eMemory 4Q25 Earnings Call Transcript

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

OPENING REMARKS

Dr. Charles Hsu, Chairman

Good afternoon, everyone. Looking back at the fourth quarter of last year, we achieved an impressive milestone with 18 licensing wins in the 3nm defense applications. In the first quarter of this year, we expect to secure an additional three 3nm licenses related to AI Data Center processors.

As these licenses progress, our PUF (Physical Unclonable Function) royalties have moved into mass production. Most notably, with our PUFrt (Root of Trust) now integrated into the NVIDIA Vera Rubin architecture, we expect royalty contributions to grow significantly in the second half of this year.

The era of AI Inference is transforming our industry. We are seeing a surge in SRAM Repair demand driven by Computing in Memory, alongside an urgent need for security in Edge AI and Physical AI.

Looking further ahead, Google and IBM anticipate that quantum computing will be commercialized within five years. As governments worldwide pivot toward Post-Quantum Cryptography (PQC), we are entering the most significant hardware security upgrade in 25 years.

We are uniquely prepared for this shift. Our foundation is built on:

- Proven Track Record: Over 130 PUF-related tape-outs to date.
- Global Reach: More than 700 process platforms worldwide are mass-producing wafers utilizing our technology.
- Massive Volume: An annual production record exceeding 9.8 million wafers (8-inch equivalent).

This solid foundation is our most irreplaceable advantage as we integrate PUF into the global chip supply chain and establish a definitive Hardware Root of Trust. We remain profoundly confident in the company's future.

Next, I'd like to invite our financial officer, Joseph Hsia, to present our fourth-quarter performance. Afterwards, our president, Michael Ho, will share our future outlook.

FINANCIAL RESULTS

Joseph Hsia, Financial Officer

Q4 2025 Financial Results

Good afternoon, everyone. Now, allow me to briefly go through our 2025 fourth-quarter financial results.

Our fourth-quarter revenue was NT$ 1.05 Billion (One point zero five billion NT dollars), up 10.1% sequentially and up 3.7% year-over-year.

Our operating expenses for the fourth-quarter were NT$ 413 Million (Four hundred and thirteen million NT dollars), increased 2.1% sequentially but down 7.2% year-over-year. Through on-going org and process optimization as well as AI transformation, we were able to improve our operational efficiency, and that led to our overall expenses remaining broadly flat despite continued business expansion.

In result, our operating income was NT$ 636 Million (Six hundred and thirty-six million NT dollars), with an increase of 15.9% compared to the previous quarter and an increase of 12.3% year-over-year.

Operating margin increased by 3 percentage points sequentially and increased by 4.6 percentage points year-over-year to 60.6% reaching a record high, reflecting disciplined cost control and improved cost efficiency. Our net income, amounting to NT$ 563 Million (Five hundred and sixty-three million NT dollars), up 15.6% QoQ and 9.4% YoY.

EPS for Q4 2025 was 7.54 NT dollars (NT$ 7.54).

Revenue across Different Streams

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

Licensing in the fourth-quarter accounted for 33.1% of the total revenue, down 0.1% sequentially but up 9.9% year-over-year.

Royalties in the fourth-quarter contributed 66.9% of the total revenue, increasing 15.9% sequentially and increasing 0.9% year-over-year.

For the full year of 2025, **Licensing** increased 10.4% year-over-year, and **Royalties** increased 5.1% year-over-year.

Revenue by Technology

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

NeoBit accounted for 22.5% of total revenue in the fourth quarter. Its licensing revenue decreased 25.5% sequentially but increased 16.5% year-over-year, while royalty revenue increased 3.6% sequentially but decreased 7.9% year-over-year.

NeoFuse accounted for 58.5% of total revenue in the fourth quarter. Its licensing revenue decreased 22.1% sequentially and 23% year-over-year, while royalty revenue increased 20.3% sequentially and 2.1% year-over-year.

PUF-Based Security IPs contributed 10.2% of total revenue in the fourth quarter, mainly driven by licensing. Licensing revenue increased 91.7% sequentially and 45.5% year-over-year, while royalty revenue accounted for less than 1% of total royalties.

MTP technology accounted for 8.8% of total revenue in the fourth quarter. Licensing revenue increased 4.7% sequentially and 29.8% year-over-year, while royalty revenue increased 13.6% sequentially and 49.9% year-over-year.

For the entire year of 2025,

NeoBit Licensing revenue increased by 16.1% year-over-year and royalty increased by 2.5%.

NeoFuse Licensing revenue increased by 0.7% and royalty increased by 5.2% year-over-year.

PUF-based security IP Licensing revenue increased by 37.4% year-over-year.

MTP technology Licensing revenue increased by 3.6% and royalty increased by 21.7% year-over-year.

Royalty Revenue by Wafer Size

Digging a little bit further into royalty's breakdown by 8-inch and 12-inch wafers.

