eMemory 1Q22 Earnings Call Transcript

May 11th, 2022, 16:00-17:00 Taiwan Time

OPENING REMARKS

Dr. Charles Hsu, Chairman

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

Our first quarter operating results are at a record high, reflecting our continuous efforts to invent new technologies and increasingly adopted by various applications.

We have accumulated more than 1000 new tape-outs in past two years, among those tape-outs, more than 200 tape-outs are below 28nm. These tape-outs are entering the mass production stage, which will continue to drive our royalty growth further. With technology development reaching 4/5nm and customers tape-outs in 6/7nm, these advance processes are the platforms for future growth.

In the first-quarter, we have began our collaboration with Arm's new v9 Confidential Computing, which incorporates our PUF-based Secure Root of Trust into Arm's v9 Confidential Computing Architecture, Arm's future decade-long architecture. This will enable us to penetrate into the high performance computing area. Moreover, we are working with Intel and Global Foundry, aiming for the US localization of semiconductor security.

All in all, we remain confident in the company's future growth.

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

FINANCIAL RESULTS

Michael Ho, President

Good afternoon everyone. Now, let's begin with our 2022 first-quarter financial results. The first-quarter revenue was seven hundred and twenty-seven million NT dollars (NT$ 727 mil), up 15.2% sequentially, and up 21.8% year-over-year.

Operating expenses were three-hundred and fourteen million NT dollars (NT$ 314 mil), up 4.7 % sequentially, and up 21.2% year-over-year, mainly attributable to the increase in salary and other related human resource expenses, such as the increase in bonuses and rewards.

Operating income is four hundred and thirteen million NT dollars (NT$ 413 mil), with an increase of 24.6% sequentially, and 22.4% year-over-year. The operating margin increased by 4.3 percentage points sequentially, and increased by 0.2 percentage point year-over-year to 56.8%.

EPS for the quarter was 4.91 NT dollars (NT$ 4.91) and ROE was 55%.

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

Licensing in the first-quarter accounted for 26.4% of the revenue, up 17.8% sequentially and up 8.3% year-over-year, or up 17.4% sequentially and up 10.2% year-over-year in US dollars.

Royalties in the first-quarter contributed 73.6% of the total revenue, increasing 14.2% sequentially, and increasing 27.6% year-over-year, or up 15.5% sequentially, and up 31.1% year-over-year in US dollars.

Total revenue in the first-quarter of 2022 grew 15.2% sequentially and 21.8% as compared to the previous year. In terms of US dollars, the total revenue increased 16% compared to the previous quarter and 24.9% year-over-year.

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

NeoBit accounted for 18.3% of total licensing revenue in the first-quarter, increasing 49% sequentially and 28.2% year-over-year. Its royalties accounted for 38.8% of total royalty, up 4.6% sequentially, but down 2.5% year-over-year.

NeoFuse accounted for 64.8% of total licensing revenue in the first-quarter, up 20.4% sequentially and up 36.9% year-over-year. Its royalties increased 19.1% sequentially and 56.2% year-over-year, due to the increasing penetration rate of OLED, ISP, Network-related, DRAM and others, accounting for 57.2% of total royalties.

PUF-Based Security IPs contributed to 3.6% of licensing revenue, decreasing 63.4% sequentially but increasing 25.8% year-over-year. Its royalties accounted for 0.1% of total royalties which is up 125.2% compared to the previous quarter, and up 100% compared to the previous year. We anticipate a very significant growth in Q2 and H2.

MTP technology accounted for 13.3% of total licensing revenue, increasing 49.3% sequentially, but decreasing 52.5% year-over-year. Royalty from MTP increased 64% sequentially, and increased 99.2% year-over-year for MCU, Wireless Charger and others.

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

8-inch wafers, which accounted for 50.7% of royalties, increased 15% sequentially, and 17.9% year-over-year due to wafer shipment increase from PMIC, MCU, sensors and others.

12-inch wafers contributed to 49.3% of royalties, increasing 13.4% sequentially, and 39.3% year-over-year due to continuous production from OLED, Networking, ISP, DTV, DRAM and others.

In total, 138 product tape-outs were completed in the first-quarter The number of tape-outs below 16nm has increased significantly, especially tape-out for 6nm high-speed computing-related applications. 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 growth of revenue to continue in the second quarter of 2022 and beyond.

