力旺電子 2024 Q4 線上法說會講稿

2025 年 2 月 12 日, 16:00-17:00

開場致詞

徐清祥, 董事長

各位股東和投資先進，

謝謝你們來參加這一次的法說會，如同前幾季所講，我們正處於一個多年的成長循環，從近期的授權案看出，各項技術都在加速導入應用，我們對未來非常有信心。

最近大家關注的焦點，在 AI 運用有機會會加速落地到 edge 端，這樣的發展，對我們而言，是非常正面的事。

我們的各項技術，從 OTP、MTP 到 Security 一系列 IP，都是在幫助晶片能夠達到更高的效能、更低的成本及更高的安全性，因為邊緣運算對功耗、效能、成本及安全性的整體要求更高，會促使客戶加速導入我們的 IP，從近期在網通、遠端遙控、智慧型監控及其他邊緣相關項授權案就可以看出。另外，美國大公司對量子電腦何時商用化時程的爭論，不管是 5 年或者 15 年以上，由於量子電腦可以在短時間內破解現行保護全球大多數資料與基礎設施的加密標準，硬體的轉換需要至少 5-10 年以上的時間，所以美國國家標準局(NIST)推出後量子加密標準，因應量子電腦所帶來的資安威脅。後量子加密的轉換，對我們的 PUF-based solutions 包含我們新開發的 PQC IP，是個巨大的機會。等一下，我就這方面跟大家說明。

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。

營運報告

何明洲，總經理

第四季營運結果

各位股東，午安。

首先，我就先針對 2024 年第四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 10 億 1 仟零 7 拾 1 萬 7 仟元，較前一季增加了 12.4%，比去年同期增加了 12.4%。

在營業費用方面，本季營業費用為 4 億 4 仟 4 佰 7 拾 8 萬 4 仟元，較上一季增加了 12.7%，也比去年同期多了 23.8%。

在營業淨利方面，本季營業淨利為 5 億 6 仟 5 佰 9 拾 3 萬 3 仟元，較上一季增加了 12.1%，且比去年同期成長了 4.9%。營業淨利率方面，較上季減少了 0.1 個百分點為 56%，也比去年同期減少了 4 個百分點。本季淨利為 5 億 1 仟 4 佰 6 拾萬 8 仟元，較上一季增加了 24.3%，也比去年同期增加了 27.5%。

本季營業利益率相較於去年同期減少 4 個百分點，主要是因為薪資酬勞的增加，因爲公司的員工分紅是以稅前淨利的 15%為基準，而今年第四季業外有匯兌收益，相較去年第四季是匯兌損失，導致業外造成的員工分紅費用差異。

總結，2024 年第四季的 EPS 為新台幣 6.89 元，股東權益報酬率為 62.5%。

在總體營收中，我們分授權金及權利金來做說明：

1. 首先，第四季的授權金佔本季營收 31.2%，金額較上一季增加了 8.5%，也比去年同期成長了 15.1%。
2. 在權利金方面，權利金佔營收比重為 68.8%，金額較上一季增加了 14.2%，且比去年同期增加了 11.3%。
3. 2024 第四季的總營收比上一季增加了 12.4%，且與去年同期比較增加了 12.4%。

以 2024 年整年度來看，

1. 授權金佔整體營收 31.4%，較去年同期增加了 22.5%。
2. 權利金則貢獻了整體營收 68.6%，比去年同期增加 16.4%。
3. 2024 總營收與去年同期相比，增加了 18.2%。

