eMemory 2Q26 Earnings Call Transcript

August 14th, 2026, 16:00-17:00 Taiwan Time

OPENING REMARKS

Dr. Charles Hsu, Chairman

Good afternoon, shareholders and investors.

First, I would like to report on our latest progress in Security IP.

Over the past few years, our Security IP has evolved from foundational OTP and PUF into PUF Root of Trust. Today, as security requirements for AI servers continue to rise, our technology has taken a major step forward—advancing from standalone Security IP to the design and integration of comprehensive Security Subsystems.

This transition is crucial for us. We are no longer providing clients with just OTP, PUF, or Root of Trust; we are now delivering fully integrated, system-level Security IP that combines encryption technology, software/firmware, and anti-tempering protection. In other words, our role within our clients' chips has become far more critical, allowing us to deliver significantly higher value. Consequently, the potential licensing fees and royalties are expected to increase significantly as well.

We have licensed to several major global memory manufacturers to integrate our Security IP into SSD systems for AI Data Centers, providing the security subsystems required to comply with Caliptra standards. Beyond SSDs, we have also expanded into another vital area of AI Servers: Memory Expansion.

As AI models grow increasingly large, the memory capacity required by AI Servers is surging rapidly. As a result, CXL is becoming a dominant interface technology for AI Server Memory Expansion. CXL Switches and their related controller chips similarly require a complete hardware security architecture. We are currently working with several CXL chipmakers to supply both Security IP and Security Subsystems.

Connecting the dots over the past few years reveals a clear trajectory. Last year, we entered AI/AGI CPUs and BMC, this year, we expanded into AI Data Center SSDs, security subsystem and now, we are penetrating CXL Switches for AI Server Memory Expansion.

This means our Security IP is expanding from a single chip inside an AI Server to multiple critical chips. Furthermore, many of these advanced chips are utilizing cutting-edge process nodes, such as 3nm, generating 10 times higher licensing and royalty than corporate average.

Another highly favorable trend for us is Caliptra.

Driven jointly by global tech giants such as Microsoft, Google, Intel, AMD, and NVIDIA, we are seeing an increasing number of AI and Data Center chips and systems adopt the Caliptra security architecture.

This indicates that the number of chips requiring Root of Trust, Security Subsystems, and related Security IP will grow significantly moving forward. Therefore, we remain highly confident in the long-term growth of our Security IP within the AI Server and Data Center markets.

Next, I would like to share updates on another key growth driver we are heavily focused on: Logic Flash.

Currently, our collaboration with foundries on Logic Flash technology is accelerating. Applications extend beyond Embedded Flash to include standalone Flash products as well. We believe the significance of Logic Flash goes far beyond adding another IP technology to our portfolio.

More importantly, it presents an opportunity to leverage a more competitive process and cost structure to gradually replace portions of existing legacy Flash technology. Flash memory represents a massive market with exceptionally broad applications.

Once Logic Flash enters mass production and begins progressively replacing conventional Flash technologies, the market opportunities and the long-term impact on our future revenue and profitability will be far-reaching.

For these reasons, we have strong confidence in our multi-year growth outlook ahead.

Next, I'd like to invite our financial officer, Joseph Hsia, to present our second-quarter performance.

FINANCIAL RESULTS

Joseph Hsia, Financial Officer

Q2 2026 Financial Results

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

The second-quarter revenue was NT$ 1,097 mil (one thousand and ninety-seven million NT dollars), up 0.2% sequentially and up 17.1% year-over-year.

Operating expenses were NT$ 431 mil (four hundred and thirty-one million NT dollars), down 0.3% sequentially but up 10.2% year-over-year.

In result, our operating income was NT$ 666 mil (six hundred and sixty-six million NT dollars), with an increase of 0.6% sequentially and an increase of 22% year-over-year.

Operating margin increased by 0.2 percentage point sequentially and increased by 2.4 percentage points year-over-year to 60.7%. Our net income, amounting to NT$ 580 mil (five hundred and eighty million NT dollars), experienced a decrease of 2.8% sequentially but an increase of 44.9% year-over-year.

EPS for this quarter was NT$ 7.77.

Revenue across Different Streams

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

Licensing in the second-quarter accounted for 39.2% of the total revenue, up 12.8% sequentially and up 35.1% year-over-year.

Royalties in the second-quarter contributed 60.8% of the total revenue, decreasing 6.4% sequentially but increasing 7.8% year-over-year.

Revenue increased by 0.2% quarter-over-quarter and up 17.1% year-over-year.

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

Licensing in the first half accounted for 37% of the total revenue, up 45.2% year-over-year.

Royalties in the first half contributed 63% of the total revenue, increasing 7% year-over-year.

