# eMemory 2Q24 Earnings Call Transcript

August 7th, 2024, 16:00-17:00 Taiwan Time

## OPENING REMARKS

**Dr. Charles Hsu, Chairman**

Good afternoon, everyone, and thank you for attending our conference call today.

As mentioned in the previous quarters, our company has entered a multi-year growth cycle. Last quarter, we shared that we've licensed our technologies to almost every foundry worldwide with more than 600 process platforms. This number of process platforms continues to grow every year. Within these process platforms, our technologies developed from OTP to more sophisticated security IPs and MTP extending to various kinds of emerging memories. The royalties received per wafer for these technologies will increase as 1) the process nodes, 2) the memory functions, and 3) the functions of the chip security IPs, all become more advanced.

Later I will introduce one of our security IPs, PUFtrng (PUF-based True Random Number Generator), which is 100 times faster than the widely used conventional one. It leverages our PUF as the perfect source of randomness.

This shows that we can continue to use our existing technologies and IPs to develop new IPs with additional functions. Not only does this show the importance and competitiveness of our intrinsic technology, but it also forms the most important foundation for our long-term growth, allowing us to continue innovation based on our core competencies. Therefore, we are very confident about our future.

Next, I'll invite our president, Michael Ho, to share our second-quarter performance and future outlook.

## FINANCIAL RESULTS

**Michael Ho, President**

Q2 2024 Financial Results

Good afternoon, everyone. Now, let's begin with our 2024 second-quarter financial results.

The second-quarter revenue was eight hundred and ninety-three million NT dollars (NT$ 893 mil), up 11.2% sequentially and up 28.2% year-over-year.

Operating expenses were three hundred and ninety-eight million NT dollars (NT$ 398 mil), up 4.1% sequentially and 21.3% year-over-year.

Operating income was four hundred and ninety-five million NT dollars (NT$ 495 mil), with an increase of 17.7% sequentially and an increase of 34.3% year-over-year.

Operating margin increased by 3.1 percentage points sequentially and increased by 2.6 percentage points year-over-year to 55.5%. Our net income, amounting to four hundred and seventy-five million NT dollars (NT$475 mil), experienced an increase of 10.3% sequentially and 35.1% year-over-year.

EPS for the quarter was 6.36 NT dollars (NT$ 6.36) and ROE was 67.3%.

Revenue across Different Streams

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

**Licensing** in the second-quarter accounted for 33.6% of the total revenue, up 31.3% sequentially and up 20.0% year-over-year.

**Royalties** in the second-quarter contributed 66.4% of the total revenue, increasing 3.3% sequentially and increasing 32.8% year-over-year.

**Total revenue** for the second-quarter increased by 11.2% compared to the previous quarter and increased by 28.2% compared to the previous year.

For the first half of 2024, the licensing and royalty revenues are as follows:

**Licensing** in the first half accounted for 31.1% of the total revenue, up 34.4% year-over-year.

**Royalties** in the first half contributed 68.9% of the total revenue, increasing 20.2% year-over-year.

Total revenue for the first half increased by 24.3% compared to the previous year.

Revenue by Technology

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

**NeoBit** accounted for 24.6% of total licensing revenue in the second-quarter, increasing 54% sequentially and increasing 30.2% year-over-year. Its royalties accounted for 26.7% of total royalty, up 11.3% sequentially and up 15.9% year-over-year.

**NeoFuse** accounted for 33.3% of total licensing revenue in the second-quarter, down 16.7% sequentially and down 11.9% year-over-year. In terms of total royalty revenue, NeoFuse royalties increased by 0.2% sequentially and increased by 39% year-over-year, accounting for 70.6% of total royalties.

**PUF-Based Security IPs** contributed 12.5% of licensing revenue, increasing 105.2% sequentially and increasing 36% year-over-year, while its royalties accounted for less than 1% of total royalties.

**MTP technology** accounted for 29.6% of total licensing revenue, up 110% sequentially and up 69.9% year-over-year. Royalty from MTP increased 11.6% sequentially and increased 86.8% year-over-year, accounting for 2.7% of total royalties.

For the first half of 2024, the revenues by technology are as follows:

**NeoBit** licensing revenue increased 43.4% year-over-year and royalty increased 1.4%, accounting for 24.9% of the total revenue.

