所谓量子，是构成物质的最基本单元，是能量，动量等物理量最小单位，不可分割。像电子、光子等构成物质的基本粒子，统称为量子。除了不可分割性，量子还具有不可克隆 （复制）性。因为克隆一个东西首先要测量这个东西的状态，但是量子通常处于极其脆弱的“ 叠加态 ”，一旦被测量就会马上改变状态，不再是原来那个量子了。 所以量子加密就是利用量子的不可克隆性以办证通信安全性的根本来源。 因为窃听信息等于先复制了这个信息， 所以量子的不可克隆性保证了量子信息本身 （或者由它生成的量子密码） 不会被复制， 因此断绝了一切窃听的可能性。

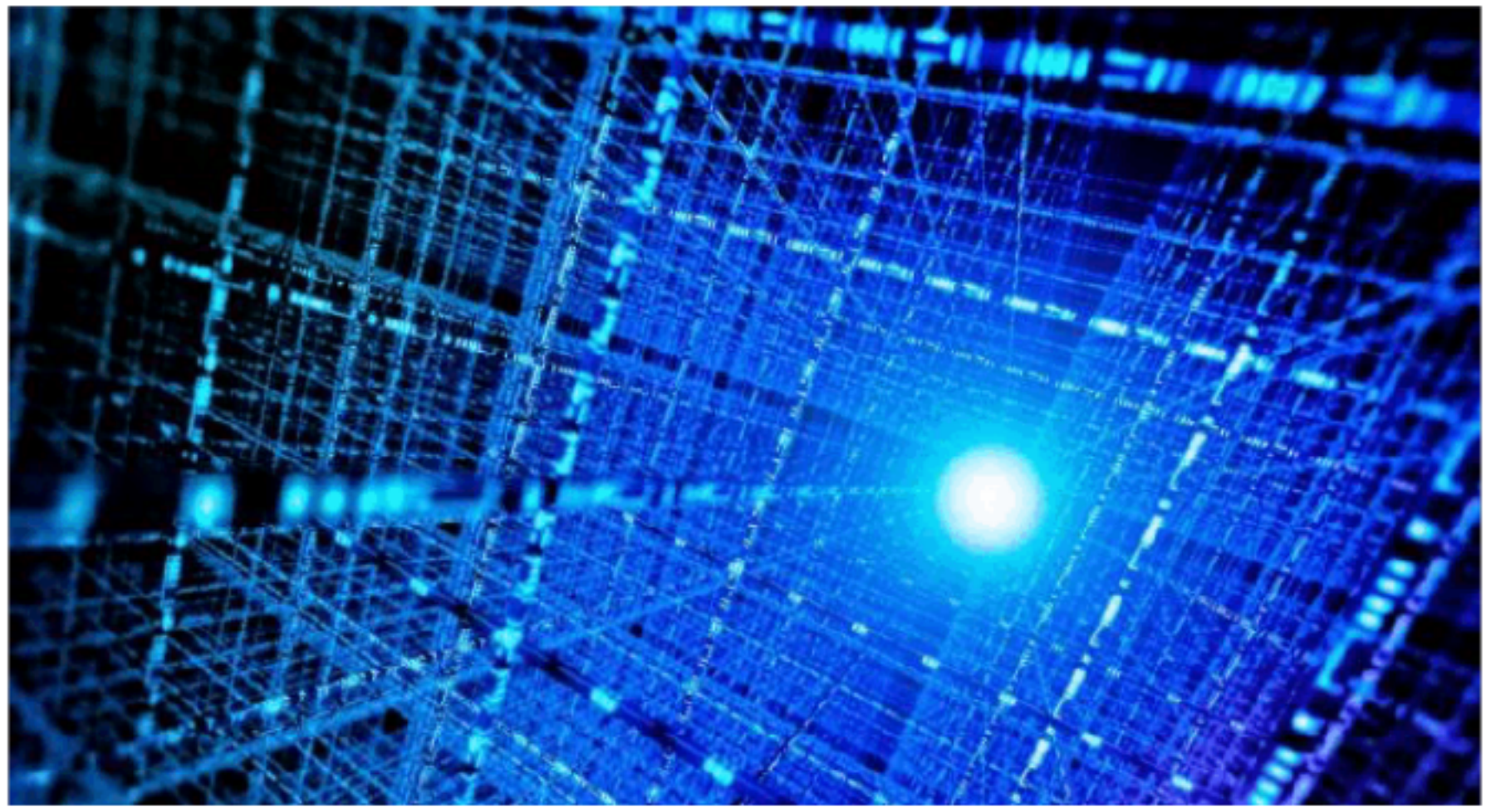
量子加密技术在密码学上的应用分类：

1、利用量子计算机对传统密码体制的分析；

2、利用单光子的测不准原理在光纤一级实现密钥管理和信息加密，即量子密码学。

根据 internetde 发展，全光网络将是今后网络连接的发展方向，利用量子技术可以实现传统的密码体制， 在光纤一级完成密钥交换和信息加密， 其安全性是建立在 Heisenberg 的测不准原理上的， 如果攻击者企图接收并检测信息发送

方的信息， 则将造成量子状态的改变， 这种改变对攻击者而言是不可恢复的， 而对收发方则可能很容易地检测出信息是否受到攻击。



量子加密的优势

量子加密比普通的电子邮件或无线电优越， 因为这种方式从理论上不可被破坏或拦截。 假如激光束里的量子被第三方观察到， 粒子自身就会改变， 这就是物理学上所谓的“ 海森堡测不准定理 ”，这种状态依赖粒子的改变来衡量。如果遇到拦截，发送者和接受者都能立刻觉察到有人在窥探。

简单来讲就是量子加密采用的原理是根据 “ 海森堡测不准定理 ” 和“ 单量子不可复制定理 ”原理建立了量子密码术的概念。 “ 海森堡测不准定理 ”是量子力学的基本原理， 指在同一时刻以相同精度测定量子的位置与动量是不可能的， 只能精确测定两者之一。 “ 单量子不可复制定理 ” 是“ 海森堡测不准定理 ” 的推论，它指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只能先做测量，而测量必然改变量子的状态，所以说量子加密是安全的。