Total revenue for the first half increased by 18.5% compared to the previous year.

Revenue by Technology

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

NeoBit accounted for 21.9% of total revenue in the second-quarter. Its licensing revenue increasing 11.2% sequentially but decreasing 22.4% year-over-year, while royalties up 9% sequentially and increasing 9.2% year-over-year.

NeoFuse accounted for 56.6% of total revenue in the second-quarter. Its licensing revenue was up by 24.8% sequentially and up 55.6% year-over-year. In terms of royalty revenue, NeoFuse royalties decreased by 13.3% sequentially but increased by 4.4% year-over-year.

PUF-Based Security IPs contributed 10.9% of total revenue, its licensing revenue decreasing 13.8% sequentially but increased 133.5% year-over-year. In terms of royalty revenue, PUF-Based royalties increased by 213.9% sequentially and increased by 1676.7% year-over-year.

MTP technology accounted for 10.6% of total revenue in the second-quarter. Its licensing revenue increased 40.2% sequentially and increased 9.3% year-over-year. Royalty from MTP was up 7.2% sequentially and increased by 19.2% year-over-year.

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

NeoBit Licensing revenue decreased by 18.5% year-over-year but royalty increased by 2.4%, accounting for 20.9% of the total revenue.

NeoFuse Licensing revenue increased by 37.9% and royalty increased by 6% year-over-year, contributing to 58.2% of the total revenue.

PUF-based security IP Licensing revenue increased by 264.6% year-over-year and royalty increased by 1317.8% year-over-year, accounting for 11.6% of the total revenue.

MTP technology Licensing revenue increased by 19.6% and royalty increased by 30.4% 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 37.5% of royalties, up 4.2% sequentially and up 1.2% year-over-year.

12-inch wafers contributed 62.5% of royalties, down 11.9% sequentially but up 12.3% year-over-year.

In total, 156 product tape outs were completed in the second-quarter. We will provide more information in the management report.

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

FUTURE OUTLOOK

Dr. Charles Hsu, Chairman

In the following section, I will address our future outlook.
Licensing Revenue: Licensing will continue its strong momentum due to robust demand for our technologies from leading edge to legacy process node, security, and next-generation Flash technologies.

Royalty Revenue: Royalty Revenue growth is expected to accelerate, driven by higher ASPs from new advanced-node applications, new application ramps, expanding PUF royalty contributions, and a growing mix of higher-royalty rate MTP

related 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, meeting growing customer demand in device identity, key protection, Secure Boot, and hardware Root of Trust.
2. **Next-Generation 1T Flash:** Our 1T NeoFlash technology is advancing across embedded and standalone applications. Its logic-process-compatible architecture offers greater scalability, lower process complexity, and better cost efficiency.

Business Development Platforms

1. **Chiplet Security Platform:** We continue to work with ecosystem partners on 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—addressing the increasingly complex security challenges of AI, advanced packaging, and heterogeneous integration amid today's geopolitical environment.
2. **Data Center Security and Caliptra Platform:** Targeting data centers and AI servers, we continue to upsell—expanding PUFrt from a hardware Root of Trust solution into a Caliptra-compatible Security Subsystem and integration services that reduce integration complexity and accelerate customer deployment.
3. **AI Compute and Root of Trust Platform:** We are extending collaboration across CPU, AI accelerator, and AI ASIC ecosystems to integrate chip-level Root of Trust, Secure Boot, device identity, and secure key protection into next-generation AI computing platforms—strengthening trust and security from silicon to system.
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 automotive OTA, PKI, and HSM integration, with potential to expand into industrial control, Edge AI, smart devices, medical, and data centers.
5. **Post-Quantum Security Platform:** We continue to strengthen our PUF-PQC portfolio with attack-resistant hardware security, including side-channel protection, to support the transition to post-quantum security standards.

This concludes my comments. Next, I will pass the time to Felix, our Head of Digital Marketing, to share with your our featured topic today.

FEATURED TOPIC

Felix Hsu, Head of DM

(Page 13: Securing the Next Generation of AI Infrastructure, the hardware anchor for Caliptra Root-of-Trust to secure Chiplets & CXL)

(Page 14: Introduction)

So what you just viewed in the video is one part of a much bigger movement happening around Caliptra and hardware-rooted security.

Before I begin, I'd like to briefly connect this presentation to some of the activities we've just been involved in. Earlier this week in Taipei, we participated in a Caliptra workshop focused on implementation and on bringing the specification closer to production silicon. We also joined two sessions at OCP APAC, where we discussed Caliptra and chiplet security from both the architecture and system perspectives.