**NeoFuse** licensing revenue increased 19.3% and royalty increased 27.3% year-over-year, contributing to 62.3% of the total revenue.

**PUF-based security IP** licensing revenue increased 26.3% year-over-year, while the royalty contribution was less than 1%, accounting for 3.3% of the total revenue.

**MTP technology** licensing revenue increased 64.3% year-over-year and royalty revenue increased 75.7%, accounting for 9.5% 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 42.5% of royalties, up 2.6% sequentially and up 26.7% year-over-year.

**12-inch wafers** contributed 57.5% of royalties, increasing 3.8% sequentially and up 37.6% year-over-year.

In total, 171 product tape-outs were completed in the second-quarter. We will provide more information in the management report.

## FUTURE OUTLOOK

**Michael Ho, President**

In the next section, I will address our future outlook.

**For licensing revenues:** Licensing revenue will continue its growth momentum due to strong demands from both foundries and chip companies.

**For royalty revenues:** We expect royalty sequential growth in H2 due to new products ramping up.

Moving on to new IP technology and business development

**New IP Technologies:**

1. NeoFuse is developing in FinFET HV process to meet customers' next generation OLED DDI plans.

2. RRAM is expanding into more processes with increased customers' demand.
3. NeoFlash continues progressing in specialty processes replacing embedded flash and external NOR flash.
4. Developing 2nm technologies with leading foundries.

**Business Development Platform:**

1. New CPU architecture for security IP will start to contribute to revenue.
2. Successfully integrated NeoFuse for SRAM repair with EDA company.

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

## CHAIRMAN REMARKS

**Dr. Charles Hsu, Chairman**

**(Page 13: A Must in Security: 100X Faster PUF-based TRNG)**

The role of a True Random Number Generator (TRNG) is crucial in fortifying secure systems against increasingly sophisticated attacks. Today, I will discuss why having just any TRNG is not enough; you need a high-speed and high-quality TRNG.

**(Page 14: True Randomness Makes Guessing Impossible)**

Before understanding the role of randomness in protecting a secure system, it is essential to know the methods used to attack these systems. This slide will explain why a True Random Number Generator is necessary for hardware security.

There are two ways to break into a secure system. The first is cryptographic analysis (cryptanalysis), a technique existing for centuries where attackers uncover weaknesses in cryptographic algorithms. Over time, such attacks have driven the evolution of cryptographic standards, with older algorithms like the Data Encryption Standard (DES) replaced by newer ones such as the Advanced Encryption Standard (AES).

The second method is implementation attacks, which target specific weaknesses within a system's implementation, exploiting the weaknesses to discover secrets within the secure system. Now, assuming that we have a well-designed secure system that

is resistant to cryptanalysis and implementation attacks, how will an attacker be able to break into the system? In this case, they will attempt to guess the secret key, as obtaining it would allow them to access a lot of confidential information from the system. To prevent an attacker from correctly guessing the secret key, we must minimize its probability. The first factor is key length, which is pre-defined by the crypto algorithms. For example, if the key length is 128-bit, it means that there are 2^128 (two to the power of one-hundred and twenty-eight) number of possible key combinations that can be generated.

The second factor is ensuring random generation of the key so that each combination is equally probable. If you refer to this diagram, you can see that after the user encrypts their secret with a randomly generated key, the probability of an attacker guessing the correct combination is reduced to 1/2^128 (one over two to the power of one-hundred and twenty-eight). Therefore, to achieve this result and reduce the likelihood of an attacker guessing the correct secret key, we must use TRNGs.

**(Page 15: High-speed TRNG: Why Throughput Matters?)**

In the next slide, I will explain why it's important to have a high-speed TRNG. By high-speed, we are referring to a high throughput, the capability of generating large volumes of random numbers in a short time.

The speed and throughput of a TRNG matters because large systems often have numerous applications and hardware components that require and consume random numbers. Many of these components cannot generate their own random numbers and rely on a hardware-based TRNG. Given the extensive number of components the throughput of the TRNG is vital to ensure numbers are generated quickly and efficiently.