第四季營收貢獻分析

在整體營收中，再以各個技術對營收貢獻來區分：

1. **NeoBit** 本季授權金較上一季減少 27.2%，且比去年同期減少 8.3%，貢獻了本季 20.9%的授權金。在權利金部分，NeoBit 貢獻 24.8%，較上一季增加 9%，也比去年同期增加 26.1%。
2. **NeoFuse** 對本季的授權金貢獻為 39.1%，較上一季增加 41.9%，也比去年同期增加 5.1%。在權利金部份，NeoFuse 在本季貢獻 73.1%，較上一季增加 16.7%，且比去年同期成長 7.8%。
3. **以 PUF 為基礎的 Security IP** 在本季貢獻了 22.6%的授權金，比上季增加 104.1%，且比去年同期增加 138.7%，惟權利金在本季貢獻低於 1%。
4. **在 MTP 技術方面**佔授權金 17.4%，授權金比上一季減少了 30.1%，也比去年同期減少 0.2%。權利金貢獻較上一季減少 5.4%，較去年同期減少 13.8%，貢獻 2%的權利金。

2024 年營收分析–產品線

在 2024 整年度，

1. **NeoBit** 的授權金較去年同期成長 22.2%，權利金成長了 14.7%，佔 2024 年總體營收的 25.2%。
2. **NeoFuse** 授權金較去年同期成長了 7.2%，權利金也成長 16.5%，貢獻了 2024 年整體營收的 61.3%。
3. **以 PUF 為基礎的 Security IP** 授權金比去年同期成長 23.4%，佔整體營收的 4.5%。
4. **MTP 相關技術**的授權金較去年同期增加 59%，權利金增加 30.3%，佔整體營收的 9%。

第四季營收分析–Wafer Size

若以 8 吋及 12 吋晶圓區分：

1. **8 吋晶圓**權利金，佔第四季權利金營收的 40.8%，較上一季增加 13.9%，比去年同期也增加 20%。
2. **12 吋晶圓**權利金，佔第四季權利金營收的 59.2%，較上一季增加 14.4%，也比年同期增加 6%。

第四季完成的設計定案有 181 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。我們也提供了更多技術和製程平台供客戶選擇與應用。

權利金方面：我們預期權利金將持續成長動能，來自於新技術、新製程平台及持續累積新高的設計定案數。在 2024 年，我們的 NTO 也達到歷史新高。

在新 IP 技術上

1. NeoFuse 持續在各種先進製程上開發，目前已在 3/4/5/6/7nm 製程節點上有客戶設計導入。
2. RRAM 正隨著多個客戶設計案的導入持續拓展到更多製程上。此外，我們也正在開發車規 RRAM IP。
3. NeoFlash 持續在特殊製程中發展，逐步取代 Embedded Flash 和 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. 加入 Arm Total Design，並提供 PUFrt 作為 CSS 中 RSE 的硬體信任根。
2. 新開發 PUFhsm，應用於汽車晶片和高效運算的嵌入式硬體安全模組解決方案。PUFhsm 結合硬體信任根 PUFrt，提供一個整合的安全解決方案。

接下來，我把時間交給 Charles。

董事長言論

徐清祥，董事長

(Page 13: Why Post-Quantum Cryptography (PQC) Needs PUF?)

(Page 14: Why PQC Needs PUF?)

隨著我們走向量子電腦可能破解現有加密技術的未來，後量子密碼學 (PQC) 變得更加重要。

PQC 專注於開發能夠抵禦量子電腦攻擊的加密系統。但為了確保 PQC 有效，我們需要可靠的方法來產生密鑰並維護這些加密系統的完整性。這就是 PUF 發揮作用的地方。

PUF 可以高效生成 PQC 所需的長密鑰，因為 PQC 的安全性依賴這些長密鑰來防禦量子運算威脅。 PUF 可以安全且高效產生建立這些長密鑰所需的唯一秘密。因此，PUF 是提供 PQC 密鑰的理想解決方案。
此外，PUF 能高效提供隨機數，這對於 PQC 抗攻擊來說至關重要。PQC 本質上是使用長密鑰來保護資料。除了抵抗量子攻擊外，加密系統還必須包含抗攻擊功能，以保護演算法中的密鑰及加密資料免受物理攻擊。隨機性對於掩飾資料處理至關重要，由於 PUF 天然具有隨機性和唯一性，因此可以有效地產生亂數，並用於抗攻擊設計中，有效實現抗攻擊的目標。

(Page 15: What is PQC?)

