【基礎科研】【戰略】從貝爾實驗談起（一）

2018-08-27 18:10:00

原文网址：http://blog.udn.com/MengyuanWang/114524356

近兩年來，中國在量子通訊（精確地說，應該是量子加密才對，即Quantum Key Distribution，因爲只有幾百個位元的密鑰是由量子手段傳輸的，密文本身還是以古典加密方式來保護並傳輸）方面有相當的投資，也宣佈了許多成果，然而這些被宣傳的成果一直是有爭議的。我因爲對相關的學術專業不是完全熟悉，所以沒有直接參與公開的討論。但是這些量子加密的技術，實際上就是所謂的貝爾實驗，而貝爾卻是我最佩服的物理學家之一；當初我會去研究並成爲Bohmian Mechanics的信徒，就是受貝爾的影響。

我在過去這一周有一點閑暇，便復習了貝爾實驗。其實貝爾定理，從理論物理的觀點來看，非常簡潔而美麗，我雖然是在20幾年前仔細研究它的，重點卻都還記得。我須要重新閱讀的，是相關的數學和實驗論文。現在掌握了較多的細節，可以寫一篇評論。

貝爾在1964年提出他的定理，當時的設定是一個思想實驗（Thought Experiment）：將一對自旋有反向糾纏的電子分開，然後分別測量它們的自旋方向。因爲原本電子A和電子B的自旋方向是不確定的，唯一已知的約束（Constraint）是必須相反，所以測量結果單獨來看都是隨機的，只有事後把兩者拿來對比，才會發現有彼此之間的關聯。

當然在量子力學裏面，每次測量自旋只能選擇三度空間裏的一個特定軸向。如果A和B的測量軸向是同一個方向，那麼由於原本已知的反向糾纏，測量結果必然是一個+一個-，或者用數學的專業用語就是相關性（Correlation，我們將簡稱Corr）=-1。如果A和B的測量軸向是相垂直的，根據測不准原理（Uncertainty Principle），相關性必須是0。

愛因斯坦假設了量子力學有符合定域性（Locality）的隱函數（Hidden Variable），那麼A和B的相關性就會遵循古典（Classical）機率，而古典理論下，A和B結果的相關性，也同樣是平行軸給出-1，而垂直軸給出0。

貝爾的慧眼在於他看出量子力學和古典理論在兩個測量軸夾角θ既不是0也不是π /2（亦即90°）時，結果是不同的。詳細來說，A和B的相關性在古典理論下，應該是Corr=2θ/π-1，而量子力學的結果，則是Corr=-cos（θ）。

於是貝爾做了一個最簡潔的設定：A和B的測量軸方向可以有同樣的三個選項a、b、c，分別對應著正北、順時針π /3（亦即60°）的東北方向和逆時針π /3的西北方向。那麼Corr（b，c）- Corr（b，a）- Corr（a，c）的古典結果是1，而量子答案卻是3/2。

如果你覺得這只是一個特例，你可以考慮隨機選取的三個a、b、c方向，那麼古典的結果永遠必須滿足絕對值| Corr（b，c）-Corr（b，a）- Corr（a，c）|≤1（其實那兩個負號也可以是正號，不等式仍然成立），這就是著名的貝爾不等式。當然量子力學的預測是可以違反這個不等式的。

貝爾的論文一發表，就有實驗學家想要驗證他的定理，但是貝爾不等式只在邏輯推理時最爲簡潔，它假設了自旋測量100%精確，以及電子從來不會失蹤，這在實驗室的環境下是做不到的。於是1971年，Clauser、Horne、Shimony和Holt修改爲四個方向a、b、c、d，各有π /4的夾角；不等式也改為有四個Corr，亦即| Corr（a，c）+Corr（a，d）+ Corr（b，c）- Corr（b，d）|

≤2，這就是所謂的CHSH不等式；其主要的改進在於不再假設自旋測量值必須100%精確，容許一點誤差。在CHSH實驗中，量子力學的結果可以高達2√2（這是由數學家Boris Tsirelson算出來的，叫做Tsirelson's Bound），明顯地違反了不等式的限制。

在1974年，Clauser和Horne進一步概括化，容許若干電子不被偵測到；這就是CH不等式。此後的所有貝爾實驗，實際上驗證的都是CH不等式。1987年，Garg和Mermin證明只要偵測率高於82%，就仍然可以定性地否決愛因斯坦的定域性隱函數假設。