Besides generating large volumes of random numbers, a high-throughput and high-quality TRNG can help prevent side-channel attacks. Side-channel attacks are one of the most popular forms of attacks, where attackers exploit leaked information from sources such as power consumption or electro-magnetic (EM) emissions to discover keys. To counter these attacks, new random numbers must be generated continuously to mask the side channel information. The middle figure shows a simplified example of a crypto operation protected by masking. In a masked operation, the random bits transform the input data into two independent sets and are sent to two separated mask operations. Compared to a single operation, separating them ensures there is no

leakage. Since the operations continually consume random numbers, the throughput of TRNG is also important in this use case.

Beyond security, there are other applications that are highly reliant on random numbers. One example is banking, where many keys or pin numbers require high-quality random numbers to ensure the security of accounts. Because the number of accounts and transactions are enormous, a high-throughput TRNG is essential as well, as shown on the third figure at the bottom.

**(Page 16: PUFtrng: 100 Times Faster than Conventional TRNG)**

Having described the importance of a high-throughput and high-quality TRNG, it's clear that our solution, PUFtrng, meets these criteria.

A unique feature of our TRNG is that it has two entropy sources. Unlike conventional TRNGs that rely on a single source, our PUFtrng combines dynamic entropy from ring oscillators (which is everchanging) with static entropy from our NeoPUF chip fingerprint (constant and unchanging).

Normally, dynamic entropy operates slowly due to the time-consuming process of collecting natural fluctuations, leading to low throughput in conventional TRNGs, as illustrated using the dashed lines. The throughput in this case is usually less than one megabit per second.

To overcome this limitation, PUFtrng uses high-quality random bits generated by PUF to refine the output of the dynamic entropy source. Typically, it takes the dynamic entropy source a long time to gather natural fluctuations. However, by using PUF for refinement we can achieve a high throughput by reducing the collection time of the dynamic entropy, yet still achieving high quality output. As shown in the figure, PUFtrng delivers throughput approximately 100 times greater than conventional TRNGs, while maintaining similar power consumption.

**(Page 17: PUFtrng: 100 Times Faster than Conventional TRNG)**

We also created animations to better show the differences between PUFtrng and conventional TRNGs:

In figures 1 to 4, we invented a simple topology optimization inside the circle to determine the randomness of the random number generators. The uniformity of the lines inside the circle indicates the randomness of the numbers. If the numbers are truly random, the circle begins to fill uniformly as more random numbers are generated. On the other hand, if the randomness of the generated numbers is poor, the lines inside the circle will not be uniformly distributed.

- **Dynamic Entropy generated by ring oscillators (Figure 1):** Within the blue circles, a single blue line represents a 10-bit random number. The dynamic entropy constantly generates random data. However, its output quality is not enough for secret keys because the lines tend to appear at similar positions, indicating that the randomness of the random numbers is poor.

- **Conventional TRNG using post-processing (Figure 2):** Here, random numbers are generated by gradually accumulating more random bits (lines) from the dynamic entropy. Over time and after going through post-processing, the output (circle) will slowly become uniform and complete.

- **Static Entropy generated by PUF (Figure 3):** Static entropy is instantly ready and does not change over time. The lines are very uniform, indicating that the results are of very high quality from the start.

- **PUFtrng using PUF refinement (Figure 4):** In PUFtrng, the generated numbers form uniform lines, indicating high quality output. Additionally, the speed of generation is much faster than the conventional TRNG. This is evident from the fact that the output (circle) generated by the lines in PUFtrng (Figure 4) appears much faster than in Conventional TRNG (Figure 2), highlighting the difference in generation speed.

Another way to understand this is to imagine conventional TRNGs as classic cars; they are functionable but not efficient. They are either slow or consume a lot of gas when running fast. In comparison, PUFtrng is like a new-energy car; it runs fast while consuming low power. Lastly, another advantage of PUFtrng is that both the dynamic entropy and static entropy are implemented in hard macro and pre-qualified across various technology nodes. This ensures superior quality compared to RTL-based TRNGs provided by other IP vendors or customers.

In conclusion, the integration of a high-speed, high-throughput TRNG is vital for maintaining system security and functionality. Our PUFtrng solution stands out with its ability to generate high-quality random numbers efficiently. This not only protects against sophisticated attacks, but also supports large-volume random number generation. With PUFtrng, we are setting a standard for high-quality TRNGs.

That concludes my remarks. Thank you very much for your time.

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!