eMemory Q4 2021 Results – Earnings Call Transcript

February 10th, 2022 16:00-17:00

Opening remark by Chairman, Dr. Charles Hsu

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

2021 is considered as one of the best years since our company was established 21 years ago. Our progress is apparent in our operational indicators such as growth and profitability, especially in the number of tape-outs. We have completed and finalized 614 designs, and almost every day, our IPs are used in at least 2 products.

Furthermore, after years of technology development and qualification, our tape-out activities are accelerating in leading edge, which will continue to drive our growth momentum for the coming years.

Looking forward to this year, we believe the multi-year growth momentum will continue, especially the growth of security-related IPs will be substantial. In addition to trends such as replacing eFuse, which we have been promoting for a while, the demand is increasing for much higher security in various applications from the cloud to the consumer end. You may wonder, why is our PUF-based IP the best choice in the market? Because we have the easiest and most secure way of generating random numbers on the chip, and random number is the foundation of all security systems, which I will explain later.

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

Operating results and future outlook by President, Mr. Michael Ho

Good afternoon everyone.

First, I will begin with our fourth-quarter results.

1) The fourth-quarter revenue was six hundred and thirty-one million NT dollars (NT$ 631 mil), up 6.2% sequentially, and up 27.1% year-over-year.
2) The operating expenses were three-hundred million NT dollars (NT$ 300 mil), up 7.9% sequentially, and up 14.7% year-over-year, mainly attributable to the increase in salary and other related human resource expenses, such as the increase in bonuses and rewards.
3) This brings us to the operating income of three hundred and thirty-two million NT dollars (NT$ 332 mil), with an increase of 4.8% sequentially, and 40.9% year-over-year. The operating margin decreased by 0.8 percentage point sequentially, and increased by 5.1 percentage points year-over-year to 52.5%.
4) Overall, our fourth-quarter EPS was 3.86 NT dollars (NT$ 3.86) and ROE was 51.4%.

For the full year of 2021, the revenue was two billion three hundred and sixty-four million NT dollars (NT$ 2.364 bil), up 33% year-over-year. The operating expenses increased by 14.8%, and the operating margin was 53.7%, with an increase of 7.4 percentage points. EPS is NT$ 14.78, and ROE is 49.3%.

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

1) Licensing in the fourth-quarter accounted for 25.8% of the revenue, down 13.8% sequentially, but up 5.3% year-over-year, or down 13.6% sequentially, but up 9.4% year-over-year in US dollars.

2) Royalties in the fourth-quarter contributed 74.2% of the total revenue, increasing 15.6% sequentially, and increasing 37% year-over-year, or up 15.1% sequentially, and up 41.6% year-over-year in US dollars.
3) In the full year of 2021, the total revenue grew 33% as compared to the previous year. Licensing and royalty have a growth of 43.4% and 29.1%, respectively. In terms of US dollars, the total revenue increased 40% year-over-year, with licensing and royalty both increasing 51.1% and 35.8%, respectively.

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

1) **NeoBit** accounted for 14.5% of total licensing revenue in the fourth-quarter, decreasing 39.7% sequentially, and decreasing 11.2% year-over-year. Its royalties accounted for 42.4% of total royalty, up 3.7% sequentially, and 1.5% year-over-year.
2) **NeoFuse** accounted for 63.4% of total licensing revenue in the fourth-quarter, up 10.4% sequentially, but down 6.3% year-over-year. Its royalties increased 27.3% sequentially and 89.6% year-over-year.
3) **Our PUF-Based Security IPs** contributed to 11.6% of licensing revenue, increasing 580.4% sequentially and 639.6% year-over-year due to the strong demand for security from various applications, many of which have continued into this year and is expected to grow in the future.
4) **As for MTP technology**, licensing revenue accounted for 10.5% of total licensing revenue, decreasing 68.2% sequentially, but increasing 11.3% year-over-year. Royalty from MTP increased 6.3% sequentially, and up 17.6% year-over-year to contribute 2.7% of total royalties.

In the full year of 2021:

1) For NeoBit, the licensing revenue increased 45.9% year-over-year, but royalty decreased 3.8%, accounting for 38.8% of the total revenue.

2) For NeoFuse, the licensing and royalty revenue grew 15.6% and 91.6% year-over-year, contributing to 51.9% of the total revenue.
3) For PUF-Based Security IP, licensing revenue increased 140.9% year-over-year, about 1.2% of total revenue.
4) For MTP technology, the licensing and royalty revenue increased 220.8% and 12.1% year-over-year, accounting for 8.1% of the total revenue.

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

1) 8-inch wafers, which accounted for 50.3% of royalties, increased 11.2% sequentially, and 13% year-over-year.
2) 12-inch wafers contributed to 49.7% of royalties, increased 20.3% sequentially, and 74.4% year-over-year.