Those discussions reinforced something we've been seeing more broadly across the industry: these security technologies are becoming increasingly important as AI servers and data-center infrastructure become more distributed and more interconnected.

So rather than trying to cover everything happening around Caliptra, I'd like to use the next few minutes to focus on the underlying reason this movement is gaining momentum. And I want to start not from security, but from the way AI compute itself is changing. AI systems are increasingly being built across multiple dies, accelerators, memory devices, and high-speed fabrics. As more components are connected together, more of those components and interfaces also need to be individually trusted and protected. That is really the story behind today's presentation.

(Page 15: AI Compute Can No Longer Scale in a Single Die)

When we talk about scaling AI compute, simply making one chip larger is no longer enough. In the past, if we wanted more performance, we could build a larger die or move to a more advanced process node. But there are practical limits to that approach,

including die size, yield, cost, power, memory bandwidth, and I/O all start to become constraints. So increasingly, the industry is scaling by composition.

There are two important architectural trends shown on this slide, and I want to separate them because they're related, but they're not the same thing.

The first one is chiplets, which operate inside the package. Instead of building one enormous monolithic SoC containing every function, we can divide the system into multiple specialized dies. So, for example, we might have a compute or CPU die, accelerator dies for GPU or NPU functions, an I/O die, a management die, a security die, or other specialized functions.

Very importantly, these dies do not necessarily need to use the same process technology. The compute portion may benefit from the most advanced node, while I/O, management, or security functions may be more economical on less advanced nodes. So chiplets give us modularity, reuse, better economics, and another way to continue scaling the processor package.

But even after we scale inside the package, we eventually hit another boundary, the processor socket and the server itself. And that's where compute express links, CXL, comes in. CXL operates at the system level, outside the processor package.

Here you can see the servers on the left connected through a CXL fabric switch to a Type-3 memory shelf on the right. Instead of memory belonging permanently to only one CPU socket, CXL allows memory and other devices to participate in a coherent fabric. That means memory can increasingly be expanded, pooled, shared, and dynamically assigned across systems.

So overall, we can think of it as: chiplets scale the processor by combining multiple specialized dies in one package. CXL scales the system by connecting processors, accelerators, and memory across the server. And that is a very important shift for AI infrastructure. We are moving away from scaling only through one larger piece of silicon and toward scaling by connecting many specialized resources together.

But composition has a security consequence. Every new die, device, link, controller, and firmware layer creates another place where trust has to be established. And that brings us to the other side of this architecture.

(Page 16: Composable AI Infrastructure Expands the Attack Surface)

The same composability that gives us flexibility and scalability also creates a much larger attack surface. Let me separate this again into the two architectural domains.

On the CXL side: We now have multiple endpoints joining a fabric, high-value memory moving across links, switches controlling connectivity, and a fabric manager potentially deciding how pooled resources are allocated. That introduces several different classes of risk. For example, if the firmware of a highly privileged infrastructure components such as the CXL switch is compromised, the impact radius can be very large, because now the attacker is not targeting only one endpoint. They may potentially manipulate connectivity, resource allocation, or the behavior of multiple devices in the fabric.

Another important area is DMA, or direct memory access. DMA itself is a legitimate and very powerful capability. The security problem is when a compromised or malicious device receives more access than it should have. If those permissions are not properly controlled, a device could potentially read or modify memory outside its authorized region. And in an environment where memory is pooled or shared, the consequence can become especially serious, including data leakage across workloads or even between tenants.

Inside the chiplet package, the security problem looks different, but the principle is the same. Now we're dealing with multiple active dies communicating across die-to-die interfaces.

A counterfeit or rogue chiplet could introduce an unauthorized component into the package or supply chain, severely affecting silicon identity and supply-chain trust. A malicious or unauthorized die can introduce hardware Trojans, manipulate transactions, leak data, or undermine the assumptions of the entire package. Recent chiplet-security research specifically highlights malicious chiplets and hardware Trojans as major system-level threats.

Chiplets may also be attacked leading to key extraction and secret leakage. If the root key or device secret is compromised, the consequence is much bigger than simply losing one piece of data. An attacker may be able to impersonate the device or undermine the trust relationships built on top of that identity.

I don't expect everyone to remember all twelve attacks on this slide, but the important point is what they collectively tell us: the trust boundary has expanded. Security can no longer exist only at the board level, or only around the CPU. What we increasingly need to know are these: Is this device or die authentic? Did it boot trusted firmware? Can I trust the keys inside it? Can I trust the communication between components? And can I prove that trust to the rest of the system?

That is why the root of trust increasingly has to move closer to the individual silicon itself. And this is where architectures such as Caliptra become very important.

