

# 力旺電子 1Q23 線上法說會講稿

2023 年 5 月 10 日, 16:00-17:00

## 開場致詞

---

### 徐清祥, 董事長

各位股東，平安！感謝各位股東抽空來參加我們的法說會。

儘管上半年權利金受整體代工廠產能利用率低的影響，我們對下半年及未來的營運成長，仍舊相當有信心。

今年的成長動能會由 security 相關的授權帶動授權金大幅成長。在過去兩年累積了超過 1000 個新產品設計定案，隨著客戶新的產品陸續進入量產階段，就會帶動我們權利金持續長期成長趨勢。而我們的技術開發已經到了 3nm，5nm 客戶也即將 tape out，6/7nm 客戶導入也在加速，這些都會增強我們未來成長的動能。

接下來，我們請總經理何明洲先生對今年第一季營運報告及未來展望做說明。

## 營運報告

---

### 何明洲, 總經理

#### 第一季營運結果

各位股東，午安。

首先，我就先針對 2023 年第一季的營運結果向各位作個報告。

在營收方面，本季營收為新台幣 6 億 6 仟 7 佰 7 拾 5 萬 1 仟元，較前一季減少了 26%，也比去年同期少了 8.2%。

在營業費用方面，本季營業費用為 3 億零 6 拾 5 萬 7 仟元，較上一季減少了 18.3%，也比去年同期少了 4.2%，主要是因為獎金減少所致。

在營業淨利方面，較上一季減少了 31.3%，也比去年同期少 11.2%。營業淨利率方面，較上季減少了 4.2 個百分點為 55%，也比去年同期少了 1.8 個百分點。

總結，2023 第一季的 EPS 為新台幣 4.2 元，股東權益報酬率為 38.9%。

在總體營收中，我們分授權金及權利金來做說明：

1. 首先，第一季的授權金佔本季營收 21.4%，金額較上一季增減少了 30.3%，也比去年同期少了 25.3%。
2. 在權利金方面，權利金佔營收比重為 78.6%，金額較上一季減少了 24.8%，也比去年同期少了 2%。
3. 2023 第一季的總營收比上一季減少了 26%，與去年同期比較減少了 8.2%。

#### 第一季營收貢獻分析

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，第一季授權金較上一季減少了 22.6%，也比去年同期少了 19.8%，貢獻了本季 19.7%的授權金。在權利金部分，NeoBit 貢獻 30.5%，較上一季減少了 31.1%，也比去年同期少了 23.2%。
2. **NeoFuse** 技術主要應用在先進製程，它對第一季的授權金貢獻 49.6%，較上一季減少了 28.5%，也比去年同期減少了 42.9%。在權利金部份，NeoFuse 在第一季貢獻了 67.8%，較上一季減少 21%，但比去年同期增加了 16.3%。
3. 以 **PUF 為基礎的 Security IP** 在第一季貢獻了 11.5%授權金，比上季少了 60.7%，但比去年同期成長了 138.2%。權利金在第一季貢獻甚少，較上一季減少了 93.8%，也比去年同期少了 46.3%。
4. 在 **MTP 技術方面**佔授權金 19.2%，授權金和上一季相當，但比去年同期增加了 8.4%。權利金貢獻較上一季減少了 19.8%，也較去年同期少了 58.2%，貢獻了 1.7%的權利金。

## 第一季營收分析–Wafer Size

若以 8 吋及 12 吋晶圓區分：

1. **8 吋晶圓** 權利金，佔第一季權利金營收的 47%，較上一季減少了 25.5%，也比去年同期少了 9.2%。
2. **12 吋晶圓** 權利金，佔第一季權利金營收的 53%，較上一季減少了 24.1%，但比去年同期增加了 5.3%。

第一季完成的設計定案有 137 個，在稍後發佈的營運報告有更詳細的說明。

## **未來展望**

---

### 何明洲, 總經理

接下來向各位報告未來的展望，我們預期第二季會是營運的低點，主要是受晶圓代工廠利用率持續下降的影響，隨著過去兩年的新產品投入生產，我們預計整體營運會在下半年恢復動能。

**授權金方面:** 授權金今年會有大幅成長，由 PUF 相關 security solution 帶動。

**權利金方面:** 隨著過去兩年累積的 1000 多個新 tape out 陸續進入量產，權利金將恢復成長動能。

在新技術及應用發展上：

1. PUF-based solution 今年會導入 5/6/7nm CPU、DPU、AI 及車用相關應用。
2. 持續與代工廠開發 NeoFlash，用以推動成熟製程滲透率。
3. 與 CPU 合作夥伴持續往最先進製程開發安全解決方案。

接下來，我把時間交給董事長。

## 董事長言論

---

徐清祥, 董事長

### How PUF-based Solutions Secure ChatGPT and AI

#### **(Page 12: How PUF-based Solutions Secure ChatGPT and AI)**

AI 在 ChatGPT 中的應用是現在熱門話題。就在上個月，三星的員工不小心透露了機密的消息，讓全球的公司意識到 ChatGPT 也有風險。今天，我將和你們討論駭客可能如何攻擊 ChatGPT 或其他 AI 系統的運作，並解釋 PUF 如何保護 AI 應用。

