# eMemory 3Q26 Earnings Call Q&A Transcript

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

## Q&A Transcript

1. **PUF-based Security IP now accounts for more than 10% of the company's revenue, with licensing revenue growing several-fold year over year. However, there are growing concerns about the sustainability of AI capital expenditure. If cloud service providers were to cut back on capital spending in the future, how significant would the impact be on the company's Security IP business?**

   >> There are three multipliers driving Security IP growth:

   The first is penetration: Hardware Root of Trust is shifting from an option to a standard feature, and Caliptra, Arm's RSE, and NIST's PQC timeline are all forces pushing it to become a requirement. For example, Arm's latest-generation data center compute subsystem, Neoverse CSS V3, has adopted our PUFrt as a core component of its Runtime Security Engine.

   The second is content per chip: expanding from a single OTP macro to a complete Security Subsystem, and then adding PQC, raises both the licensing fee and the royalty on the same chip.

   The third is process technology: most of these chips are built on advanced nodes, where the royalty per wafer is far higher than on mature nodes.

   PUF is only beginning to enter the mass-production stage, so the base is still quite low. This is similar to the early days of AI servers, when the priority was simply getting products out quickly and pushing performance to the limit, so security was not a primary consideration. Caliptra also only began to gradually establish its specifications two years ago. Coupled with the recent global cybersecurity incidents, even if overall capital expenditure slows, hardware security will in fact accelerate.

   In addition, Security IP is not limited to data centers; automotive, industrial, and MCU applications are all adopting it. After data centers, Edge AI and robotics will be the next wave.

2. **AI is enabling hackers to launch faster and more sophisticated attacks, yet semiconductor IP takes years to move from design to mass production. How does eMemory ensure that chips designed today remain secure years from now?**

   >> AI has accelerated the speed at which hackers discover vulnerabilities, meaning software-based antivirus solutions are no longer enough. Security must be built directly into the silicon foundation.

   eMemory's defense strategy is divided into two lines of defense: 'Proactive Prevention' and 'Post-Breach Containment.'

**1. First Line of Defense**: Creating an Unclonable 'Chip ID' (Preventing Intrusion)

Through eMemory's PUF (Physically Unclonable Function) technology, each chip generates a unique, unclonable 'fingerprint' during manufacturing that serves as a Hardware Root of Trust. This locks down critical keys and ensures secure boot every time the system powers on, stopping hackers at the door.

**2. Second Line of Defense**: Built-in Hardware 'Emergency Brake' (Rapid Post-Breach Recovery)

Facing increasingly powerful AI-driven attacks, we cannot simply assume a system will never be breached. Instead, we must ensure that even if hackers break in, they cannot steal sensitive data or maintain long-term control.

To achieve this, we combine PUF, Non-Volatile Memory (NVM), and key management technologies to create a hardware-level Kill Switch:

**- Instant Isolation & Destruction:** Once an anomaly is detected, the hardware immediately isolates compromised zones, invalidates exposed keys, and cryptographically erases confidential data.

**- Secure Reboot:** Once the threat is neutralized, the system relies on its underlying trusted hardware fingerprint to regenerate new keys and restore normal operations.

In summary, chip security in the AI era is not just about defense—it is about rapid post-attack Cyber Resilience. This remains the core focus of eMemory's long-term innovation in hardware security IP.

3. **Open-source Caliptra makes the Root of Trust architecture, firmware, and even the PQC algorithm engine openly available. Given this, why would chip companies still need to license security IP from eMemory? What exactly do eMemory's extensive patent portfolio and technologies protect?**
**In addition, with China actively pursuing semiconductor self-sufficiency, how does eMemory mitigate the risk of its IP being replicated, reverse-engineered, or circumvented?**

>> Thank you for this very important question.

I would like to address it from two perspectives: our technology moat and our business model.

