eMemory 1Q23 Earnings Call Transcript

May 10th, 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.

Although the first half of this year was affected by foundries' overall low utilization rate, we are still very confident about our long-term growth.

With the rapid increase in security demand, our license will be driven by PUF-related solutions. Since we have more than 1000 new product tape outs over the past two years, royalty will regain its growth momentum as these new products enter mass production. Lastly, we are developing 3nm with key partners, 5nm customers will tape out soon, and 6/7nm customer adoption is accelerating, all of these will speed up our future growth.

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

FINANCIAL RESULTS

Michael Ho, President

Q1 2023 Financial Results

Good afternoon everyone. Now, let's begin with our 2023 first-quarter financial results. The first-quarter revenue was six hundred and sixty-eight million NT dollars (NT$ 668 mil), down 26% sequentially and down 8.2% year-over-year.

Operating expenses were three hundred and one million NT dollars (NT$ 301 mil), down 18.3 % sequentially, and down 4.2% year-over-year, mainly attributable to the decrease in bonuses and rewards.

Operating income was three hundred and sixty-seven million NT dollars (NT$ 367 mil), with a decrease of 31.3% sequentially and 11.2% year-over-year. The operating margin decreased by 4.2 percentage points sequentially and decreased by 1.8 percentage points year-over-year to 55%.

EPS for the quarter was 4.2 NT dollars (NT$ 4.20) and ROE was 38.9%.

Revenue across Different Streams

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

Licensing in the first-quarter accounted for 21.4% of the total revenue, down 30.3% sequentially and 25.3% year-over-year.

Royalties in the first-quarter contributed 78.6% of the total revenue, decreasing 24.8% sequentially, and 2% year-over-year.

Total revenue for the first-quarter decreased 26% compared to the previous quarter and decreased 8.2% compared to the previous year.

Revenue by Technology

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

NeoBit accounted for 19.7% of total licensing revenue in the first-quarter, decreasing 22.6% sequentially and down 19.8% year-over-year. Its royalties accounted for 30.5% of total royalty, down 31.1% sequentially and down 23.2% year-over-year.

NeoFuse accounted for 49.6% of total licensing revenue in the first-quarter, down 28.5% sequentially and down 42.9% year-over-year. In terms of total royalty revenue, NeoFuse royalties decreased 21% sequentially but increased 16.3% year-over-year, accounting for 67.8% of total royalties.

PUF-Based Security IPs contributed to 11.5% of licensing revenue, decreasing 60.7% sequentially but increasing 138.2% (one-hundred and thirty-eight point two percent) year-over-year. Its royalties accounted for less than 1% of total royalties which is down 93.8% compared to the previous quarter, and down 46.3% compared to the previous year.

MTP technology accounted for 19.2% of total licensing revenue, remained the same sequentially but increased 8.4% year-over-year. Royalty from MTP decreased 19.8% sequentially and 58.2% year-over-year, accounting for 1.7 of total royalties.

Q1 2023 Royalty Revenue by Wafer Size

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

8-inch wafers, accounted for 47% of royalties, decreasing 25.5% sequentially and 9.2% year-over-year.

12-inch wafers contributed to 53 % of royalties, decreasing 24.1% sequentially but increasing 5.3% year-over-year.

In total, 137 product tape-outs were completed in the first-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 the second quarter to be a trough of the year, mainly due to the continued decline in the foundry utilization rate. With new customers' tape outs moving into production, we expect revenue to pick up momentum in the year's second half.

For licensing revenues: Licensing will significantly grow during the rest of the year, driven by PUF-based security solutions.

For the royalty revenues: With more than 1000 new products tape out in the pipeline, royalty will regain growth momentum as new tape outs move into production.

Moving on to new IP technology and business development:

1. This year, PUF-based solutions will be adopted in 5/6/7nm CPU, DPU, AI and Automotive-related applications.

2. We continue working with foundries to develop NeoFlash to increase the penetration rate of mature processes.
3. Lastly, we continue developing PUF-based security solutions in the most advanced processes with CPU partners.

