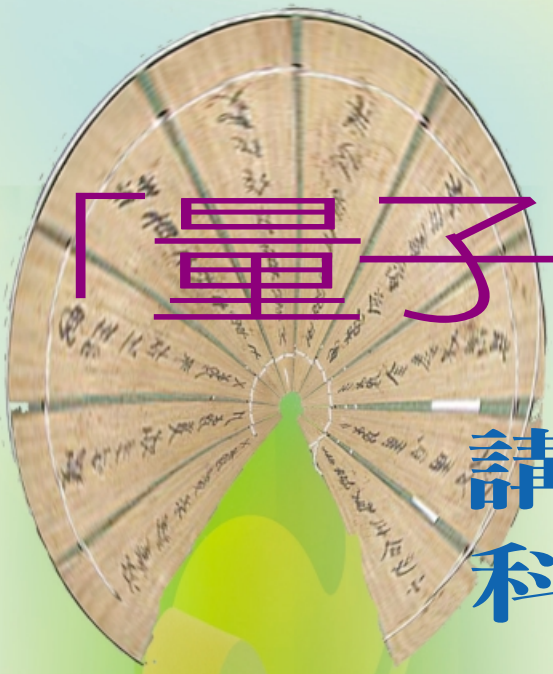
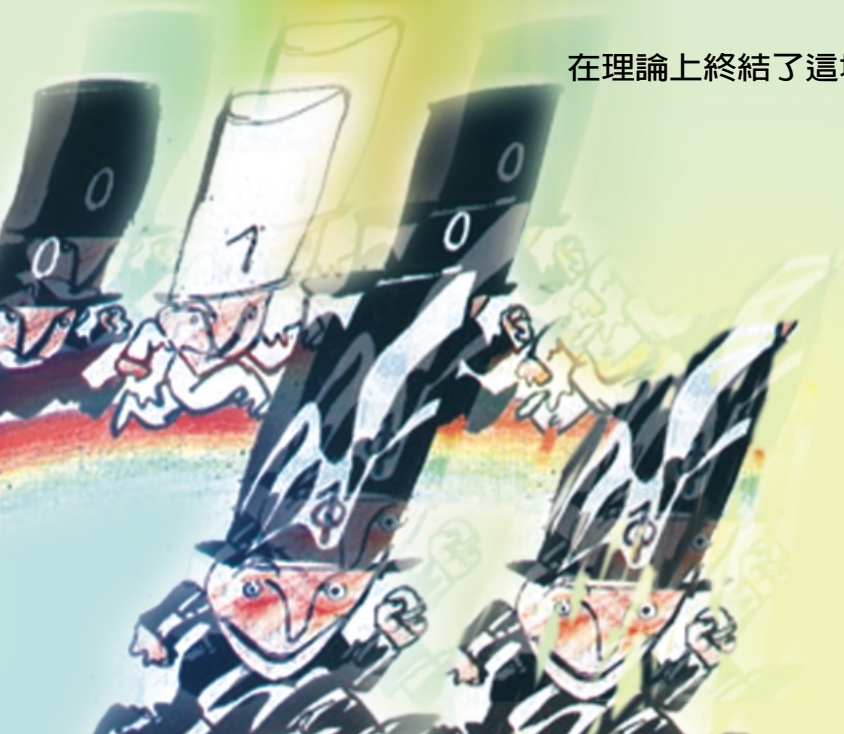
一般報導

從「女書」到「量子密碼」

講悄悄話的科學與藝術



保密與竊聽是人類文明的特性，
所謂「知己知彼，百戰百勝」，
保密者與竊聽者之間的戰爭，
從古到今，綿延不絕。
量子密碼法的出現，
在理論上終結了這場長達幾千年的爭鬥。



張志義

楔子

話說湖南省江永地區存在一種奇特的文字，稱爲「女書」。顧名思義，就是女人專用的文字，男人是看不懂的。女書傳女不傳男，有長遠的歷史。有人說因爲封建社會重男輕女，絕大部分女性沒有受教育的機會，不懂漢字，所以創造了「女書」作爲書寫工具。