First, open-source standardization is not competition for eMemory; it makes the overall market bigger. Open-source Caliptra has indeed made the security "design blueprint and algorithm engine" freely available, which greatly lowers the barrier for customers to adopt security. But it is important to understand that the most fundamental foundation of security lies at the physical layer. No matter how good the blueprint is, the house still needs a physical safe and keys. Every chip, whether Caliptra 1.0 or 2.x with PQC algorithms added, requires three hardware elements that are tightly bound to the semiconductor process: a unique chip identity, OTP for storing keys, and a qualified random-number entropy source. Algorithms can be open-sourced, but these three hardware elements cannot. What eMemory's more than 1,000 patents protect is precisely how to reliably manufacture these physical hardware roots of trust at every foundry and every process node. The more widely Caliptra is adopted,

the more customers need our NeoFuse and NeoPUF as the underlying foundation, and the faster our IP can be deployed again and again across all kinds of chips.

Second, regarding China's push for semiconductor self-sufficiency and the risk of IP being copied or bypassed, eMemory has a very unique and robust business-model moat. Our IP is embedded directly in the foundries' process platforms, and the royalties for OTP/MTP are collected from the foundries. As long as a customer tapes out and produces on that platform, the foundry pays us royalties based on production volume. Even where an end chip company uses PUF-related IP and must pay an additional royalty, we collect it under the contract based on the wafer volumes provided by the foundry. This eliminates at the source any possibility of customers privately copying or bypassing our IP.

4. **In the second half of this year, AMD, Intel, Arm, Google, and Meta all announced new-generation data center chips, and AI chips are no longer limited to Nvidia. eMemory has noted that Arm's latest data center compute subsystem has adopted PUFrt. Do these non-Nvidia platforms also adopt the Caliptra security architecture? How does eMemory's penetration of the Arm, AMD, and Intel ecosystems compare with its penetration of the Nvidia ecosystem?**

>> Caliptra is jointly driven by AMD, Google, Microsoft, and NVIDIA through OCP and CHIPS Alliance. It is a specification defined by cloud service providers and is vendor-neutral. Therefore, regardless of whose platform it is, every data center chip needs to have a verifiable identity. Our progress in non-NVIDIA ecosystems is quite concrete. Arm's latest data center compute subsystem, Neoverse CSS V3, has adopted our PUFrt as a core component of its Runtime Security Engine, which means that CPU customers adopting Arm CSS will also bring our IP with them. Our collaboration with Intel Foundry focuses on PUF at 14A and 18A. PUFrt integrated with the Caliptra Subsystem has also been adopted by multiple BMC, SSD, and networking chip vendors. We are not betting on any single ecosystem. Whichever platform wins, our IP will be in it.

5. **The company's license fees and royalties have continued to grow, but the total number of tape-outs disclosed each quarter appears to have declined compared with the past. How does management interpret this trend? What does it indicate about changes in the company's customer mix and process-node mix?**

>> The change in total tape-outs reflects a structural trend in the semiconductor industry, where the big players get bigger and R&D resources are increasingly concentrated on advanced process nodes. For eMemory, this is a case of quality outpacing quantity, and we interpret it from two angles:

First, customers' R&D strategies are shifting from spreading across many projects to concentrating resources on flagship products. eMemory already has very high penetration in mature nodes, with more than 2,000 chip customers. Over the past two years, as demand for advanced processes, AI, and high-performance computing has grown rapidly, some of our major customers have reallocated their R&D resources: where a customer might previously have done around 10 mature-node tape-outs a year, it now concentrates on one or two flagship products a year at 7nm, 5nm, or more advanced nodes.

Second, the value (ASP) of each tape-out has increased significantly. Advanced-node chips have very high development costs and technical barriers, so the corresponding license fees and future royalties are several times higher than those for mature nodes. As a result, although total tape-outs have declined as customers focus their R&D, the value of each project has risen substantially, and overall license fees and future revenue contribution have continued to grow strongly.

So, fewer tape-outs do not indicate weaker demand. Rather, they reflect a shift toward higher-value advanced-node projects, which is positive for our medium- to long-term profitability.

