X基和Y基分别对应的β_a取值为0和1，并调制一个随机相位 $\varphi_a \in [0,2\pi)$，然后制备相干态$|\sqrt{\mu_a}/2e^{i(\pi k_a+\pi\beta_a/2+\varphi_a)}\rangle_A$。同样，Bob生成$k_b$，$\beta_b$和$\varphi_b \in [0,2\pi)$，然后制备$\sqrt{\mu_b}/2e^{i(\pi k_b+\pi\beta_b/2+\varphi_b)}\rangle_B$。
- Step 2测量——Alice和Bob将他们的光脉冲发送给一个非可信的拥有测量设备的Eve，Eve产生单光子干涉，并进行单光子检测，记录响应的检测器（ D1或 D2）。
- Step 3声明——Eve宣布他的检测结果，然后Alice和Bob分别宣布β_a，φ_a和β_b，φ_b。其中Alice和Bob不需要公布所选择的随机相位，只公布切片指标$\Delta_{k(a,b)}$即可。他们仅保留具有匹配值的部分并丢弃所有其他部分。

两种新型量子密钥分发协议

TF-QKD协议

- Step 4筛选——Alice和Bob多次重复以上步骤。当Eve宣布一个成功的检测(有且只有一个检测器D1或D2响应)，并且并且切片指标相匹配时，Alice和Bob令k_a和k_b 成为生密钥比特。如果Eve声明是D1响应，Alice和Bob的密钥比特不变。如果Eve声明是 响应，Bob翻转他的密钥比特。
- Step 5参数估计——Alice和Bob根据所有保留的原始数据推算出增益和量子误比特率，然后估计量子比特误码率。
- Step 6密钥精简——Alice和Bob对筛选的密钥位执行纠错和保密放大，生成私钥。



两种新型量子密钥分发协议

PM-QKD协议

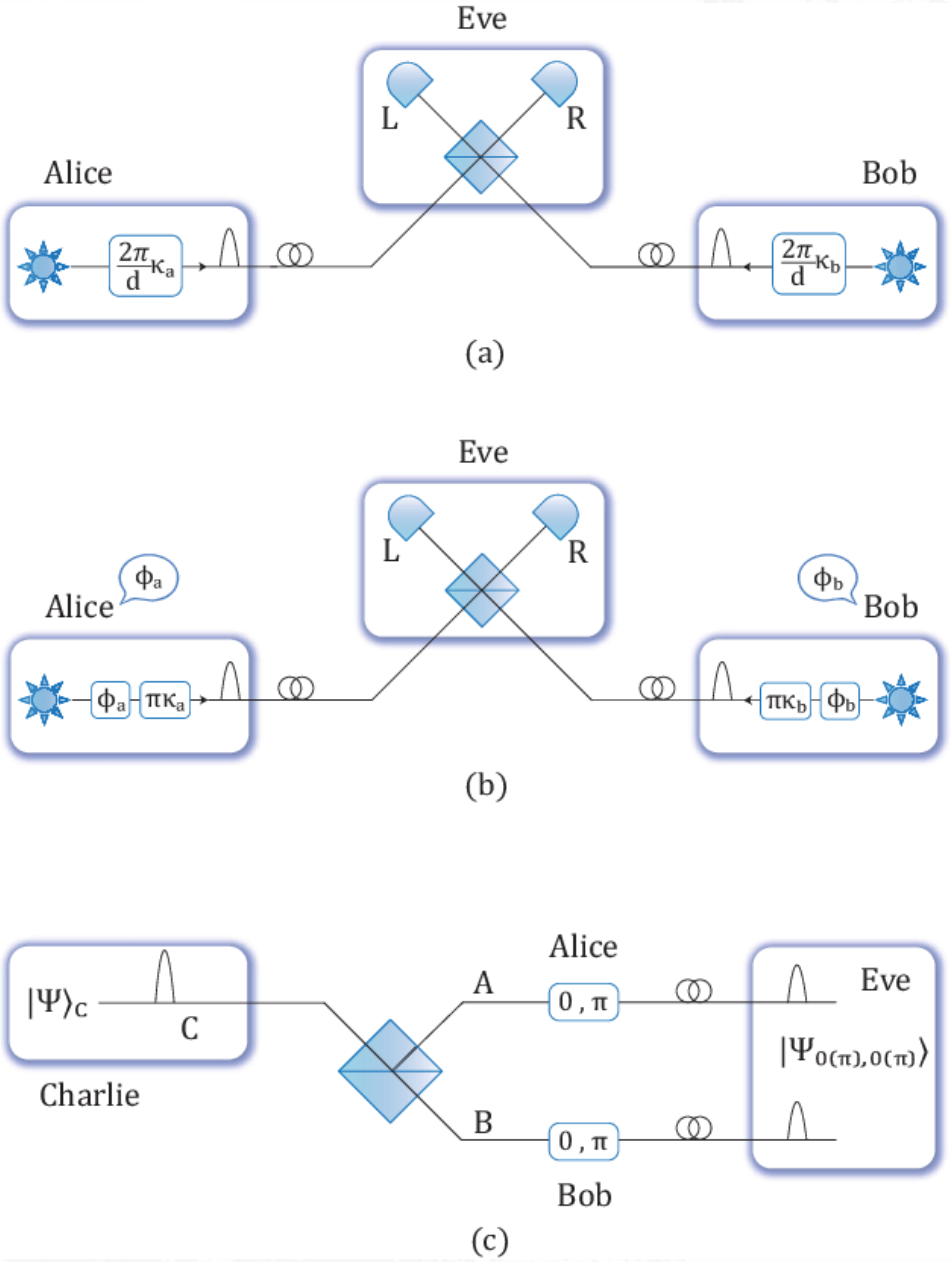
上述的TF-QKD协议提出的单光子干涉方案使得密钥率与透射率的平方根成比例，克服了没有量子中继器的量子密钥分配的速率-距离限制，但是要求有完美的初始态准备。而马雄峰等人于2018年提出的PM-QKD协议，相位信息可以直接编码在不同光子数态的相对相位上，是一个基于相干态本身的协议，其具体步骤如下：

