eMemory 3Q26 Earnings Call Q&A Transcript

November 13th, 2026, 16:00-17:00 Taiwan Time

Q&A Transcript

1. **PUF-based Security IP 已占公司營收一成以上，授權金年增數倍；但市場上正在討論 AI 資本支出的可持續性。若未來雲端業者資本支出下修，對公司 Security IP 業務的影響會有多大？**

>> Security IP 的成長有三個乘數：

第一是滲透率：Hardware Root of Trust 正從選配變成標配，Caliptra、Arm 的 RSE，以及 NIST 的 PQC 時程，都是推動它成為必要條件的力量。例如，Arm 最新一代資料中心運算子系統 Neoverse CSS V3，已將我們的 PUFrt 作為 Runtime Security Engine 的核心元件。

第二是每顆晶片的內容：從一個 OTP macro 逐步擴展到完整的 Security Subsystem，再加入 PQC，同一顆晶片的授權金與權利金都會更高。

第三是製程：這些晶片多採用先進製程，每片晶圓的權利金遠高於成熟製程。

我們現在 PUF 才開始要進入量產階段，基期相當低。這與 AI Server 發展初期類似，先求有、求快，優先將效能發揮到極致，因此 Security 並非主要考量。Caliptra 也是 2 年前才開始逐步建立相關規範，加上近期發生全球性資安事件，即使整體資本支出放緩，硬體安全反而會更加速進展！

加上 Security IP 也不只應用在資料中心，車用、工業與 MCU 都正在導入；資料中心之後，Edge AI 與機器人也會是下一波。

2. **AI 讓駭客攻擊變得更快更難防，但晶片設計到量產要好幾年。力旺如何確保現在設計的晶片，在未來幾年內依然安全？**

>> AI 大幅加快了駭客發掘系統漏洞的速度，這意味著單靠軟體防毒及防護機制，已經不足以因應未來的資安威脅。安全防護必須從晶片最底層的硬體架構開始建立。

力旺的防禦策略分為兩道防線：「主動預防（Proactive Prevention）」與「入侵後控制（Post-Breach Containment）」。

第一道防線：建立無法複製的晶片身分（預防入侵）

透過力旺的 PUF（物理不可複製功能）技術，每一顆晶片在製造過程中，都能產生獨一無二、無法複製的「數位指紋」，作為硬體信任根（Hardware Root of Trust）。

這個獨特的晶片身分，可以用來保護關鍵金鑰，並確保系統每次開機時都能進行安全開機（Secure Boot），從晶片底層建立可信任的安全基礎，防止未經授權的程式或攻擊者入侵。

第二道防線：內建硬體緊急煞車機制（入侵後快速復原）

面對日益強大的 AI 駭客攻擊，我們不能只是假設系統永遠不會被入侵，而是必須確保即使遭到攻擊，駭客也無法竊取敏感資料，或長期掌控系統。

為此，力旺結合 PUF、非揮發性記憶體（NVM）及金鑰管理技術，建立硬體層級的緊急應變機制：

- 即時隔離與金鑰失效： 一旦偵測到異常，系統可透過硬體安全機制隔離遭到入侵的區域，使可能暴露的金鑰失效，並透過密碼學機制安全抹除機密資料。

- 安全重新啟動： 威脅排除後，系統可利用底層可信任的硬體身分，重新產生金鑰，恢復系統正常運作。

總結來說，AI 時代的晶片安全，不只是如何防禦攻擊，更重要的是遭受攻擊後，如何迅速控制風險、恢復系統，建立具備快速復原能力的資安韌性（Cyber Resilience）。

這也是力旺長期投入硬體安全 IP 創新的核心方向。

3. 開源資安架構 Caliptra 把邏輯跟演算法都免費開放了，客戶為什麼還要付費向力旺授權？我們的專利到底保護了什麼？另外，中國全力推半導體自主化，力旺如何防範 IP 被仿製或繞過的風險？

