力旺電子 2Q23 線上法說會講稿

2023 年 8 月 9 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。

今年上半年為公司營運的低點，隨著過去累積的新產品設計定案進入量產階段，下半年營運會逐季往上。下半年會有 6/7nm 的客戶應用陸續進入量產階段，5nm 客戶導入自駕、data center 及 AI 相關應用，與 CPU 夥伴在 3nm 的合作順利進行，我們對公司未來多年成長，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 2023 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 6 億 9 仟 6 佰 6 拾 2 萬 5 仟元，較前一季增加了 4.3%，但比去年同期少了 12.5%。

在營業費用方面，本季營業費用為 3 億 2 仟 7 佰 8 拾 6 萬 5 仟元，較上一季增加了 9%，主要是因爲獎金增加所致。

在營業淨利方面，較上一季增加了 0.5%，但比去年同期少了 19.9%。營業淨利率方面，較上季減少了 2.1 個百分點為 52.9%，也比去年同期少了 4.9 個百分點。

總結，2023 第二季的 EPS 為新台幣 4.71 元，股東權益報酬率為 53.5%。

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 35.8%，金額較上一季增加了 74.6%，也比去年同期多了 24.4%。
2. 在權利金方面，權利金佔營收比重為 64.2%，金額較上一季減少了 14.8%，也比去年同期少了 25%。
3. 2023 第二季的總營收比上一季增加了 4.3%，但與去年同期比較減少了 12.5%。

第二季營收貢獻分析

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，本季授權金較上一季增加了 101%，也比去年同期多了 27.6%，貢獻了本季 22.7%的授權金。在權利金部分，NeoBit 貢獻 30.5%，較上一季減少了 14.6%，也比去年同期少了 42.8%。
2. **NeoFuse** 技術主要應用在先進製程，它對本季的授權金貢獻 45.4%，較上一季增加了 60%，也比去年同期多了 20.5%。 在權利金部份，NeoFuse 在本季貢獻了 67.5%，較上一季減少 15.3%，也比去年同期少了 10.2%。
3. **以 PUF 為基礎的 Security IP** 在本季貢獻了 11%授權金，比上季增加了 66.3%，但比去年同期減少了 41.4%。權利金在本季貢獻低於 1%，較上一季增加了 123.3%，但比去年同期少了 18.8%。
4. **在 MTP 技術方面**佔授權金 20.9%，授權金比上一季多了 89.9%，也比去年同期增加了 239%。權利金貢獻較上一季減少了 1.6%，也較去年同期少了 58.4%，貢獻了 1.9%的權利金。

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 44.5%，較上一季減少了 19.2%，也比去年同期少了 34.5%。
2. **12 吋晶圓**權利金，佔第二季權利金營收的 55.5%，較上一季減少了 10.9%，也比去年同期少了 15%。

第二季完成的設計定案有 147 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，我們預期下半年營運會逐季成長。

授權金方面: 下半年授權金可望較上半年大幅成長。

權利金方面: 隨著新應用陸續進入量產階段，我們預計下半年權利金逐季成長。

在新技術及應用發展上:

1. 5nm 設計授權需求強勁，今年會導入自駕、Data Center 及 AI 相關應用.

2. 3nm 驗證在多家代工廠順利開展，客戶也提出需求，我們跟 CPU 合作夥伴的進展也很順利，持續開發更高等機密運算。

3. 22nm 新興記憶體 MRAM 及 ReRAM 陸續完成驗證，也開始導入客戶產品設計。

接下來，我把時間交給董事長。

董事長言論

徐清祥, 董事長

Page 12: Forefront of Security: Confidential Computing:

大家應該還記得我之前的演講有提到的機密運算 (Confidential Computing)，現在比兩年前變得更重要了。今天我會更詳細地描述機密運算、Nvidia 怎麼使用機密運算來保護 GPU，以及用 PUF 的機密運算與其他方法有甚麼不同、為什麼它更安全。

(Page 13: What is Confidential Computing?)

許多應用電腦程式處理個資等數據，例如健康或金融服務，或因為某些法規，都可能被未經授權的使用者透漏，影響到數據的機密性和完整性。這也就是為什麼我們需要建立機密運算，也稱為“通過在硬件的可信執行環境中執行計算來保護正在使用的數據”。（Nvidia 給出的機密計算的官方定義）

這張圖我以前用過，但我想重申一下數據的工作原理。數據由不同的階段組成：data-at-rest, data-in-transit and data-in use。為了確保使用中數據的完整性和機密性，需要機密運算。

在機密運算中，部署可信執行環境（TEE）來提供與主操作系統分離的環境，不暴露於系統其餘部分的情況下處理數據。

(Page 14: Confidential Computing Illustrated)

這張圖描述了機密運算怎麼保護資料，例如，核心處理單元 (CPU) 具有安全區域和非安全區域。常規 CPU 上的應用程式和操作系統無法訪問安全區域。然而，通過機密計算，來自應用程序/操作系統的數據可以儲存在 CPU 上單獨隔離的 TEE 下的安全區域。

