eMemory 2026 Q3 Earnings Call Transcript

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

OPENING REMARKS

Dr. Charles Hsu, Chairman

Good afternoon, distinguished shareholders, investors, and members of the media.

In the third-quarter of 2026, eMemory delivered record-high operating results, highlighted by a more than 200% year-over-year surge in security-related revenue.

This milestone confirms that our Security solutions have become a primary engine of company growth.

Looking ahead to the fourth quarter and beyond, we remain highly confident in our growth trajectory, which is anchored by three strategic pillars:

1. Advanced-Node Ramp & Next-Gen Process Qualification: Customer designs in advanced nodes and security applications are steadily entering mass production, driving sustained royalty expansion. Simultaneously, we are accelerating the qualification and development of our technologies across multiple foundries at the 2-nanometer node and beyond.

2. Structural Demand for Silicon-Level AI Security: AI is fundamentally reshaping the global cybersecurity landscape. As AI models, cloud infrastructure, and software supply chains face increasingly sophisticated threats, software-only defenses are no longer sufficient. True security must be built from the ground up, establishing a Root of Trust directly at the silicon level—precisely the core domain eMemory has pioneered for decades.

3. Next-Generation Security Innovation: We are spearheading the next wave of chip security by accelerating the integration of PUF technology with PQC.

While PUF provides every chip with an immutable hardware identity, PQC future-proofs systems against emerging quantum computing threats. Furthermore, we are licensing multiple foundries to develop a disruptive secure memory that integrates PUF with 1T Flash, purpose-built for edge computing, robotics, and Physical AI.

Driven by the accelerating mass production of advanced nodes, the structural imperative for AI hardware security, and our breakthrough PUF-integrated 1T Flash memory, eMemory is well-positioned to enter its next phase of growth.

We will continue to leverage our deep R&D capabilities and technological innovation to serve as the trusted silicon security partner for the global semiconductor industry. Thank you for your continued trust and support.

Next, we will further report on our third-quarter financial results and future outlook. Thank you all!

FINANCIAL RESULTS

Joseph Hsia, Financial Officer

Q3 2026 Financial Results

Good afternoon, everyone. Now, let's begin with our 2026 third-quarter financial results.

The third-quarter revenue was NT$ 1,210 mil (one thousand two hundred and ten million NT dollars), up 10.4% sequentially and up 27.1% year-over-year.

Operating expenses were NT$ 446 mil (four hundred and forty-six million NT dollars), up 3.5% sequentially and up 10.3% year-over-year.

In result, our operating income was NT$ 765 mil (seven hundred and sixty-five million NT dollars), with an increase of 14.8% sequentially and an increase of 39.4% year-over-year.

Operating margin increased by 2.5 percentage points sequentially and increased by 5.6 percentage points year-over-year to 63.2%. Our net income, amounting to NT$ 639 mil (six hundred and thirty-nine million NT dollars), experienced an increase of 10.2% sequentially and an increase of 31.2% year-over-year.

EPS for this quarter was NT$ 8.56.

Revenue across Different Streams

Next, let's move on to revenue contributions by licensing and royalty.

Licensing in the third-quarter accounted for 36.4% of the total revenue and was up 2.6% sequentially and up 27% year-over-year.

Royalties in the third-quarter contributed 63.6% of the total revenue and were up 15.4% sequentially and up 27.1% year-over-year.

Revenue was up 10.4% quarter-over-quarter and up 27.1% year-over-year.

For the first nine months of 2026, the licensing and royalty revenues are as follows:

Licensing in the first nine months accounted for 36.8% of the total revenue and was up 38.2% year-over-year.

Royalties in the first nine months contributed 63.2% of the total revenue and were up 13.4% year-over-year.

Total revenue for the first nine months increased by 21.4% year-over-year.

Revenue by Technology

With that, I will comment on our revenue contribution by specific IPs.

NeoBit accounted for 18.2% of total revenue in the third-quarter. Its licensing revenue was down 46.3% sequentially and down 68.1% year-over-year, while royalties were up 5% sequentially and up 22.3% year-over-year.

NeoFuse accounted for 57.9% of total revenue in the third-quarter. Its licensing revenue was down 4.2% sequentially but up 30.1% year-over-year. In terms of royalty revenue, NeoFuse royalties were up 19.2% sequentially and up 25.7% year-over-year.

PUF-Based Security IPs contributed 14.5% of total revenue. Its licensing revenue was up 48.4% sequentially and up 198.1% year-over-year. In terms of royalty revenue, PUF-Based royalties were up 25.9% sequentially and up 656.5% year-over-year.