>> 謝謝這個非常關鍵的問題。

我可以從技術護城河與商業模式兩個維度來向大家報告：

第一，開源標準化，對力旺來說不是競爭，而是把市場大餅做大。開源的 Caliptra 確實把資安的「設計藍圖與演算法引擎」免費化了，這大大降低了客戶導入資安的門檻。但大家要明白，資安最核心的根基在於實體物理層（Physical Layer）。這就好比設計圖再好，房子還是要裝上實體的保險箱與鑰匙。每一顆晶片，不論是 1.0 還是加了 PQC 演算法的 2.x，都需要三樣與半導體製程高度綁定的硬體元素：晶片的專屬身份 ID、存放金鑰的 OTP，以及合格的亂數熵源。演算法可以開源，但這三樣硬體元件無法開源。力旺這一千多件專利，保護的就是「如何在每一家晶圓廠、每一個節點，穩定製造出這些硬體物理信任根」。Caliptra 越普及，客戶越需要我們的 NeoFuse 和 NeoPUF 來做底層支撐，我們的 IP 就能越快在各種晶片中重複導入。

第二，關於中國市場自主化與 IP 防製的風險。力旺擁有非常獨特且穩固的商業模式護城河。我們的 IP 是直接內嵌在晶圓代工廠的製程平台裡面，OTP/MTP 的權利金是向晶圓代工廠收取，只要客戶在該平台投片生產，代工廠就會依產量計算權利金給我們，即使終端晶片公司使用 PUF 相關 IP，需要支付額外的權利金，我們也能依據晶圓代工廠提供的量產片數，按照合約收取。從源頭就杜絕了被客戶私自拷貝或繞過的可能性。

4. 今年下半年 AMD、Intel、Arm、Google、Meta 都發表了新一代資料中心晶片，AI 晶片不再只有 Nvidia 一家。公司提到 Arm 最新的資料中心運算子系統已採用 PUFrt。請問這些非 Nvidia 的平台是否也採用 Caliptra 安全架構？力旺在 Arm、AMD、Intel 這些生態的滲透程度，與在 Nvidia 生態相比如何？

>> Caliptra 是 AMD、Google、Microsoft、NVIDIA 在 OCP 與 CHIPS Alliance 共同推動的，它是雲端業者定的規格，不分晶片商，所以不論平台是誰的，每一顆資料中心晶片都要有可驗證的身分。我們在非 Nvidia 生態的進展其實很具體：Arm 最新一代資料中心運算子系統 Neoverse CSS V3，已經把我們的 PUFrt 作為 Runtime Security Engine 的核心元件，代表採用 Arm CSS 的 CPU 客戶都會帶到我們；與 Intel Foundry 的合作聚焦在 14A, 18A 的 PUF；整合 Caliptra 子系統的 PUFrt 也已被多家 BMC、SSD 與網通晶片廠採用。我們不押單一生態，哪個平台贏，裡面都有我們的 IP。

5. 公司授權金（License Fee）與權利金維持成長，但觀察到每季公告的 Tape-out（開模/定案）總數卻較過去下滑，請問經營團隊如何解讀這個趨勢？這背後代表了怎樣的客戶與製程結構變化？

>> Tape-out 總數的變化，反映的是半導體產業「大者恆大」、研發資源向先進製程集中的結構性趨勢。對力旺而言，這是「質的提升」超越「量的增長」，我們主要從兩個層面來解讀：

第一，客戶研發策略由「多點布局」轉向「集中資源開發旗艦產品」。力旺在成熟製程已建立極高的滲透率，累積超過 2,000 家晶片客戶。過去兩年，隨著先進製程與 AI / 高效能運算需求快速成長，我們許多主要客戶重新調整研發資源配置：過去一年可能在成熟製程進行約 10 顆 Tape-out，如今則將資源集中於 7 奈米、5 奈米乃至更先進的節點，每年精準導入 1 至 2 顆旗艦級產品。

第二，單一 Tape-out 的價值（ASP）顯著提升。先進製程晶片的開發成本與技術門檻極高，相應的授權金（License Fee）與未來量產權利金（Royalty），均較成熟製程高出數倍。因此，雖然 Tape-out 總數因客戶研發聚焦而減少，但單一案件的價值大幅提升，整體授權金與未來營收貢獻反而持續強勁成長。