8-inch wafers accounted for 36.2% of royalties, up 3.3% sequentially but down 10.5% year-over-year.

12-inch wafers contributed 63.8% of royalties, up 24.5% sequentially and up 8.8% year-over-year.

A total of 201 product tape-outs were completed in the fourth quarter. We will provide more information in the management report.

Next, I would like to pass the floor to our President Michael Ho to share more about our future outlook.

FUTURE OUTLOOK

Michael Ho, President

Good afternoon, everyone. In the following section, I will address our future outlook.

For **Licensing revenue**, we expect continued strong growth, driven by increases in both the number of licenses and the average license price across our foundry and fabless customers.

For **Royalties**, growth is accelerating, driven by the ramp-up of mass production across various new applications, higher ASPs from advanced nodes, additional PUF-related royalties, and higher royalty rates from MTP-related IPs.

New application ramp-ups include:
- Mobile: RF ICs for U.S.-based smartphone modem platforms.
- Automotive: ADAS, networking-related applications, ISP, and LiDAR.

- Cloud AI: BMCs, SSD controllers, networking-related applications, CXL controllers, and DIMMs.
- Edge and Endpoint: Embedded controllers for notebooks and PCs, as well as security applications for various smart devices, including printer cartridges using embedded PUF for anti-counterfeiting.

IP & Security Platforms

- OTP: Advanced GAA OTP IP development with leading foundries, extending toward sub-3nm nodes.
- RRAM: Embedded RRAM platforms with key foundries and IDM for FinFET, BCD and automotive applications.
- NeoFlash: Deployment across foundries for BCD and mixed-signal processes in 12-inch fabs.
- Security IP: PUF-PQC achieves NIST FIPS 205 and SP 800-208 certification, reaching a milestone in comprehensive Post-Quantum Cryptography protection.

Security Ecosystem Expansion

- Chiplet Security: End-to-end authentication and supply-chain trust for advanced packaging.
- CPU platform collaboration: PUF-based Security Root of Trust integrated with major CPU platforms.
- Automotive & Healthcare: PUF-based HSM servers supporting secure OTA and privacy protection.

This concludes my comments. Next, I will pass the time to Charles.

CHAIRMAN REMARKS

Dr. Charles Hsu, Chairman

(Page 15: eMemory's technology enables AI memory systems to be high-yield, reliable, and secure)

As you have seen in the video, this is just one clear example of how our IP can power AI in reliable and efficient manners; and particularly, to overcome current pain points encountered by using current technology, such as eFuse, for AI implementation.

Thus, to follow, I would like to present to you a more comprehensive view of eMemory's technologies, and how we can enhance reliability and security across various memory architectures.

In today's AI-driven world, memory systems face three critical challenges: achieving high yield at advanced process nodes, ensuring reliability under extreme workloads, and maintaining robust security. eMemory addresses all three through our innovative Logic NVM and PUF-based security solutions.
Let me walk you through how our technology enables the AI memory ecosystem—from on-package memory all the way to system-level storage.

(Page 16: Core Technology - Logic Process NVM)

At the heart of eMemory is our Logic NVM technology—that is, Non-Volatile Memory built using standard logic fabrication processes.

- **First, One-Time Programmable memory, OTP.** This includes our NeoBit mainly on 8 inch wafers for mature nodes and NeoFuse on 12 inch wafers mainly for both mature and advanced nodes. OTP is programmed once and cannot be altered—perfect for storing permanent data.
- **Second, Multiple-Time Programmable memory, MTP.** Our NeoEE, NeoMTP, and NeoFTP solutions allow reprogramming multiple times, offering flexibility for firmware updates and configuration changes.
- **Third, Flash memory** with our NeoRRAM and NeoFlash products, providing the highest rewrite endurance for code storage and execution.

Together, they can be used in a wide range of critical applications.

- For instance, we use OTP to repair defective memory cells in DRAM and SRAM, restore faulty pixels in image sensors, and trim analog circuits to meet specifications. These directly translate to higher manufacturing yields and lower costs.
- MTP and Flash enable on-chip code storage and execution, eliminating dependency on external memory. They also support product version control and post-manufacturing customization.
- For security applications, OTP provides the foundation for storing unalterable hardware keys—the root of trust for any secure system. Once programmed, these keys cannot be modified, even by sophisticated attacks.

(Page 17: Logic NVM Solving Traditional NVM Pain Points)

Compared to traditional NVM, Logic NVM possesses several advantages.

