

2021 年京都獎紀念講座

資訊科學之旅

作者：姚期智 譯者：高玉齡

作者簡介

姚期智是中央研究院院士，美國科學院外籍院士，美國科學與藝術學院外籍院士，國際密碼協會會士和中國科學院院士。他是 2000 年涂林獎得主，是目前唯一的一位獲得此獎項的華人。現在是北京清華大學交叉信息研究院院長，他也是香港中文大學博文講座教授、新竹國立清華大學榮譽講座，以及國立臺灣大學特聘研究講座教授，香港中文大學（深圳）傑出大學教授。研究專長領域有演算法分析、計算理論、密碼學和量子計算。



（稻盛和夫基金會授權）

各位女士、先生，很高興來到這裡。首先，讓我表達獲得京都獎是一個莫大的榮譽。在了解歷屆獲獎者和他們的輝煌成就之後，我為自己被認為值得與他們齊名而深感自愧弗如，也很高興和榮幸在這裡演講。

今天，我想談談我的成長過程，如何進入資訊科學領域，以及一路走來的歷程。更詳細的，我將首先介紹一下我的成長背景，然後是談談我小時候對物理學的癡迷，這促成了我後來選擇的第一個職業。然後講講我如何偶然轉行成為一名資訊科學家。接著我想簡要介紹一下我的一些研究，我在思考些什麼問題以及為什麼它們很有趣。我做最後總

結前，我想向對我的生活和研究工作有重大影響的幾個人致敬。

我的成長經歷

我 1946 年出生於中國上海。不久後，全家搬到了香港，然後又搬到了臺灣。我在一個幸福的中產階級家庭長大，家中有慈愛的雙親和兩個非常親密的手足。

我自幼深受中國傳統價值觀薰陶，尤其是非常重視文化和學識。令我和我父母欣慰的是，我是一名優秀的學生，學生時期成績一直是名列前茅。

本文譯自：<https://www.youtube.com/watch?v=9BPksehCgOU>

本刊感謝稻盛和夫基金會（Inamori Foundation）同意翻譯轉載，翻譯之文責由本刊自負。



(稻盛和夫基金會授權)

我記得我小時候喜歡數學、科學和歷史。例如：我對展現不尋常勇敢和智慧的歷史人物著迷，偉大的科學家如伽利略和牛頓是我的英雄，也因為他們的才華以及為自己的信仰挺身而出的勇氣，令我大為震撼與敬畏。我夢想著有一天自己也會成為這樣的人。

早期對物理學的癡迷

在我高中三年級的某一天，我偶然得到一份愛丁頓爵士（Arthur Eddington）關於相對論的筆記，其中給出了相對論最生動、最簡單的推導。

論述大致如下：由實驗，我們知道光有恆定的速率。從這一事實，我們可以通過聰明的論述得出我們熟悉的「時間」觀念不可能是一個絕對普適的觀念，而這是長期以來每個人都認為理所當然的事情。

這段論述給我留下了深刻的印象。我發現，物理學可以像偵探故事一樣吸引人，而且比「福爾摩斯」影集中的任何一集聰明的情節都更具想像力。這令我深受鼓舞。於是 1963 年，我在大學選擇了主修物理。

不久之後，費曼的物理學講義出版了。傳說加州理工學院想徹底的重組他們的大一物理學課程，費曼同意這樣做，條件是他只教一次。由此誕生了傳奇的 3 卷物理學講義《費曼物理學講義》（*The Feynman Lectures on Physics*）。

這套書讓我大開眼界。難以解釋的高階觀念，僅

使用初等數學就可以解釋和推導出來。這真是令人印象深刻，讓我看物理學的深度和它的美。

事實上，這是我第一次覺得自己真正理解了量子力學的原理。30 年後，當我開始從事量子計算領域的工作時，費曼對量子現

象的解釋在我看來仍然是最有啟發性和最有用的解釋。這讓我確認下來，決定在大學畢業後繼續在物理學深造。1967 年，我大學畢業後服了一年兵役，之後前往哈佛大學攻讀物理學研究所。1972 年，我在格拉肖教授（Sheldon Glashow）的指導下獲得了物理學博士學位。我終於成了一個認證過的真正物理學家，但這並沒有持續多久。