MTP technology accounted for 9.4% of total revenue in the third-quarter. Its licensing revenue was down 6.7% sequentially but up 29.4% year-over-year. Royalty from MTP was up 15.2% sequentially and up 36.1% year-over-year.

For the first nine months of 2026, the revenues by technology are as follows:

NeoBit Licensing revenue was down 39.3% year-over-year, while royalty was up 8.6%, accounting for 20% of the total revenue.

NeoFuse Licensing revenue was up 35.1% and royalty was up 12.3% year-over-year, contributing to 58.1% of the total revenue.

PUF-based security IP Licensing revenue was up 234.2% and royalty was up 927.5% year-over-year, accounting for 12.6% of the total revenue.

MTP technology Licensing revenue was up 22.9% and royalty was up 32.5% year-over-year, accounting for 9.3% of total revenue.

Royalty Revenue by Wafer Size

Now, let's look at royalties for 8-inch and 12-inch wafers.

8-inch wafers accounted for 34.9% of royalties, up 7.3% sequentially and up 9.2% year-over-year.

12-inch wafers contributed 65.1% of royalties, up 20.2% sequentially and up 39.3% year-over-year.

In total, 162 product tape outs were completed in the third-quarter. We will provide more information in the management report.

And next, in the following section, I will address our future outlook.

FUTURE OUTLOOK

Joseph Hsia, Financial Officer

Licensing revenue: Licensing is expected to sustain its strong momentum, supported by robust demand for our technologies across leading-edge and legacy process nodes, hardware security, AI infrastructure, and next-generation Flash applications.
Royalty revenue: Royalty growth is expected to continue accelerating, driven by higher ASPs from advanced-node applications, ongoing ramp-up of new customer products, increasing contributions from PUF-related deployments, and a growing mix of higher-royalty-rate applications.

New IP Technologies

1. **Advanced-Node OTP and PUF-based Hardware Security:** Continuing to develop and qualify next-generation OTP and PUF-based hardware security solutions for 2nm GAA and sub-2nm nodes, addressing growing customer requirements for device identity, key protection, Secure Boot, and hardware Root of Trust.
2. **Next-Generation 1T Flash:** Our 1T logic technology continues to advance across both embedded and standalone memory applications. Its logic-process-compatible architecture offers greater scalability, simplified process integration, and enhanced cost efficiency, making it an attractive solution for future AI, industrial, and edge computing applications.

Business Development Platforms

1. **Data Center and AI Compute Security Platform:** Accelerating adoption of Caliptra across CPU, AI accelerator, and AI ASIC ecosystems is driving strong demand for our security solutions, ranging from foundational Hardware Root of Trust IP to Caliptra-compatible Security Subsystems and turnkey integration services. As AI infrastructure continues to scale, trusted computing is becoming a fundamental requirement across next-generation silicon platforms.
2. **Post-Quantum Security Platform:** AI makes software and firmware cheaper to attack. Arriving quantum computing can further challenge existing cryptographic engines. We continue to strengthen our PUF-PQC portfolio with attack-resistant hardware security technologies, including side-channel protection, to support customers' transition to the post-quantum era and emerging security standards.

3. **Chiplet Security Platform:** Together with ecosystem partners, we are building an end-to-end security framework for chiplet-based systems, covering supply-chain traceability, identity and authentication, secure provisioning, die-to-die communication, key management, and Hardware Root of Trust. These capabilities help address the growing security challenges arising from AI computing, advanced packaging, heterogeneous integration, and today's evolving geopolitical landscape.
4. **HSM Edge Server and SECaaS Platform:** The PUF-based HSM Edge Server combines device identity, key and certificate management, secure OTA updates, signature verification, privacy protection, and Post-Quantum Cryptography migration. Early opportunities are progressing in Root CA, enterprise AI token-exchange signing, DID wallets, as well as automotive OTA, industrial control, Edge AI, and data center applications.

This concludes my comments. I will now hand it over to Felix, our Head of Digital Marketing.

FEATURED TOPIC

Felix Hsu, Head of DM

(Page 13: Securing AI Infrastructure from the Silicon Up: Modular Hardware Trust for Agentic & Physical AI)

Good afternoon, everyone.

Today, I'd like to highlight a critical shift in AI infrastructure: security is moving directly into silicon.

As seen at recent industry events such as the AI Infra Summit and OCP Global Summit, the market focus is shifting from pure compute capacity to hardware-rooted trust.

We are entering a new phase. We're moving beyond generative AI toward Agentic AI, where software agents independently make decisions and execute actions, and Physical AI, which drives robotics and autonomous systems.

