eMemory 3Q25 Earnings Call Transcript

November 14th, 2025, 16:00-17:00 Taiwan Time

OPENING REMARKS

Dr. Charles Hsu, Chairman

Good afternoon, everyone. Thank you all for attending eMemory's third-quarter investor conference.

Looking ahead to the fourth quarter, in addition to achieving record-high revenue, we've also made several major breakthroughs. First, in security applications, we have secured a 10-year contract for U.S. government defense projects on multiple 3nm applications, which marks a significant milestone in promoting our PUF technology. This began with our partnership agreement with the U.S. Defense Advanced Research Projects Agency (DARPA) for Toolbox Initiative in 2021. Now, our technology is officially being adopted in defense-related deployments, in addition to more than 100 applications accumulated in the past.

Security application standards have always been driven by government and system-level initiatives. From DARPA to the OCP (Open Compute Project) alliance — formed by major data center players — and its Caliptra standard, PUF technology is now on a clear path toward large-scale commercialization.

The second major breakthrough is in Flash memory, particularly our embedded ReRAM and NeoFlash technologies. As memory performance has become a bottleneck in chip computing, technologies that replace external memory with embedded non-volatile memory (eNVM) solutions are entering commercial adoption. Our NeoEE technology has already been designed into DDR5 modules to replace the EEPROM used in DDR4, and is expected to enter mass production next year. Recently, we've also received multiple major customer engagements for NeoFlash and embedded ReRAM as alternatives to external NOR Flash.

Because security applications generate higher royalty income per wafer and drive demand for high asp advanced process nodes, and because MTP and Flash royalties are typically 1.5 to 3 times higher than OTP, these factors will collectively lead to a structural increase in average royalty per wafer.

Looking ahead to next year, we have new applications with our IPs entering mass production to accelerate royalty growth across major industries:

- RF chips for a leading U.S. smartphone customer's in-house modem module
- DDR5-related applications for a major Korean memory manufacturer
- AI servers featuring secure BMCs, SSD controllers, and networking chips with our PUF IPs
- Automotive applications in ADAS, networking, and infotainment
- PC/NB (notebook) designs using our IP for secure embedded controllers
- And numerous ASIC applications from various customers.

We have also started our Security-as-a-Service business with multiple customers. Our long-term effort to build foundational technologies and ecosystem has created a strong competitive moat. With a royalty-based, recurring revenue model, the potential for future revenue growth is tremendous. We are very confident about our growth prospects for next year and beyond.

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

FINANCIAL RESULTS

Joseph Hsia, Financial Officer

Q3 2025 Financial Results

Good afternoon, everyone. Now, let's begin with our 2025 third-quarter financial results.

The third-quarter revenue was nine hundred and fifty-two million NT dollars (NT$ 952 mil), up 1.7% sequentially and up 5.9% year-over-year. Revenue in U.S. dollars was thirty-two million (US$ 32 mil), representing an 8.2% increase from the previous quarter and a 15.9% increase year-over-year.

Operating expenses were four hundred and four million NT dollars (NT$ 404 mil), up 3.4% sequentially and up 2.4% year-over-year.

Operating income was five hundred and forty-eight million NT dollars (NT$ 548 mil), with an increase of 0.5% sequentially and an increase of 8.6% year-over-year.

Operating margin decreased by 0.7 percentage point sequentially but increased by 1.5 percentage points year-over-year to 57.6%. Our net income, amounting to four hundred and eighty-seven million NT dollars (NT$ 487 mil), experienced an increase of 21.8% sequentially and an increase of 17.7% year-over-year.

EPS for this quarter was 6.52 NT dollars (NT$ 6.52).

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, up 9.1% sequentially and up 19.4% year-over-year. In U.S. dollar terms, this represents a sequential increase of 12.4% and a year-over-year increase of 28%.

Royalties in the third-quarter contributed 63.6% of the total revenue, decreasing 2.1% sequentially and decreasing 0.6% year-over-year. In U.S. dollar terms, this represents a sequential increase of 5.9% and a year-over-year increase of 10.1%.

Total revenue for the third-quarter increased by 1.7% compared to the previous quarter and increased by 5.9% compared to the previous year. In U.S. dollar terms, total revenue rose 8.2% sequentially and 15.9% year-over-year.

For the first three quarters of 2025, the licensing and royalty revenues are as follows:

Licensing in the first three quarters accounted for 32.3% of the total revenue, up 10.6% year-over-year. In U.S. dollar terms, licensing revenue grew 13.6% year-over-year.

Royalties in the first three quarters contributed 67.7% of the total revenue, increasing 6.7% year-over-year. In U.S. dollar terms, royalty revenue increased 8.9% year-over-year.