**6. Facing Root of Trust solutions from major players like Synopsys, Cadence, and Rambus, as well as free eFuse offered by foundries, what are eMemory's differentiation and competitive moat? Is there a risk of being replaced?**

>> 1. **Technological Differentiation**: Complementary OTP and PUF for a Complete Security Architecture.

Physically Unclonable Function (PUF): Unlike foundry eFuse, which requires writing and storing keys—leaving them vulnerable to extraction or compromise—eMemory's NeoPUF leverages natural physical variations from chip manufacturing to generate unique keys on the fly without storing raw secrets, offering superior security.

Component-to-System Integration: By combining OTP (for configuration storage) and PUF (for key generation) with cryptographic engines, eMemory delivers a one-stop solution ranging from foundational hardware identity to a complete Root of Trust (such as PUFrt and PUFcc).

2. **Competitive Moat**: Cross-Foundry and Cross-Process Mass Production Experience.

With over 20 years of dedication to Logic Non-Volatile Memory (Logic NVM), eMemory has established technology platforms and an extensive mass production track record across multiple foundries and process nodes. For customers requiring multi-fab manufacturing, advanced nodes, or high reliability, this IP portability and silicon-proven experience cannot be easily replicated by competitors in the short term.

3. **Coopetition and Market Segmentation** (Why We Won't Be Replaced).

Collaboration Rather Than Pure Competition with Most EDA/IP vendors:

5 of the global top 10 IP companies are also our customers (including ARM). Furthermore, two of the major players mentioned in your question also offer our OTP or PUF to jointly build more comprehensive security solutions for customers.

Clear Market Segmentation from Foundry eFuse: Foundry-provided eFuse is only suitable for basic, low-density storage needs.

Once customers require high density, high reliability, key generation, or a complete hardware Root of Trust, they must rely on specialized IP from eMemory.

eMemory's strategy is to achieve win-win partnerships with both foundries and major IP vendors.

**7. As Post-Quantum Cryptography (PQC) is gradually being incorporated into hardware security architectures, what progress has eMemory made in PQC technology and customer adoption? Could PQC become a new growth opportunity for Data Center Security?**

>> We invested in PQC early, and today we can say that we have full standards coverage, full certification, and customers already adopting it.

In terms of progress, we launched the industry's first PUF-based PQC solution in March 2025. In July of the same year, we obtained NIST CAVP certification covering FIPS 203 ML-KEM and FIPS 204 ML-DSA, and in January this year we completed FIPS 205 SLH-DSA and SP 800-208 LMS/XMSS. In other words, we cover all of the PQC standards NIST has published to date. On the customer side, leading server BMC suppliers and HPC vendors have already incorporated PUFsecurity's PQC into their chip designs. As to whether this is a new growth opportunity for data centers, my answer is yes, for the following reasons:

First, the timeline is now fixed. On October 27, NIST formally finalized IR 8547: all RSA and ECC, regardless of key length, will be deprecated after 2030 and disallowed after 2035. The U.S. NSA's CNSA 2.0 also requires that national security system equipment newly procured from 2027 onward comply with the new standards.

Second, the hardware must be done now. The verification algorithms in a chip's boot ROM and the public-key hashes burned into fuses cannot be changed after tape-out. Chips finalized this year and next will enter mass production in 2028 to 2030 and remain in service beyond 2035, so PQC support must be designed in now; it cannot be patched in later through firmware updates. In its final document, NIST also specifically noted that hardware security modules and TPMs have long design cycles, and that vendors should integrate PQC immediately.

Third, the market is larger than Caliptra. Within Caliptra, the PQC algorithm engine is open source, but the key seeds and entropy source it requires can be provided by PUFrt. Meanwhile, many peripheral chips inside data centers, as well as edge AI chips outside them, will not integrate the full Caliptra but still need PQC secure boot and firmware verification, requiring a small-area, low-power, CAVP-certified PQC engine. This is exactly the target market for PUFsecurity's PQC products. PQC therefore increases both the content and the unit value of every one of our security projects.