(Page 17: Caliptra Root of Trust Requires a Physical Security Anchor)

Caliptra gives us an open architecture for establishing a hardware Root of Trust in modern devices. But there is an important distinction here between the digital Root-of-Trust architecture and the physical security foundation underneath it.

On the left, we have the Caliptra subsystem. The Caliptra core includes things such as the RISC-V processor, cryptographic functions, SRAM and ROM, the mailbox, and the firmware responsible for implementing the security architecture. But ultimately, all of that digital security logic has to anchor itself to something physical in silicon.

There are three foundational requirements, which we also call foundational security primitives, I want everyone to remember. First, a unique device secret, UDS. We need something unique to the individual piece of silicon that can establish device identity and support key derivation. Second, secure non-volatile storage. Security-critical information — lifecycle state, configuration, seeds, or other protected values — needs to survive power cycles and remain protected from unauthorized modification. Third, trustworthy entropy. All of the cryptography above this layer ultimately depends on good randomness. If the entropy is weak or predictable, the keys derived from it can also become weak or predictable.

So Caliptra provides the architecture and framework for the Root of Trust. But the foundation of that trust still has to terminate in physical properties and protected state inside the silicon. That is the physical security anchor. And those requirements map very naturally to technologies of hardware security that eMemory and PUFsecurity have already been developing for many years.

(Page 18: PUFrt Provides the Physical Anchor Beneath Caliptra)

This is where we move from the architecture to the actual silicon implementation. For the unique device secret, we use NeoPUF. Rather than simply programming the root secret into conventional memory, NeoPUF derives device-unique information from the intrinsic physical characteristics of each individual piece of silicon. That gives us a silicon-bound foundation for device identity and key derivation.

For secure nonvolatile storage, we have NeoFuse, our OTP technology. NeoFuse provides protected storage for security-critical information such as lifecycle values, seeds, configuration, or other persistent security assets.

For entropy, we provide the physical noise source supporting the TRNG, giving the cryptographic system the randomness required for secure key generation and operation.

And we're extending this foundation into the post-quantum era through PUF-PQC.

Importantly, we view these IPs as different pieces of the same security foundation: identity, protected storage, trusted entropy, and cryptographic agility. And together, these are the types of silicon-level primitives that a framework such as Caliptra ultimately needs in order to establish trust. But having the primitives is only part of the problem. For customers, the next question is how to integrate all of these pieces into a complete, validated security subsystem.

(Page 19: From Hardware Anchor to Security Platform)

And this is really where our strategy goes beyond selling individual IP. We start with PUFrt as the hardware anchor. Around that, we add the required anchor IP, post-quantum security capabilities, and importantly our integration experience with Caliptra.

Because from a chip designer's perspective, the difficult question isn't just, ‘Can I license a PUF?’ The real question is: How do I turn the specification into silicon that actually works? How do I connect the hardware primitives to the Root of Trust architecture? How do I validate the interfaces? How do I shorten integration and verification time?

That is why we're moving toward a validated subsystem approach. And once that foundation is available, the same security architecture can scale across accelerator boards, AI servers, rack-scale systems and eventually data-center infrastructure.

What starts as a few very small security blocks in silicon can ultimately become the trust foundation for a much larger computing platform. And that brings us back to where we started, this increasingly composed AI system.

(Page 20: Trust Must Extend Across Every Layer of AI Infrastructure)

AI infrastructure is becoming distributed across multiple layers. At the system level, CXL can protect data moving across a link through mechanisms for confidentiality, integrity, and replay protection. But protecting the link does not automatically mean that the device on the other end should be trusted. That endpoint still needs an identity, trusted firmware and secure boot, and it also needs to be able to prove its state through attestation.

The multi-die package follows similar principles: each active chiplet may have its own identity, keys, firmware, lifecycle state, and relationship with the other dies in the package.

So trust increasingly has to extend from: the data center... to the rack... to the server... to the device... to the package... and ultimately down to the individual silicon. And that is why our foundational IP is so important.

Technologies such as NeoPUF, NeoFuse, our entropy source, and PUF-PQC may be physically small pieces of the overall AI system, but they provide some of its most fundamental security properties: a unique identity, protected state, trustworthy randomness, and cryptographic trust. PUFrt brings those capabilities together as the physical hardware anchor, while Caliptra provides the architecture that builds a Root of Trust on top of them.

So as AI compute becomes more composable and more distributed, we believe security has to follow exactly the same direction: trust must also become distributed, but it must remain anchored in silicon. And that is the role we see for eMemory and PUFsecurity's foundational IP: providing the silicon trust foundation that enables secure chiplets, secure CXL-connected devices, and ultimately the next generation of AI infrastructure.

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!