最早的貝爾實驗是1972年的Freedman和Clauser所做，當時就已經把電子換成光子、自旋換成偏極化方向（Polarization）。這是因爲電子的傳播必須有真空，而光子沒有這個限制，而且可以使用各式各樣的光學儀器，非常方便。只有糾纏光子對的產生，比較有問題；他們使用鈣原子的雙光子輻射，雜訊很强，但是仍然得到結果，突破了CHSH不等式的限制。

到了1980年代初，法籍物理學家Alain Aspect把上一代的實驗的多項細節進行了改善，得到了更嚴密的結果。然後在1990年代末期，Weihs和Zeilinger又做了許多改進，尤其是光子源換成能把藍色激光光子轉化為一對紅光光子的非綫性晶體，大幅降低了雜訊，第一次使A和B的距離達到幾百米的層級。潘建偉就是Zeilinger的博士生，後來回到中國，繼續鑽研改善實驗細節，目前已經做到距離上千公里的程度，《Science》在2017年稱之爲世界第一。

最近幾年，對潘建偉的批評，主要在兩個方面：首先他對量子力學理論的理解，比較陳舊，甚至可以說是有謬誤（我自己也曾經批評過他一次，參見前文《如何創造研究熱點和一些其他物理話題》）；其次他的實驗結果，雖然是世界領先，但是在量子加密上的應用，卻有些潛在問題。我在下面分別詳細討論。

我在哈佛念博士的時候，曾經聽到一位老教授說："做實驗的只是有博士學位的水電工。"愛因斯坦也曾說："專家只是訓練有素的狗。"我認爲這兩個說法都有失偏頗。那位老教授是做凝態理論的，不知道超弦論者所示範的把理論物理搞成玄學，30年前大概也還沒見過近年來理論物理界玩弄行銷學、追尋無實際意義的研究熱點的例子；至少做實驗的必須搞出真正可複製的科學結果。愛因斯坦的意思則是專家只須要對自己的行業極端熟悉，不一定有創見，也不一定有常識。潘建偉的確是一個典型的專家，他的成就是前人發明的直接延伸（墨子衛星的設計原理，和Zeilinger的實驗一模一樣，只是在光學和電子儀器上，精度又提高了許多），除了做雙光子貝爾實驗特別專精在行之外，他對量子力學的理解似乎比較有限，大概連貝爾的論文都沒仔細看過，否則就必然不會公開用哥本哈根詮釋來科普，而會去研究Bohmian Mechanics。但是我不覺得這很重要，或者他名利雙收有什麽不對，因爲專家對人類和國家的貢獻往往遠超常人（老讀者可能記得，我的人生觀認爲人生的目的，在於為人類群體利益做出最大貢獻，參見前文《留給人類的知識遺產》，文中提到我很佩服的Kerr博士，也是一位典型的專家），而且1）他做的是實打實的物理；2）他的確在一個有競爭的環境下，做到世界領先；3）他的研究方向，對國防有相當的意義（這一點比較複雜，請詳見下文）。有些人可以爭論這幾點都有運氣的成分，但是任何一個人的成就，本來就必然受運氣影響；以成敗論英雄，仍然可以算是公平合理的。

潘建偉的實際缺點，可能在於他在功成名就之後，開始聽不進實話了。他被賦予了很高的政治地位和權力，可以簡單地將批評者封口。一個實事求是的科學工作者（例如楊振寧先生），不會運用這個權力，但是最近大陸媒體上已經找不到批評潘建偉的文章了。有關他量子力學上的理解缺失，我已經在前面解釋過，沒有什麽重要性：一個專家的價值是由他在本行專業內的成就決定，量子理論不是他的本行，隔行如隔山（我自己對物理實驗也基本是個外行，不過至少我是做現象學出身，所以必須能真正看懂他們的論文；而且老讀者應該也知道我向來不務正業、興趣廣汎，不是典型的專家），他懂不懂都不要緊。其實他只要有自知之明，不要再公開談量子理論，也不要允許團隊中其他實驗者去發表明顯錯誤的、基於哥本哈根詮釋的科普，就可以完全避免這方面的爭議；同樣的，他這方面的批評者其實也無須太執著，這是物理數學上的問題，與國計民生沒

有關係，提過一次讓大家知道有疑點就夠了；潘建偉的成就是真的，不必成爲意氣之爭。然而徐令予所提出的量子加密實際應用上的潛在問題，對國運可以造成的影響卻大得多，值得大家深思。