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

CHAIRMAN REMARKS

Dr. Charles Hsu, Chairman

How PUF-based Solutions Secure ChatGPT and AI

(Page 12: How PUF-based Solutions Secure ChatGPT and AI)

Recently, AI's application in ChatGPT has been a hot topic. Just last month, Samsung employees accidentally leaked proprietary information, making companies worldwide aware of some of the risks associated with ChatGPT. Today, I will talk about how ChatGPT, or even AI operations, can be attacked. Then, we will discuss how our PUF-based technology can help secure AI operations.

(Page 13: Asking ChatGPT about Security)

ChatGPT is a great tool that can answer even the most complex questions. That's why we decided to challenge it and see if ChatGPT itself is aware that it needs security and how its program goes about it.

As you can see from the screenshot on the right when asked, "How do you secure ChatGPT" the answer is listed there. We've highlighted some keywords we thought were important and listed how our company can help solve the problems according to the bullet point numbers.

1. To address the first part → PUF can be used to generate keys for encryption.
2. Likewise, the second bullet mentions authentication and access control → we can use PUF as a unique ID and can generate secret keys for authentication.

3. The third point is how ChatGPT identifies security breaches → This would also require the system to be able to identify users. PUF can be utilized to generate such ID.
4. The fourth part is how ChatGPT regularly updates and fixes its system → as this is typically done over-the-air, PUF-based IPs is capable of signing FW/SW updates.
5. Lastly, the fifth bullet is about security awareness training → by adopting hardware security, we can limit the chances of human error.

With these points in mind, it's easy to see how our security solutions can be applied to AI applications, and I will further explain how it is done in the following few slides.

(Page 14: Major Attacks in AI)

Before understanding how our security solutions work, we must first understand some popular attacks that can happen not only in ChatGPT, but AI systems in general.

- Poisoning attack: A poisoning attack happens when the attacker tampers with training data, which will then affect the training model, allowing the hacker to manipulate the results through the model.
- Backdoor attack: hackers may also replace the model during a backdoor attack by adding additional neurons to the model.

(Page 15: Major Attacks in AI cont.)

- Evasion attack: even after a model has been trained, hackers can still manipulate data, resulting in an evasion attack, leading incorrect output because of modified input data.
- Stealing attack: this attack applies to all stages of the AI model. Training data, model parameters, user data, etc., are all valuable know-how vulnerable to be stolen from AI hardware.

(Page 16: How to Prevent Attacks on AI)

These four attack methods described are ways all AI systems can be attacked, from training to output results. Each type of attack requires different protection methods and solutions.

- Poisoning attack: the problem with a poisoning attack is training data may be corrupted. We need to sign the training data to ensure the integrity of data.
- Backdoor attack: with backdoor attacks, the biggest problem is modifying, replacing, or even stealing the model. Not only does this require signing the model to protect its integrity, but it also needs additional encryption and key management to prevent hackers from gaining access to the model.

(Page 17: How to Prevent Attacks on AI cont.)

- Evasion attack: unlike the previous methods that target the training and model, evasion attacks pose a problem with input data. Attackers can tamper with input data to influence the output or result. That's why we must authenticate and provision users using a unique ID (UID) and encrypt the assets.
- Stealing attack: the last attack is the theft of all the AI assets. To avoid attackers stealing valuable data and know-how from AI hardware, we need a UID, signing, encryption and an anti-tamper hardware design to dissuade the attackers.

(Page 18: Securing AI with PUF-based Solutions)

Of all the problems we have mentioned, PUF can play a role in solving these issues. We have developed two types of security IP: one is a hardware root of trust, and the other is a crypto co-processor.

The root of trust IP (PUFrt) combines PUF (Physical Unclonable Function), secure OTP and a true random number generator (TRNG). Besides, we have implemented multiple anti-tampering techniques to defend against attacks.

On top of that, our crypto co-processor (PUFcc) comes with all of the above and has cryptographic hardware accelerators built in.

With all of the industry-standard crypto algorithms supported, we also have firmware and software so that our crypto co-processor can enable advanced security protocols and applications.

After understanding the risks of each stage of the AI used to operate ChatGPT, it is easy to see that PUF-based solutions are sufficient for all security requirements throughout the AI product lifecycle. From training data to inference results, the AI developer's know-how must be protected from copying and stealing. PUF-based solutions are secure and cost-effective, and the IP blocks make them best suited for securing AI applications.

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, 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 IP innovation and security solutions for our customers and bring higher returns for our shareholders. Thank you!