我卻有點懷疑這種說法不夠全面。因爲女書是表音文字，一字一音（用當地土話發音），共有一千個字左右，所以要學會女書估計並不特別容易。那麼當地的女性之間爲什麼會有女書流傳下來呢？我猜部分是因爲從前社會保守，對女性的約束特嚴，有些女人的心事、八卦和悄悄話，是不足爲男人道，也不想讓男人知道的，所以女人才會用女書來記事和通信。如果這個猜想成立的話，那麼女書也可以說有「女人密碼」的功能。

傳統密碼

不論古今中外，個人或集體，男人或女人，祕密通訊的要求，是人類文明的普遍現象。上至有關軍國大事的公文，下至私人之間的書信，其中都可能有不想爲外人知道的內容。也正因如此，才會有人不擇手段，去偷看或竊聽別人不願曝光的祕密。打從遠古的年代開始，人類便設計出各種隱藏通訊內容的辦法。隨著人類文明的發展，通訊技術不斷提升，保密的要求也越來越普遍。尤其是在資訊主宰的二十一世紀，電子郵件與網路交易日益頻繁，通訊的隱密性已成爲與日常生活息息相關的議題。

「密碼學」是隱藏通訊內容的科學與藝術。最古老的祕密通訊方式是把訊息藏起來，以躲過敵人的偵察。喜歡武俠小說的讀者也許會記得，在《射鵰英雄傳》裡，《武穆遺書》的藏書地點便是寫在一幅山水畫的襯底夾層紙上的。可是藏匿法有一個大弱點，也就是一旦被發現的話，其內容也就馬上曝光了。

故此後來又陸續發展出各式各樣的辦法，其中「替代法」是相當有代表性的一種。替代法就是用一個字替代另一個字，使原文變得亂七八糟，只有擁有替代對照表的人才能解讀。近代的做法是把原文寫成一串數字，便於發送。以下是一個用數字替代羅馬字母的例子：

A－6　B－38　C－32　D－4　E－8　F－30　G－36
H－34　I－39　J－31　K－78　L－72　M－70　N－76
O－9　P－79　Q－71　R－58　S－2　T－0　U－52
V－50　W－56　X－54　Y－1　Z－59

按照這個替代表，「The enemy is coming （敵人來啦）」就變成了一串藏有訊息的密碼數字：034887687013923297039763 6。就算敵方攔截到這串數字，也會不知所云。可是這個方法也不是很安全，假如敵方知道原文使用的語言，便可以根據該語言的特性及上下文理，不難推斷出替代的方式。