As autonomy grows, so does the attack surface. Trust can no longer rely solely on software; it must be anchored in the hardware.

At eMemory and PUFsecurity, we provide the foundational silicon trust required for this transition. Today, I'll show how our modular security IP captures value across the entire expanding AI ecosystem.

(Page 14: More Autonomous AI Needs Stronger Hardware Security)

To understand our market opportunity, let's first look at the AI stack.

At the top sit autonomous applications. Below them are virtualized, isolated execution environments. Supporting all of this is an expanding silicon footprint: CPUs, GPU accelerators, DPUs, storage, and management controllers.

At the base of every trusted chip is the Hardware Root of Trust. It assigns a unique chip ID, validates secure boot, and enables platform attestation.

This is vital for Agentic AI. Before an agent executes high-value tasks or accesses sensitive data, the ecosystem must verify the identity and integrity of the underlying hardware. Software security alone cannot guarantee this.

As AI becomes more autonomous, hardware-rooted trust becomes a mandatory requirement, driving higher IP content per chip across layers of the data center.

(Page 15: Integrated HSMs Bring Security Closer to AI Workloads)

A key architectural shift among hyperscalers is bringing cryptographic security directly into servers.

Traditionally, data centers relied on centralized, standalone Hardware Security Modules (HSMs). While essential for enterprise-wide key management, relying solely on centralized HSMs at AI scale creates latency bottlenecks, network dependency, and rising operational costs.

To solve this, hyperscalers are adopting integrated HSM architectures, moving key management and crypto operations directly into the server or SoC.

This hybrid approach optimizes performance, lowers latency, and allows security to scale linearly with compute. This trend directly expands our company's silicon footprint and licensing opportunities inside next-generation AI servers.

(Page 16: PUFrt: A Hardware Security Anchor for Multiple Applications)

Our core technology that addresses this demand is PUFrt, PUF-based Root of Trust.

PUFrt combines physical unclonable function (PUF) technology with non-volatile memory to create a silicon-based security anchor. It delivers a unique hardware fingerprint, secure OTP storage, and a high-quality True Random Number Generator (TRNG).

Its strength lies in its versatility across multiple high-growth use cases:

In Integrated HSMs, PUFrt acts as the hardware anchor for secure key storage and local cryptographic execution.

It also serves as the foundational silicon trust for open standards such as Caliptra. Caliptra is an open-sourced hardware Root of Trust standard backed by major hyperscalers across CPUs, GPUs, DPUs, and BMCs.

By supplying the fundamental trust anchor for Caliptra and custom HSMs, a single IP platform allows us to target virtually every silicon segment in the AI data center.

(Page 17: Reusable Security Foundation for Different Integrations)

Our modular IP architecture gives chip designers maximum flexibility, accelerating our time-to-market and customer adoption.

PUFrt supports two main integration paths:

1. Dedicated HSM ASICs: Serving as the physical security root in standalone security processors that protect multi-SoC boards.
2. Embedded SoC Integration: Directly integrated into custom CPUs, AI accelerators, DPUs, or management controllers (BMCs).

Where advanced security is required, customers can layer on PUFhsm, incorporating Post-Quantum Cryptography (PQC) through our PUF-PQC solution.

Importantly, PUFrt has successfully completed independent security evaluation under OCP S.A.F.E. Scope 3, proving its resilience against physical side-channel attacks. This third-party validation reduces integration risk for Tier-1 customers and shortens design-win cycles.

(Page 18: From AI Demand to Silicon Security Market)

To conclude, our growth thesis rests on five key catalysts:

1. Autonomous AI Expansion: Agentic and Physical AI make silicon-level trust mission-critical.
2. Edge & Localized Hardware Security: Security is moving onto the chip to eliminate latency and scaling bottlenecks.
3. Standardization via Caliptra: Widespread adoption of open standards accelerates customer design wins and IP reuse.
4. Modular Product Portfolio: Our IP range, spanning PUFrt, PUFhsm, and PQC, allows us to capture value in both discrete and embedded configurations.
5. Clear Market Trajectory: These structural tailwinds directly drive long-term licensing and royalty growth for eMemory and PUFsecurity.

Thank you. I welcome your questions.

CLOSING REMARKS

Dr. Charles Hsu, Chairman

For more information about our PUF-based security IPs and technology, we encourage you to visit our PUFsecurity website at https://www.pufsecurity.com/ and check out our articles and other materials.

Thank you once again for your patience and support for eMemory. We will continue to work hard on technology and IP innovation and PUF-based hardware security solutions for our customers and bring higher returns for our shareholders.

Thank you!