# eMemory Q1 2021 Results – Earnings Call Transcript

**May 12th, 2021 16:00-17:00**

## Opening remark by Dr. Charles Hsu, Chairman of eMemory

Good afternoon, everyone. Thank you for attending our conference call today. As mentioned previously, we have entered a multi-year growth cycle.

According to the royalty report received in the first quarter, the contribution of 12-inch is accelerating, and its contribution will exceed 8-inch by the end of this year. Following the applications of 28nm process nodes, the applications of 16nm and beyond are entering into production, which will contribute to our royalties in the future.

As for our new technology, we are confident with the development and adoption across various markets. I will explain more about the importance of PUF for Security applications in a short while.

Next, I will invite Rick, to report our first quarter operating results and the outlook of our business.

---

## Operating results and future outlook by Dr. Rick Shen, President of eMemory

Thank you, Charles. Good afternoon, everyone.

I will first begin with our first-quarter results.

1) First quarter revenue was five hundred and ninety-seven million NT dollars (NT$ 597 mil), a sequential increase of 20.1%, and 43.6% year-over-year, or up 22.2% sequentially, and 51.5% year-over-year in US dollars.

2) The operating expenses were two hundred and fifty-nine million NT dollars (NT$ 259 mil), down 0.9% sequentially, but up 17% year-over-year, mainly attributable to expenditure increases such as human resource expenses, rewards, bonuses, and the compensation of employees and directors.
3) This brings us to the operating income of three hundred and thirty-eight million NT dollars (NT$ 338 mil), with an increase of 43.5% sequentially, and 74.1% year-over-year. Therefore, the operating margin increased by 9.2 percentage points sequentially and 9.9 percentage points year-over-year to 56.6%.
4) Overall, our first quarter EPS was 3.93 NT Dollars (NT$ 3.93) and ROE was 54.6%.

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

1) Licensing in the first quarter accounted for 29.7% of the revenue, up 14.6% sequentially, and 66.3% year-over-year, or up 16.7% sequentially, and 76.2% year-over-year in US dollars.
2) Royalties in the first quarter contributed 70.3% of the total revenue, increased 22.7% sequentially, and 35.8% year-over-year, or up 24.7% sequentially, and 43.1% year-over-year in US dollars.

In terms of revenue contribution by technologies, the results are as follows:

1) NeoBit accounted for 15.4% of total licensing revenue in the first quarter, increased 3.3% sequentially, and 13.4% year-over-year. Its royalties accounted for 50.8% of total royalty, up 8.9% sequentially, and 7.1% year-over-year, mainly due to demand and content increases of applications such as PMIC, MCU, and Sensor-related.
2) NeoFuse accounted for 51.3% of total licensing revenue in the first quarter, down 17.6% sequentially, but up 21.6% year-over-year. Its royalties increased 44.5% sequentially, and 99.4% year-over-year due to the continuous production of existing and new applications such as TDDI, OLED, ISP, Multimedia, and Networking-related. This brings the royalty of NeoFuse to 46.7% of total royalties.

3) Our PUF-Based Security IP contributed to 3.1% of licensing revenue in the first quarter. Although this technology has not contributed to any royalty, engagement with industrial leaders is still actively ongoing. Thus, we expect more significant contributions from PUF this year.
4) As for MTP technology, licensing revenue increased 2-fold sequentially, and 6-fold year-over-year to account for 30.2% of licensing revenue in the first quarter. Royalty from MTP decreased 3.2% sequentially, and 8.2% year-over-year to contribute 2.5% of total royalties. Currently, our MTP team is working with partners on developing MRAM, ReRAM, and AI memory. Both ReRAM and AI Memory have been verified with proven results.

Now looking at royalties for 8-inch and 12-inch wafers:

1) 8-inch wafers, which accounted for 54.8% of royalties, increased 10.2% sequentially, and 16.2% year-over-year, due to demand and content increases of applications such as PMIC, MCU, and Sensor-related.
2) 12-inch wafers contributed to 45.2% of royalties, increased 42.1% sequentially, and 70.9% year-over-year, due to the continuous production of TDDI, OLED, ISP, DRAM, Multimedia, and Networking-related such as DTV, STB, WiFi 6, Bluetooth, Ethernet, Switch, and TWS.

There were 155 product tape-outs completed in the first quarter, a record-high quarterly number, reflecting increasing demand for our IPs. We will provide more information in the management report that will be released later today.

In the next section, I will address our future outlook. We expect the growth of revenue to continue in the second quarter of 2021 and beyond.

1) For licensing revenue, there is continuing strong demand from NeoFuse, PUF-based solutions, and MTP. We expect licensing revenue to continue its growth this year.

