量子密钥分发(QuantumKeyDistribution，QKD)是一种密钥的安全传输方式，可以在相距很远的两个通信终端之间发送。在安全通信过程中，需要用密钥对信息进行加密和解密。密钥的安全性保证了信息的安全性。

与传统方式不同，量子密钥分发在理论上是无条件安全的，其安全性由量子力学的基本原理来保证。量子不可克隆定理表明，不可能完美地克隆任何量子态。因此任何对量子密钥分发过程的窃听，都可能改变量子态本身，导致误码率很高，这样窃听就能被发现。一般来说，QKD过程中量子态的传输是通过对光子进行编码、传输和测量来实现的。

量子密钥分发最重要和最独特的特性之一是，如果第三方试图窃听密码，双方都会知道。这个性质是基于量子力学的基本原理：量子系统的任何测量都会对系统产生干扰。第三方试图窃听密码。必须通过某种方式来测量，而这些测量会带来可检测的异常。通过量子叠加态或量子纠缠态传输信息，通信系统可以检测是否存在窃听。当窃听低于某一标准时，可以生成安全密钥。

量子密钥分发的安全性是基于量子力学的基本原理，而传统密码学是基于一些数学算法的计算复杂度。传统密码术可以&#039；t检测窃听，所以它可以&#039；我不能保证密钥的安全性。

量子密钥分发仅用于生成和分发密钥。，而且没&#039；传递不了任何真实的信息。在一些加密算法中可以使用密钥来加密消息，加密的消息可以在标准通道中传输。与量子密钥分发相关的最常见的算法是一次性码本。如果使用秘密的随机密钥，该算法具有可证明的安全性。。在实际应用中，量子密钥分发经常与对称密钥加密方法一起使用，如高级加密标准。还有量子密钥分发的情况，使得在完美单光子源和探测器假设下的比较不容易实现。

QKD技术自1984年提出以来，已经研究了30多年，取得了丰富的成果。从在初始离散变量中编码光子偏振或相位的BB84协议到基于纠缠光源的E91协议。相位分布式参考协议中的DPS协议和COW协议，以及连续变量QKD协议和测量设备无关(MDI-QKD)协议，在理论和实验上都取得了不断的进展。同时QKD商用系统的生产，QKD网络的建设，世界范围内QKD应用的研究也标志着QKD技术的实际进步。

团队霜已经建立了一套&quot即插即用QKD系统。。该系统是第一个考虑光源不完美性，并实现实时后处理的系统。同时，我们还对QKD进行了理论研究，探讨了离散变量协议中不可置信光源的波动性，分析了连续变量协议的安全性。现在我们的研究包括离散变量协议和连续变量协议的理论和实验研究，以及测量设备无关协议的相关研究。