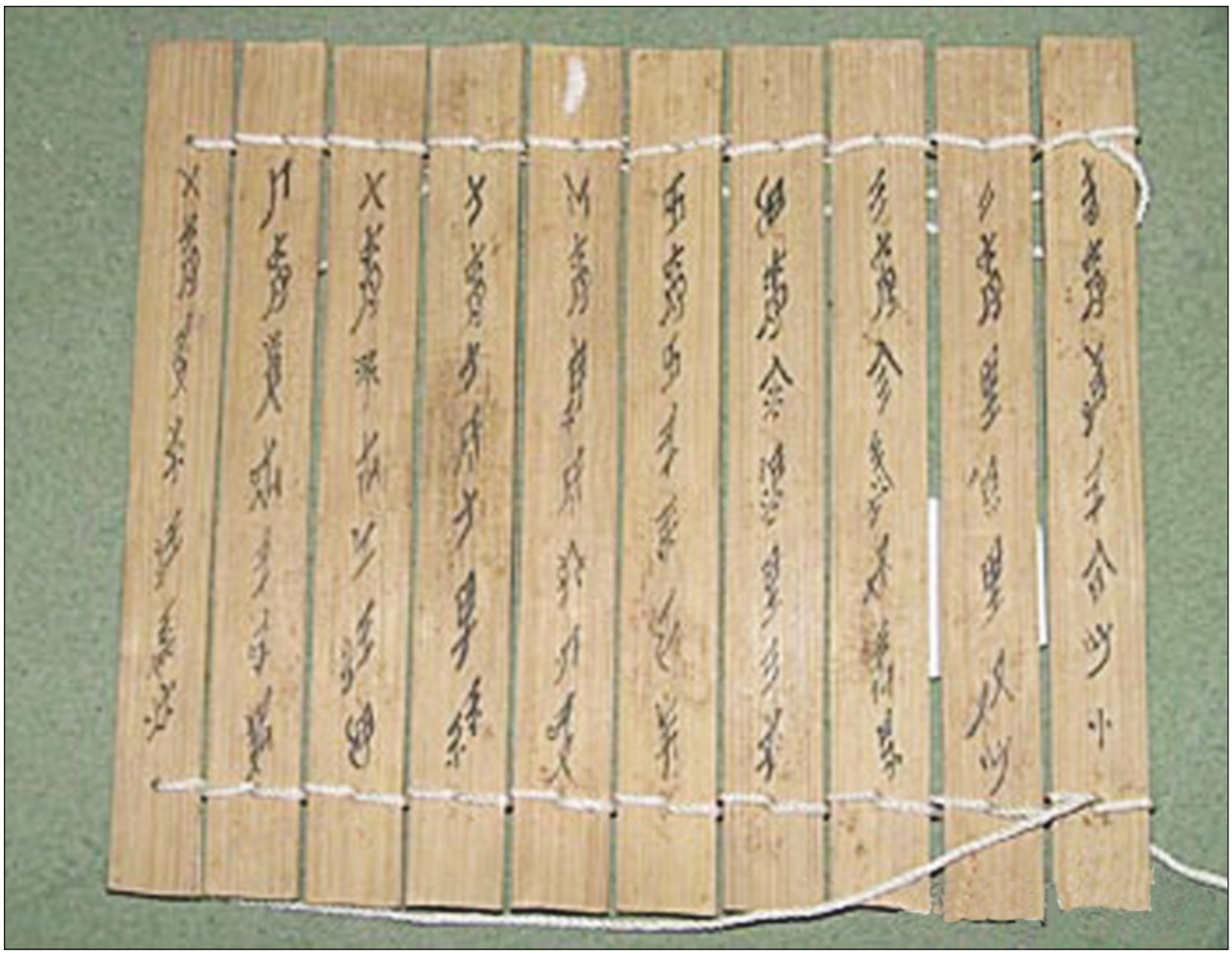
有趣的是，在第二次世界大戰期間，美國軍方曾用「那華荷」印地安語傳發密碼，這是少數未被破解的密碼之一，原因很簡單，因爲日本和德國軍中沒有人懂這種語言。但這個辦法畢竟不是很方便，因爲美國軍隊中懂得這種印地安語的人員也很少，所以無法廣泛採用。

早在一九一八年，一位美國工程師范南 （G. Vernam） 發明了一種二次加密的方法，明顯提高了通訊的隱密性。這個密碼法需要一串無序的數字，稱爲「鑰匙」，如果把鑰匙加在替代法的密碼上（不進位），那麼結果將是一串敵人無法解讀的亂碼。收信人用密碼減去鑰匙，便可輕易把原文譯出。請看下面的例子：

原文： The enemy is coming（敵人來啦）
訊息： 034887687013923297039763 6（替代法密碼）
鑰匙： 491506382791504782930746 2
密碼： 425383969704427979969409 8（訊息加鑰匙）
解碼： 034887687013923297039763 6（密碼減鑰匙）

可以證明，假如祕密鑰匙和訊息一樣長，而且每條鑰匙只使用一次的話，那麼這個密碼是無法破解的。經歷了漫長歲月的演變，密碼技術至此可說已接近頂峰了。很顯然，這個密碼法的安全性，完全等同於鑰匙的安全性，所以在傳送鑰匙的過程中，要確保沒有人能偷看，這就是所謂的「鑰匙傳送問題」，是現代密碼學的核心。

免洗餐具用一次便丟掉，確實很方便；但在現代頻繁的通訊中，要每次更換一把新的鑰匙實在太麻煩了，幾乎不可能。在平常商業與私人的信件中，很多訊息是



http://www.people.com.cn/media/200208/22/NewsMedia_203105.jpg

女書的竹簡

有時效性的，往往並不需要永久保密，所以一般是每隔一段時間才換一把鑰匙。現今世界上最先進及最方便的加密方法是「RSA密碼法」，這是一九七七年由美國麻省理工學院的三個學者李瓦士、夏米爾及艾道曼（Rivest, Shamir, and Adleman）所發明的。

這個方法最大的優點是省略了鑰匙傳送的手續，因爲用來加密的鑰匙是公開的，沒有祕密可言。但是解碼的鑰匙卻是保密的，放在收信人的保險箱裡。這是一種非常特殊的非對稱密碼法，因爲加密與解密的鑰匙並不相同。