總結而言，Tape-out 總數的變化並不代表需求下滑，而是力旺的客戶結構正加速向高價值的先進製程移轉，對公司中長期的獲利結構是正面且健康的發展。

6. 面對 Synopsys、Cadence、Rambus 等大廠的 Root of Trust（信任根）方案，以及晶圓代工廠免費的 eFuse，力旺（eMemory）的差異化與護城河是什麼？是否有被取代的風險？

>> 1. 技術差異化：OTP 與 PUF 互補，打造完整安全架構

PUF 物理防複製功能，相對晶圓廠 eFuse 需將金鑰寫入儲存，有被破解風險；力旺的 NeoPUF 利用晶片製造的物理特性「即時生成」獨一無二的金鑰，不需直接儲存原始秘密，安全性更高。

從元件到系統的整合： OTP（儲存設定）與 PUF（生成金鑰）互補，再結合加密引擎，能提供從底層硬體身分到完整 Root of Trust（如 PUFrt、PUFcc）的一站式解決方案。

2. 競爭護城河：跨代工廠與跨製程的量產經驗

力旺深耕邏輯製程非揮發性記憶體（Logic NVM）逾 20 年，擁有跨晶圓代工廠、跨製程節點的技術平台與龐大量產實績。對於需要跨廠生產、先進製程或高可靠度的客戶而言，IP 的可移植性與驗證經驗是競爭者短期難以複製的。

3. 競合關係與市場區隔（為何不會被取代）

與 大部分的 EDA/IP 大廠是「合作」而非純競爭： 全球最大 IP 公司 ARM，是我們客戶，全球前十大 IP 公司有 5 家也是客戶。提問中提到的兩家也同時提供我們的 OTP 或 PUF，共同為客戶打造更完整的安全方案。

與晶圓廠 eFuse 做出市場區隔： 晶圓廠內建的 eFuse 僅適合「低密度、最基本」的儲存需求；一旦客戶需要高密度、高可靠度，或具備金鑰生成與完整硬體信任根的安全防護，就必須仰賴力旺的專業 IP。

總結：

力旺的策略是與晶圓廠及大廠合作共贏，在 AI、車用與資料中心對硬體安全需求大增的趨勢下，持續從底層 NVM 延伸至完整的硬體安全平台，具備穩固的不可替代性。

7. 隨著 Post-Quantum Cryptography 逐步納入硬體安全架構，公司目前 PQC 相關技術及客戶導入進展如何？PQC 是否有機會成為 Data Center Security 的新成長機會？

>> PQC 我們很早就投入，到今天可以說「標準齊、認證齊、已有客戶導入」。

進度上，我們在 2025 年 3 月推出業界第一個 PUF-based PQC 方案；同年 7 月通過 NIST CAVP 認證，涵蓋 FIPS 203 ML-KEM 與 FIPS 204 ML-DSA；今年 1 月再完成 FIPS 205 SLH-DSA 與 SP 800-208 LMS/XMSS。換句話說，NIST 目前已發布的 PQC 標準我們全部涵蓋。客戶方面，領先的伺服器 BMC 供應商以及 HPC 廠商已經把熵碼 PQC 導入晶片設計。至於是不是資料中心的新成長機會，我的答案是肯定的，理由是：

第一，時間表確定了。NIST 在 10 月 27 日正式定稿 IR 8547：所有 RSA、ECC 不論金鑰長度，2030 年後列為不建議使用、2035 年後禁止。美國 NSA 的 CNSA 2.0 也要求 2027 年起新採購的國安系統設備須符合新標準。

第二，硬體必須現在就做。晶片開機 ROM 裡的驗證演算法、燒在 fuse 裡的公鑰雜湊，tape-out 之後就改不了。今年、明年定案的晶片，量產在 2028 到 2030 年，服役到 2035 年以後，所以現在設計就必須支援 PQC，不能靠事後韌體更新補。NIST 在定稿中也特別點名：硬體安全模組與 TPM 設計週期長，供應商應立即整合 PQC。

第三，市場比 Caliptra 更大。在 Caliptra 裡，PQC 演算法引擎是開源的，但它需要的金鑰種子與熵源可由 PUFrt 提供；而資料中心內的周邊晶片、以及資料中心以外的邊緣 AI 晶片，很多不會整合完整的 Caliptra，卻同樣需要 PQC 安全開機與韌體驗證，需要小面積、低功耗，又能通過 CAVP 認證的 PQC 引擎，這正是熵碼 PQC 產品的目標市場。所以 PQC 讓我們每一個安全專案的內容變多、單價也變高。

