eMemory 2Q23 Earnings Call Transcript

August 9th, 2023, 16:00-17:00 Taiwan Time

OPENING REMARKS

Dr. Charles Hsu, Chairman

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

We expect our revenue to grow sequentially in the second half of the year due to strong licensing and accumulated new tape outs entering into the production stage. There is a very strong demand for our 5nm and 3nm solutions, especially from Mobile, Data Center, AI and Autonomous Driving. We are very confident in our future growth for many years to come.

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

FINANCIAL RESULTS

Michael Ho, President

Q2 2023 Financial Results

Good afternoon, everyone. Now, let's begin with our 2023 second-quarter financial results. The second-quarter revenue was six hundred and ninety-seven million NT dollars (NT$ 697 mil), up 4.3% sequentially but down 12.5% year-over-year.

Operating expenses were three hundred and twenty-eight million NT dollars (NT$ 328 mil), up 9% sequentially, mainly attributable to the increase in bonuses and rewards.

Operating income was three hundred and sixty-nine million NT dollars (NT$ 369 mil), with an increase of 0.5% sequentially but decreasing 19.9% year-over-year. The operating margin decreased by 2.1 percentage points sequentially and decreased by 4.9 percentage points year-over-year to 52.9%.

EPS for the quarter was 4.71 NT dollars (NT$ 4.71) and ROE was 53.5%.

Revenue across Different Streams

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

Licensing in the second-quarter accounted for 35.8% of the total revenue, up 74.6% sequentially and 24.4% year-over-year.

Royalties in the second-quarter contributed 64.2% of the total revenue, decreasing 14.8% sequentially and 25% year-over-year.

Total revenue for the second-quarter increased by 4.3% compared to the previous quarter but decreased by 12.5% compared to the previous year.

Revenue by Technology

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

NeoBit accounted for 22.7% of total licensing revenue in the second-quarter, increasing 101% sequentially and up 27.6% year-over-year. Its royalties accounted for 30.5% of total royalty, down 14.6% sequentially and down 42.8% year-over-year.

NeoFuse accounted for 45.4% of total licensing revenue in the second-quarter, up 60% sequentially and up 20.5% year-over-year. In terms of total royalty revenue, NeoFuse royalties decreased by 15.3% sequentially and 10.2% year-over-year, accounting for 67.5% of total royalties.

PUF-Based Security IPs contributed to 11% of licensing revenue, increasing 66.3% sequentially but decreasing 41.4% year-over-year. Its royalties accounted for less than 1% of total royalties, up 123.3% compared to the previous quarter, but down 18.8% compared to the previous year.

MTP technology accounted for 20.9% of total licensing revenue, up 89.9% sequentially and up 239% (two hundred and thirty-nine) year-over-year. Royalty from MTP decreased 1.6% sequentially and 58.4% year-over-year, accounting for 1.9% of total royalties.

Q2 2023 Royalty Revenue by Wafer Size

Now, let's look at royalties for 8-inch and 12-inch wafers.

8-inch wafers, accounted for 44.5% of royalties, down 19.2% sequentially and 34.5% year-over-year.

12-inch wafers contributed 55.5% of royalties, decreasing 10.9% sequentially and decreasing 15% year-over-year.

In total, 147 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.

We expect our revenue to grow sequentially in the year's second half.

For licensing revenues: We expect the licensing revenue to increase significantly compared to the first half of the year.

For the royalty revenues: As new applications gradually enter the mass production stage, we expect royalties to grow quarter after quarter for the rest of the year.

Moving on to new IP technology and business development:

1. The demand for 5nm design licensing is very strong. We have customer adoption for Autonomous Driving, Data Centers and AI-related this year.
2. We are developing 3nm in several foundries with many customer requests and continue cooperating with CPU partners for 3nm Confidential Computing.
3. 22nm emerging memory MRAM and ReRAM completed verification with customer design-ins.

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

CHAIRMAN REMARKS

Dr. Charles Hsu, Chairman

Page 12: Forefront of Security: Confidential Computing

If you remember my previous talk, I mentioned confidential Computing, which has become even more relevant than two years ago. Today, I will share with you a more detailed version of how it works, what Nvidia is using Confidential Computing for, and most importantly, how exactly a PUF-based Confidential Computing method differs from others and why it's more secure.

(Page 13: What is Confidential Computing?)

In many applications, computers deal with sensitive data, or face certain data regulations, such as health or financial services. The integrity and confidentiality of these data can be compromised by unauthorized parties. This is why we need to establish Confidential Computing, otherwise known as "the protection of data in use by performing the computation in a hardware-based Trusted Execution Environment." (*Official definition of Confidential Computing as stated by Nvidia*)

You might have seen this diagram before, but I wanted to reiterate how data works. Data is comprised in different stages: data-at-rest, data-in-transit and data-in-use. To ensure the integrity and confidentiality of data-in-use, Confidential Computing is needed.

In Confidential Computing, a Trusted Execution Environment (TEE) is deployed to provide an isolated environment separated from the main operating system where data can be processed without exposure to the rest of the system.