舉個例子，假如一位愛麗絲（Alice）小姐與外界有祕密通訊的需要，那麼她先選定兩個非常巨大的質數（P, Q）作爲她的私人鑰匙（解密用的），然後P和 Q的乘積 $N = P \times Q$ 便是加密用的公開鑰匙，她可以把公開鑰匙印在名片上或在網路上公布。現在有一位包普（Bob）先生想寫一封密函給愛麗絲，他首先得知道愛麗絲的公開鑰匙，按照一個特定的方法把信件加密後送出。在收到密碼後，愛莉絲再用她的私人鑰匙（P, Q）解出原文。

讀者也許會問，既然 N是公開的，那任何人只要把N分解成 P 和 Q，不就可以得到愛麗絲的私人鑰匙了嗎？這的確問到了重點。經驗告訴我們，給定兩個質數（P, Q），要求其乘積N是很容易的事，小學生也會做。但是已知乘積N，倒過來求其因子（P, Q），卻並無簡易快速的辦法；基本上只能一個一個因子去檢查，但這是很費工夫的事。尤其當N是一個幾百位數的天文數字時，儘管用最快速的電腦來算，也要耗上天文數字的時間。因此，一般認爲RSA密碼法雖然不能號稱絕對安全，但實際上已經足夠安全了。可是，眞的嗎？

在一九九四年，美國IBM研究實驗室的科學家蕭彼得（P. Shor）發現，對於量子電腦來說，因子分解是一件

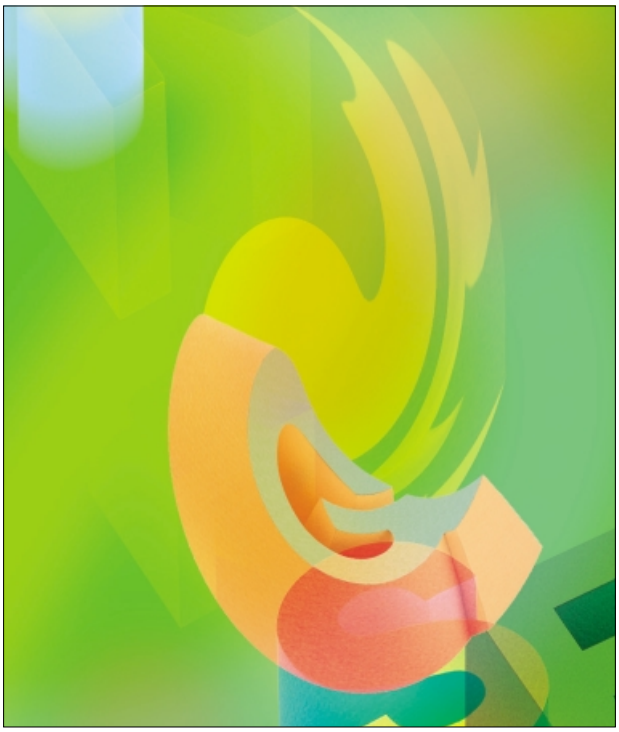
容易不過的事情。所以，如果今天我們懂得如何建造大型量子電腦的話，那麼RSA密碼法便一文不值了。

給大家一個概念：二〇〇一年十二月，IBM宣布他們成功建造了一部能分解15=3x5的量子電腦！所以估計一部能夠破解RSA密碼的量子電腦，也許幾十年後才會出現。在此之前，大家暫且可以安枕無憂。但是，一些天生敏感的人還是會放不下心，總覺得有人可能已發明了什麼祕而不宣的好方法，每天都在竊聽我們的祕密，只有絕對安全的密碼法才能讓他們睡得安穩。那麼絕對安全的密碼法是可能的嗎？答案是肯定的，量子密碼！

量子密碼

二十世紀的物理學是建立在兩條支柱上的，其一是相對論，其二是量子力學。前者是描述高速度運動的現象，而後者則是描述微觀粒子運動的規律。經過近一個世紀的考驗，這兩條支柱仍然屹立如山。也就是靠著這兩條支柱，物理學在上一個世紀才會有突飛猛進的發展。

