

## 力旺電子 2021 年 第四季線上法說會講稿

2022 年 2 月 10 日 16:00 – 17:00

### 董事長引言：

各位股東，平安！感謝各位股東抽空來參加我們的法說會。

2021 年是我們成立 21 年最好的一年，就各項營運指標：成長性及獲利率，特別是在 tape out 數，我們完成 614 個設計定案，幾乎每天都有 2 個產品導入我們的技術，經過多年的技術開發和認證，我們的在先進製程的產品導入正在加速，這將繼續推動我們未來幾年的增長勢頭。這些動能將會延續我們的成長到未來幾年。

展望今年，我們會持續我們的成長動能，特別是在 security 的相關技術會有大幅成長。除了我們推廣以久的取代 eFuse 的趨勢，還有從雲端到消費端，各項應用晶片對於導入更加安全 IP 的需求。為什麼我們的 PUF 相關 IP 是最好的選擇，因為我們是目前最容易且是最安全去產生加密系統裡最重要的亂數機制，等一下我會針對這方面再做說明。

接下來，我們請總經理何明洲先生對去年第四季營運報告及未來展望做說明。

### 總經理營運報告：

各位股東，午安。

首先，我就先針對 2021 年第四季的營運結果向各位作個報告：

- 1) 在營收方面，本季營收為新台幣 6 億 3 仟 1 佰 3 拾 9 萬 8 仟元，較前一季增加 6.2%，也比去年同期成長 27.1%。
- 2) 在營業費用方面，本季營業費用為 2 億 9 仟 9 佰 6 拾 7 萬 7 仟元，較上一季增加 7.9%，也比去年同期成長 14.7%，主要是因為薪資等人事費用增加、及相關獎金增加。

- 3) 在營業淨利方面，較上一季增加了 4.8%，也比去年同期成長 40.9%。營業淨利率方面，較上季減少 0.8 個百分點為 52.5%，但比去年同期成長 5.1 個百分點。
- 4) 總結，2021 第四季的 EPS 為新台幣 3.86 元，股東權益報酬率為 51.4%。

今年整年度的營收為 23 億 6 仟 3 佰 8 拾 2 萬 4 仟元，較去年同期成長了 33%，營業費用增加了 14.8%，營業淨利率成長了 7.4 個百分點為 53.7%。EPS 為新台幣 14.78 元，股東權益報酬率為 49.3%。

在總體營收中，我們分授權金及權利金來做說明：

- 1) 首先，第四季的授權金佔本季營收 25.8%，金額較上一季減少 13.8%，但比去年同期成長 5.3%。以美金計價，金額較上一季減少 13.6%，但比去年同期成長 9.4%。
- 2) 在權利金方面，權利金佔營收比重為 74.2%，金額較上一季成長 15.6%，也比去年同期增加了 37%。以美金計價，金額較上一季成長 15.1%，也比去年同期增加了 41.6%。
- 3) 2021 年整年度的總營收較去年同期成長了 33%，授權金與權利金各成長了 43.4% 和 29.1%。以美金計價營收較去年同期成長了 40%，授權金與權利金各成長了 51.1% 和 35.8%。

在整體營收中，再以各個技術對營收貢獻來區分：

- 1) NeoBit 主要應用在成熟製程，第四季授權金較上一季減少 39.7%，也比去年同期減少 11.2%，貢獻了本季 14.5% 的授權金。在權利金部分，NeoBit 貢獻 42.4%，較上一季成長 3.7%，也比去年同期增加了 1.5%。
- 2) NeoFuse 技術主要應用在先進製程，它對第四季的授權金貢獻 63.4%，較上一季增加了 10.4%，但比去年同期減少 6.3%。在權利金部份，NeoFuse 在第四季貢獻了 54.8%，較上一季增加 27.3%，也比去年同期成長了 89.6%。
- 3) 以 PUF 為基礎的 Security IP 在第四季貢獻了 11.6% 授權金，比上季成長 580.4%，比去年同期成長 639.6%，原因是來自各項應用的強勁需求，很多案子延續到今年，預期會持續強勁成長。
- 4) 在 MTP 技術方面，佔授權金 10.5%，授權金較上一季減少 68.2%，但比去年同期增加了 11.3%。權利金貢獻較上一季增長 6.3%，也較去年同期成長 17.6%，佔權利金營收的 2.7%。

在 2021 年整年度，

- 1) 來自 NeoBit 的授權金較去年同期成長 45.9%，但權利金減少 3.8%，佔 2021 年全年度總體營收的 38.8%。
- 2) NeoFuse 授權金較去年同期成長了 15.6%，權利金也成長 91.6%，營收佔比超過 Neobit，貢獻了 2021 年全年度的整體營收 51.9%。
- 3) 以 PUF 為基礎的 Security IP 授權金比去年同期成長了 140.9%，佔全年度整體營收的 1.2%。
- 4) 來自 MTP 相關技術的授權金較去年同期成長 220.8%，權利金也增加 12.1%，佔全年度整體營收的 8.1%。