(Page 14: Confidential Computing Illustrated)

To understand how Confidential Computing works, please look at the left graph. For example, Core Processing Units (CPU) have a secure and non-secure zone. Applications and OS on regular CPUs cannot access the secure zone. However, with Confidential Computing, sensitive data from apps/OS can be stored in the secure zone under individually isolated TEEs on the CPU.

(Page 15: Confidential Computing in Nvidia's GPU for AI)

Another example of Confidential Computing is in Graphic Processing Units (GPU). GPU has its own Hardware Root of Trust (HRoT) to enable an isolated TEE for protecting the integrity and confidentiality of data and code during the transfer from CPU to GPU, and processing in the GPU.

Nvidia uses Confidential Computing for their AI training. As you can see on the graph, during code/data transfers from CPU to GPU, multiple individual TEEs are created through the GPU's HRoT so that unauthorized entities are prevented from accessing the AI application data and code.

Therefore, the TEE needs to have robust and hardware-based security (Hardware Root of Trust) to secure the following actions:

1. Device Authentication: when users/devices are communicating with the GPU, they have to confirm if the firmware and software of the GPU are secure. The GPU also needs to authenticate the firmware and software from OS/apps to check that they have not been tampered with.
2. Data Integrity and Confidentiality: a better way to understand it is that the data being transferred will be encrypted/decrypted with encryption keys exclusive to the CPU and GPU.

(Page 16: PUF-based HRoT for TEE)

Now that we know the role of the TEE, let's identify the role of the HRoT. The HRoT in TEE can help protect the integrity and confidentiality of data and codes. It consists of key storage, key generation, key protection, and cryptographic engine, all combined for comprehensive security.

Our PUF-based Crypto Coprocessor IP (PUFcc) can fulfil the role of all functions mentioned above. Our secure OTP consisting of both our Anti-fuse technology and PUF-based technologies creates secure key storage that hides the keys and their whereabouts from potential attackers. Furthermore, our PUF-based TRNG can efficiently generate truly random keys to protect data and code.

PUFcc also includes additional components and cryptographic engineering which performs security functions such as Encryption/Decryption, authentication, and signing.

(Page 17: PUF-based Key Storage vs. Conventional)

For the HRoT, I would like to focus on key generation and key storage by comparing our own technology to conventional methods. Our PUF-based OTP helps the industry migrate to a very high-level security regime by improving the security of key storage and key generations.

Conventional key storage eFuse, which is insecure for many reasons:

1. Burning of the Fuse: eFuse requires the fuse's burning to determine the key (whether it is 1 or 0). This method is easy to reverse-engineer by looking at which fuse was burnt. There's also the risk of the fuse "growing back" because the thin piece of metal can sometimes reattach itself, which causes the key to disappear.
2. Density: another problem with eFuse is it cannot overcome 8kbit in density due to yield loss. Therefore, as technology migrates to more advanced nodes, eFuse is insufficient.

With our anti-fuse OTP (NeoFuse), we won't face any issues with reverse engineering, size/density, or even key disappearance. We use an electron tunnelling method at the transistor level, which can shrink with process nodes and cannot be seen under a microscope.

Combining our OTP with our PUF-based technologies makes key storage even more secure. When used with PUF's unique value different from chip-to-chip, the key's address can be scrambled and stored in a unique randomized location on the Secure OTP to make the key storage ultra secure.

(Page 18: PUF-based Key Generation vs. Conventional)

As for key generation, the Conventional True Random Number Generator (TRNG), used for Hardware Root of Trust (HRoT) is not PUF-based.

By comparing PUF-based TRNG vs Conventional TRNG in the three categories, PUF-based is superior for the following reasons:

1. High Entropy (The degree of randomness): PUF-based TRNG has much better and much higher entropy because it is derived from the PUF seed, which is perfect random sources, making it truly random. Conventional TRNG uses digital circuits to generate random numbers which have low entropy (our entropy is about 100x, meaning 100 times randomness) .
2. High Speed: Another critical feature of TRNG is speed. For PUF-based TRNG, the speed can generate a high volume of keys/RNG about 100x faster. On the other hand, conventional TRNG requires a lot more post-processing, which slows the speed.
3. Less Power Consumption: Lastly, the power consumption with PUF-based is also around 100x lower, again, this has to do with the post-processing that conventional TRNG requires, leading to more cost and energy used.

(Page 19: Summary)

1. Confidential Computing is a must in the GPU of AI applications because it provides the Integrity and Confidentiality of data and code.
2. Compared to Conventional Hardware Root of Trust, eMemory's PUF-based Hardware Root of Trust provides the best quality unique identities (UID), secure key storage, and much higher speed key generation for CPU/GPU/DPUs to facilitate its Confidential Computing.

All the differences mentioned above are why Confidential Computing architectures are moving away from conventional solutions towards PUF-based. Arm, for example, is putting our solution as reference design for its V9 confidential computing. With our developments reaching the most advanced process nodes, we expect increasing adoption for our security solutions in the future.

This concludes my remarks. 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!