# 何謂量子通信

六區活動總幹事 廖建利

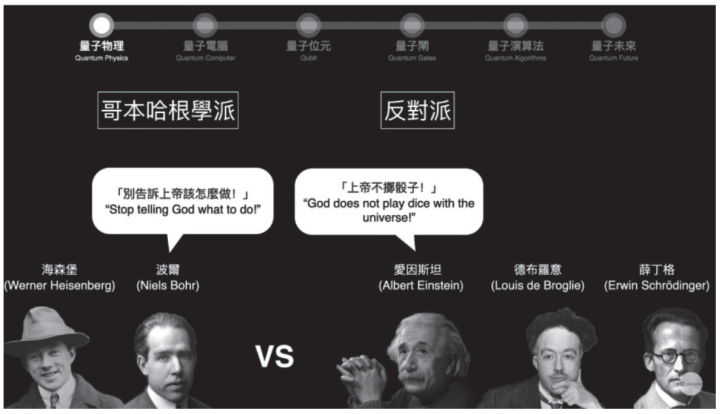
近年，量子理論與技術的蓬勃發展，藉由量子的神秘力量，人類將有機會在不同領域當中，實現無法想像的應用。因此，建構完善的量子產業鏈，已成為國家與企業之間爭相發展的重點項目之一，也成為下一個世代必學的重點課題，以下將用短短的敘述來解釋外星科技。

1900年42歲的普朗克在德國物理學會發表了標準光譜之能量分佈定律，指出黑體幅射的電磁波能量有一個最小基本單位E=Hf

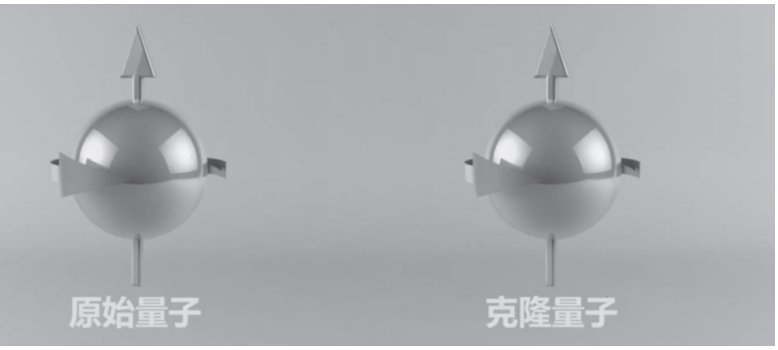
E=Hf ◀ 普朗克常數

其中E是能量，f是頻率，H是身為三大基本物理學常數之一的普朗克常數而這個能量的最小單位就被稱為量子（quantum），量子物理就從這裡，開始被發展起來。

然而量子微觀世界的概率與不確定性，仍飽受質疑，以致於物理學界分裂為二大陣營，一方是以波爾為首的哥本哈根學派，另一方則是由愛因斯坦為首的反對派，雙方激戰，難分難解，其二大派別分別在微觀粒子的疊加態與量子糾纏的特性，關於疊加態（Superposition）會以某種機率分佈在同一時間處於多重狀況，直到被測量的時間點，造成波涵數塌縮，而退相干為本徵態，回到古典物理的遊戲規則，而量子糾纏則是粒子與粒子之間跨越時空的連結。

然而一般人受電影影響，總認為量子能進行超光速通信，這在目前依然只是一種幻想，因為沒有科學家知道該怎麼實現，那麼，量子通信技術到底是什麼高科技呢？他又高在那裡呢？其實量子通信技術要解決的其實是通信安全問題，人們為了通信安全，想出了各種各樣的加密方法，可惜的是，道高一尺，魔高一丈，再厲害的加密算法，都能以現代的破譯技術進行破解，舉例說量子電腦就具有超級強大的破解能力，因為再厲害的加密方式都無法抵擋量子電腦的強大破解運算能力，所以為了從源頭解決問題，也就是徹底杜絕竊取或破解，正所謂解鈴還須繫鈴人，答案就是量子通信，其量子不被竊取或破解的原理，真正在於實現違反現有的通信設備傳輸技術，傳統的通信技術，之所以會被竊聽，關鍵在於通信過程中，信息被複製了無數份。

