eMemory 4Q24 Earnings Call Transcript

February 12th, 2025, 16:00-17:00 Taiwan Time

OPENING REMARKS

Dr. Charles Hsu, Chairman

Good afternoon, everyone. Thank you for joining our conference call today.

As we've mentioned in previous quarters, we are currently entering a multi-year growth cycle. The recent licensing activity indicates that our technologies are being adopted at an increasing rate, and we are very optimistic about the future.

Recently, there has been a growing focus on the potential for faster AI deployment at the edge, which is a very encouraging trend for us. Our technologies, including OTP and MTP, along with a variety of security IPs, enable chips to achieve improved performance, reduced costs, and enhanced security. Since edge computing demands lower power, higher cost-effectiveness, and stricter security, this will accelerate our customers' adoption of our IPs. This trend is already reflected in our recent licensing across various applications, such as networking, BMC, smart surveillance, and other edge-related applications.

Moreover, there is an ongoing discussion regarding the timeline for the commercialization of quantum computing, with opinions varying on whether it will occur in five years or fifteen. Quantum computers have the capability to quickly compromise current encryption standards that safeguard a significant portion of global data and infrastructure. Considering that hardware transitions typically take between 5 to 10 years at least, the U.S. National Institute of Standards and Technology (NIST) has implemented post-quantum cryptography (PQC) standards to mitigate the cybersecurity risks associated with quantum computing. This transition presents a significant opportunity for our PUF-based solutions, including our newly launched PQC IPs. Later, I will provide further insights on this topic.

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

FINANCIAL RESULTS

Michael Ho, President

Q4 2024 Financial Results

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

The fourth-quarter revenue was one point zero one billion NT dollars (NT$ 1.01 bil), up 12.4% sequentially and up 12.4% year-over-year.

Operating expenses were four hundred and forty-five million NT dollars (NT$ 445 mil), up 12.7% sequentially and up 23.8% year-over-year.

Operating income was five hundred and sixty-six million NT dollars (NT$ 566 mil), with an increase of 12.1% sequentially and an increase of 4.9% year-over-year.

Operating margin decreased by 0.1 percentage point sequentially and decreased by 4 percentage points year-over-year to 56%. Our net income, amounting to five hundred and fifteen million NT dollars (NT$515 mil), experienced an increase of 24.3% sequentially and increased 27.5% year-over-year.

This quarter's operating margin fell by 4 percentage points compared to the same time last year, mainly because of rising salaries and bonuses. Employee bonuses are calculated at 15% of pre-tax profit. Unlike the foreign exchange loss we experienced in the fourth quarter of 2023, this quarter we benefited from a foreign exchange gain. This variation in non-operating results resulted in higher bonus payouts, which contributed to the decrease in the operating margin.

EPS for the quarter was 6.89 NT dollars (NT$ 6.89) and ROE was 62.5%.

Revenue across Different Streams

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

Licensing in the fourth-quarter accounted for 31.2% of the total revenue, up 8.5% sequentially and up 15.1% year-over-year.

Royalties in the fourth-quarter contributed 68.8% of the total revenue, increasing 14.2% sequentially and increasing 11.3% year-over-year.

Total revenue for the fourth-quarter increased by 12.4% compared to the previous quarter and increased by 12.4% compared to the previous year.
For the full year of 2024, total revenue increased by 18.2% compared to the previous year. Total licensing and royalties increased by 22.5% and increased by 16.4%, respectively.

Revenue by Technology

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

NeoBit accounted for 20.9% of total licensing revenue in the fourth-quarter, decreasing 27.2% sequentially and decreasing 8.3% year-over-year. Its royalties accounted for 24.8% of total royalty, up 9% sequentially and up 26.1% year-over-year.

NeoFuse accounted for 39.1% of total licensing revenue in the fourth-quarter, up 41.9% sequentially and up 5.1% year-over-year. In terms of total royalty revenue, NeoFuse royalties increased by 16.7% sequentially and increased by 7.8% year-over-year, accounting for 73.1% of total royalties.

PUF-Based Security IPs contributed 22.6% of licensing revenue, increasing 104.1% sequentially and increasing 138.7% year-over-year, while its royalties accounted for less than 1% of total royalties.

MTP technology accounted for 17.4% of total licensing revenue, down 30.1% sequentially and down 0.2% year-over-year. Royalty from MTP decreased 5.4% sequentially and decreased 13.8% year-over-year, accounting for 2% of total royalties.

For the full year of 2024, the revenues by technology are as follows:

NeoBit licensing revenue increased 22.2% year-over-year and royalty increased 14.7%, accounting for 25.2% of the total revenue.

NeoFuse licensing revenue increased 7.2% and royalty increased 16.5% year-over-year, contributing to 61.3% of the total revenue.

PUF-based security IP licensing revenue increased 23.4%, accounting for 4.5% of the total revenue.

MTP technology licensing revenue increased 59% year-over-year and royalty revenue increased 30.3%, accounting for 9% 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 40.8% of royalties, up 13.9% sequentially and up 20% year-over-year.

12-inch wafers contributed 59.2% of royalties, increasing 14.4% sequentially and up 6% year-over-year.

In total, 181 product tape outs were completed in the fourth-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.

Regarding licensing revenue: We anticipate that licensing revenue will continue its growing momentum due to increasing demand from both foundries and end chip customers. We continue to launch new IPs, and available on increasing number of process nodes on worldwide foundries.

As for royalty revenue: We expect royalty revenue to continue its growth trend, driven by a robust number of tape outs in the pipeline that are moving into production. In 2024, we achieved a record-high in NTO numbers.