轉行：從物理學到計算機科學

1973 年，當時我在麻省理工學院攻讀博士學位的妻子法蘭西斯（Frances）^① 向我介紹了演算法。

「演算法」現在已經是頻繁出現的日常詞彙了。但是，在當時這個名詞，對大多數人來說，還是相當陌生的。當時，我接觸到高德納教授（Donald Knuth）^② 編寫的《電腦程式設計藝術》（*The Art of Computer Programming*）的第 3 冊的早期草稿，在麻省理工學院並不廣為流傳。這是一本很有名的

^① 譯註：儲楓（Frances Yao），是北京清華大學交叉信息研究院的講席教授和香港城市大學電腦科學系的名譽教授。

^② 譯註：高德納是在他 1977 年代訪問中國之前儲楓幫他取的中文名字。他也是 1996 年京都獎得主和排版軟體 TeX 和字型設計系統 Metafont 的發明人。

關於演算法的書，一個多麼了不起的傑作，它介紹了一門引人入勝的新科學。

閱讀後，我開始不斷思考書中所提出的研究問題，深陷其中而無法自拔，以至於我很快就辭去了物理學博士後的工作，轉而全職攻讀資訊科學研究所學程。

我記得我母親當時很擔心，因為我似乎放棄了這麼多年的物理工作，但我的妻子非常支持我。所以我成為了伊利諾伊大學的資訊科學系的研究生。非常感謝劉炯朗教授願意指導我。

研究工作概況

現在我想談些關於我的研究。最初，我專注於解決演算法中現有的未解問題，例如最小生成樹（minimal spanning tree）、B 樹（B-tree）等等。但畢業不久後，我開始對研發資訊科學的新架構和新理論產生興趣。

幾十年來，我有機會在幾所一流大學工作。我在柏克萊、史丹福待過了 10 年，隨後在普林斯頓度過了 18 年。2004 年，我加入了清華大學，直至今日。

我在每個時期都做一些不同的事情。很有趣的是，我在不同時期關注的主題，它們與時代的變化和資訊科學作為一門學科的發展，以及身處的大學環境都有很大關係。

接下來，我想要介紹三個主題，極大極小複雜度（minmax complexity），通信複雜度（communication complexity），以及密碼學（cryptography）和安全多方計算（multi-party secure computation, MPC）。

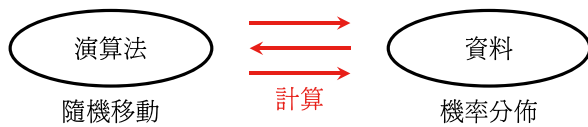
我發現做研究最好的方法是提出深刻、大膽和關鍵性的問題。如果你能提出好問題，那麼就一定會做好研究，得出對研究界來說實用且有重大意義的結果。現在我將對每個主題的主要問題及其重要性進行討論。

極大極小複雜度

第一個是 1977 年提出的極大極小複雜度問題。它在我心中有很特殊的位置，因為這是我第一次提出了自己的研究問題，並找到了很好的解決方法。我們知道，演算法本質上很像食譜。例如在烹飪中，食譜會告訴你每一階段的步驟，例如放 3 盎司鹽或幾克肉。

1970 年代中期，有一種新的演算法引起了人們的注意，也就是「隨機演算法」（randomized algorithm）。這種新演算法結合了「隨機移動」（stochastic moves）。如果用烹飪來比喻的話就是，不明確告訴你有放兩勺鹽的步驟，而是讓你用擲硬幣來決定是放兩勺鹽，還是放一杯紅酒。