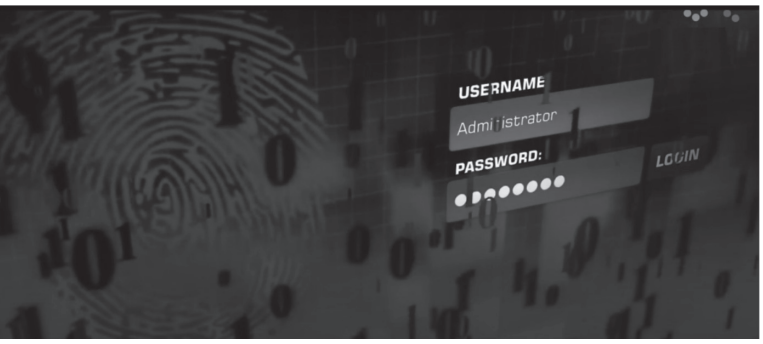



傳統通信過程，就是叫來一億個快遞員，都各別從信息端取A單元信號，送出去，然後又叫來一億個快遞員，再個別從信息端取B單元信號，送出去，就這麼每一個單元信號都叫一億個快遞員，那麼竊聽者在半路上攔截了幾個快遞員，搶走了物品，在這個過程中，傳送方和接收方都是渾然不知的，因為同樣的快遞員實在是太多了。

目前科學界就想出了一個應對策略，那就是不要叫來那麼多的快遞員，每一個單元信號就叫一個快遞員，每個快遞員從傳送方就只拿一個獨一份的單元信號，這樣一來如果有一個快遞員中途被攔截了，那麼接收方馬上就會發現單元信號是不完整的，這就等於發現了竊取者，這就是量子通信的核心原理。

目前全球公認將這技術做的最好的，就是中國，2016年08月16日成功發射墨子號量子實驗衛星，全世界第一個在500公里高的太空軌道，把一顆一顆的光子準確的打到地面的接收器，這就如同將一枚硬幣，扔進50公里外的一個礦泉水瓶中，但實際遠遠比這還難，因為衛星在繞著地球轉，也就是搭著一輛高速行駛的高鐵朝著50公里外的一個礦泉水瓶扔硬幣，相比的科技大國日本，目前為止只能實現一次扔一億個硬幣，然而這些尚只是原理，還不是量子通信的全部，因為，要真正實踐不被竊聽，還有一個至關重要的問題，在單光子通信方案中，有一個可能的漏洞，假如有一個竊取者在中途攔截了快遞員，打開快遞，把裡面的信息複製一份出來，讓這快遞員繼續送貨，這樣不就能偷偷竊取信息了嗎？信息的發送和接收方並不知道有人已經複製了信息，但萬幸的是量子科技家發現了量子世界的又一個神奇規律，這個規律叫做量子不可克隆原理，什麼是克隆呢？就是在不破壞原物的情況下，做一個和原物一模一樣的複製品，這必須要保證原物和複製品都完好無損，這時您就無法區別誰是原物，誰是複製品了，這其中又關乎到量子的自旋態，因為一個量子的自旋態在沒被測量前，是處在不確定中的，只有被測量後才能被確定下來，正是這個原因，使得一個

量子的自旋態永遠也不可能，被另一個量子克隆，一個量子的量子態只能被傳遞出去，而不能被克隆，你可以複雜出一個一模一樣的量子，但是…對不起，一旦您複製成功了，原始量子也必然被破壞了，這就是量子力學中的量子不可克隆原理。




再來，我們回到快遞員比喻，在量子世界中，雖然你可以把快遞員攔截下來，但是你只要一打開快遞盒，讀取裡面的訊息，那…對不起，這個快遞盒就被徹底破壞了，你不可能在發送一模一樣的快遞給接收方，而您也不可能克隆出一個快遞，一個自己留下一個發送出去，正是因為有量子不可克隆原理的存在，才使得單光子通信成為了絕對安全，也就成為不可能被竊聽的量子通信，他在未來的軍事、國防、和國家安全、或企業機密領域達到安全的目的。