我不想引起大家的誤解，所以在這裏特別先提出兩個對比的例子，也就是我以前已經一再批評過的超弦和核聚變。超弦連基本方程式都寫不下來，每一個計算都是基於假設和近似，前前後後疊了幾十層的假設和近似，所以任何結論都可以搞得出來。像是我提過的它有10^500個解，最近有一部分超弦論者，以哈佛物理系的Cumrun Vafa爲首，開始鼓吹這麼多解很尷尬，必須修改假設，變成無解，比較好看。這樣的僞科學已經虛僞到反科學的地步了，然而他們卻是全世界高能理論的主流，每年消耗幾十億美元的預算；超弦對人類社會的反饋，我們卻可以100%地確定，在無限未來都不會大於零。

超弦的問題出在物理層次，核聚變的物理沒有問題，毛病出在工程上。不論他們宣稱在局限（Confine）等離子體（Plasma）的溫度和時間上，有多少突破，要萃取最後聚變產生的極大量高速中子，有效轉化成電能，卻不損壞超導磁鐵和真空隔層，才是真正的關鍵。這不但現在做不出來，在工程上要從何著手都毫無頭緒，那些每隔幾周就吹噓進步的中外團隊和公司，也絕對閉口不談。所以我認爲，核聚變發電的商業應用，有99%的可能性在50年內無法達成。

潘建偉的量子加密，基於我在前面詳細解釋了的貝爾實驗，在物理和工程層面都沒有問題；毛病出在應用層面上。雖然目前是否所有的工程難題都已解決，還有爭議，但是我覺得持之以恆，應該總是可以做到的。然而即使工程上已經完全優化，它還是只能解決A點到B點之間，通訊被敵方用物理方法攔截的危險。如果A不知道B的確切位置，或者沒有直綫視界（例如運動中的戰術通訊），就不能使用。如果A和B之間必須中繼（例如長途光纖），那麼中繼站也必須極度保密（這和量子信號不能被簡單複製有關，參見Quantum No-cloning Theorem）。所以量子加密這個國防應用，其實是有限而且昂貴的。它之所以會出風頭，主要是因爲量子計算機的發展可能會破解當前的數學加密手段。這些“古典”的加密方法既方便、又便宜，而且是全程保護，不只限於某些段落。加密學的特點，在於其總强度由最弱的環節決定，所以只要古典加密仍然安全，量子加密就毫無實用價值。

因此，總結來説，量子加密只有在量子計算有了突破的前提之下，才有實用上的意義。那麼目前量子計算的進步到了哪裏呢？一般我們用Qbit（量子位元）的數量為指標，而這也正是那些量子計算的專家們（請注意，量子加密和量子計算是完全不同的兩個行業，所需的工程專業能力並沒有太大的重叠）忽悠大衆的地方。詳細來説，量子位元和古典計算機的位元不一樣，它有兩個層次：一個是物理層次，一個是邏輯層次，其中許多個物理位元才構成一個邏輯位元，而後者才對應著古典計算機的位元，可以用於實際計算。現在量子計算機的設計至少有幾十種，如果物理位元越容易做，每個邏輯位元就需要越多的物理位元，所以單純比較物理位元的數目，毫無意義。真正有意義的標杆是破解256古典位元的密碼，這需要上千個量子邏輯位元。那麼最新的成果是什麼呢？IBM在去年號稱做出50個位元的量子計算機，并且暗示今年能達到75個。但是、但是、但是，讀者大概可以猜到，他們説的是物理位元。真正的重點問題是，2018年世界最先進的量子計算團隊，可以做出幾個邏輯位元？答案是這些團隊同樣閉口不談的，因爲它是零！

量子計算在未來幾年會有什麼樣的發展，沒有人能確定；然而我的估算是有80%的可能性要花20年以上才會達到能破解古典密碼的地步（請注意，這個百分比估算值是否精確並不重要，要點在於沒有人能確定它必然會很快成功）。其實這並不是沒有前例：1970年代有了迷你計算機之後，同樣有一個熱潮要開發AI（人工智能），其熱度不遜於現在的量子計算；結果一直到2012年，英偉達做出了GeForce 680，其計算能力高出40年前的迷你計算機達6個數量級左右，這些人工智能的點子才有了足夠的工程基礎，可以實用化。當前的量子計算，仍然在工程的初始攻關階段，前途未卜。這並不是量子保密團隊的過失，但是量子計算是量子保密的實用前提，現實如此，我們必須直面其不確定性。