說來有點奇怪，雖然量子力學的理論在上世紀初便建立完備了，但直到六〇年代末才有人想到把它用在密碼學上。如是又經過了十多年的探索，到了一九八四年，美國的賓納（C. Bennett）與加拿大的巴沙（G. Brassard）二人，終於發明了一種利用量子特性的密碼法，是絕對安全的。這個稱爲BB84的方法有技術上的困難需要克服；所以還不能交給愛麗絲與包普使用；但比起建造量子電腦來說卻又容易許多了。所以也許不用等幾十年，量子密碼法將在某些領域全面取代傳統的RSA密碼法。



李男提供

要解釋量子密碼法的原理，讓我們先介紹量子世界的一些奇特現象。在微觀量子的世界裡，有很多觀察量是不連續的。就以大家都熟識的光來說吧，它有波動的特性，但也有量子的特性；光的最小不可分割的單位叫做光子。光子會自旋（自我轉動），也稱爲偏振。

它的偏振方向不是連續的，假如我們用垂直偏振儀（寫作 ＋）去測量任何一粒光子，那麼結果不是橫向偏振的（寫作 －），便是縱向偏振的（寫作｜），絕對不會得到有點橫向又有點縱向的結果。同樣，假如我們用交叉偏振儀（寫作 × ）去測量光子，那麼結果不是左斜偏振的（寫作＼），便是右斜偏振的（寫作／），也不會得到有點左或有點右的結果。

在平常生活裡，「橫看成嶺側成峰」是一種心理現象。但在微觀世界裡，從不同的角度去「看」量子，確實會得到不同的結果。例如，用＋偏振儀去測量一粒 －（或｜）偏振的光子，則儀器肯定會告訴你這是一粒 －（或｜）偏振的光子。但同樣一粒光子，假如用 × 偏振儀去測量的話，則結果是不可預料的，可能是＼偏振，也可能是／偏振，各有一半機會。

反過來也一樣，用 ＋ 偏振儀去測量左右斜偏振的光子，則結果也是不可預料的；可能是－偏振，也可能是｜偏振，機率也是一半一半。這眞是一件不可思議的事情，因爲日常經驗告訴我們，無論左看右看上看下看，「對面的女孩」是不會變成男孩的！

大家都知道電腦是用二進法的。二進法裡只有兩種個位數（0，1），所以電腦需要一個能表示 0 和 1 的基本零件，叫做「位元」（bit）。很顯然，因爲光子有兩個可分辨的偏振態，我們可以用光子來做位元。例如，我們可以用橫向偏振的光子（－）代表 0，縱向偏振的光子（｜）代表 1，來建造一部電腦；這在理論上是完全不成問題的。但請注意，光子可不是普通的位元，而是奇特的「量子位元」（qubit, 讀作q-bit）！與一般電腦裡的位元

相比，「量子位元」有兩個奇異的特性：

(1) 除了0與1之外，它也可以處在既非0也非1的狀態！叫做0與1的疊加。如果我們去測量一粒奇怪的非0非1光子，則有可能得到0，也有可能得到1，不一定。左右斜偏振的光子便是處在這種非0非1的狀態。

(2) 測量會改變量子的狀態。假設我們用 ＋ 偏振儀去測量一個斜偏振的光子，如果答案是橫向（－）的，那麼被測量後的光子便變成橫向偏振態，而不會停留在原來的斜偏振態。也就是說，量子是一種非常脆弱的東西，一碰就會「破」或「變」！所以隨便給你一個光子，你是無法準確決定它的偏振狀態的。你當然可以測量它，但只能做一次，問題是一次測量並不能告訴你關於這粒光子全部資料。這就是有名的「測不準原理」。

在量子的世界裡，不論原子、電子、光子或其他粒子，其觀察量也許不盡相同，但這兩個特性是普遍存在的。粗略地說，量子電腦主要是利用量子態的非 0 非 1 的疊加特性，而量子密碼的重點則是量子的「測不準」特性。現在讓我們看看「測不準原理」如何確保通訊的絕對隱密。

上面說過，假如愛麗絲與包普各有一把相同的祕密鑰匙，而且這把鑰匙只用一次，那麼他們之間的通訊便不怕別人竊聽了。所以問題的核心是如何在兩人之間建立安全的鑰匙。簡單地說，量子密碼法的程序是這樣的：愛麗絲送一長串偏振化的光子給包普，其中有些光子代表 0，有些代表 1，但次序是混亂的（連包普都不知道）。收到光子後，包普隨便用 ＋ 或 × 偏振儀測量每一粒光子的偏振，把結果記下來。然後兩人通個電話，交換部分資料，確定沒有人在搞鬼，最後建立鑰匙。