**8. Some companies in the market are already claiming that AI can replace traditional EDA tools or even design chips directly. Could customers eventually use AI to design their own chips and bypass licensing IP from eMemory? Could this pose a threat to the company’s business model?**

>> We believe AI will indeed change the semiconductor design industry, significantly improving design efficiency and even automating some design work that previously required substantial manpower. However, we must distinguish between advances in chip design tools and the value of core semiconductor IP technology, which are two different levels. AI can help design circuits, but it cannot easily replace technologies that have gone through years of R&D, process integration, reliability qualification, and proven mass production.

Take eMemory's Embedded NVM as an example. Our technology starts from innovation in the most fundamental transistor structures and device technology, protected by a comprehensive and tightly knit patent portfolio. It has gone through long periods of R&D, process integration, reliability qualification, and continuous optimization across successive foundry process generations, and must ultimately be validated by adoption in customers' actual products and mass-production records.

For memory technology in particular, reliability matters far more than design efficiency alone. Memory stores the data, configurations, and critical information that chips and systems need to retain over the long term. If data loss or a reliability problem occurs, the impact may extend beyond the memory itself to the entire chip's functionality, system operation, and even the product's whole life cycle.

Embedded NVM is typically integrated into the chip at the early stage of product design. Once the product enters mass production and is widely deployed, the cost of subsequent replacement or redesign is very high. Customers are therefore choosing not only whether the circuit can be designed, but, more importantly, whether the technology can be assured to remain stable and reliable in actual processes and long-term use environments.

This is also why our customer stickiness is very high: once our technology is adopted, there are almost no cases of replacement. For physical memory and Security IP like ours, which require long periods of validation, mass production, and scale, AI is an important tool for improving R&D efficiency and technological competitiveness, not a competitor.

**9. The company has already entered 3nm and more advanced process nodes. What is eMemory's technology roadmap for 2nm and below? Have advanced process nodes already created meaningful barriers to entry?**

>>We continue to invest in advanced process technologies. At 3nm, multiple customers have already adopted our technologies at a major foundry, with some products entering mass production. For 2nm, we expect to complete qualification next year and begin customer adoption, while also expanding our development to other foundries. Our strategy is to engage as early as possible with foundries and customers on new process nodes. IP development takes a considerable amount of time, from technology development and silicon validation to customer design-in and, ultimately, mass production. By the time a new process enters commercial mass production, the IP suppliers that truly matter have usually already invested years in R&D and validation. We are therefore continuing to develop OTP and PUF-based Security technologies for more advanced nodes, while also developing memory IP for the new processes. At advanced nodes, the barrier is not simply whether an IP can be ported. It must meet customer requirements for reliability, performance, area, power, and security. We believe our accumulated process expertise, patent portfolio, customer relationships, and mass-production track record are very important competitive advantages and a strong moat for the company.

**10. Recent developments at NVIDIA have brought renewed investor attention to key-man risk and management succession at technology companies. Given that eMemory has also been led by its founder for many years and is highly technology-driven, does the company have a succession plan in place? How does eMemory ensure that its core technologies, customer relationships and long-term strategy are not overly dependent on any single executive?**

>> Succession is not simply a question of who the next person will be. What matters more is whether the company's technologies, customer relationships and decision-making capabilities have been institutionalized and built into the team. eMemory today is no longer a company whose operations rest on any single individual. We have continued to build complete management teams across R&D, sales, finance and operations, and we rely on the Board and our corporate governance framework to safeguard the company's long-term development. Succession planning is a topic that the Board and management team have long taken seriously, but we will not comment on specific candidates at this stage. From an investor perspective, I believe the more important point is that even as the management team transitions across generations, the IP, patents, foundry partnerships, customer relationships and business model that eMemory has built will continue to operate. That is the most fundamental way to mitigate key-man risk.