Total revenue for the first three quarters increased by 7.9% compared to the previous year. In U.S. dollar terms, total revenue grew 10.4% year-over-year.

Revenue by Technology

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

NeoBit accounted for 23.2% of total licensing revenue in the third-quarter, increasing 34.2% sequentially but decreasing 11.3% year-over-year. Its royalties accounted for 25.3% of total royalty, down 6.2% sequentially and decreasing 3.1% year-over-year.

NeoFuse accounted for 42.8% of total licensing revenue in the third-quarter, up 18.4% sequentially and up 70.9% year-over-year. In terms of total royalty revenue, NeoFuse royalties decreased by 0.8% sequentially and decreased by 0.7% year-over-year, accounting for 71.4% of total royalties.

PUF-Based Security IPs contributed 14.5% of licensing revenue, increasing 8.1% sequentially and increasing 44.1% year-over-year, while its royalties accounted for less than 1% of total royalties, up 83.9% compared to the previous quarter, and increasing 326.9% compared to the previous year.

MTP technology accounted for 19.5% of total licensing revenue, decreasing 21.3% sequentially and decreasing 13.3% year-over-year. Royalty from MTP up 0.9% sequentially and increased by 24.8% year-over-year, accounting for 3.1% of total royalties.

For the first three quarters of 2025, the revenues by technology are as follows:

NeoBit licensing revenue decreased by 7.1% year-over-year but royalty increased by 6.3%, accounting for 24.4% of the total revenue.

NeoFuse licensing revenue increased by 27.7% and royalty increased by 6.5% year-over-year, contributing to 62.3% of the total revenue.

PUF-based security IP licensing revenue increased by 25.7% year-over-year, accounting for 4.2% of the total revenue.

MTP technology licensing revenue decreased by 3.3% but royalty increased by 13% year-over-year, accounting for 9.1% 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 40.6% of royalties, down 0.6% sequentially and down 1.4% year-over-year.

12-inch wafers contributed 59.4% of royalties, down 3.1% sequentially but was flat compared to the same period last year.

In total, 173 product tape outs were completed in the third-quarter. We will provide more information in the management report.

Next, I'll invite Michael to share our future outlook.

FUTURE OUTLOOK

Michael Ho, President

Hello everyone, I will now present our future outlook.

We expect our business momentum to accelerate:

Licensing growth will be driven by:

1. 10 years contract including 18 3nm tape outs for US defense applications and 3nm CPU for AI server will drive strong PUF security license growth.
2. Strong licenses for embedded ReRAM and NeoFlash technologies that replace external memories.

Royalty growth is expected to accelerate due to customers' tape outs moving into mass production for:

1. RF chips for a leading U.S. smartphone customer's in-house modem module.
2. DDR5-related applications for a major Korean memory manufacturer.
3. AI servers featuring secure BMCs, SSD controllers, and networking chips.
4. Automotive applications in ADAS, networking.
5. Secure embedded controllers for PC/ NB.
6. ASIC applications from various customers.

In technology development:

1. OTP: Continuing joint development with TSMC on 2nm technologies and IPs.
2. ReRAM: Co-developing FinFET technologies and IPs with Korea's largest company.
3. NeoFlash: Collaborating with multiple foundries to develop BCD process technologies and IPs at various nodes.
4. Security: Accelerating the development of security server hardware and software for Security-as-a-Service.

In business platforms:

1. Jointly developing end-to-end chiplet security solutions with multiple partners to ensure chiplet supply chain protection. The main collaborations focus on supply chain security and chip authentication, ensuring that every chip's role can be securely verified locally.
2. Collaborating with Arm to develop PUF-based Security Root of Trust to enhance the security capabilities of Arm's Runtime Security Engine.
3. Working with automotive system suppliers and hospitals to provide a PUF-based HSM server platform for OTA software protection and DID-based personal privacy protection.

The establishment of these platforms will contribute to future revenue growth.

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

CHAIRMAN REMARKS

Dr. Charles Hsu, Chairman

(Page 14: PUF Technology on National Security)

Since we have signed 10 years contract for our 3nm PUFrt's to be used in defense applications, today, I'd like to talk about hardware root of trust in national security.

In many ways, a country's security depends heavily on its defense capabilities. As we build more electronics, automation, and artificial intelligence into modern defense systems, keeping them secure becomes absolutely critical. Take drones and robots, for example, they're already being used on the battlefield. If control over these systems were ever lost, the results could be disastrous. That's why, to truly protect national

security, we must make sure our weapons and defense equipment are fully secured against any kind of threat.

