学习要点：

1. 了解保密通信和量子密钥分发的发展概况
2. 了解量子密钥分发协议，如 BB84 协议
3. 量子密钥分发的实验演示

（一）经典保密通信简介

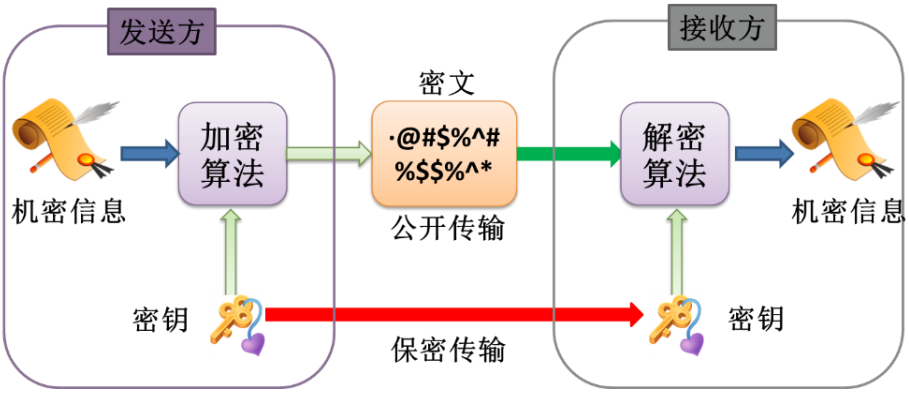

图 1：保密通信流程图

上图给出了保密通信的一般性流程图。保密通信分为加密、传输、解密 3 个过程：发送者将需要发送的机密信息通过某种加密机制（密钥+加密算法）转化为密文；接收方接收到密文后采用和发送方匹配的解密机制（密钥+解密算法）对密文进行解密，从而得到所传递的机密信息。

在保密通信过程中，密钥和加解密算法（一般来说，加密算法和解密算法都是匹配一致的）是保证信息安全的关键。在安全性证明中，一般认为加解密算法是公开的。因此，保密通信中信息的安全完全取决于密钥的安全和加解密算法的复杂性。根据发送方和接收方密钥是否对称一致，现代密码体制可以分为公钥体制（也称为对称密码体制）和私钥体制（也称为对称密码体制）。

（1）公钥密码体制：在该密码体制中，接收方的密钥分为私钥（自己保存的密钥）和公钥（公开发布的密钥）两部分。发送方采用接收方的公钥来加密信息，然后将信息传输给接收方，接收方收到信息后再采用自己的私钥进行解密操作，从而获取信息。根据上面的描述可以看出，要在公钥密码体制中保证信息的安全，就必须保证窃听者无法通过接收方公开的公钥推算出私钥，而这一点可以通过数学上的单向函数来解决。所谓单向函数是指，从条件 A 推算出条件 B 很容易，但要从条件 B 推算出条件 A 的难度会随着 B 的长度呈指数级增加。比如，目前广泛用于网络、金融行业的 RSA 加密算法就是基于数学上大数质因子分解的难题来设计的。

虽然数学上的单向函数能够在一定程度上保证公钥密码体制的安全性，但从理论上讲其安全性对计算机的依赖能力具有明显的依赖。特别是，1994 年 Peter Shor 提出，如果能够构建量子计算机，那么就可以在多项式时间内完成大数质因子的分解，从而使得公钥密码体制的安全性受到严重威胁。

（2）私钥密码体制：在该密码体制中，发送方和接收方事先共享了完全相同的密钥。发送方用这个密钥加密信息，然后将密文传输给接收方，而接收方则采用相同的密钥来解密信息。因此，私钥密码体制的安全性完全取决于密钥的安

全性和加解密算法的复杂性。不过，幸运的是，Shannon 在 1954 年从信息论上证明了一种称为“一次一密（One-time pad，OPT）”的加解密方法，利用该加解密方法后仅需要保证密钥的安全性就可以保证信息的安全性。换言之，在 OPT 加解密算法下，密钥的安全性是决定信息安全的唯一因素。OPT 的具体方法如下：密钥具有完全的随机性；密钥的长度和需要传递的信息长度一致；密钥仅使用一次。可以看出，虽然 OPT 方法可以保证信息的安全，但其对密钥量具有较高的要求，因此无法满足日常实际应用的要求。

