力旺電子 2024 Q2 線上法說會講稿

2024 年 8 月 7 日, 16:00-17:00

開場致詞

徐清祥, 董事長

各位投資股東，大家午安，感謝大家來參加今天的法人說明會，也非常感謝股東長期以來的支持。

如同前幾季所講，公司已進入多年成長循環。上次法說提到我們已在全球的各代工廠建製超過 600 多個製程平台，而平台的數量每年都在持續增加，我們建構在這些平台的技術從 OTP 進展到各種更複雜的 security IP，MTP 也擴展到各種新型記憶體。隨著，1) 製程更先進、2) 記憶體功能更強、3) 晶片安全 IP 的功能更強，我們每片晶圓收到的 IP 權利金也將隨之增加。

稍後我會介紹我們其中一項 security IP 技術，PUFtrng (以 PUF 為基礎的亂數產生器)，它的速度比目前傳統的 TRNG 快 100 倍，這是因為我們利用了我們的 PUF (晶片指紋，完美的亂數來源)作為絕佳的隨機來源。

這說明我們可以持續利用我們既有的技術和 IP，開發出各種具有附加功能的 IP。這不僅彰顯了我們自有技術的重要性和競爭力，也讓我們能在核心競爭力上持續創新，是我們長期成長的重要根基，因此我們對公司的未來非常有信心。

接下來，我們請總經理何明洲先生對今年第二季營運報告及未來展望做說明。

營運報告

何明洲，總經理

第二季營運結果

各位股東，午安。
首先，我就先針對 2024 年第二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 8 億 9 仟 3 佰零 1 萬元，較前一季增加了 11.2%，比去年同期增加了 28.2%。

在營業費用方面，本季營業費用為 3 億 9 仟 7 佰 8 拾 2 萬 9 仟元，較上一季增加了 4.1%，也比去年同期多了 21.3%。

在營業淨利方面，本季營業淨利為 4 億 9 仟 5 佰 1 拾 8 萬 1 仟元，較上一季增加了 17.7%，且比去年同期成長了 34.3%。營業淨利率方面，較上季增加了 3.1 個百分點為 55.5%，也比去年同期成長了 2.6 個百分點。本季淨利為 4 億 7 仟 5 佰零 9 萬 6 仟元，較上一季增加了 10.3%，也比去年同期增加了 35.1%。

總結，2024 年第二季的 EPS 為新台幣 6.36 元，股東權益報酬率為 67.3%。

在總體營收中，我們分授權金及權利金來做說明：

1. 首先，第二季的授權金佔本季營收 33.6%，金額較上一季增加了 31.3%，且比去年同期成長了 20.0%。
2. 在權利金方面，權利金佔營收比重為 66.4%，金額較上一季增加了 3.3%，且比去年同期增加了 32.8%。
3. 2024 第二季的總營收比上一季增加了 11.2%，且與去年同期比較增加了 28.2%。

以 2024 上半年度來看，

1. 授權金佔上半年整體營收 31.1%，較去年同期增加了 34.4%。
2. 權利金則貢獻了上半年整體營收 68.9%，比去年同期增加 20.2%。
3. 2024 上半年總營收與去年同期相比，增加了 24.3%。

<u>第二季營收貢獻分析</u>

在整體營收中，再以各個技術對營收貢獻來區分：

1. **NeoBit** 本季授權金較上一季增加 54%，且比去年同期成長了 30.2%，貢獻了本季 24.6%的授權金。在權利金部分，NeoBit 貢獻 26.7%，較上一季增加了 11.3%，也比去年同期增加了 15.9%。
2. **NeoFuse** 對本季的授權金貢獻為 33.3%，較上一季減少了 16.7%，也比去年同期減少了 11.9%。在權利金部份，NeoFuse 在本季貢獻了 70.6%，較上一季增加了 0.2%，且比去年同期成長了 39%。
3. **以 PUF 為基礎的 Security IP** 在本季貢獻了 12.5%的授權金，比上季增加了 105.2%，且比去年同期增加了 36%，惟權利金在本季貢獻低於 1%。
4. **在 MTP 技術方面**佔授權金 29.6%，授權金比上一季增加了 110%，也比去年同期增加了 69.9%。權利金貢獻較上一季成長了 11.6%，也較去年同期成長了 86.8%，貢獻了 2.7%的權利金。