- In terms of manufacturing complexity, traditional NVM requires 10 or more additional masks beyond the standard logic process—that's more than tens of extra manufacturing steps. Our Logic NVM? No additional masks needed, which makes it a dramatically simpler process.
- Those extra process steps in traditional NVM also mean longer manufacturing cycles and significantly higher costs. Logic NVM uses the same equipment, comparable process flow, resulting in substantially lower costs.
- Complex processing results in lower yield. Traditional NVM suffers from this. Logic NVM, built on mature, standard logic processes, typically maintains high yields even at advanced nodes.
- A shorter development cycle is also a major advantage of Logic NVMs. Traditional NVM requires the development of new transistor models, extensive R&D, and lengthy testing before deployment. Logic NVM uses existing logic devices and models which can be integrated and deployed rapidly without reinventing the wheel.
- Scalability is critical for future implementation. Traditional NVM has limited expansion capacity due to requirement of new equipment investments. Logic NVM is highly scalable—no new equipment needed due to its logic processes compatibility.

We have noticed major chip manufacturers are increasingly adopting Logic NVM. It's not just because it's better, it's economically essential at advanced nodes.

(Page 18: PUF-Based Hardware Security)

OK, now let me introduce our second core technology: PUF-based hardware security. PUF stands for Physical Unclonable Function and in fact, our anti-fuse PUF, NeoPUF, was developed from our OTP and serves as the foundation for our security IP solutions.

Think of PUF as a silicon fingerprint. Just as no two human fingerprints are identical, no two chips produce the same PUF signature—even chips from the same wafer. This hardware key is essentially invisible to attackers, making it extremely difficult for them to extract or clone.

During the past six years we have developed several security IPs based on this foundation.

- For Root of Trust, our secure OTP stores immutable data, TRNG generates true random numbers, and combined with NeoPUF, our PUFrt IP provides chip-unique IDs and keys, establishing a hardware-anchored trust foundation.
- By integrating with crypto-processors, we offer PUFcc for cryptographic coprocessing and PUFhsm for hardware security modules—enabling secure key management and cryptographic operations.
- In terms of cryptography, we support a comprehensive suite of cryptographic algorithms—traditional standards like RSA, ECC, AES, and SHA, as well as PQC for post-quantum cryptography, and many others, providing complete cryptographic coverage for any security requirement.
- Our solutions have achieved multiple critical certifications. For post-quantum cryptography, we have NIST CAVP certification covering FIPS 203, 204, and 205, plus SP 800-208. For random number generation, we've also achieved NIST CAVP and ESV validations. For platform security, our solutions are PSA Level 2 Ready, and Level 3 Root of Trust certified. Additionally, we hold SESIP Level 3 certification for IoT security evaluation. This comprehensive certification portfolio ensures our solutions meet the most stringent security requirements across all major industries.

Altogether, these security approaches that have been validated, can provide in-depth defense networks to secure modern systems.

(Page 19: Where eMemory Fits in AI Memory Systems)

With our IPs in mind, now let me show you how our technologies enable the entire AI memory hierarchy.

- **SRAMs** are the fastest caches embedded directly in GPUs, TPUs, and NPUs of AI accelerators. At advanced nodes like 3nm and below, SRAM cells are extremely sensitive to manufacturing variations. With the ability to repair defective SRAM, HBM, and DRAM cells, our OTPs dramatically improve SRAM yield and lowers the cost of chips.
- **High Bandwidth Memory, HBM**, are on-package 3D stacked DRAM, providing massive bandwidth for AI training and inference. HBM stacks can be 8, 12, or even 16 layers high; and since a single defect can compromise the entire stack,

embedded memory repair ensures stack integrity. Our OTP can endure thermal and electrical stress and thus, guarantees long-term data memory retention and operational stability under extreme AI workloads.

- **Server DRAMs** including GDDR6/7 and the emerging SOCAMM and DDR5 standards also benefit from our embedded memory repair solution by OTP. Whereas, our MTPs enable flexible memory management for DIMM configurations in DDR5 and SOCAMM standards. With these IP, we enable cost-effective AI chip mass production. When there are millions of AI server modules, a few percentage points of yield improvement translates to hundreds of millions in cost savings across the industry.
- **CXL Memory** represents the future of data center memory architecture, where memory pooling and disaggregation happen at the infrastructure level. Since CXL memory pools are accessed by hundreds of servers, our PUFrt security solution is critical here; without proper security, data leakage becomes a critical risk. PUFrt enables multi-tenant data isolation, ensuring that when multiple customers share the same physical memory infrastructure, their data remains cryptographically separated.
- **For storage memory**, our PUF-based solutions protect data storage within NVMe and SSD controllers to safeguard AI models, which can be worth millions in development costs and proprietary data.

Lastly, let me re-emphasize the key message here: IP and technologies provided by our company, eMemory and PUFsecurity, are AI memory system-enabling technologies.

In summary, with our technology, AI memory systems achieve three critical goals simultaneously:

- High Yield, which is necessary for economic AI chip production at advanced nodes
- High Reliability required for AI inference workloads in mission-critical applications
- High Security demanded by enterprise and cloud AI deployments with multi-tenant environments

This is what makes AI systems truly scalable and deployable in production environments.

This is what I would like to share with you today. Thank you for listening. Next, we will enter the Q&A session.

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!