對於一個這麼簡單的設計，爲什麼竊聽者會束手無策呢？原因就在量子奇妙的測不準特性。假設有一個竊聽者，有辦法暗中攔截愛麗絲的光子，做一些測量後再送給包普，那麼她是否可以得知愛麗絲傳的是什麼光子呢？答案是否定的。「測不準原理」告訴我們，因爲愛麗絲送出來的光子串是無序的，所以竊聽者無法測定任一粒光子的偏振，因此也無從得知它代表的是 0 或 1。再者，測量一般會改變光子的偏振狀態，「凡測過的，必留下痕跡」！所以竊聽者不法的行爲，在愛麗絲與包普通電話時將無所遁形。

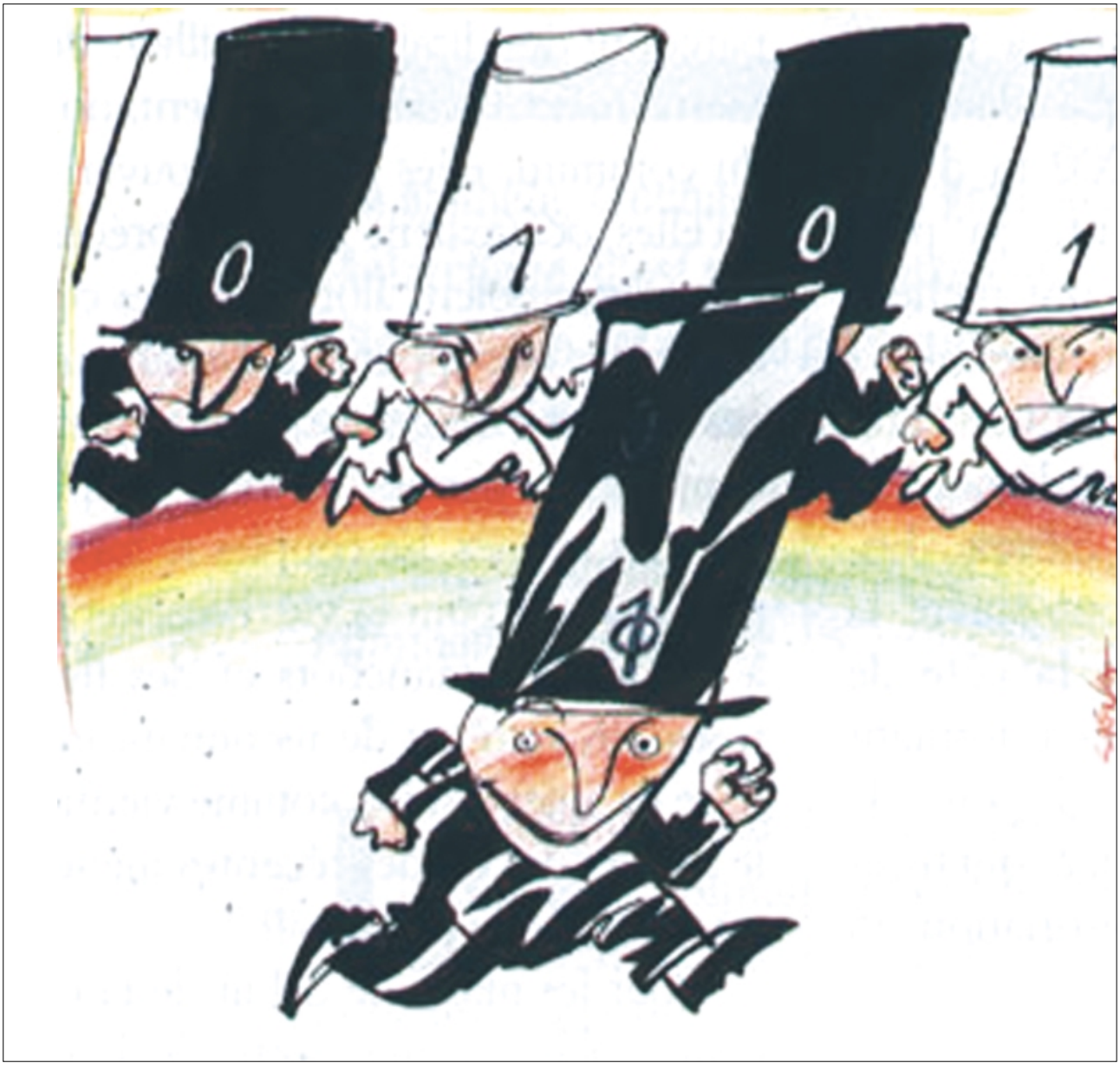
以下是BB84量子密碼法較詳細的操作步驟，有點兒複雜，但也不會很複雜。有信心的讀者，我鼓勵你繼續看下去。加油！