當然，量子破密和量子保密對國防都有極大的潛在影響，即使只有20%的機率會在可見的未來實用化，在當前世界霸權即將交替的國際情勢下，也不能冒險，所以國家投入足夠的財力、人力、物力來維持競爭力，是正確的政策。然而過猶不及，如果過度投資在新方向，反而忽視了對傳統技術（亦即古典保密和破密學）的投入，那麼就會有80%的機率落敗，這顯然也是不智的。尤其是目前中國境內，對"量子通訊"有了狂熱，如果趕鴨子上架，硬是在客觀條件未成熟的背景下趕急應用，那麼必然會因爲整個通訊網絡的其他環節不能跟上，而造成實際的總體安全性低於自我認知的情形，而這本身就是保密/破密戰爭中最危險的情況之一。

所以潘建偉在他自己專業範圍內（也就是貝爾實驗），不願意受雜音騷擾，是一回事；但在量子加密的應用上，其關鍵在於加密學和量子計算，這些都超出他的專業和控制，所以又是另一回事。如果不鼓勵像徐令予這樣的批評家發言（徐不一定永遠是對的，但是只要他對事實與邏輯有尊重，能做理性的討論，就對科學的發展和應用有助益），不出面更正過度誇張的宣傳，就會對國家造成潛在危害。我希望這篇文章能提醒他或其他決策者的注意，讓他們瞭解在這方面做誠實討論的重要性，從而使決策沒有偏頗，達成最優的結果。

【後註一】有讀者告訴我，潘建偉的量子保密技術用的是所謂的BB84 Protocol，和貝爾實驗無關。我卻一直以爲他用的是E91 Protocol，也就是正文中所提的CH實驗。2017年，他在《Science》發表了有關墨子衛星的論文，裏面強調他把CH實驗的距離拉長到創紀錄的1200公里，所以我覺得E91才對。

如果潘真的用了BB84，那麼本文的前後兩半就沒有了關聯，但是卻不影響文章的主旨，亦即量子加密的實用性仍未確定，在這方面的公開理性討論有其價值。

【後註二】我找到了一篇今年初的文章，裏面引用哈佛教授Alan Aspuru-Guzik的評論，說以目前的技術，大約需要10000個物理位元，才能拼出一個邏輯位元。未來有可能會進步到800個物理位元就足夠的地步，不過那是空頭支票；參見https://www.quantamagazine.org/the-era-of-quantum-computing-is-here-outlook-cloudy-20180124/。而量子計算最新的世界記錄是Google剛剛在八月宣佈了有72個物理位元的量子計算機。

---

6 条留言

mgs 2018-08-27 19:26:00

人工智能领域也是各种炒作，其实现在只不过是一些数据拟合，完全没有认知能力 关于核聚变，有这样一种看法 咳，我老早就说过，这世界上的所有问题，什么可不可控，连不连续，可不可积，可不可导，analytic or not ，说到底都是尺度问题，控制尺度合适，什么玩意儿都能搞。 像热核聚变这回事，你们的思路就错了，小尺度当然不好控了。你把尺度放太小，连烧煤都是不可控的对吧。太阳的核聚变，没啥控制了吧，但就是尺度大，离的远，到咱们这儿就成了稳定太阳能，可控的一米。 要我说，去荒无人烟的地方，弄个青海湖那么大的池子，沿着湖边建一圈潮汐发电站，然后每隔几个小时往里扔一颗深水氢弹，算好波动时间距离，人造潮汐涨落在岸边发电，稳的不要不要的。考虑到这世界上，其实基本上所有的发电手段都是在烧水，咱这技术手段哪能算丢人。 也不要担心被气化蒸发炸到天上去的水嘛，还是会变成降雨落回来的，没准还能改善当地的气候微循环。 作者：Trac Indr 链接：https://www.zhihu.com/question/267170674/answer/416503799 来源：知乎 著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。

> 你知道他是在開玩笑吧？

entanglement 2018-08-28 01:59:00

大家應該是叫 BB84 Protocol, 先生筆誤了吧 如果是用 BB84 Protocol, 理論上並沒有中繼站被竊聽的問題 另外先生所謂的"邏輯位元" , 我個人理解為在數個qubit上作non-local 的unitary transformation 如果沒有理解錯誤,我認為他們是能夠產生邏輯位元的