若以 8 吋及 12 吋晶圓區分：

- 1) 8 吋晶圓權利金，佔第四季權利金營收的 50.3%，較上一季增加 11.2%，也比去年同期成長 13%。
- 2) 12 吋晶圓權利金，佔第四季權利金營收的 49.7%，較上一季增加 20.3%，也比去年同期成長 74.4%。

第四季完成的設計定案有 163 個，創歷史單季新高，顯示我們 IP 需求仍非常強勁，在稍後發佈的營運報告有更詳細的說明。

接下來向各位報告未來的展望，我們預期今年第一季會延續成長動能。

- 1) 授權金方面：授權金會增長，因我們的 IP 需求相當強勁，特別是 NeoFuse 和 PUF 相關解決方案。
- 2) 權利金方面：我們預期 8 吋及 12 吋權利金將持續成長動能，除了出貨量持成長外，還有平均每片權利金價格。
  - a) 受惠於 5G 手機、車用和 IoT 相關的 PMIC、MCU、Fingerprint 及 Sensor 相關應用的量產增加，我們預期 8 吋權利金能持續成長。
  - b) 12 吋的應用類別及量產規模持續增加，特別在 TDDI、OLED、ISP、DTV、STB、WiFi 6/6E, Bluetooth、Ethernet、Switch、TWS 及 DRAM 等應用，會持續帶動權利金強勁成長。12/16 奈米及 7 奈米 FinFET 的權利金在第四季已經開始貢獻，預期可望繼 28nm 之後，成為下一個成長動能。

在新應用開發上：

- 1) 我們新應用開發的重點是在安全防護的領域，NeoFuse 取代 eFuse 做為密鑰儲存已經是趨勢，應用都往更先進製程，我們的 OTP 也導入 7 奈米及 6 奈米車用製程。
- 2) 目前也有 PUF-based 相關 IP 的導入，在 IoT、工業自動化、AI、區塊鏈、FPGA、Data Processor Unit (DPU)、Mobile Storage (UFS) 及自動駕駛應用上持續開展。PUFrt (信任根 IP) 及 PUFcc (安全處理器 IP) 也已經在不同應用中有客戶導入。
- 3) 我們 2/7 已發布新聞稿 ARMv9 機密運算選擇我們的 PUFrt 做為最重要的信任跟運作基礎，這是公司成立以來相當重要的進展，今年會有一系列共同行銷的活動開展。

在新技術發展上：

- 1) 在第四季，我們有發佈公司安全強化型一次可編程 (OTP) 矽智財 NeoFuse 在台積電 N5 製程開始設計定案，是一個整合 NeoFuse OTP 與 NeoPUF 安全矽智財的安全 OTP，並且延續 7 奈米支援多樣化的產品應用，包括高階到中階行動產品、消費性應用、人工智慧、網通、5G 基礎架構、繪圖處理器、DPU、以及高效能運算，目前正在進行可靠性驗證，也正與多家客戶討論合作。
- 2) 我們的 ReRAM IP 已通過聯電 40nm 驗證，而 22nm 開始設計定案。我們是世界上第一家提供這種新興記憶體並為車用、邊緣運算、AI 和 AIoT 市場提供更全面解決方案的公司之一。我們會將 ReRAM 技術擴展到更先進的製程和一些特殊製程，例如 BCD 和高壓製程。
- 3) 我們持續開發新的安全功能 IP，包括以 PUF 為基礎的安全協處理器及以 PUF 為基礎的 secure element。
- 4) 為 BCD 和 28 奈米及下的嵌入式快閃記憶體開發 NeoFlash，以解決傳統嵌入式快閃記憶體技術問題。

接下來，我把時間交給董事長。

### 董事長說明 PUF 對於隨機數產生的重要性：

首先，隨機數有什麼用途？

*“隨機數是密碼系統的基本要件，用於將不可預測的數據注入加密算法和協議，使產生的數據流不重複且幾乎不可猜測”*

## 什麼是密碼學？

*“密碼學是一種資訊安全策略，是保障資訊安全的藝術和科學。”*

為了保障資訊的安全，需要三個要素：

1. 身份認證：身份認證確保連線另一端的人確實是他所自稱的人。
2. 機密性：機密性確保只有交易的授權人才能提取有意義的資訊。
3. 完整性：完整性確保交易資訊在從發送者到預期接收者的途中沒有未檢出的變更或干擾。

隨機數是數據安全所有面向的基礎因為它可和密碼學一起使用，使數據變得不可預測和不可猜測。

然而安全機制的強度與其使用的數字隨機性成正比。如第 16 頁所示，如果隨機性夠高，則使用隨機數加密后的數據可能是不可見的。

## 產生隨機數的方法

### 軟體隨機數產生器

現代電腦程式可以使用軟體所產生的偽隨機數，而不是真隨機數。由於電腦只是受人類指令支配的機器，它只會重複人類設定它執行任務的幾個步驟。因此，電腦本身不可能產生無法預測的數據，所以無法產生隨機數。