因此，對於傳統的思維方式來說，這看起來是一種瘋狂的做事方式。但在 1970 年代，人們已經證明以這種方式執行演算法是有優勢的，在某些情況下，它們會產生一些令人讚歎的結果。但人們還無法理解這些算法的侷限性。因此，這讓我問了自己一個問題。到底哪個演算法更好？是當時剛剛提出的隨機化方法，還是用傳統的方法觀察資料分佈，並在執行過程中調整演算法呢？但是，一旦人們以這一種方式敘述問題，就會跳出一個最令人驚喜的聯繫，從而令人對隨機演算法有很多深刻的了解。



當把隨機演算法與傳統分佈方法進行比較時，可以將它們視為隨機演算法和資料之間的賽局。演算法可以根據資料選擇如何隨機移動，而資料，對手，可以選擇分佈方式，從而使演算法的運行變得更加困難。在馮諾曼（John von Neumann）的賽局理論（game theory）極大極小原理（minmax principle）的作用下這兩種方法恰好達到了它們的極限。這個聯繫給出了我們想要證明的定理，也就是說事實上這兩種方法是相同的。這為理解隨機演算法提供了新途徑。在現在，這種在當時還算新穎的演算法已經成為許多密碼演算法和 AI 演算法的預設模型（default model）。

人們想了解隨機演算法的侷限性是有原因的。因此，在這 40 多年來的時間裡，我發現的演算法仍然被許多研究人員用來解決他們的問題。

通信複雜度

第二個主題是我在 1979 年所提出的通信複雜度。

讓我先解釋一下這個數學問題，愛麗絲和鮑勃是兩個在不同地點的人，他們各自持有一段 n 個位元（bit）的資料，例如 x 和 y 。我們想要解決的問題是：假設它們想要聯合計算某個量 F ，它們之間需要通信多少位元，這就是這個函數的通信複雜度。

當然，這取決於你在計算什麼函數，例如，要計算這兩個整數的和是奇數還是偶數只需要兩個位元的通信。每個人只需告訴對方它是偶數還是奇數，

然後他們就可以知道答案了。

另一方面，如果你想計算 x 是否大於 y ，那麼它將需要 n 個位元。你需要把整個字串（string）從一個人發送給另一個人才能解決這個問題。

更深一層的是，你必須意識到並證明，沒有比這種方式來解決這個問題更好的方法了。一般來說，這是一個相當困難的問題。如果我給你一個關於 F 的計算複雜度，那需要相當高深的數學分析才能完成。

