eMemory 4Q25 Earnings Call Q&A Transcript

February 11th, 2026, 16:00-17:00 Taiwan Time

Q&A Transcript

1. **The company continues to highlight growth in foundry and design-in licenses. With foundries expanding capacity and our TAM increasing, why hasn't our royalty revenue growth outperformed the foundries?**

   >> The expansion of TAM does not translate immediately and proportionally into royalty revenue, as there is an inherent time lag between the two. Whether it is technology licensing at foundries or design licensing with chip customers, the cycle from contract signing, design-in, and customer mass production to royalty recognition typically takes time—especially for advanced nodes and more complex applications.

   Over the past two years, while industry growth was concentrated in advanced nodes, many of our licenses were still in the design and integration phase and had not yet reached high-volume production. Currently, our penetration rate among major foundries' 12-inch capacity is around 1.4%. To date, we have built a solid pipeline, with more than 100 tape-outs at 16nm and below. As these designs gradually move into mass production, we see meaningful room for further growth.

2. **Given the rising memory costs that MediaTek and Qualcomm cited as a headwind for consumer demand, how does eMemory view the potential impact on overall business performance?**

   >> This year, revenue contributions from a major U.S. smartphone customer have primarily benefited from increased content per device, including the following factors:

   1. Increased content from modem-related chips, driven by broader adoption across modem modules.
   2. Migration to more advanced processes, with PMICs moving from 0.13μm to 55nm and OLED driver ICs transitioning from 28nm to 16nm, resulting in higher ASP per wafer.
   3. Higher DDI content driven by foldable smartphones, where the number of display driver ICs has increased from one to two per device.

   Furthermore, we also benefit from a natural hedge in the 'after-market.' Even when new smartphone sales slowdown, the demand for replacement panels remains robust. Because every panel replacement requires a new DDI, this inelastic demand allows us to offset any weakness in the new device market and maintain a resilient revenue base.

3. **Using NVIDIA's next-generation platforms, such as Vera Rubin, as an example of the industry's move toward confidential computing and hardware security architectures, could you share more insight into its design-in progress and commercialization timeline in this area?**

   >> Within NVIDIA's Vera Rubin architecture, the integration of Caliptra as a Hardware Root of Trust for rack-scale confidential computing has become a core design. This reflects a pivotal, once-in-two-decades structural upgrade in hardware security. As Agentic AI demands significantly higher security, protection is no longer an optional add-on but a foundational element integrated directly into the silicon architecture.

With the protection provided by Caliptra, model developers like OpenAI and Anthropic can securely deploy their multi-billion-dollar models on third-party cloud platforms. They can trust that even on external servers, their model weights remain encrypted and accessible only to their authorized code.

We have already secured multiple design wins within this framework. As we deepen our collaboration with global CSPs (Cloud Service Providers), our Security IP will support the evolving requirements for hardware security and confidential computing in the upcoming Caliptra 2.0. Combined with the essential demand for SRAM repair in inference chips, we expect our penetration within the AI server market to continue expanding.

4. **Given that 3nm products currently in mass production have not yet contributed to royalty revenue, how should we think about the adoption trajectory at 3nm going forward? What are the key drivers that support future penetration?**

   >> It's common for the initial wave of 3nm SoCs in mass production to utilize design legacies from previous generations as customers prioritize a fast time-to-market. However, we are seeing a clear shift for the next wave of 3nm applications.

   As designs become increasingly complex and security requirements more stringent, customers are moving toward proven, pre-validated, and highly integrated IPs. They need system-level security solutions that can be seamlessly integrated into their advanced architectures. This is precisely where our competitive advantage lies—offering a silicon-proven security foundation that reduces design risk and accelerates deployment for our customers.

5. **Could you share an update on customer adoption progress for Post-Quantum Cryptography (PQC) solutions?**

   >> Our PUF-based PQC hardware security solution has successfully met NIST FIPS 205 and SP 800-208 standards. Covering critical applications such as key exchange and digital signatures, our technology fully complies with NIST's currently defined core PQC specifications and is ready for commercial adoption.

   In terms of application progress, our PQC solutions have already been adopted by several server-related chip customers. These designs utilize our IP to meet NIST-compliant post-quantum security requirements, serving as a critical component of the Hardware Root of Trust within high-security systems.