（二）量子密钥分发及 BB84 协议

量子密钥分发（Quantum key distribution，QKD）是一种利用量子力学基本原理来进行密钥分发的方法，其主要目的是解决 OPT 加密方法中密钥高速、安全、实时分发这一关键问题。和传统的经典密钥分发协议相比较，QKD 的最大优势在于，利用了量子力学的基本原理后，任何针对密钥的窃听行为都会扰乱传送密钥的量子状态，从而留下痕迹被合法通信双方发现。换言之，QKD 提供了一种信息论安全（information-theoretical security）,或称无条件安全(unconditional security),的密钥分发技术。

早在 1969 年，哥伦比亚大学的 Stephen Wiesner 就基于量子态的特性提出了“不可伪造的电子钞票”的概念【1】，其中就蕴含了 QKD 的基本思想，但由于该思想过于新奇，而且在当时的技术条件下根本无法实现，所以一直没有引起大家的关注，文章也直到 1983 年才得以发表。随后，受 Wiesner 思想的启发，C.H. Bennett 和 G. Brassard 指出可以利用量子态的特性来解决密码学中的密钥安全分发问题，并于 1984 年提出了第一个 QKD 协议，即现在被广泛使用的 BB84 协议【2】。

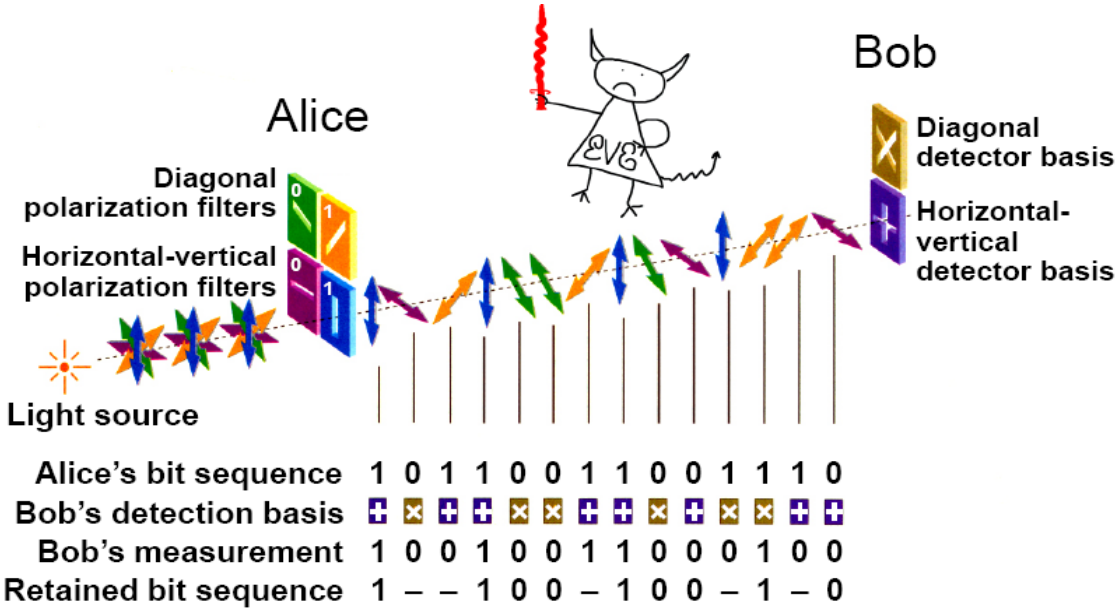

图 2：偏振编码 BB84 协议流程图

BB84 协议采用粒子（包括光子、原子、粒子、电子等均可）作为量子态的编码载体，但对于通信而言，光子在传输速度、抗环境噪声等方面具有天然的优势，因此我们采用光子的偏振为例来简要说明 BB84 协议的工作原理（如图 2 所示）。