For national security reasons, it's also essential to build a strong domestic supply chain for chip manufacturing. In the United States, Intel, GlobalFoundries, and Tsmc Arizona are the major suppliers directly or indirectly serving national defense needs. Our NeoPUF-based security solutions have been licensed to these foundries, enabling them to meet their defense customers' growing demand for trusted and reliable hardware security.

Our NeoPUF technology is not only proven at the most advanced manufacturing nodes, but also recognized as a key enabler of secure, next-generation defense systems.

(Page 15: PUF: The Foundation of National Security)

Our defense and communication systems today are built through complex, multi-tier global supply chains. From chip design, to fabrication, to final system integration, each stage is a potential attack surface. If even one component is counterfeit or tampered with, a single vulnerability could compromise an entire weapons system or communication network.

That's why PUF, the Physically Unclonable Function, is so critical. PUF creates a unique and unforgeable hardware identity for every chip. It serves as a hardware root-of-trust, enabling secure verification, key generation, and device authentication, directly from silicon itself.

In short, PUF transforms each chip, drone, radio, or satellite into a trusted and traceable element within a national defense ecosystem and protects the defense equipments and weapons.

(Page 16: What Applications in Defense Are Using PUF?)

Let's now look at how PUF is applied across different layers of defense. These can be grouped into three levels: device level, system level, and supply chain level.

At the device level, PUF gives every chip a unique, unclonable fingerprint. This allows us to verify authenticity and prevent counterfeit devices from entering the network. It also enables secure key generation. The key is created from the chip's own physical traits, not injected from outside, which means it can't be stolen or altered. This is vital

for communication equipment, encrypted radios, tactical equipment, and field-deployed systems that must resist tampering.

At the system level, PUF ensures that every mission system, such as missile controllers or communication units, operates only with authorized firmware. It also supports secure boot and runtime attestation, preventing unauthorized code or firmware manipulation. PUF also enables lightweight authentication for distributed IoT or sensor networks, allowing even low-power battlefield devices to maintain zero-trust operation.

Finally, at the supply chain level, PUF helps verify the origin and authenticity of critical components. For example, every microprocessor, FPGA, or avionics module can be tied to a PUF-based certificate that proves it is genuine. This allows tracking and verification from fabrication through deployment, preventing counterfeit components from entering the system.

Across all three layers, PUF brings authenticity, integrity, and traceability to national defense systems.

(Page 17: Applying PUF to Supply Chain Management for Defense)

Next, let us now connect these ideas to the defense supply chain. PUF provides protection throughout the entire product lifecycle, from silicon to system operation.

At “Design and Fabrication” stage, PUF IP is embedded directly into the. Each chip generates its own unique ID, making it secure from birth. This ensures authenticity at the hardware level before the device even leaves the factory.

At “Assembly and Testing” stage, when parts are integrated, each module can be authenticated through PUF-based ID. This process identifies counterfeit or modified components early in production.

At “Logistics and Deployment” stage, every shipment can be linked to a PUF-signed digital certificate, maintaining a clear and verifiable chain of custody. It prevents component swapping or fake deliveries during transportation.

At “Operation and Maintenance” stage, once deployed, the system can perform continuous attestation using a PUF-based hardware security module. This verifies firmware integrity and ensures that every unit in the field remains authentic and secure.

With PUF, the entire defense supply chain becomes transparent, traceable, and tamper-resistant.

(Page 18: NeoPUF: Excels in National Defense)

Finally, let's talk about why our NeoPUF is ideal for defense devices.

NeoPUF has been carefully designed to provide stable, reliable, and secure hardware identities, even under demanding environmental conditions such as wide temperature ranges, voltage variation, and exposure to radiation.

First, NeoPUF demonstrates strong reliability. Its positive-feedback amplification mechanism allows each device to reach a stable state quickly, so variations in temperature or electrical noise have minimal influence. This ensures consistent and repeatable responses, which is critical for long-term operation in defense and aerospace systems.

Second, NeoPUF shows excellent tolerance to radiation. Because it is based on quantum tunneling through the gate oxide rather than bistable SRAM elements, radiation effects which cause the soft error in SRAM commonly occur in space will not impact NeoPUF.

Third, NeoPUF is inherently resistant to tampering and duplication. Its physical structure is fixed during fabrication and cannot be modified afterward. This makes unauthorized duplication or alteration extremely difficult.

Finally, NeoPUF is adaptable across the defense ecosystem. It can be integrated into a wide range of mission systems, from secure communication networks and radar control units to satellites, drones, and surveillance platforms. This adaptability allows defense organizations to build a unified trust architecture across different domains, ensuring every connected system operates with consistent implementation of hardware-based trust.

In summary, NeoPUF provides a proven and stable foundation for hardware-based trust, supporting the long-term security and resilience required in national defense supply chains.

This is what I would like to share with you today. Thank you.

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!