For the licensing revenues, licensing revenue will grow due to the continued strong demand for our IPs, especially NeoFuse and PUF-related solutions.

For the royalty revenues, 8-inch and 12-inch royalties will continue their growth momentum with increasing wafer shipment and wafer ASP.

1) 8-inch royalties will grow due to demand and content increase for PMIC, MCU, Fingerprint, and Sensor-related in 5G, Automotive, and IoT-related applications.
2) 12-inch royalties will have a strong growth with increasing penetration rate in OLED, ISP, DTV, STB, WiFi 6/6E, Network-related, DRAM and others.. The royalties for 12/16nm and 7nm FinFET continue to contribute in the first-quarter and are expected to become the next growth driver after 28nm.

Moving on to new business development:

1) The focus of our new application development is in the field of security. Business activities for PUF-based security solutions are continuing to progress in IoT, Industrial IoT, AI, Blockchain, FPGA, Data Processor Unit (DPU), Mobile Storage (UFS) and Automotive applications.
2) Furthermore, eMemory's OTP/PUFrt plays an important role as the root of trust in the Armv9 Confidential Computing Achitecture (CCA). We provide the most fundamental security protection for the next decade of confidential computing. Furthermore, we have also started to license security IPs in Intel foundries.

For new IP technology development:

1) N4 and N5 are on the verification stage with customers' request for adoption.
2) Our ReRAM is being deisgned into AI applications.
3) Lastly, NeoFlash is being licensed to multiple foundries for specialty processes such as BCD.

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

CHAIRMAN REMARKS

Dr. Charles Hsu, Chairman

Why PUF is Pivotal to Metaverse Security

(Page 15: What is Metaverse?)

The Metaverse is a hot topic, especially among today's generation of technology users. It can be defined as "a virtual-reality space in which users can interact with a computer-generated environment and other users".

Essentially, it is the next phase of the internet. The Metaverse is an immersive experience moving away from 2D into 3D, allowing users to enter an artificial virtual world.

(Page 16: The Seven Layers of Metaverse)

Initially, the Metaverse emerged as a concept in the games market, however, the Metaverse has quickly evolved to include major tech companies, alongside emerging innovators, as the “inhabitants” building this new ecosystem.

According to Jon Radoff, an entrepreneur, author, and game designer, the conceptual framework of the Metaverse consists of seven tiers. Starting from what the consumers will be experiencing, to the backbone of the Metaverse.

The first layer is Experience. Where users engage and interact with the Metaverse through games, social experiences, live music, and so on.

The second layer is Discovery. This is where people learn and discover an experience and where information sharing occurs.

The third layer is the Creator Economy. This includes everything aiding content creators to generate and monetize the Metaverse, such as design and graphic tools, animation systems, and financial technologies.

The fourth layer is Spatial Computing, which refers to the software that merges Virtual and Augmented Realities. In other words, allowing us to digitize the physical world surrounding us.

The fifth layer is Decentralization, which refers to the absence of a single authority within the Metaverse. This creates a more permissionless, democratized structure and allows creators to retain ownership over their own data and products.

The sixth layer is Human Interface, which is the hardware that helps us access the Metaverse, including gadgets and technologies like biosensors and spatial computing.

And the seventh is the base layer, Infrastructure. This is what ties everything mentioned above together. It involves material science, cloud computing, telecommunication, and semiconductors, all working efficiently and safely together in a network.

(Page 17: Security Needs in Metaverse)

Based on the seven layers, six cores are needed to realize Metaverse. For any activities that occur in the Metaverse, whether a simple interaction with your friend, or shopping for property, it will consist of some, if not all of the six core technologies. This includes: 1) Blockchain, 2) Interactivity, 3) Games, 4) Artificial Intelligence, 5) Networks, and 6) The Internet of Things.

Each of these core technologies will require a security element. Digital assets, such as NFTs, for example, exist on a Blockchain to safeguard their ownership in a decentralized ledger. Identity protection, confidentiality, and authentication protect user identity on connected devices in the Metaverse, and interactions promote connected data and more.

The Metaverse has the potential of multiple “universes”, promoting communication, virtual assets, virtual transaction, and more functions than we can imagine across these “universes.” However, for the Metaverse to operate, the fundamental need for security elements, such as root keys, encryption/decryption, authentication, and confidentiality, still holds true, no matter how many “universes” exist inside the Metaverse.

