力旺電子 公司簡介

力旺成立於 2000 年，由清大教授徐清祥博士與學生們一起成立。我們總經理沈士傑就是徐董的第一屆博士班學生，還有其他公司現在的主管。實驗室 8 年，公司成立 20 年，28 年他們都在一起。公司主管級以上幹部，從加入公司到現在，都沒有離開過。我們也出了一本教課書，現在正在寫第二本，有關硬體安全，清大有兩門課在教我們公司的技術。第一本教課書書名叫 “Logic Non-Volatile Memory: The NVM Solutions from eMemory”，Amazon 有賣。

股權結構來說，成立的時候徐董跟學生沒錢，那時力晶集團投資了 30%。2011 年掛牌上櫃，到 2016 年力晶集團已經在市場出清所有持股，退出董事會，目前跟我們只是單純客戶關係。我們目前的前三大股東是新加坡政府基金，瑞典銀行跟美國最大基金公司 Capital，持股都將近 6 年，他們同時也是台積電最大外資股東。

力旺跟其他公司最大的不同是獨特的生意模式，跟技術的含金量，等一下我會就這兩部分再做說明。我們是做矽智財 (IP)，什麼是矽智財？矽指的就是半導體，把半導體晶片當做是一個人身體，身體是由很多器官組成，晶片裡的每個器官就是一種矽智財。比如最有名的安謀 (ARM)，他們做的是處理器，就想成是晶片的心臟，我們做的叫嵌入式非揮發性記憶體，非揮發性記憶體就是沒電的時候記的東西要記住，好像是個小腦。設計晶片，就是把不同的 IP 去做排列組合，好像在堆積木，有的自己發明，有的晶圓廠會提供，其他沒有的就跟第三方授權。我們跟 ARM 就是專門在做第三方授權的這個生意。目前超過 700 個專利權，技術授權給全世界 24 家代工廠，10 家 IDM，超過 1800 家晶片公司客戶。每年使用我們的技術的晶片超過 50 億顆，每隻手機都有用到我們的 IP。比如下半年美國手機廠要推出的 5G 手機，裡面就有 20 顆電源管理晶片，全部都有用到我們的技術。我們從 2013 年起，就是全球前十大半導體智財權公司，在我們這個技術領域，幾近於獨佔。如果以財務指標每股獲利、ROE、營業利潤率來看，是全球最高獲利率的 IP 公司。

我們第一個技術 Neobit 是 2000 年初的發明，這個技術主要是用在 8 吋，2003 年第一個客戶是日本瑞薩半導體，2005 年損平。第一個成長是因爲智慧型手機，螢幕驅動晶片、電源管理晶片及指紋辨識晶片，都有相當大的比例使用我們的 IP，在 8 吋晶圓的

滲透率大約 20%。在 2010 年我們開始研發 12 吋的技術 NeoFuse，這技術在 2013 年拿到專利權，便開始在全世界代工廠的製程開發，2015 年導入第一個晶片客戶是瑞昱。經過這麼多年的技術開發與導入，已經導入的有機上盒、電視晶片、網通晶片還有很多類的晶片，去年也導入了全世界最大的半導體公司的晶片。隨著客戶的產品陸續進入量產階段，就會帶動我們權利金成長，我們很有信心，公司已經開始進入下一個多年的成長循環。

為什麼我們這麼有信心，因爲這跟我們的生意模式有關，很多未來的營收來源，都已經做完了。

我們營收 25-30%是來自授權金（一次性的），70%以上來自於權利金（就是可以一直收）。我們是全世界半導體 IP 公司中權利金比例最高的。並不是所有 IP 都能收到權利金，事實上絕大部分都收不到。比如，第二大 IP 公司 Synopsys 就在法說會上公開講他們做的 IP，客戶並不願意付權利金，所以他們都是以賣斷收授權金為主。

為什麼我們收的到權利金，因為這是我們自己發明的技術，無到有的技術，是電晶體的最基本的架構。我們把技術授權給晶圓代工廠，晶圓代工廠會先支付我們一筆技術授權金，之後我們會根據各代工廠不同的製程做法，去設計適合這製程的 IP，再花 2-3 年的時間去通過不同的驗證。驗證完成後，我們就找真正使用這技術的客戶晶片公司，像是高通、聯發科，把我們的技術再授權給他們，收設計授權費。根據他們所需要的規格，設計 IP，客戶把我們設計的 IP 放進去他們的晶片設計，這時候我們就完成產品的設計定案 (tape out)。Tape out 之後，客戶還要再花 1-2 年或更久，去找他們的客戶，比如說是手機公司。等到確定量產的數量之後，晶片客戶就會去有我們技術的代工廠製程去投片。等到量產之後，晶圓廠收到晶片客戶的錢，在下一個季度，就會根據已經談定的權利金比例，一般是某個比例的晶圓代工價格，支付權利金給我們。