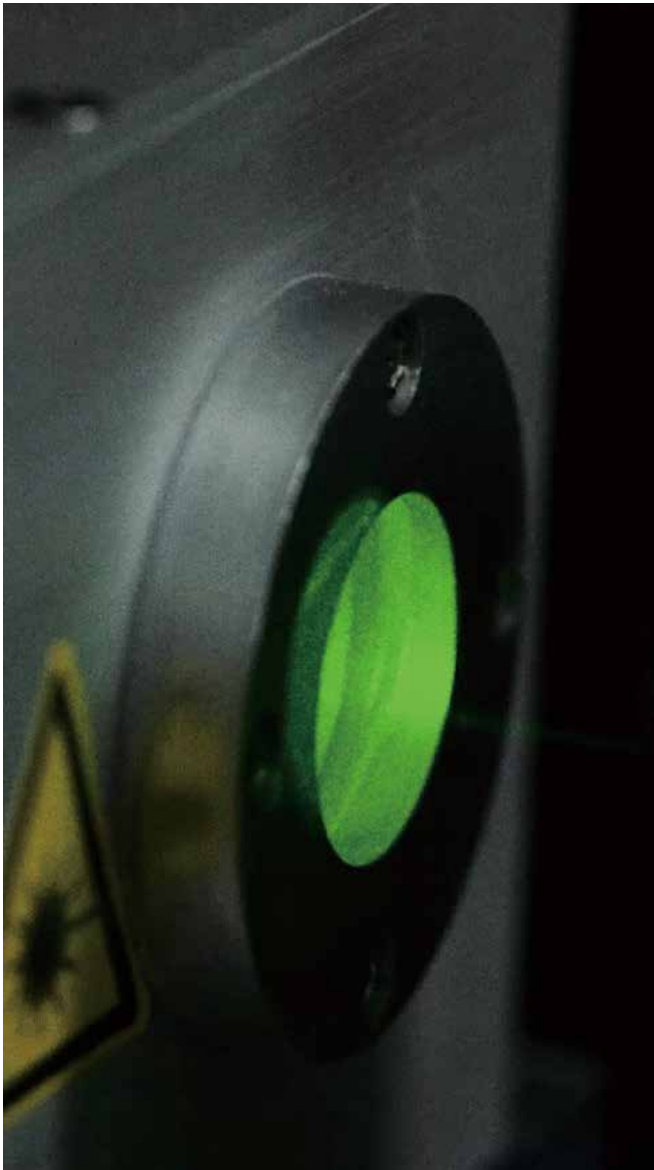
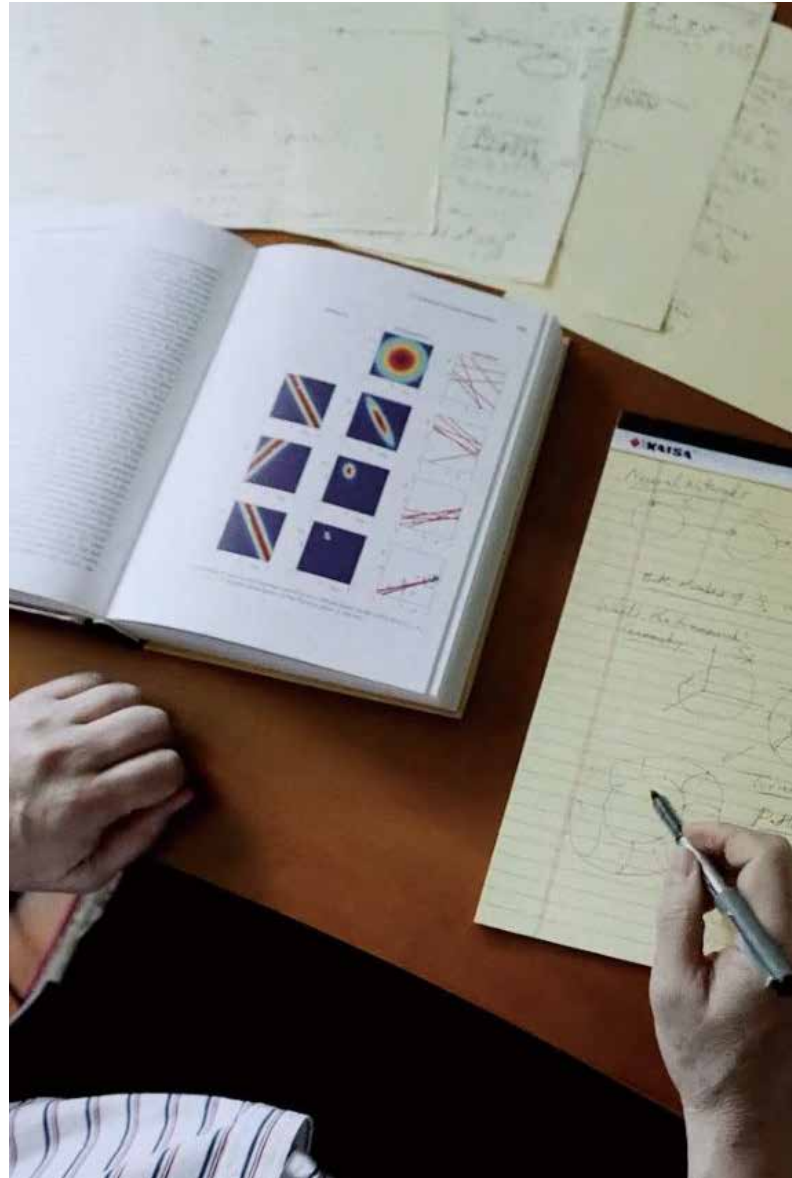
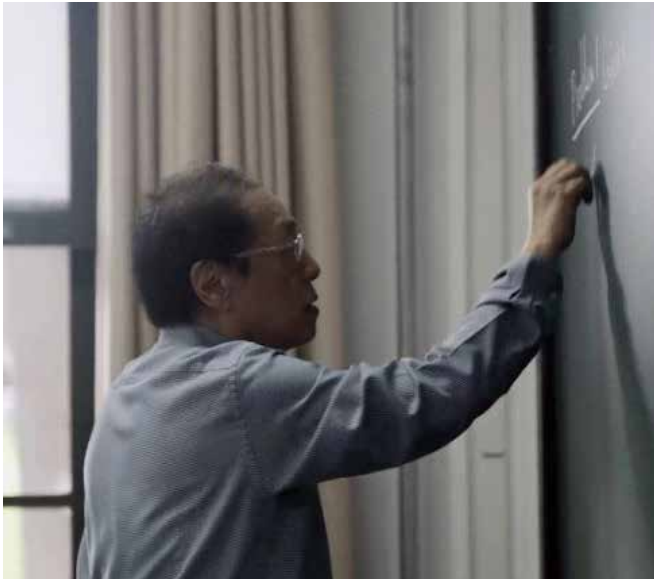
考慮通信複雜度的原因是，計算模式在 1970 年代的後期發生了很明顯的變化。從之前大家都熟悉的大型電腦計算，逐漸轉向我們現在所熟悉的網路計算。人們對以分佈式方式解決問題感興趣，許多人願意以協作方式解決問題。因此，這意味著我們必須把過去的計算模型調整為網路模型。在這個新的世界裡，因為我們必須移動資料，通信成本通常是很高的。因此，我剛剛向你們介紹的通信複雜度的概念就是為了模擬和反映這種變化。自從該模型被提出和分析以來，通信複雜度在從晶片設計到資料串流（data streaming）的各個領域都得到了廣泛的應用。