- Step 1准备状态——Alice随机生成一个密钥比特k_a和一个随机相位$\varphi_a \in [0,2\pi)$然后制备相干态$|\sqrt{\mu_a/2}e^{i(\pi k_a+\pi\beta_a/2)}\rangle_A$。同样，Bob生成$k_b$和$\varphi_b \in [0,2\pi)$，然后制备$|\sqrt{\mu_b/2}e^{i(\pi k_b+\pi\beta_b/2)}\rangle_B$。
- Step 2测量——Alice和Bob通过量子信道将他们的光脉冲A和B发送给一个非可信的Eve, Eve需要执行单光子干涉测量并记录响应的检测器(L或R)。

两种新型量子密钥分发协议

TF-QKD协议和PM-QKD协议

- Step 3声明——Eve宣布他的检测结果。然后Alice和Bob分别宣布随机相位 φ_a 和 φ_b 。其中Alice和Bob不需要公布所选择的随机相位，只公布切片下标即可。
- Step 4筛选——Alice和Bob多次重复以上步骤。当Eve宣布一个成功的检测(有且只有一个检测器L或R响应)，Alice和Bob令 k_a 和 k_b 成为生密钥比特。如果Eve声明是一个R响应，Bob翻转他的密钥比特 k_b。即当且仅当 $|\varphi_a-\varphi_b|=0$ 或 π 时，Alice和Bob的生成密钥都不变；当 $|\varphi_a-\varphi_b|=\pi$ 时，Bob翻转他的密钥比特。
- Step 5-6类似于TF-QKD协议。



04 *Part Four*

量子密钥分发协议安全性比较

量子密钥分发协议的安全性比较分析

MDI-QKD协议、TF-QKD协议、PM-QKD协议

MDI-QKD协议， TF-QKD协议， PM-QKD协议是兼顾实用性与安全性的三种比较前沿的新型量子密钥分发协议，虽然其实现设备较为相似，但具体操作与数据分析却有着很大的区别。三者的比较如图所示。

协议	MDI-QKD协议	TF-QKD协议	PM-QKD协议
密钥率	$O(\eta)$	$O(\sqrt{\eta})$	$O(\sqrt{\eta})$
诱骗态	是	是	是
基转换	是	是	否
相位锁定	否	是	否
干涉测量类型	双光子干涉	单光子干涉	单光子干涉
安全性证明	是	否	是

请您批评指正，谢谢

Professional Commercial Project Plan

封面和内页所有素材均可自由编辑