軟體隨機數產生需要一個種子，作為數學演算法的輸入以產生偽隨機數。

然而，使用軟體產生的隨機數存在三個缺點：

1. 初始化方程式需要一個種子值。
2. 產生的數字序列最終會自我重複。
3. 隨機數是數學產生的，因此不具有真隨機性，這表示軟體產生的隨機數無法提供高等級的加密保護。

基本上，為了提供高安全等級，我們必須求助於物理世界來提取本質上真正具有隨機性的東西，從中我們可以得到真隨機數。真隨機數是物理設備產生的東西，在它被產生之前我們無法得知其數值。

### 硬體隨機數產生器

硬體隨機數不需要種子，因為它們不是計算出來的數值，也不是通過可重複算法得出的。

那接下來的問題是，我們可以確定哪些過程或設備的行為是真的不可預測的？

**例如：**

我們可以通過每 10 秒計算一次交叉路口的乘客人數來找到一個隨機數。如果數字是奇數，我們可以將其設置為 “1”。如果數字是偶數，我們將其設置為 “0”。2560 秒後我們可以得出一個 256 位元的隨機數。

對於 256 位隨機數，要正確猜測它的概率為

$$1 \text{ 除以 } 2^{256} = 2^6 \times 2^{250} = 64 \times (10^3)^{25} = 64 \times 10^{75} \approx 10^{77}; \frac{1}{10^{77}}$$

$10^{77}$  是 1 後面有 77 個零，(1 兆是  $10^{12}$ )。這幾乎是零！

另一個例子，我們可以量測左右兩個電晶體的寬度。即使繪製的寬度相同，在製造後的寬度仍可能略有不同。若左側較長則設置為 “1”，若左側較短則設置為 “0”。通過量測 256 對電晶體，我們可以獲得 256 位隨機數。

**但在上述舉例中，有幾點需要注意：**

1. 這不能在晶片上以電子方法完成。
2. 隨機性不夠；例如，對於上述提到的乘客舉例，取決於交叉路口是否繁忙，我們可能會得到多個連續的 1 或 0。對於電晶體寬度的舉例，製程影像可能會發生偏差，使電晶體在某一側的寬度總是比另一側長。

因此，我們真正需要解決的問題是：

- 1) 隨機數需要能夠在晶片上以電子方法進行量測。
- 2) 隨機數的隨機性需要夠高，以至於無法預測或被重現。

在 NeoPUF 的發明中，我們提取了電子在電晶體閘極介電層中發生的量子穿隧行為。

穿隧行為與介電薄膜的品質高度相關。薄膜品質的微小差異將導致穿隧機率具有的明顯的差異。因此我們可以量測兩個相鄰電晶體閘極介電層的電子穿隧行為，如果右側的穿隧電流較大，我們將其定義為數字“0”，若電流較小則定義為數字“1”。從 256 對相鄰的電晶體當中，我們可以產生 256 位元的隨機數。

這樣的行為具有真隨機性，原因為： 1) 因為薄膜是均勻地生長在矽基板上，由電晶體不同而造成的穿隧行為差異無法被預測。 2) 穿隧電流可以透過電子方式進行量測。 3) 薄膜品質的差異呈現隨機分佈，因此產生的隨機數具有高隨機性。

我們可以在每個晶片上通過提取量子穿隧效應來產生隨機數，作為控制晶片安全性的唯一硬體密鑰。

透過 PUF 產生的隨機數，我們建構了數個基本的安全功能，例如信任根(PUFrt)、安全協處理器(PUFcc)和安全元件 (PUFse)，提供了一個高度安全的新架構。

這次發佈和安謀 (Arm)的合作以及和英特爾晶圓代工服務(Intel Foundry Service) 的合作，主要方向都是基於我們量子穿隧 PUF 專利(NeoPUF)的安全解決方案，包含硬體信任根(hardware root-of-trust)以及安全協同處理器(secure co-processor)。

為了能在雲端應用(cloud application)做好機密運算(confidential computing)，PUF-based 硬體信任根在下一代 CPU 是極為重要的，所以安謀選擇熵碼科技的旗艦產品 PUFrt 作為 Armv9 機密運算參考架構的安全子系統。PUFrt 完整整合密鑰生成與安全存儲，以及安全運行中不可或缺的真亂數產生器。這次的合作可幫助客戶在設計的一開始在選用運算核就把安全設計一起無縫導入。

放眼未來 security 在 AI、DPU、FPGA、IoT、車載等各個應用的重要性和需求成長，此次和 IFS 的合作即是一個很好的管道，讓英特爾晶圓代工先進製程平台上的客戶可直接導入我們的安全 IP，以符合當前產業對於安全供應鏈以及零信任(zero-trust)相關應用上的需求，尤其是美國市場。我們的共同願景是讓全球客戶在享有先進製程提供的運算效能時，也擁有最好的晶片安全設計。

### **董事長結論：**

我們會不斷努力的創新，提供客戶更好的 IP 與安全解決方案，也會為股東帶來更高的回報。公司會持續朝向每顆晶片都會用到我們的 IP 的目標前進。感謝各位股東長期對力旺的支持！