> 是筆誤，多謝更正。不過BB84仍然依賴單光子跑完全程；目前單光子能可靠在光纖裏跑的距離，還是在100公里左右，中繼站絕對是必要的。一旦有了中繼站，那麼它當然成爲Single point of failure。 AI我不熟；邏輯位元的細節如果錯了，請指出參考資料，我會去研究。邏輯位元需要多個物理位元的原因是錯誤糾正，畢竟保持qbit在糾纏態是很不容易的。我看過很多理論論文，討論如何做出邏輯位元，但是幾個月前有一篇文章說這些都是騙人的，實際上還沒有一個團隊能實際做出一個可靠穩定的邏輯位元。不過我沒有保存那篇文章，所以現在找不到了。當然，那個作者可能說錯了，或者我記錯了。 我一向覺得只要先做了足夠的研究、盡力不犯錯，事後被更正沒有什麼丟臉的；畢竟討論一個議題，經常比確定自己沒說錯話更重要。

desertfox 2018-08-28 03:58:00

只有最後一部分看得懂, 如果延伸其旨意的話, 王先生此文想談的應該是中國科研在項目開發, 投入和宣傳方面的問題. 我不知道在中國大陸科研的項目審核是怎樣的一個系統, 有那些單位和標準, 只知道軍方在這方面應該比較嚴謹. 其方針是跟上一代領先一代, 我想跟上一代在驗證上不會有問題, 但是領先一代的判定在研發階段就很難說了. 王先生對潘健偉量子通訊實用上的疑慮恐怕對潘本人不會引起多大的反响; 因為這就像搞專利一樣, 就你一個團隊深入旁人跟不上, 所以在專利確定之前任何質疑都會被視為干擾. 好在王先生本文也提到了古典加密還是有它的安全空間, 那麼談這個問題就可以牽涉到所謂領先一代的投入方向是否正確, 會不會有預算的排擠作用和在宣傳上是否過分樂觀形成誤導. 潘健偉這項研究最近在媒體上已沒有什麼報導了, 所以他的進度不得而知. 或許是遇到瓶頸, 也或許是因為受到最近中美衝突大環境的影響中央在科技發展的宣傳上轉變為收斂. 但就宣傳這一塊而言, 我個人的看法是他們一向做得不好; 因為那幾乎是凡有開發就說得興高采烈. 而大部分的人跟我一樣, 在科學上沒有王先生的根底純屬吃瓜群眾, 所以你宣傳上抬的越高, 到時候如果出了問題那群眾的失望就會越大. 所以凡事應該實事求是, 有十分才說十分, 在那以下最好是遞減. 所以在這裡我其實是借題發揮, 對中共的宣傳感到不滿. 然而這是另一的題目, 等王先生再有這方面的論述大家再來討論吧.

> 沒有關係，文章的前半原本就是專爲理工科讀者寫的。其實，貝爾定理已經是很精深的話題，就算是高能物理博士也多半不熟。我也是想試試我以簡馭繁的功力，看看能否用幾個段落把它解釋出來。 現代科技，極爲專精，內行很容易誤導外行。我把他叫做Tyranny of Expertise；這是我經常批評的對象之一。

mgs 2018-08-28 07:50:00

我知道他在开玩笑，但这不是没来由的 核爆炸的和平利用：和平利用核爆炸的几方面实例-中国工程物理研究院 http://www.caep.ac.cn/hwkp/hwzs/10150.shtml (5) 用于核爆氘能能源 1977年，苏联科学院院士A·A萨哈洛夫在纽约发表的《核能与西方自由》一文中，曾把解决聚变能源的希望寄托在地下核爆炸爆室里。九十年代初，在中俄和平利用核爆炸双边讨论会上，曾提出了利用地下“纯聚变”核爆炸建造地下聚变电站的大胆设想。设想如图6.4所示。

> 不管埋得多深，產生的放射性還是遠超貧鈾幾十個數量級，至少會污染地下水。這在和平時期，是不可能接受的。

虐猫狂人薛定谔 2018-08-29 04:12:00

我只想确认我的理解是不是正确，请王博士赐教。 无论是王博士说的Bohmian Mechanics，还是传统的哥本哈根学派解释，都是实验无法证实或者证伪的吧？如果实验无法验证，纠结太多背后逻辑上不同的假设，就像研究无法验证的弦论了。

> 只有一層假設，爲了解決邏輯上的矛盾，還是合理的。 哥本哈根詮釋，連數學上的定義都寫不出來，遑論邏輯的正確性；所以根本不值得考慮。

膠柱鼓瑟 2018-09-05 09:41:00

怎麼AI的突破是來自英偉達遊戲顯卡廠 英特爾和IBM等都沒超過它嗎

> AI的計算，在有專門爲它設計的NPU之前，用GPU比CPU效率高很多。

返回索引页