現在我來解釋一下什麼是 PQC。PQC 代表後量子密碼學，其中包括保護資料免受量子電腦潛在威脅的加密算法。量子電腦在解決特定的數學問題方面有望勝過傳統電腦。這

對許多加密算法，尤其是被廣泛使用的 RSA 和 ECC 構成嚴重威脅，因為它們的安全性是依賴於量子電腦可以有效解決的問題。PQC 算法提供安全通訊和資料保護，即使面對量子運算的進步，量子電腦成為現實，讓我們的互聯世界依然安全。

(Page 16: Why is PQC Needed?)

那麼，為什麼 PQC 現在就如此重要? 隨著量子運算的進步，對能夠抵禦量子攻擊的加密的需求變得迫切。我們今天使用的許多系統都會長期保留加密資料，有時長達數年甚至數十年。想想金融交易、個人資訊或敏感的政府資料，如果這些資料採用易受量子攻擊的方法加密，那麼將來可能會面臨風險。我們越早實施 PQC，就越早能保證我們的資料在有量子的未來保持安全。

為了因應後量子世界，美國國家標準與技術研究所 (NIST) 持續帶頭開發能夠抵禦量子運算攻擊的新型加密標準。經過多個評估階段，NIST 於 2024 年正式宣布以 Module-Lattice Based Key Encapsulation (ML-KEM)、Lattice-based Digital Signature、Hash-based Digital Signature 作為 PQC 演算法標準。全球各地的組織也正在採用這些新標準來保護我們的資料免受潛在的量子威脅。而我們將在本季推出基於前兩個標準的 PQC IP。

(Page 17: How PUF-based Solutions Help PQC?)

考慮到我們的資料在未來保持安全的必要性，以及開發新加密系統所需的時間，現在開始轉換到 PQC 非常重要。這樣，當量子電腦足夠強大到構成威脅時，我們已經做好準備。

通常，PQC 算法需要更高的運算複雜性和更長的密鑰儲存需求。接下來，我來解釋我們的 PUF-based Solutions 如何幫助 PQC。我們的 PUF-based Root of Trust (PUFrt) 由以下幾個組件組成。首先，NeoPUF 能為每個裝置生成唯一的 ID，用於為 PQC 產生長密鑰。再來是 NeoFuse OTP (OTP)，一種用於儲存 PQC 密鑰的面積高效且安全的方案。與 eFuse 相比，OTP 提供更高的安全性，特別是在先進製程中，同時對於更大的資料量也有更高的面積效率。

包括 PQC 在內的現代加密技術容易受到側信道攻擊 (Side-Channel Attacks)，因此，我們的解決方案內建真隨機數產生器 (TRNG)，可持續提供大量隨機數。這些隨機數對於阻止破壞 PQC 密鑰的攻擊非常重要。

此外，為了成功轉換到 PQC，加密系統必須同時適應傳統演算法和 PQC 演算法，並能夠在兩種算法或混合解決方案之間靈活選擇。透過將 PUFrt 整合到安全子系統中，可以有效整合 PQC 演算法所需的大型複雜密鑰管理，以及一般傳統演算法的密鑰生成管理。如剛剛所提到，PUFrt 可以產生高品質且唯一的 PQC 密鑰，並安全地儲存在 OTP 中，保護其機密性和完整性，同時防止未經授權的存取和篡改。此外，TRNG 也會持續產生大量隨機數，用於抵抗 Side-Channel Attacks，增強系統內密鑰管理的整體安全性。

總結來說，為了在量子運算威脅下確保我們資料的長期安全，整合 PUF-based Solutions 的安全子系統相當重要。這種方式可以讓我們在轉換到 PQC 時，維持高度安全性與靈活性。

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!