New IP Technologies:

1. NeoFuse is advancing various derivative processes at leading edge nodes, having secured design wins in 3/4/5/6/7nm process nodes.
2. RRAM is broadening into automotive grade, and already have multiple customer design wins.
3. NeoFlash continues its progress in specialty processes, aiming to replace embedded flash and external NOR flash.
4. Developing 2nm technologies in collaboration with leading foundries.

Business Development Platform:

1. We have joined Arm Total Design and introduced PUFrt as the hardware root of trust for the RSE in CSS.
2. We have developed PUFhsm, an embedded Hardware Security Module solution for automotive chips and high-performance computing (HPC). Together with the hardware root of trust (PUFrt), PUFhsm provides a comprehensive secure enclave solution.

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

CHAIRMAN REMARKS

Dr. Charles Hsu, Chairman

(Page 13: Why Post-Quantum Cryptography (PQC) Needs PUF?)

(Page 14: Why PQC Needs PUF?)

As we approach a future where quantum computers may be able to compromise our existing encryption techniques, the importance of Post-Quantum Cryptography (PQC) increases significantly.

PQC aims to create cryptographic systems that can withstand attacks from quantum computers. To ensure PQC's effectiveness, we need reliable methods for key generation and maintaining the integrity of these cryptographic systems, which is where PUF come into play.

PUF can effectively generate the long keys necessary for PQC, as the security of PQC relies on these extended keys to defend against quantum computing threats. PUF can securely and efficiently produce the unique secrets needed to create these long keys, making it an ideal choice for key provision in PQC.

Additionally, PUF can generate random numbers efficiently, which are crucial for preventing tampering in PQC. The essence of PQC lies in safeguarding data with long keys, and beyond being resistant to quantum attacks, cryptographic systems must also incorporate anti-tampering features to protect keys and encrypted data from physical threats. Randomness is vital for obscuring the data process, and since PUF naturally possesses randomness and uniqueness, it can be utilized in designs that resist attacks, effectively implementing anti-tampering strategies.

(Page 15: What is PQC?)

Now, I will explain what PQC is. PQC stands for post-quantum cryptography, which includes cryptographic algorithms designed to protect data from the potential risks associated with quantum computers. These quantum computers are anticipated to outperform classical computers in solving specific mathematical problems, which poses significant risks to many cryptographic methods, particularly the widely used RSA and ECC algorithms, as their security relies on algorithms that quantum computers can efficiently solve. PQC algorithms are intended to ensure secure communication and data protection, even in the face of quantum computing advancements, thereby maintaining security in our interconnected world when quantum computers become a practical reality.

(Page 16: Why is PQC Needed?)

So, why is PQC essential at this moment? As quantum computing progresses, the demand for encryption capable of resisting quantum attacks becomes critical. Many systems in use today retain encrypted data for extended periods, sometimes for years or even decades. Consider financial transactions, personal data, or sensitive government information. If this data is encrypted with methods that are susceptible to quantum attacks, it could be at risk in the future. The sooner we implement PQC, the sooner we can guarantee the security of our data in a quantum future.

To prepare for a post-quantum environment, the National Institute of Standards and Technology (NIST) has been spearheading the development of new cryptographic standards that can endure quantum computing threats. Following multiple evaluation phases, NIST officially announced in 2024 the adoption of Module-Lattice Based Key

Encapsulation (ML-KEM), Lattice-based Digital Signatures, and Hash-based Digital Signatures as the standards for post-quantum algorithms. Organizations globally are now embracing these new standards to safeguard our data against potential quantum risks. We will be launching our PQC IPs based on the first two standards in this quarter.

(Page 17: How PUF-based Solutions Help PQC?)

Given the necessity for our data to remain secure in the future and the time required to develop new encryption systems, it is essential to begin transitioning to Post-Quantum Cryptography (PQC) now. This proactive approach will ensure that we are prepared by the time quantum computers become capable of posing a threat.

Typically, PQC algorithms involve increased computational complexity and more extensive key storage requirements. I will now outline how our PUF-based solutions facilitate PQC. Our PUF-based Root of Trust (PUFrt) comprises several components. First, there is NeoPUF, which generates a unique ID for each device, enabling the creation of long secret keys for PQC. Next is NeoFuse OTP (One-Time Programmable), a compact and secure method for storing PQC keys. In comparison to eFuse, OTP offers superior security, particularly in advanced nodes, while also being more area-efficient for larger data sizes.

Modern cryptographic systems, including PQC, are susceptible to side-channel attacks; therefore, our solution incorporates a built-in True Random Number Generator (TRNG) that continuously supplies a substantial amount of random numbers. These random numbers are crucial in thwarting attacks aimed at compromising PQC keys.

Moreover, for a successful transition to PQC, the cryptographic system must accommodate both traditional and PQC algorithms, allowing for flexible selection between them or hybrid solutions. By integrating the PUFrt into the security subsystem, it can effectively handle the large and complex keys needed for PQC algorithms alongside the smaller keys for traditional algorithms, eliminating the need for separate key generation for both systems. As previously mentioned, PUFrt can produce high-quality, unique PQC keys that are securely stored in OTP, safeguarding their confidentiality and integrity while preventing unauthorized access and tampering. Additionally, the TRNG continuously generates a significant volume of random numbers, which are utilized for countering side-channel attacks, thereby enhancing the overall security of key management within the system.

In conclusion, to ensure the long-term security of our data against quantum computing threats, the integration of a PUF-based security subsystem is vital. This approach will allow us to maintain high levels of security and resilience as we transition to PQC. 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!