Step1：发送方 Alice 和接收方 Bob 约定如下的编码规则

表 1：Alice 和 Bob 编码规则，其中⊕称为水平基，⊗称为对角基。

比特 / 制备-测量基	0	1
⊕	竖直偏振（H）	水平偏振（V）
⊗	右旋偏振（R）	左旋偏振（L）

Step2：Alice 采用偏振控制器随机的将光子的偏振状态制备为 H、V、R、L 之一，并通过窃听者控制的信道传输给 Bob。

Step3：Bob 接收到 Alice 的光子后，随机采用水平基（⊕）或者对角基（⊗）进行测量，并记录测量结果。由于信道损耗的存在，Alice 发送的单光子仅能以一定的概率到达 Bob 的接收装置（单光子探测器），因此 Alice 和 Bob 仅记录保留 Bob 探测到信号时的数据比特信息。

Step4: Alice 和 Bob 从记录的 *N* 个数据比特中随机选取 *m* 个比特并估计数据的比特错误率（quantum bit error rate, QBER）。如果 QBER 大于给定的阈值，则 Alice 和 Bob 放弃此次通信，并重新返回 Step2；如果 QBER 小于给定的阈值，则 Alice 和 Bob 进入 Step5。。

Step5：Alice 和 Bob 对剩余的 *N-m* 个比特数据进行纠错和私密放大处理，进而提取出无条件安全的密钥。纠错的目的是保证 Alice 和 Bob 的密钥的一致性；私密放大的目的是擦除窃听者的信息，保证密钥的私密性。

BB84 协议提出后，众多研究者对其安全性进行了证明，但由于详细的数学证明过程比较复杂，在此不进行详细说明，感兴趣的同学可以参考文献【3-5】。不过，QKD 的安全性基础主要包括以下基本思想：

（1）单光子是光场的最小能量单元，具有不可分割性；

（2）单光子量子态具有不可克隆性，即无法通过一次测量 100%准确的单光子的偏振状态；

（3）单光子偏振状态的测量结果具有概率性，即仅当量子态处于测量算子的本征态时，测量者才能 100%的得到精确的测量结果。

（三）基于 BB84 协议的 QKD 实验

理论分析表明，E91 协议和 BB84 协议具有完全相同的安全性证明基础，换言之，两者在安全性上具有等价性。因此，我们主要利用 BB84 协议来进行 QKD 的演示，其光路图和实验步骤如下所示。

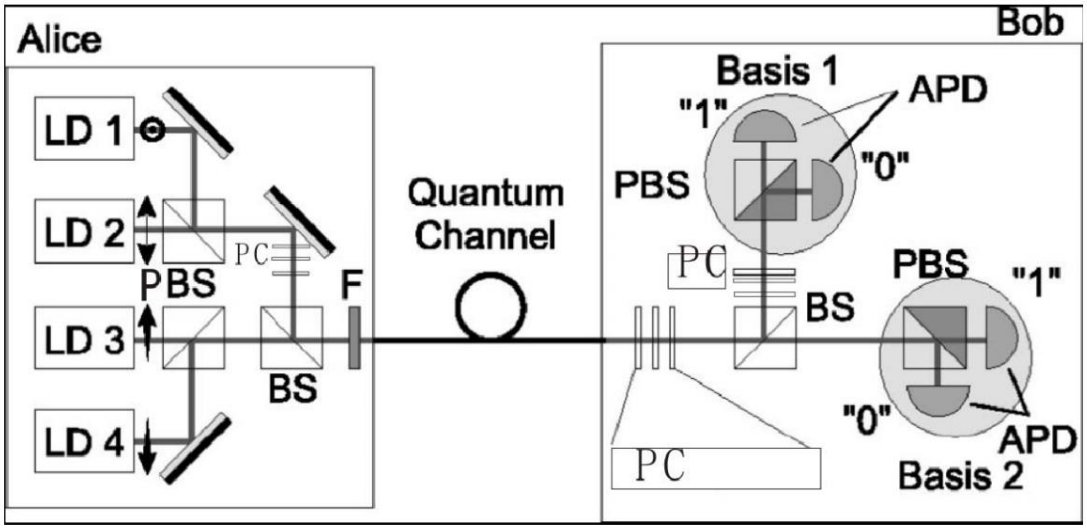

图 3. BB84 协议 QKD 实验光路示意图

实验步骤

发送方：采用 4 个激光二极管，并分别将每个激光二极管的输出光信号的偏振制备为 H、V、R、L。然后通过两个偏振分束器（PBS）和一个分束器（BS）将四个激光二极管的输出光信号耦合到一个统一的输出信道上。发送方采用一个光衰减器将光信号的强度衰减到单光子水平（平均光子数约为 0.1~0.5 左右）。实验中，发送方随机的触发四个激光二极管中的一个发光，从而保证每次随机的发送一个偏振量子态。