密碼學和 MPC

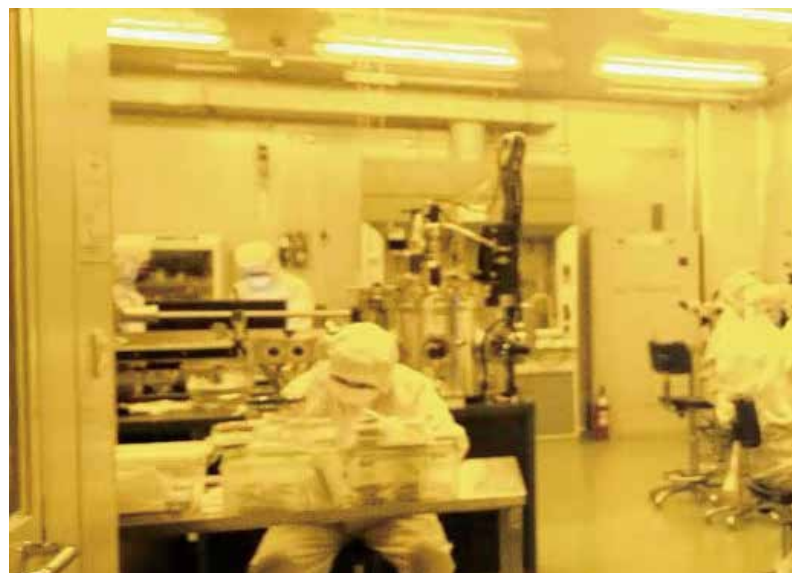
最後一個話題我要討論的是關於密碼學和 MPC。

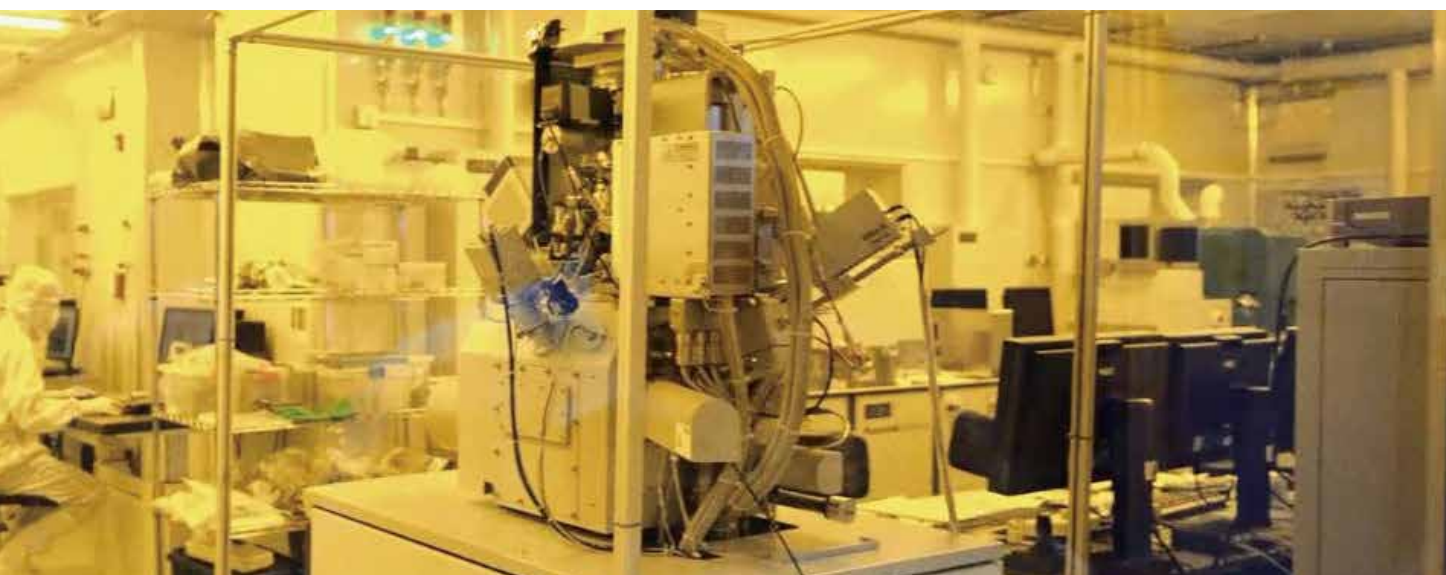
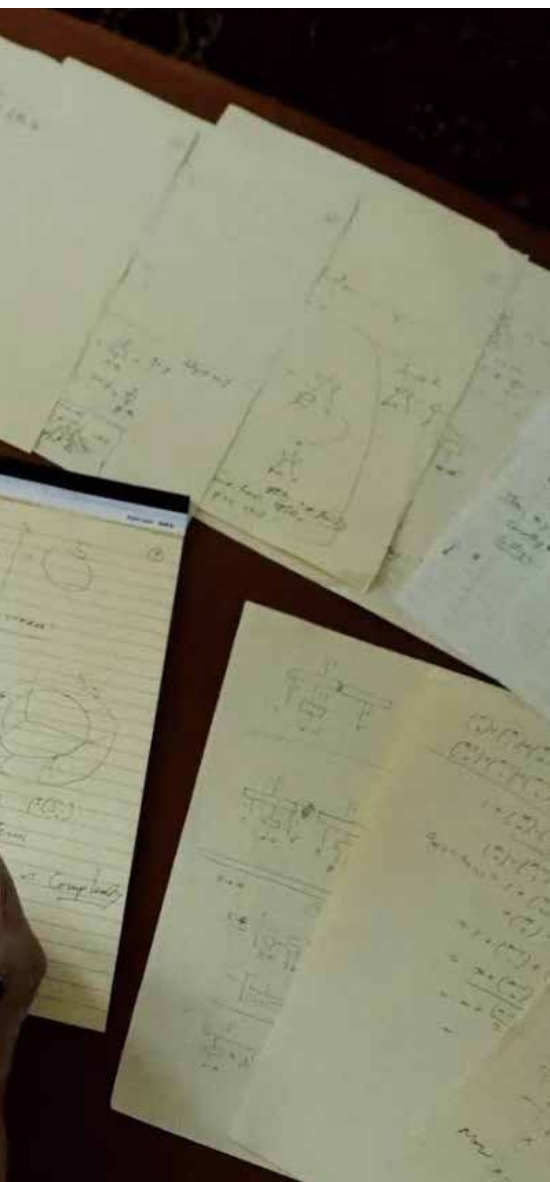
1982 年，我寫了 3 篇論文，這 3 篇論文對現代密碼學做出了重大貢獻。這 3 篇論文涉及多列夫／姚安全模型（Dolev-Yao secure model）^③、虛擬