2024 上半年營收分析–產品線

在 2024 上半年度，

1. **來自 NeoBit** 的授權金較去年同期成長 43.4%，權利金成長了 1.4%，佔 2024 上半年總體營收的 24.9%。
2. **NeoFuse** 授權金較去年同期成長了 19.3%，權利金也成長 27.3%，貢獻了 2024 年上半年的整體營收 62.3%。
3. **以 PUF 為基礎的 Security IP** 授權金比去年同期成長 26.3%，權利金貢獻低於 1%，佔上半年整體營收的 3.3%。
4. **來自 MTP 相關技術**的授權金較去年同期增加 64.3%，權利金增加 75.7%，佔上半年整體營收的 9.5%。

第二季營收分析–Wafer Size

若以 8 吋及 12 吋晶圓區分：

1. **8 吋晶圓**權利金，佔第二季權利金營收的 42.5%，較上一季增加了 2.6%，且比去年同期增加了 26.7%。
2. **12 吋晶圓**權利金，佔第二季權利金營收的 57.5%，較上一季增加了 3.8%，也比年同期增加了 37.6%。

第二季完成的設計定案有 171 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。

授權金方面：受到晶圓廠和晶片公司強勁需求的推動，授權金將繼續保持增長動能。

權利金方面：由於新應用在先進製程開始量產，我們預期下半年權利金逐季成長。

在新 IP 技術及業務發展上

特殊製程 (如：HV in FinFET、BCD、emerging memory 及 embedded flash)：

1. NeoFuse 在 HV 製程正往 FinFET 發展，以滿足客戶下一代 OLED DDI 的需求計畫。
2. RRAM 隨著客戶需求的增加，正擴展到更多的製程。
3. NeoFlash 持續發展特殊製程，以替代 embedded flash 與 external NOR flash。
4. 正與第一線的代工廠合作開發 2nm 技術。

在 Business 合作平台上

1. 用於新 CPU 架構的 security IP 將開始貢獻營收。
2. 已成功將 NeoFuse 整合進 EDA 公司的 SRAM repair 相關產品功能中。

接下來，我把時間交給 Charles。

董事長言論

徐清祥，董事長

(Page 13: A Must in Security: 100X Faster PUF-based TRNG)

面對日益複雜的攻擊，真隨機數產生器(TRNG)在增強安全系統防禦上極為重要。今天，我將帶各位探討為什麼擁有隨意一種 TRNG 是不夠的，您需要的是高速且高品質的 TRNG。

(Page 14: True Randomness Makes Guessing Impossible)

在了解隨機性如何保護安全系統之前，我們必須先知道攻擊這些系統的方法。這張投影片將解釋為什麼真隨機數產生器(TRNG)對於硬體安全是必要的。

有兩種方法可以侵入安全系統。第一個是密碼分析，這是一種存在了幾個世紀的技術，攻擊者可以利用它來發現加密演算法的弱點。這種攻擊推動了加密標準的發展，從較舊的演算法如資料加密標準(DES)，到取而代之的新演算法像是高級加密標準(AES)。

第二種方法是 implementation attack，它針對系統中的特定弱點。這些攻擊利用這些弱點來發現安全系統內的秘密。

現在，假設我們有一個設計良好的安全系統，可以抵抗密碼分析和 implementation attack，那麼攻擊者如何侵入系統？在這種情況下，攻擊者仍然會嘗試猜測密鑰，因為拿到密鑰之後就可以從系統中取得很多機密訊息。

為了防止攻擊者正確猜出密鑰，我們必須把攻擊者正確猜到密鑰的機率降到最低。第一個要素是密鑰長度，它是由加密演算法預先定義的。例如，如果密鑰長度為 128 位元，則表示可以產生 2^128 (2 的 128 次方)個可能的密鑰組合。

第二個要素是隨機生成高亂度的密鑰，以確保每一組密鑰產生的機率都相等。參考此圖可以看到，在使用隨機生成的密鑰加密後，攻擊者猜中密鑰組合的機率降低到 1/2^128 (1/2 的 128 次方)。

因此，為了達到這個結果並減少攻擊者猜中密鑰的可能性，我們必須使用 TRNG。

(Page 15: High-speed TRNG: Why Throughput Matters?)