6. **We've discussed how Post-Quantum Cryptography (PQC) will drive demand for our security solutions. Do you foresee a trend toward localization in this field—where, for example, the U.S. mandates the use of domestic IP providers while China does the same?**

   >> Regarding the localization of security solutions, it is important to note that commercial electronics are part of a global market. For data to be inter-operable across borders, security applications must adhere to the same unified standards. Currently, the global benchmark for security algorithms is primarily set by NIST (National Institute of Standards and Technology) in the U.S. Our PUF-based security solutions provide high-integrity hardware security that aligns with these international standards. This is why we have a robust customer base in both the U.S. and China—because their end-products are designed for and sold to the global market.

7. **Could you please provide a detailed explanation of your agreement with DARPA? If DARPA adopts eMemory's solutions, will DARPA's suppliers also adopt these solutions? If so, how does eMemory proceed with such business opportunities?**

   >> When our technology is adopted within DARPA programs, it indicates that the solution has undergone practical validation in high-security systems, covering key requirements such as hardware root of trust, key protection, and system integration. These programs typically establish reference security design frameworks that enable relevant system suppliers and ecosystem partners to evaluate and consider adoption in subsequent projects.

   In practice, when these suppliers plan products for defense, aerospace, or other high-security infrastructure, they often prioritize architectures that have already been validated through DARPA programs, as this helps reduce both design and qualification risks.

8. **Regarding the trending topic of Co-Packaged Optics (CPO), will your IPs be required for these types of optical communication solutions?**

   >> We already have customers adopting our solutions in 4nm chips, and we also have startup customers that were recently acquired by industry leaders and have adopted our solutions. As data transmission speeds accelerate to 800G and 1.6T, the precision required for optical-electrical conversion becomes extremely high. In the field of Co-Packaged Optics (CPO), our OTP acts as both a 'Digital ID' and a 'Precision Calibration Profile.'

   There are four core reasons why our OTP is essential for CPO:

   1. **Precision Calibration:** Since every silicon photonics chip has slight manufacturing variances, our OTP stores laser power and wavelength parameters to ensure each chip achieves peak transmission performance.
   2. **Security & Authentication:** CPO modules are high-value components for AI data centers. We provide Unique IDs (UID) and Secure Boot to prevent hardware counterfeiting and ensure the integrity of firmware execution.
   3. **Optimized Configuration:** CPO modules contain multiple complex components. Our OTP records hardware revisions and default parameters—such as equalization settings—allowing the system to automatically recognize and optimize the device upon startup, significantly reducing system integration complexity.
   4. **Space Efficiency & Reliability:** Space is extremely limited in CPO packaging. Unlike traditional external EEPROMs, our OTP is integrated directly into the chip. This not only saves critical board space but also ensures data remains permanent and tamper-proof.

9. **Chip iteration cycles have shortened from two years to just one. Is this trend a net positive or negative for the company?**

   >> This is actually a very positive trend for us. As a provider of hard IP, our solutions need to be process-qualified before it can be adopted by customers. In the past, for chips manufactured on the foundry’s most advanced nodes, completing our IP validation in time for first-wave designs was often challenging. As a result, adoption typically occurred when customers migrated from the previous process node.

Now, as customer migration cycles are accelerating, the likelihood of IP replacement also increases, and the transition to the next generation can happen faster. In addition, with chiplet-based architectures, even if the compute die moves to a leading-edge node such as 2nm, our IP can be introduced earlier through a 3nm chiplet and integrated into the main system via advanced packaging.

10. **Could you update us on the collaboration with Arm?**
    >> Our collaboration with Arm has evolved from a pure IP licensing model into broader ecosystem collaboration. On the technical side, we align our Hardware Root of Trust with Arm-based security subsystems and reference designs to support confidential computing in edge AI and cloud data centers. At the same time, we continue integrating OTP and PUF technologies on advanced-node platforms to meet system-level security needs.

11. **Do you have any ASIC customers currently integrating our IPs, and what are the specific applications?**
    >> We have successfully secured multiple ASIC design wins, with several key projects already moving into advanced nodes. Our IPs are being integrated into critical designs such as AI Accelerators, CPUs, ISPs, and high-speed interfaces like SerDes, specifically targeting high-performance applications in AI and HPC.
    Furthermore, we continue to expand the adoption and application of our IPs across advanced process platforms through strategic collaborations with our ASIC design service partners. This collaborative approach allows us to scale our presence and capture the growing demand in the high-end application market.