^③ 譯註：多列夫（Daniel Dolev）是一位以色列資訊科學家，以在密碼學和分佈式計算方面的研究而著名。



(柏盛和夫基金會授權)



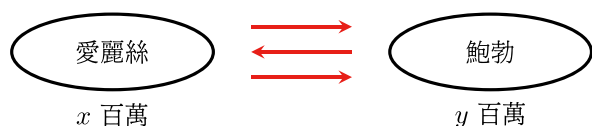


亂數產生 (pseudo random number generation) 和 MPC。今天我只談最後一個問題。

MPC 是一個加密概念，使我們可以對加密資料進行計算。如果您使用 MPC，就有可能讓多個資料庫在不洩露它們自己的資料的情況下進行聯合計算。

讓我用一個例子來解釋一下這一點。我將引用在論文中提到的著名的百萬富翁 (Millionaires' Problem) 的例子。

兩個百萬富翁，愛麗絲和鮑勃，他們希望在不透露任何定量信息的情況下知道誰更有錢。所以愛麗絲有 x 百萬，鮑勃有 y 百萬。因此數學問題是，他們想要彼此交流來知道 x 是否小於 y 。問題是，是否有可能進行一次對話，讓雙方在不知道對方資料的情況下又知道誰更富有呢？



直覺上來說你會認為這是不可能的。我怎樣才能在不透露任何一方任何信息的情況下找出誰更富有呢？如果你想幾分鐘你就會意識到，如果採用 1982 年的信息安全定義，也就是向農 (Claude Shannon) ⁴ 的資訊理論 (information theory)，那確實是不可能的，你可以證明在那個模型下是不可能的。

但我認為，需求是所有發明之母。如果真的有需要的話你肯定會想盡一切辦法。所以，如果你跳脫框架去思考，事實證明這是可能的。說到跳脫框架，我們的意思是拋棄向農在這種情況下所規定的非常僵硬的條條框框，然後把涂林納入其中，

我不會對此著墨太多。但事實證明，如果你把安全定義放寬一些，讓它變成一個務實且足夠好的標準，那麼這個問題事實上是可解的。

具體的說，我用「亂碼電路」 (garbled circuit) 實現了解決方案。在過去近 40 年的發展中，它在硬體和演算法方面取得了進步，現在幾乎是可行的。而這方面的研究工作也很多，準備在金融科技 (financial technology, FinTech)、數據交易 (data trading)、藥物研發等方面開展工作。

目前我還有一些其他的研究主題，就僅簡單列出來，而不一一詳述了。我的主題包括：

- A** 量子計算：這是一種革命性的方法，並且有望實現指數級增速的計算技術；
- B** 拍賣理論 (auction theory)：它們會將無定形的經濟問題放在簡潔的賽局理論框架中；
- C** AI：這項技術見證了，例如 AlphaGo 等，機器學習演算法取得的令人難以置信的壯舉，但成功的原因依然成謎。