這個生意模式表示，我們現在 70%以上的收入是來自於 2-4 年，甚至更久前的努力。我們的營業費用率大概是 50%，我們正在做的授權金加起來不到 30%，表示我是賠錢在做 RD，我們一定要幫助客戶成功，我們才能真正收到錢。等於我們現在做越多，未來存的糧食越充分！我們生意模式另一個特點，因爲我們跟晶圓廠簽的授權合約沒有終止日，只要工廠有用到我們的技術生產晶圓，就得付權利金。這比新藥還好，一般專利權

的年限是 17 年，我們 2000 年初的第一個發明，到現在還在收權利金，而且佔權利金比例還有 60%以上。目前我們一半以上的權利金收入來自於台積電，所以台積電是我們最大的客戶。

接下來，介紹我們的技術，我盡量用白話的語言來形容，裡面涵概一點非常難的量子力學。我剛剛講，我們是發明一種電晶體的架構，去做記憶體的儲存。可以想像一下，一個指甲上的大小，裡面含有幾億個不同的電晶體。一般的電晶體，沒電的時候，是沒辦法做儲存的工作。儲存什麼？在晶片裡，所有的資料跟訊號，都是用 0 跟 1 來呈現。我們發明的電晶體，就是要有辦法，在沒電的時候，把 0 跟 1 記住。

怎麼做到呢？利用半導體物理學上的量子穿隧效應。什麼是量子穿隧，白話講，就是穿牆術。本來沒有通道，利用氧化層天生的缺陷，缺陷越多，越容易產生量子穿隧。所以，當我們施以適當的電壓，電子因爲量子穿隧，穿過氧化層叫 1，沒穿過叫 0。看似簡單，事實上非常困難，因為很難控制。我們在這方面有幾百個專利。因為是量子穿隧，所以他所存的 0 或是 1，在外觀上是看不到，而且這個隱形的隧道，除非是在 600 度以上的高溫，是不會受任何環境因數如溫度或壓力而改變，所以產生的數據可以至少存在 10 年以上，而且非常穩定。

相對現在絕大晶片使用的是一種叫 eFuse 的技術，是用大電流去燒斷 fuse，想像 fuse 就像保險絲一樣，燒斷是 1，沒燒斷是 0，只要做反向工程，把晶片剝皮，是很容易被看到，非常不安全。加上 eFuse 沒辦法隨製程微縮而變小，越往先進製程走，面積越大，能存的資料更少，甚至得加一道光罩，增加成本。加上是用大電流去燒斷，很耗電，而且不能在晶片封裝後才寫入，很不方便。所以在過去 20 年，我們就是在一個一個晶片上取代 eFuse。8 吋已經取代 20%，12 吋的取代正在開始。

接下來，介紹我們認為是我們公司最重要的技術，NeoPUF，也是我們認為可以把我們公司的成長延伸到 5-10 年之後。什麼是 PUF，中文叫物理不可複製，簡單講就是物件本身與生俱來獨一無二的特徵點。以我們人來講，就是生物特徵，如指紋、眼睛的虹膜或臉部辨識。這種晶片的 PUF 技術研究，存在已久，很多學術文章在討論，也一直有公司想做或在做這方面的生意，但一直都有問題，所以目前還沒有被真正大量應用。

這類技術真正引起注意，是從 2015 年開始，美國國防部 DARPA 開始想要去推廣，導入商用晶片。為什麼? 因為美國國防部懷疑 20%的軍用晶片是偽造晶片，因為軍用晶片都是跟商用晶片共用。晶片怎麼被偽造？有幾種方法，剛剛上面有講到反向工程，因為 eFuse ，抄線路圖，重新仿造。最普遍的是 recycle，回收廢棄的電子產品內的晶片，重新包裝，流回市面。比如俄羅斯首次嘗試到火星的太空任務以失敗收場，就是發現火箭上有偽造晶片。飛機失事，找不到原因，有可能是因爲裡面有偽造晶片。