12. **With the U.S. pushing for localized semiconductor manufacturing, would this pose any challenges to the company, given that it has historically relied primarily on foundries in Taiwan and China?**
    >> Our technology is licensed to foundries and IDMs worldwide, extending far beyond just China and Taiwan. Both U.S. domestic semiconductor companies and major global foundries with manufacturing bases in the United States utilize our IPs. As the demand for advanced nodes and security-integrated platforms continues to surge, we believe this broad geographical presence positions us favorably to capture these growth opportunities.

13. **Who are your main competitors in the Security IP market, and how does your competitiveness compare to theirs?**
    >> When looking at the landscape, we see three other main players: Rambus, Cadence (following their acquisition of Secure-IC), and Synopsys.
    Rambus and Cadence excel in software encryption and protocols, whereas we focus on the hardware physical layer. Because of this, our roles are often complementary—in fact, they are our potential customers.
    As for Synopsys and their SRAM PUF technology, our NeoPUF offers a clear advantage in physical stability. We fully align with the Caliptra hardware standards, and importantly, NeoPUF doesn't require complex error correction or 'helper data.' By eliminating these extra requirements, we significantly simplify the system architecture. Combined with our radiation-hardened reliability, our PUF-based security IPs remain the top choice for high-security applications.

14. **TSMC is reducing its mature node capacity. Does this mean we are losing that market segment entirely?**
>> We observe that foundries are engaging in a strategic reallocation of capacity rather than a simple reduction in mature nodes. Many customers are migrating to advanced platforms—for instance, transitioning PMICs from 8-inch to 12-inch wafers—or leveraging other fab capacity. This shift has no material impact on our customers' production or on our business. In fact, we believe this disciplined capacity management helps stabilize supply and demand, ultimately fostering a more favorable pricing environment.

15. **Have there been recent price hikes for mature nodes? What is our outlook on foundry pricing?**
>> As major foundries adjust their capacity and tighten supply for mature nodes, we are hearing from our customers about potential increase of mature node wafer price. However, the extent of such price adjustment depends on the specific foundry’s strategy and utilization rates. Compared to the previous period of price erosion, the current trend of price stabilization and potential recovery is quite positive for our royalty revenue.

16. **Will PUF become the market mainstream in the foreseeable future? Compared to current security solutions, what specific problems does it solve that make it a 'must-have' for chip designers?**
>>Our PUF technology serves as a Unique ID and a secure key. Beyond its current role in AI accelerators and data center security, it is becoming essential for the expansion of Edge AI and Physical AI. As we move toward an autonomous world, every autonomous device will require a unique identity and its own cryptographic keys to protect both data and assets. We are providing the foundational trust for this future.

17. **As AI tools are reshaping the software industry, do you see any comparable impact or structural change emerging in the semiconductor IP industry?**
>> We believe the IP industry is fundamentally different from pure software services. Regarding AI, we see it as an enabler, not a disruptor. While AI can optimize workflows, it cannot replicate our core value: the invention of the underlying transistor technology. Our moat is built on patented innovations, decades of process know-how, and a silicon-proven track record. These are foundational assets rooted in long-term trust and physical engineering—things AI tools alone simply cannot replace.
As we move into advanced nodes, the requirements for reliability, yield, and security become even more stringent. This increases the industry's reliance on actual mass-production experience and platform-level expertise, which creates a significant barrier to entry. Therefore, rather than diminishing the long-term value of the IP industry, we believe AI will further widen the gap between companies with proven silicon success and those without. It strengthens our competitive moat.

18. **Could management share what tangible results have been observed from the recent transformation initiatives?**
>> We believe our transformation must be reflected in measurable financial results. Over the past year, we have focused on optimizing our costs and processes to build a more resilient, flexible, and efficient business that can better withstand market volatility.
On the revenue side, as long as the foundry pricing remains stable and avoids further declines, our existing business mix is well-positioned for steady growth. On the operational side, through ongoing process

improvements and cost discipline, our operating margin improved by 3.4 percentage points last year. This indicates that our transformation is successfully translating into tangible profitability.

With high margins and low CapEx, our business model is built for operating leverage. As we scale, we expect efficiency gains to drive stronger earnings, while maintaining financial discipline throughout our transformation.