所有這些都是非常有趣的新領域，而且還在持續發展中。如你所見，我研究過很多不同的主題。這些多樣且豐富多彩的主題，實際上不僅反映了我個人的品味，也反映了半個世紀以來資訊科學的蓬勃發展，以及我們今天所看到的日益增長的跨領域聯繫。

我的勵志導師

最後，我想談談關於我人生中遇到的人們。

⁴ 譯註：向農是美國數學家、電子工程師和密碼學家，被譽為資訊理論的創始人。1948 年，向農發表了劃時代的論文〈通訊的數學原理〉 (A Mathematical Theory of Communication)，奠定了現代資訊理論的基礎。

在這些年來，作為一名資訊科學家，我有幸遇見許多才華橫溢的人。我特別幸運的有兩位具啟發性的導師，格拉肖教授和高德納教授。

格拉肖教授是我在哈佛大學的物理學博士指導教授。他是最先預言存在魅夸克（charm quark）這種粒子的人之一，也是這種粒子最熱情的支持者。

我從格拉肖教授那裡學到，在科學上你必須大膽，你必須堅持不懈的堅持你的信仰。

我從他身上學到的另一件事是，數學和物理是不同的。對於物理學家來說，最重要的是能夠找出物理事實的法則，而不是堅持精確的數學論證。我認為這種務實精神對我以後的研究有很大幫助。

還有一件事是我從格拉肖教授那裡學到的：生活應該是有趣的。

1971 年春天，作為一個年輕的學生，我跟隨他去法國馬賽的 CNRS（Centre national de la recherche scientifique，法國國家科學研究中心）研究休假（sabbatical）。這是一個多麼神奇和迷人的城市，那也是我第一次到歐洲。那年夏天的晚些時候，他帶我去了義大利西西里的一個暑期研習會。

這是一次非常美妙的經歷。格拉肖教授給我上的這一課讓我明白，生活的樂趣和對知識的追求可以兼而有之。

現在，我想提一下高德納教授。正如我之前所提到的，當我讀到《電腦程式設計藝術》時，它幾乎改變了我的生活。在這本著作中，他確實開創了一個新的研究領域，也激勵了一代又一代新的資訊科學家。例如，通過閱讀他的書，我開啟了自己的資訊科學生涯，並解決了他在書中所純熟精湛設定的一些問題。

後來，我有幸在史丹福與他共事。眾所周知，除了數學和資訊科學之外，高德納教授在許多方面都很出色。他是一位才華橫溢的管風琴演奏家。他還是一位作曲家、小說家……，所以他是非常多才多藝的。而且他真誠大方，總能看到他人身上好的一面。

結語

總而言之，雖然有一些波折，我在資訊科學領域還是經歷了一段美好的旅程。我發現，一開始就走錯方向可能並不一定是劣勢。事實上，早期的物理訓練至少在兩個方面對我很有幫助。首先，我了解到在物理學中好的理論是什麼樣子的，比如經典的相對論和量子力學。之後，這對我建構資訊科學的理論時，有很大的幫助。我從物理學中受益的第二件事是它的務實精神。它教會我解決手邊的特定問題。不管用什麼方法，你都應該根據情況使用、學習或發明解決問題的方法，最終目標是解決問題。

科學的理念是追尋真理。在追尋的過程中，我們會發現科學的規律和科學的美，它可以激勵人心。它還帶來了可以改善人類的現狀，為未來所面臨的挑戰做好準備的創新。

我完全認同稻盛和夫基金會（Inamori Foundation）的願景：科學和人文應該為人類的進步而共同努力。我很榮幸能獲得京都獎，也很榮幸能做這次演講，與大眾分享我的經歷。非常感謝。🙏

譯者簡介

高玉齡是業餘科普翻譯作者。