8. 目前市場上已經有人宣稱可以利用 AI 取代傳統 EDA，甚至直接設計晶片。請問客戶未來是否可以透過 AI 自行設計晶片，跳過與力旺的 IP 授權合作？這是否會對公司的商業模式造成威脅？

>> 我們認為，AI 確實會改變半導體設計產業，大幅提升設計效率，甚至讓部分過去需要大量人力的設計工作自動化。

但我們必須區分，晶片設計工具的進步，與半導體核心 IP 技術的價值，是兩個不同的層次。AI 可以協助設計電路，但不代表能夠取代一項經過長期研發、製程驗證及實際量產考驗的半導體技術。

以力旺的 Embedded NVM 技術為例，我們的技術從最底層的電晶體結構與元件技術創新開始，有完整且緊密的專利布局與保護，並經過長時間的研發、製程整合、可靠度驗證，以及不同世代晶圓製程的持續優化，最後還必須經過客戶實際產品導入及量產紀錄的驗證。

特別是記憶體技術，可靠度的重要性遠高於單純的設計效率。記憶體儲存的是晶片及系統需要長期保留的資料、設定與關鍵資訊，一旦發生資料遺失或可靠度問題，影響的可能不只是記憶體本身，而是整個晶片功能、系統運作，甚至產品的整個生命週期。

Embedded NVM 通常在產品設計初期就整合進晶片，一旦產品進入量產並廣泛部署，後續更換或重新設計的成本非常高。因此，客戶選擇的不只是能不能把電路設計出來，更重要的是能不能確保這項技術在實際製程及長期使用環境下持續穩定可靠。

這也是為什麼我們的客戶黏著性非常高，一旦導入後，幾乎沒有被替換的情況。對我們這類需要長時間驗證、量產與規模化的實體記憶體與 Security IP 而言，AI 是提升研發效率及技術競爭力的重要工具，而不是競爭者。

9. 公司已經進入 3 奈米及更先進製程，請問 2 奈米以下的技術布局如何？先進製程是否已經形成明顯競爭門檻？

>> 公司一直持續投入先進製程技術開發，3nm 除了主要代工廠已經有多項產品客戶導入及開始量產外，2nm 也預計在明年完成相關驗證，開始進入晶片客戶導入階段。技術開展，也擴及其他代工廠。我們的策略是盡可能提前參與晶圓代工廠及客戶的新製程開發。IP 產業的特性是，從技術開發、晶圓驗證、客戶設計導入到最終量產，通常需要相當長的時間。因此，當一個新製程進入商業量產時，真正有價值的 IP 供應商，往往已經投入多年研發及驗證。公司目前持續布局更先進製程的 OTP 及 PUF-based Security 技術，也同步發展適用於新製程的記憶體 IP。先進製程的競爭，不只是能否完成 IP 移植，而是必須在可靠度、效能、面積、功耗及安全性等方面，符合客戶要求。我們長期累積的製程經驗、專利組合、客戶合作關係及量產紀錄，會是公司非常重要的競爭優勢與護城河！

10. 最近 NVIDIA 的事件讓市場重新關注科技公司的 Key-Man Risk 與接班問題。力旺同樣是一家由創辦人長期帶領、技術導向很強的公司，請問公司是否已有接班人計畫？未來如何確保核心技術、客戶關係及公司策略不會過度依賴單一管理者？

>> 接班不能只看「下一個人是誰」，更重要的是公司的技術、客戶關係與決策能力能不能制度化、團隊化。力旺發展到今天，已經不是由單一個人支撐公司的營運。我們在技術研發、業務、財務及營運管理上，都持續培養完整的管理團隊，也透過董事會與公司治理機制確保公司的長期發展。接班規劃是董事會與管理團隊長期都很重視的議題，但現階段我們不會針對特定人選做評論。對投資人而言，我認為更重要的是，即使管理團隊世代交替，力旺累積的 IP、專利、晶圓廠合作、客戶關係及商業模式都能持續運作，這才是降低 Key-Man Risk 最重要的基礎。