在下一張簡報中，我將解釋為什麼擁有高速 TRNG 很重要。這裡指的高速是代表高產出，也就是在短時間內產生大量隨機數的能力。

TRNG 的速度和產出量很重要，因為大型系統通常有許多應用程式和硬體元件需要使用隨機數。而這些元件無法自己產生隨機數，必須依賴基於硬體的 TRNG。由於需要隨機數的元件數量眾多，TRNG 能快速且有效的產生隨機數就非常重要。

除了能產生大量隨機數外，高產出和高品質的 TRNG 還可以抵抗 side-channel attack。Side-channel attack 是最常見的攻擊形式之一，攻擊者利用從功耗或電磁輻射等來源所洩漏的資訊來找到密鑰。為了對抗這些攻擊，必須不斷產生新的隨機數來屏蔽 side-channel 資訊。中間的圖為一個受屏蔽保護的加密操作的簡化範例。在屏蔽操作中，隨機位元將輸入資料轉換為兩個獨立的集合，並傳送到兩個單獨的屏蔽操作。與單一操作相比，將它們分開可以確保不會洩漏密鑰。這樣的操作會不斷消耗隨機數，因此 TRNG 的產出量在這個案例中也相當重要。

除了安全性之外，還有其他高度依賴隨機數的應用，例如銀行業務。銀行業務中有許多交易都是需要帳號對應的密碼才能完成，因此需要高品質的隨機數來確保機密性和安全性。由於銀行客戶的交易量是非常大的，因此高產出的 TRNG 也至關重要，如底部第三張圖所示。

(Page 16: PUFtrng: 100 Times Faster than Conventional TRNG)

了解到高產出和高品質 TRNG 的重要性後，我們的解決方案 PUFtrng 很明顯符合這些標準。

我們的 TRNG 其中一個獨特之處是它有兩個熵源。與依賴單一來源的傳統 TRNG 不同，我們的 PUFtrng 將環形振盪器的動態熵(會不斷變化)與 NeoPUF 晶片指紋的靜態熵(是常數且不變的)相結合。

由於收集自然雜訊的過程非常耗時，動態熵運行緩慢，導致傳統 TRNG 的產出較低，如下方虛線所示。這種情況下的產出通常小於每秒一兆位元。

為了克服這個限制，PUFtrng 使用 PUF 產生的高品質隨機位元來提高動態熵源的輸出。這樣我們就可以透過減少動態熵的收集時間來實現高輸出量，並確保高品質的輸出。如圖所示，在相同功耗下，PUFtrng 的產出量約為傳統 TRNG 的 100 倍。

(Page 17: PUFtrng: 100 Times Faster than Conventional TRNG)

我們也製作了動畫來更好地展示 PUFtrng 和傳統 TRNG 之間的差異：

在圖 1 到圖 4 中，我們發明了一個簡單的拓樸優化(topology optimization)來定義亂數產生器的隨機性。圓圈內線條的均勻性代表數字的隨機性。如果數字是真正隨機的，當有更多隨機數生成，圓圈內部就會開始均勻填充。另一方面，如果生成的數字隨機性較差，則圓內的線條將不會均勻分佈。

- **環形振盪器產生的動態熵 (圖 1)：**在藍色圓圈內，一條藍線代表一個 10 位元隨機數。動態熵會不斷產生隨機資料。然而，它的輸出品質對於金鑰來說是不夠的，因為線條往往出現在相似的位置，表示隨機數不均勻。
- **使用後處理的傳統 TRNG (圖 2)：**傳統的亂數產生器是透過從動態熵逐漸累積更多隨機位元(線)來產生的。隨著時間的推移，經過後處理後，輸出(圓)會慢慢變得均勻且完整。
- **由 PUF 產生的靜態熵 (圖 3)：**由 PUF 生成，靜態熵可以立即準備就緒，不會隨時間變化。線條非常均勻，表示結果從一開始就具有非常高的品質。
- **透過 PUF 改良的 PUFtrng (圖 4)：**在 PUFtrng 中，產生的數字形成均勻的線條，表示高品質的輸出。此外，PUFtrng 生成速度比傳統的 TRNG 快得多。從圖中可以明顯看出生成速度的差異：PUFtrng (圖 4)中的線產生的輸出(圓)比傳統 TRNG (圖 2)中的線產生的速度快得多。

另一種比喻的方式是將傳統 TRNG 想像成經典老車，車子可以正常運作，但效率不高。它們可能速度很慢，或是在快速行駛時消耗大量汽油。相較之下，PUFtrng 就像一輛新能源汽車，它的運行速度快，功耗低。最後，PUFtrng 的另一個優點是動態熵和靜態熵均在 hard macro 中實現，並在各種技術節點上進行驗證，相較於其他 IP 供應商或客戶以 RTL 為基礎的 TRNG，有更卓越的品質。

最後總結，整合高速、高產出的 TRNG 對維護系統安全和功能至關重要。我們的 PUFtrng 解決方案優於他者方案，可有效率地產出高品質隨機數。不僅可以防止複雜的

攻擊，也支援大容量隨機數產生。我們的 PUFtrng 正在為高品質 TRNG 樹立更高的標準。

以上就是我們本次的分享內容，謝謝您的聆聽。

接下來，我們將進入 Q&A 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!