2) For royalty revenues, 8-inch and 12-inch royalties will continue their growth momentum. 8-inch royalties will grow due to demand and content increases for PMIC, MCU, and Sensor-related in 5G, Automotive, and IoT-related applications. 12-inch royalties will have strong growth as customer productions are increasing for TDDI, OLED, ISP, DTV, STB, WiFi 6, Bluetooth, Ethernet, Switch, TWS, DRAM and others. In addition, royalties from 16nm and below have started to kick in. We expect to see 7nm customers move into production and start contributing to royalty.

For new business development:

Our new applications are centered on the business development of hardware security.

1) NeoFuse, in advanced processes, is being adopted for secure Key Storage and is seeking to replace the conventional e-Fuse. We expect that this will be a trend for hardware security as applications are moving to more advanced processes. Our effort in the past is also gradually being seen with higher adoption and penetration rate.
2) Business activities of PUF-based security solutions are in progress in applications of IoT, industrial IoT, AI, Blockchain, FPGA, Data Processor Unit (DPU), Mobile Storage (UFS), and Automotive. In addition, our PUFrt and PUFiot have been adopted by several customers across various applications.
3) As for the collaboration with ARM, since customer adoption cases have been very successful, we intend to expand the cooperation to more product applications in the future.

For new IP technology development:

1) 6nm OTP has demonstrated successful silicon results and is going into qualification smoothly. As for 5nm plus (N5P) is on the way to characterization and expected to have good results in this quarter.
2) In Q1, we have announced the adoption of our IP by Achronix for FPGA Hardware Root of Trust to enhance security at the semiconductor chip level.

3) We also continue to develop our PUF-based solution to implement HSM (Hardware Security Module), which can be embedded in the chip to provide a security function for network applications.

Now, I'll pass the time to Charles.

----------------------------------------------------------------------------------------------------------

**PUF is the Key for Zero Trust Security by Dr. Charles Hsu, Chairman of eMemory**

Thank you, Rick.

(Page 15)

I would like to introduce the subject of Zero-Trust, which has received significant attention recently as the security risk of the IoT becomes increasingly consequential and more widely reported. Zero Trust security has the following features as shown in page 15.

1) Never trust, always verify
2) Only Authenticated and authorized devices are permitted
3) De-perimeterization security protection
4) It is identity-centric policy

Let me explain what they are:

1) The traditional security strategy and principles are based on 'castle and moat', or the so-called 'Security Perimeter' strategy.
2) In a traditional network, employees who work inside the enterprise network are protected by Internet firewalls, etc. within the 'Security Perimeter' and are 'Trusted' by default, while employees working remotely are left outside the security perimeter and remain 'Untrusted', requiring them to provide strong verification.

However, as many edge devices are being connected directly to the internet, it is very difficult to provide a secure perimeter or boundary to protect everything inside a secure network. Therefore, each device should utilize a mixture of encryption, secure computer protocols, secure computer systems, and device-level authentication, rather than the reliance of an organization on its network boundary to the Internet. This is the so-called 'Zero-Trust' security strategy, in which the device trusts only itself and will always verify the accessing party.

So, a Zero-Trust security model, creates de-perimeterization of the traditional security boundaries within a network, as the exiting defenses are no longer effective. The device relies on its Unique ID for verification each time for access (during authorization) or to be accessed (during authentication).

The defense wall transforms from a single large perimeter to a small perimeter for each device individually.

(Page 16)

In a short summary, Zero Trust security is needed as the following situations increase:

1) Work from home during COVID-19 has become normal practice.

2) Remote working is set to continue for many enterprises.

3) Increased deployment of cloud-based services.

There is no way to maintain the old "Security Perimeter" anymore in this Zero-Trust era! Instead, a new borderless or "de-perimeterization" approach is urgently needed!

(Page 17)

Zero-Trust networking is based on the principle of 'Never Trust (by default), Always Verify,' and therefore requires authenticated verification. A PUF is best suited to perform this function and is set to become essential for creating a zero-trust network.

Our PUF based technologies can provide a self-generated ID for unique identification and a self-generated key, both of which are inherently created in the PUF. This sets us apart from the conventional methods, which require an injected ID and a key from outside of the device, exposing the attack surface before the key is injected into the device. In addition, the injected key and ID are stored at the key storage memory which is not as safe as storing in PUF.

(Page 18)
The key in the PUF can be used with most crypto engines to provide comprehensive security services, such as unique identity generation, authenticity, confidentiality, integrity, and non-repudiation, which are essential for a zero-trust network.

In conclusion, as security becomes more of a concern for electronic devices, Zero-Trust networking will push the secure boundary from a single large perimeter into the device itself. PUF is the basis of ‘Root of Trust’, will play a very important role and become essential to the success of the Zero-Trust security model.

---------------------------------------------------------------------------------------------------------

**Closing comment by Dr. Charles Hsu, Chairman of eMemory**

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!