我們在 2015 年得到這方面的訊息，開始想怎麼去用我們的電晶體架構去做成符合 PUF 功能的技術。所以我們設計一對 NeoFuse 的電晶體，就是我們 NeoPUF，施以電壓，兩個電晶體的各自氧化層的缺陷一定不一樣，缺陷比較多的會先穿過，就叫 1，沒穿過的叫 0。假設我們設計了 256 對這樣的電晶體，施加電壓，就會產生 256 組 0 跟 1 的數據。假設左邊穿過叫 1，右邊穿過叫 0，但我們不知道是哪一邊會先穿過。簡單形容，好像我們模擬擲銅板，正面或反面，正面是 1，反面是 0。如果出來是正面，我們就記錄 1，是反面我們就記錄 0，而且這一次是正面或反面，跟下一次擲出來是正面或反面並無關聯。一組擲 256 次，產生 256 個 0 或 1，下一組也擲 256 次，又是另一個 256 個 0 跟 1 的組合，這兩組數據重覆的機率是 2 的 256 次方之一。

這是什麼樣的概念，就是把全世界的沙子加在一起，也找不到一粒重覆一樣，這叫完美或天生亂數，natural randomness! 我們做了很多實驗，發現了我們的 NeoPUF 符合完美亂數的要求，也就去申請專利，很快就拿到，還得到半導體最高榮譽 ISSCC 年度傑出論文獎。而我們的 PUF 也是目前唯一符合美國國防部 DARPA 對完美亂數的 16 項要求。

舉例，假設晶片有設計進去我們的技術，一片晶圓不管有幾萬顆晶片，每顆晶片一生產出來就會有其獨特的一連串的 0 跟 1 個數字，就想成是天生出來就有一個 QR code, 或者 bar code.

有完美，就有不完美，那不好的 PUF 做出來會怎樣，那就是亂數不夠亂，就是可能 1 萬個就會產生重覆的數字，那這樣做晶片獨一無二的特徵點就會有問題。

PUF 除了當身分證之外，還有很多重要的功用，比如做亂數產生器。什麼是亂數產生

器？比如，我們上網時，被要求設定密碼，常常網頁會出現建議，說我們設的密碼不安全，會建議一組更強的密碼，就是一堆看起來很亂的數據，就是軟體的亂數產生器自動產生。或者，想要去買比特幣，交易所會給你一組很亂的亂數，當作錢包，這也是軟體亂數產生器產生。

軟體因爲是算法，有其規律，所以現在全世界都在擔心量子電腦的出現。Google 號稱他們的量子電腦，可以在 300 秒內，破全世界軍方的密碼。所以現在最安全的就是用硬體來產生亂數。目前有硬體的亂數產生器，非常的貴，而且很複雜，貴跟複雜是因爲要去達成完美亂數，可能是用不同的晶片或材料，去採取自然界的雜訊，做成一個模組，或複雜的 IP 組成。比如 IBM 做一個硬體安全模組賣給 Visa, 一個 4 萬美金，所以像我們做匯錢交易時，都會收到一組號碼，幾秒中輸入，時間到沒輸入，又會換另一組號碼，這跟錢有關，所以都是用昂貴的硬體亂數產生器產生的。

所以，天生亂數，就是現在整個 security 行業在找的聖杯，我們的 NeoPUF 就是這個聖杯，讓晶片本身可以有看不到、猜不到、找不到的鑰匙，來保護資訊的最根本安全。

因為有了這個核心技術，我們在去年 5 月成立了 100%持有的子公司 PUFsecurity，基於 NeoPUF，發明了一系列不同功用的安全 IP，把剛剛提到非常昂貴的硬體亂數產生器或其他功用的安全模組，用 IP 來呈現，直接做進去晶片內。等於把幾千、幾萬美金的功用，簡化到一個 IP 去完成，變的非常便宜、方便使用跟安全。也唯有如此，硬體安全才能普及化。而對我們公司而言，也多了更多的技術可以授權，收權利金。目前已經有多個客戶導入晶片設計，準備量產。在 COVID-19 發生之後，這部分的需求，大幅增加。因為人類必需因應新常態，就是越來越多的遠端工作及溝通活動。5G 之後帶動的 AI，是 machine talks to machines , IoT 萬物連網，晶片跟晶片溝通，自駕車跟人命有關，security 一定是必要的！我們現在正和很多國際各領域的領導大廠，在討論合作事宜，未來會有越來越多的晶片導入這項技術。

我們現在也在開發軟體，希望將公司轉型成 security as a service 的公司，因爲有 NeoPUF 這個核心技術，我們以後可以做的生意非常多，比如雲端跟物聯網的鑰匙管理，區塊鍊的數位簽章，金融交易的安全認證等，太多的應用都需要！

最後結尾，我用我們董事長成立公司的時候跟同仁講的，他認爲未來每顆晶片都會用到我們的技術，而這個信念會藉由我們的核心技術 NeoBit/NeoFuse/NeoPUF 來實現。