一、 首先，愛麗絲和包普約定，以－偏振和＼偏振的光子代表 0，｜偏振和／偏振的光子代表 1。愛麗絲送出的光子串裡四種光子都有，每種出現的機會是四分之一，其次序是完全混亂的。每送出一粒 － 或＼的光子，她記下 0，｜或／的則記下 1，這是愛麗絲的原始數據。

二、 收到光子後，包普隨意選用 ＋ 或 × 偏振儀，逐粒測量光子的偏振。結果是 － 或＼的，他記下 0，｜或／的則記下 1。測完之後，包普得到一串長長的 0 與 1，這是包普的原始數據。

三、 讓我們稱 － 或｜偏振的光子爲 ＋ 光子，＼或／偏振的光子爲 × 光子。愛麗絲告訴包普她送出的每一粒光子是 ＋ 光子或是 × 光子，而包普則告訴愛麗絲他測量每一粒光子用的是 ＋ 或 × 偏振儀，但其他資料保密。經過對比之後，他們在各自的原始數據裡，只保留相符合的部分，丟棄不符合的。爲什麼呢？假設愛麗絲送了一粒 － 偏振的光子給包普，她會記下 0，並宣稱這是一粒 ＋ 光子。如果包普用 ＋ 偏振儀去測量的話（相符），結果一定是 － 偏振（代表 0），所以在兩人的原始數據串裡，這粒光子都是代表 0。但如果包普錯用了 × 偏振儀的話（不相符），則結果可能是＼（代表 0），也同樣可能是／（代表 1）；但愛麗絲不知道（因爲數據是不公開的），所以這個數據要丟掉。

四、 細心的讀者也許已看出來，丟掉了所有「不相符」的數據後，愛麗絲與包普的數據串變成完全相同，可以用來作祕密鑰匙。如果沒有人竊聽的話，這是完全正確的。但是隔牆有耳，還是小心爲妙。他們有什麼辦法把竊聽者抓出來呢？其實很簡單，他們可以隨意挑一部分數據告訴對方。假如這部分數據完全吻合的話，則有人竊聽的機會微乎其微，於是便可以用最後剩下的數據作爲鑰匙。但假如不完全吻合的話，則證明中途一定有人動了手腳，這次的結果便得丟棄了。愛麗絲與包普得先設法把漏洞堵住，然後重新再來，直到完全沒問題爲止。



http://www.qubit.org/intros/comp/comp.html

你抓得到我嗎—非0非1的量子資訊，量子態 ψ 可以同時處在狀態｜0＞和｜1＞之中，即為｜0＞和｜1＞的任意線性疊加。

保密與竊聽是人類文明的特性，所謂「知己知彼，百戰百勝」，保密者與竊聽者之間的戰爭，從古到今，綿延不絕。有些時候保密者占上風，別的時候竊聽者占上風，各領風騷若干年。量子密碼法的出現，在理論上終結了這場長達幾千年的爭鬥；可以說，竊聽者從此沒輒了！今天，利用光纖，已能夠把量子密碼傳送到幾十公里以外，誰知道明天會如何呢？可以想像，絕對安全的量子密碼必然會最先用在國防通訊上。說不定在某些國家的總統府與國防部之間，早已開始利用量子熱線通話了。 □

深度閱讀資料

高銀仙、義年華原作，宮哲兵編著 （民80），女書：世界唯一的女性文字，婦女新知基金會出版部，台北。

賽門．辛著，劉燕芬譯 （民89），碼書：編碼與解碼的戰爭，台灣商務，台北。

Bouwmeester, D, A. Ekert, and A. Zeilinger （2000） *The Physics of Quantum Information*, Springer－Verlag, Berlin, Germany.

張志義
中央研究院物理研究所