#### **(Page 13: Asking ChatGPT about Security)**

ChatGPT 是一個很棒的工具，甚至可以回答最複雜的問題，所以我們決定問問他自己本身是否意識到它也需要安全保護，以及它會如何保護自己。

如右邊截圖所示，當被問“如何保護 ChatGPT 時”，答案就列在那裡了。我們 highlight 了一些我們認為重要的關鍵字，並根據要點列出了我們公司如何幫助解決這些問題。

1. 對應到第一點 → PUF 能夠產生加密用的金鑰。
2. 同樣的，第二點提到身份驗證和權限控管 → 我們可以使用 PUF 作為唯一身分識別 (UID)，並產生密鑰供身份驗證使用。
3. 第三點是 ChatGPT 如何識別安全漏洞 → 這同樣也需要系統能夠辨別使用者。PUF 正好能夠產生對應的身份識別碼。
4. 第四部分是 ChatGPT 如何定期更新和修復係統 → 這通常是通過無線方式完成的，PUF-based IP 能藉由數位簽章來保護軟韌體更新。
5. 最後，第五點是關於安全重要性的訓練 → 隨著導入硬體安全的程度越高，我們越能降低人為失誤的風險。

考慮到這些要點，我們的安全解決方案很適合用在 AI 應用，我將在下面先解釋如何保護 AI。

## **(Page 14: Major Attacks in AI)**

在了解我們的 PUF 安全解決方案如何保護 AI 之前，我們必須先了解在 ChatGPT 和 AI 系統上常見的幾種攻擊類型。

**Poisoning attack**: 若駭客竊改了訓練資料，訓練完的模型會被大大影響，等同駭客能夠操縱訓練結果。

**Backdoor attack**: 駭客也可能替換模型，加入特定場景才會啟用的類神經元，好比後門程式一樣。

## **(Page 15: Major Attacks in AI cont.)**

**Evasion attack**: 即便是已經訓練好的模型，駭客也可以改 Input data 導向錯誤的結果。

**Stealing attack**: 對 AI 的開發或使用者而言，訓練資料、模型參數、用戶資料等都是珍貴的 know-how，有任何一種被偷去都會造成巨大的損失。

## **(Page 16: How to Prevent Attacks on AI)**

所描述的這四種攻擊方法是所有 AI 都可以被攻擊的方式，從訓練到輸出結果。每種類型的攻擊都需要不同的保護方法和解決方案。

**Poisoning attack**: 問題是訓練資料可能被汙染。我們需要對訓練資料進行和數位簽章以防止這種情況發生。

**Backdoor attack**: 最大的問題是修改、替換甚至竊取模型。這不僅需要簽章，還需要額外的加密和密鑰管理，以防駭客取得模型。

## **(Page 17: How to Prevent Attacks on AI cont.)**

**Evasion attack**: 針對 input data 的攻擊方式，駭客可以改輸入的 input 影響 model 或結果。這就是為什麼我們必須使用唯一識別碼(UID)對用戶進行身份驗證，對資產進行加密。

**Stealing attack**: 最後一種攻擊是竊取所有 AI 資產。為了避免攻擊者取得有價值的數據和專有技術，我們需要 UID、簽章、加密和 anti-tampering 設計來阻止攻擊者破解 AI 運作的硬體。

## (Page 18: Securing AI with PUF-based Solutions)

在我們提到的所有問題中，PUF 可以起到解決這些問題的作用。

我們開發了兩種類型的安全 IP：一種是硬體信任根，另一種是加密協處理器。

我們的信任根 IP (PUFrt)結合了 PUF(Physical Unclonable Function)、安全強化的 OTP 和真隨機亂數產生器(TRNG)。此外，我們還加了多種抗攻擊技術來預防各式攻擊。

不止於此，我們的加密協處理器(PUFcc)帶有上述功能，並也有內建的密碼學算法硬體加速器。

除了支持所有國際標準的密碼學算法以外，我們還提供有韌體和軟體，讓我們的加密協同處理器能夠支持更進階的安全協議和應用。

在了解 ChatGPT 的 AI 的每個階段的風險之後，不難看出 PUF -based 安全解決方案能夠滿足 AI 產品生命週期的所有安全需求。從訓練資料 到推論結果，必須保護 AI 開發者的 know-how 不被複製和竊取。PUF -based IP 能以低成本提供極強的安全防護，是最適合保護 AI 的矽智財方案。

接下來，我們會開始 Q&A 的環節。

## 結論

---

### 徐清祥, 董事長

如果大家想了解更多有關公司在安全 IP 的進展，歡迎上 PUFsecurity 的官網 <https://www.pufsecurity.com/> 上看，有很多文章跟課程。

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!