(Page 15: Confidential Computing in Nvidia’s GPU for AI)

機密運算的另一個例子是圖形處理單元 (GPU)。GPU 擁有自己的硬體信任根 (HRoT)，可啟用隔離的 TEE，以在從 CPU 傳輸到 GPU 以及在 GPU 中進行處理的過程中保護數據和代碼的完整性和機密性。

Nvidia 使用機密運算進行人工智慧訓練。如圖所示，在從 CPU 到 GPU 的代碼/數據傳輸過程中，通過 GPU 的 HRoT 創建多個單獨的 TEE，從而防止未經授權的實體訪問 AI 應用程式和代碼。

因此，TEE 需要具有強大的硬體的安全性，透過硬體新信任根來保護：

1. 設備認證：這與上一個場景相反——即，當用戶/設備與 GPU 通信時，他們還必須確認 GPU 的硬體和軟體是否安全，在操作系統/應用程序與 GPU 之間通信時也要進行身份驗證，以確保其未被篡改。

2. 從 CPU 到 GPU 的數據完整性和機密性：更好的理解方式是，正在傳輸的數據將使用 CPU 和 GPU 專有的加密密鑰進行加密/解密。

(Page 16: PUF-based HRoT for TEE)

現在我們大概了解了 TEE 的作用，接下來讓我來解釋一下 HRoT (Hardware Root of Trust)的作用。TEE 中的 HRoT 可以幫助保護數據和代碼的完整性和機密性。它由密鑰儲存、密鑰生成、密鑰保護和密碼引擎組成，所有這些相結合以實現全面的安全性。

我們的 PUF 的加密協處理器 IP (PUFcc)可以實現上述所有功能。我們的安全 OTP 由反熔絲技術和 PUF 的技術組成，可創建安全的密鑰儲存，從而向潛在攻擊者隱藏密鑰及其行踪， PUF 的 TRNG 也可以有效地生成真正的隨機密鑰來保護數據和代碼。

PUFcc 還包括附加組件和加密工程，用於執行加密/解密、身份驗證和簽名等安全功能。

(Page 17: PUF-based Key Storage vs. Traditional)

對於 HRoT，我想通過將我們自己的技術與傳統方法進行比較來重點關注密鑰生成和密鑰儲存。我們基於 PUF 的 OTP 通過提高密鑰儲存和密鑰生成的安全性，幫助行業遷移到非常高級別的安全機制。

傳統密鑰儲存 eFuse，其不安全的原因有很多：

1. 保險絲的燒毀：eFuse 需要保險絲的燒毀來確定密鑰（是 1 還是 0）。通過查看哪個保險絲被燒毀，這種方法很容易進行逆向工程。保險絲還存在“重新生長”的風險，因為薄金屬片有時會自行重新連接，從而導致鑰匙消失。

2. 容量：eFuse 的另一個問題是由於良率損失，它無法克服 8kbit 的密度。因此，隨著技術向更先進的節點遷移，eFuse 已經不夠用了。

借助我們的反熔絲 OTP (NeoFuse)，我們不會面臨任何逆向工程、尺寸/密度甚至密鑰消失的問題。我們在電晶體級別使用電子穿隧方法，這種方法可以隨著製程節點的縮小而在顯微鏡下看不到。

將我們的 OTP 與基於 PUF 的技術相結合，使密鑰儲存更加安全。當與晶片間不同的 PUF 獨特值一起使用時，密鑰的地址可以被加擾並儲存在安全 OTP 上的唯一隨機位置，從而使密鑰儲存超級安全。

(Page 18: PUF-based Key Generation vs. Conventional)

密鑰產生目前用的傳統亂數產生成器 (TRNG)，不是 PUF 做出來的。

通過三個類別中比較 PUF 的 TRNG 與傳統 TRNG， PUF 的 TRNG 勝出，原因如下：

1. 熵（隨機程度）：PUF 的 TRNG 具有更好、更高的熵，因為它源自 PUF 種子和其他隨機源，使其成為真正的隨機。傳統的 TRNG 使用數位電路來生成具有低熵且短 100 倍的隨機數。

2. 速度：TRNG 的另一個關鍵特性是速度。對於 PUF 的 TRNG，產生大量密鑰/RNG 的速度大約快 100 倍。另一方面，傳統的 TRNG 需要更多的後處理，這會降低速度。

3. 功耗：最後，PUF 的功耗也降低了 100 倍左右，這又與傳統 TRNG 需要的後處理有關，導致使用更多的成本和能源。

(Page 19: Summary)

1. 機密計算是人工智能應用程序的 GPU 中必須的，因為它提供了數據和代碼的完整性和機密性。

2. 和傳統的信任根比較，eMemory 硬體信任根以 PUF 提供最好的身份(UID)、安全密鑰儲存和更快的密鑰生成速度，促進 CPU/GPU/DPU 的機密計算。

上述所有這些差異就是機密計算架構從傳統解決方案轉向 PUF 的原因。例如，Arm 正在 v9 Confidential Computing 設計中採用我們的解決方案，隨著我們的技術進展我們能夠在先進製程吸引更多客戶。

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!