接收方：接收方采用一个 BS 来随机选择测量基。经 BS 透射的光信号经过一个 PBS，从而完成对 H/V 偏振的测量。经 BS 反射的光信号，先经过一个偏振控制器（偏振旋转波片），然后再经过一个 PBS，从而完成对 R/L 偏振的测量。

（四） 预习思考题

1、回顾偏振光实验，说明 λ / 2 波片， λ / 4 波片的工作原理；
2、如何检测一个任意方向的线偏振光？
3、是否可以通过将水平偏振的光与竖直偏振的光合束得到一个 45° 线偏光？
4、单光子为什么不能直接用功率计测量？
5、检验单光子探测器的探测效率可以用强光吗？
6、BB84 协议的原理和步骤。
7、密钥分发过程中，为什么需要有同步信号？

（五）提高知识（学有余力的同学参考学习）

1、提高知识一：BB84 的安全性

BB84 协议的严格安全性证明需要用到纠缠和量子熵等概念，因此较为复杂，感兴趣的同学们可以参考文献【3-5】，这里我们仅在最简单的截取-重发攻击下进行简单的说明介绍。

1、截取-重发攻击模型：

Step1：窃听者 Eve 随机的选择水平基（⊕）或者对角基（⊗）测量 Alice 发送的量子态；

Step2：Eve 根据自己的测量结果重新制备一个量子态发送给 Bob，具体对应规则如下

Eve 测量基	Eve 测量结果	Eve 重新发送量子态
水平基（⊕）	H	H
	V	V
对角基（⊗）	R	R
	L	L

2、安全性分析（误码率分析）

下面分析窃听者在截取-重发攻击模型下对系统误码率的影响。为了分析的简单，假设 Alice 和 Bob 的信道是理想信道，即当没有窃听者存在时系统的误码率为 0（所谓误码率是指 Alice 和 Bob 最后共享密钥不一致的概率）。

根据 Alice 所发送四个量子态的等价性，仅分析 Alice 发送水平偏振 H 时的情况，其余三种情况具有完全相同的结果。此时，Alice 和 Bob 测量结果的概率如下表所示：

Alice 发送量子态	Eve		Bob ⊕	
	测量结果	概率	测量结果	概率
H	H	1/2	H	1
	V	0	/	/
	R	1/4	H	1/2
			V	1/2
	L	1/4	H	1/2
			V	1/2

注：根据 BB84 协议的规定，只有 Alice 和 Bob 的基一致时，所对应的 bit 才会保留下来做密钥，因此只考虑 Bob 采用水平基测量的情况。

从上表可以看出，Bob 测得 V 态的概率为

$$P_V = \frac{1}{4}\times\frac{1}{2}+\frac{1}{4}\times\frac{1}{2}=\frac{1}{4}$$

即由于 Eve 的存在，Alice 和 Bob 最终的数据中将存在 25%的误码率。此时，Alice 和 Bob 仅需在最后的数据中拿出小部分来进行误码率计算就可以发现窃听者的存在。

在前面的讨论中，假设 Alice 和 Bob 的信道是理想的，但实际的信道总是存在一定噪声，因此，在实际系统中，即使没有窃听者存在，Alice 和 Bob 的数据也存在一定的误码率，那这是否会影响 QKD 的应用呢？答案是否定的，因为我们可以在噪声信道模型下进行安全性分析。事实上，信道噪声只会降低密钥产生量，而不会影响其安全性。理论分析表明，只要系统的误码率小于 11%，Alice 和 Bob 就可以通过纠错和私密放大步骤提取出无条件安全的密钥。

2、提高知识二：基于纠缠的 E91 量子密钥分发协议【6】

（1）Pauli 矩阵

分别定义三个方向的 Pauli 矩阵具有如下形式

$$\hat{\sigma}_x=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\hat{\sigma}_y=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\hat{\sigma}_z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