Without the proper security measures, attacks in the Metaverse could result in the loss of one’s wealth or worse, resulting in physical harm. There have been instances of cryptocurrency exchanges being attacked where individuals have lost all their crypto coins. In the case of the Metaverse, if an individual’s identity is hacked, their property and digital assets can be taken away.

(Page 18: Metaverse Ecosystem)

Together, the seven layers create the Metaverse ecosystem, and within the ecosystem are key players. For example, Discord and Nintendo are major companies that make up the Experience layer; Facebook and Google are part of the Discovery layer; Adobe and Unity supply tools in the Creator Economy layer; Google AI offers the programs for Spatial Computing; IBM and Ethereum enable Decentralization; Microsoft and Oculus create the Human Interfaces, and Intel and Qualcomm create the Infrastructure that brings everything together. This is just a small sample of companies that have entered, or are entering, the Metaverse space.

Several of these companies currently collaborate with eMemory directly and have incorporated our IPs into their designs and products. These companies also need to protect their systems when it comes to security. Moreover, for those companies that we don’t currently work with directly, our IPs may be found in the Infrastructure that still enables experiences in the Metaverse.

Since eMemory and PUFsecurity are collaborating with Arm in their new Armv9 CPU architecture, which introduces Confidential Computing Architecture as their method of securing data for the next decade. Our Hardware Root of Trust IP, PUFrt, will provide hardware security to the new generation of computing, potentially spanning across different security solutions in fields such as automotive, device, infrastructure, and IoT, all of which are foundational parts of the Metaverse.

(Page 19: Scenarios in Metaverse)

Building off the seven layers described earlier, let’s imagine a scenario that applies.

Logging into the Metaverse alone requires spatial computing that allows the system to map out the space around you, a human interface such as your headset, display screen and haptic touch gloves to experience the Metaverse, and the infrastructure such as the system hardware and software that builds the “universe” you’re entering.

Although it is a simple act of logging-in, if the device, such as the VR glasses used to enter Metaverse is hacked, the hacker can even damage the person’s health, in this case, their eyesight, with illegal operations, such as high lamination. With PUF-based hardware security, the chip-fingerprint of our VR glasses is now one-of-a-kind and only you can access it.

Similar scenarios could be applied to more complicated experiences such as a virtual gathering for a movie with your friends, or a work-related scenario, like a virtual meeting with your coworkers. In such cases, you can imagine that the attacks will complicate further as there are more layers and requirements for security, whether in communication between users, authentication of identity, etc.

(Page 20: Why PUF is Pivotal to Metaverse Security?)

The possibilities for Metaverse are endless, making the potential threats in the Metaverse endless too. Pervasive data collection of users' private information, including personal information, behavior, location, habit, lifestyle, and communication, is already commonplace. Because of this, network credential theft, identity theft, and ransom attacks are just a few of the many growing security concerns. Simple vulnerabilities in a device, or with identity credentials, can potentially lead to user identity misuse.

PUF-based security enables us to prepare for the threats of the Metaverse by protecting user identity, data, and privacy.

So, to do our part in protecting the future of computing, eMemory is looking to achieve the following:

PUF, which most of you know, is the acronym for Physical Unclonable Function, is a physically defined "chip-fingerprint" that serves as a unique identity for semiconductors and is tamper-proof. PUF's digital fingerprint could help secure the Metaverse in the same way by providing a unique, unforgeable user identity and credentials for each individual entering the Metaverse.

Furthermore, eMemory's quantum-tunneling technology creates the best PUF available on the market today. By using silicon variations during the manufacturing process, PUF can be used to generate keys. Keys are essential during the exchange of information in the Metaverse because they are the basis for encryption/decryption and other security functions.

This brings us to my next point. Our integrated security solutions derive truly secret keys to protect identities, assets, and transactions. Not only does PUF generate keys, but our PUF-based IP solutions also utilize eMemory's patented OTP technology to securely store these secret keys. PUF can also protect device Firmware to ensure normal operations and avoid potential threats because it has a PUF-based hardware root-of-trust, the basis of secure OTP.

Lastly, PUF-based NFTs can uniquely identify any virtual object in the Metaverse. Because of its indivisible, irreplaceable, and unique characteristics, NFTs can represent digital assets or identity.

CLOSING REMARKS

Dr. Charles Hsu, Chairman

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!