通过简单计算可以发现，这三个矩阵的本征值都是 1 或者-1。如果记

$$|\uparrow\rangle=\begin{pmatrix}1\\ 0\end{pmatrix},\quad |\downarrow\rangle=\begin{pmatrix}0\\ 1\end{pmatrix}$$

分别是 $\hat{\sigma}_z$ 矩阵本征值为 1 和-1 的本征态。那么，

（a）$\hat{\sigma}_x$ 的本征态可以写为

$$|x_1\rangle=\frac{1}{\sqrt{2}}\left(|\uparrow\rangle+|\downarrow\rangle\right)=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix}$$

$$|x_{-1}\rangle=\frac{1}{\sqrt{2}}\left(|\uparrow\rangle-|\downarrow\rangle\right)=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix}$$

（a）$\hat{\sigma}_y$ 的本征态可以写为

$$|y_1\rangle=\frac{1}{\sqrt{2}}\left(|\uparrow\rangle+i|\downarrow\rangle\right)=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix}$$

$$|y_{-1}\rangle=\frac{1}{\sqrt{2}}\left(|\uparrow\rangle-i|\downarrow\rangle\right)=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -i\end{pmatrix}$$

（2）纠缠（Entanglement）

纠缠是量子力学所允许的一种特殊的量子态，其具备一些在经典力学看来完全违背常识的特性。假设两个自旋为 1/2 的电子处于如下状态：

$$|\psi\rangle=\frac{1}{\sqrt{2}}\left(|\uparrow\rangle|\downarrow\rangle-|\downarrow\rangle|\uparrow\rangle\right)\qquad(1)$$

其中 $|\uparrow\rangle$（$|\downarrow\rangle$）分别表示 Pauli 矩阵 $\hat{\sigma}_z$ 自旋向上（向下）的本征态。可以看出，方程（1）所表述的量子态具有如下性质：

- 沿着 Z 方向单独测量每个电子的自旋，测量结果都是概率性的，电子的自旋将以 1/2 的概率塌缩到状态 $|\uparrow\rangle$，以 1/2 的概率塌缩到状态 $|\downarrow\rangle$。
- 无论两个电子在空间上间距多远，沿 Z 方向测量其中一个电子的自旋状态后，另一个电子的自旋状态也瞬时完全确定，而且两个电子的测量结果存在确定性的关联（对于方程 1 所表述的量子态而言，两个电子的自旋存在确定性的反关联）。
- 沿任意 $\vec{n}$ 方向测量两个电子的自旋时，测量结果都存在确定性的反关联，

即 $\langle\psi|\sigma_{\vec{n}}^{1}\sigma_{\vec{n}}^{2}|\psi\rangle=-1$。

（3）E91 协议

Step1：Alice 和 Bob 共享处于方程（1）所表述的纠缠态。

Step2：Alice 和 Bob 分别独立、随机的沿 Z 方向 $\hat{\sigma}_z$ 或 X 方向 $\hat{\sigma}_x$ 测量电子的自旋，并记录测量结果（Alice 和 Bob 约定自旋向上表述比特 0，自旋向下表述 bit 1）。

Step3：Alice 和 Bob 随机选取部分测量结果，并估计系统误码率。如果误码率高于给定阈值，则返回 Step1 重新开始；如果误码率低于给定的阈值，则进入下一步。

Step4：Alice 和 Bob 对剩余比特数据进行纠错和私密放大处理，以保证他们共享的密钥具有一致性和私密性。

参考文献

【1】S. Wiesner. Conjugate Coding[J]. Sigact News, 15, 78 (1983)

【2】C.H. Bennett，and G. Brassard．Proceedings of IEEE International Conference on Computers，Systems and Processing，Bangalore，1984(New York：IEEE).

【3】V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev. The security of practical quantum key distribution. Rev. of Mod. Phys. 81, 1301-1350 (2009).

【4】X.F. Ma. Quantum cryptography: From theory to practice. PhD. Thesis, (2008). (see also arXiv:0808.1385v1)

【5】F.H. Xu, X.F. Ma, Q. Zhang, H.K. Lo, and J.W. Pan. Quantum crytography with realistic devices. (See arXiv:1903.09051)

【6】A.K. Ekert. Phys. Rev. Lett. 67(6), 661-663 (1991).