There were 163 product tape-outs completed in the fourth-quarter, which reflects that our IP demand remains strong. We will provide more information in the management report.

In the next section, I will address our future outlook. We expect the growth of revenue to continue in the first quarter of 2022 and beyond.

1) For the licensing revenues, licensing revenue will grow due to the continued strong demand for our IPs, especially NeoFuse and PUF-related solutions.
2) For the royalty revenues, 8-inch and 12-inch royalties will continue their growth momentum with increasing wafer shipment and wafer ASP.
    a. 8-inch royalties will grow due to demand and content increase from the mass production of 5G, Automotive and IoT-related PMIC, MCU, Fingerprint and Sensor-related applications.

b. 12-inch royalties will have a strong growth as products in TDDI, OLED, ISP, DTV, STB, WiFi 6/6E, Bluetooth, Ethernet, Switch, TWS and DRAM applications are ramping up production. The royalties for 12/16nm and 7nm FinFET have also started to contribute in the fourth quarter and is expected to become the next growth driver after 28nm.

Now, looking at new business development:

1) The focus of our new application development is in the field of security. There is already a trend replacing eFuse for secret key storage with NeoFuse, and applications are migrating to more advanced processes. Besides replacing eFuse for security key storage, and was also adopted by automotive applications in 7nm and 6nm.
2) Current 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. Our PUFrt (Root-of-Trust IP) and PUFcc (Crypto Co-Processor IP) have been adopted by several customers across various applications.
3) We just announced that our PUFrt was selected by Arm for the secure sub-system of the Armv9 confidential computing architecture. This is significant breakthrough for our IP to be adopted by leading processor application markets.

For new IP technology development:

1) In the fourth quarter, we have verified our security-enhanced NeoFuse OTP, which was designed in TSMC's N5 process. It is an integrated NeoFuse and NeoPUF IP with high security function. NeoFuse supports a variety of product applications, including those in high-end to mid-end Mobile, Consumer, AI, Networking, 5G Infrastructure, GPU, DPU and High-performance Computing. At present, we are discussing further collaborations with customers.

2) Our ReRAM IP has been qualified in UMC's 40nm process, and tape-out has begun for the 22nm process. We are one of the world's first companies to provide this emerging memory and offer more comprehensive solutions for Automotive, Edge Computing, AI and AIoT markets. We will extend ReRAM technology to more advanced process nodes and specialty processes such as BCD and high voltage.
3) Next, we will continue to develop new security functional IPs, including PUF-based Security Co-Processors and PUF-based Security Elements.
4) We will also develop NeoFlash in BCD as well as 28nm and below processes to solve the technology problem of traditional embedded Flash.

Next, I will pass the time to Charles.

The importance of PUF for random number generation

By Chairman, Dr. Charles Hsu

(Page 14: Section Page)

Let's begin with**: What is the Random Number used for?**

"Random numbers are fundamental building blocks of cryptographic systems and used to inject unpredictable data into cryptographic algorithm and protocols to make the resulting data streams unrepeatable and virtually unguessable"

(Page 15: Revisiting the Goals of Security)

What is Cryptography?

"Cryptography is an information security tactic which is the art and the science of keeping messages secure."

To keep messages secure, there needs to be three elements:

1. **Authentication**: Authentication ensures the person on the other end of the connection is who they say they are.

2. **Confidentiality**: Confidentiality ensures only the authorized person listening to the transaction is able to extract meaningful information.

3. **Integrity**: Integrity ensures there are no undetected changes or interferences to the transaction as it travels from the sender to the intended recipient.

(Page 16: Randomness is Pivotal in Security)

Random Numbers are fundamental to all aspects of data security since it can be used with cryptography to make data unrepeatable and unguessable.

However, the strength of a security mechanism is directly proportional to the randomness of the number it uses.

As shown in page 16, only if the randomness is high enough, the data after encryption with random numbers can be invisible.

(Page 17: Methods of Generating Random Numbers)

Methods of generating random numbers

In general, there are two ways of generating random numbers, one is…

Software Random Number Generator

Modern computer programs can use software generated, pseudo-random numbers, rather than true random numbers. Since a computer is only a machine dictated by human instruction, it will only repeat the few steps for the tasks we tell it to do. Therefore, computers alone cannot generate random numbers since it is impossible to generate something that is unpredictable by a computer.

Software Random Number generation requires a seed, which is used as an input in the algorithm of a mathematical computation to create pseudo-random numbers.
However, there are three disadvantages to using software generated Random Numbers:

1. A seed value is required to initialize the equation.
2. The generated sequence of numbers will eventually repeat itself
3. The Random Numbers are generated mathematically and are therefore, not truly random. This means the software generated numbers are unable to provide high level of cryptographic protection.

Basically, in order to provide a high security level, we have to resort to the natural physical world to extract something that behaves truly random by nature. From there, we can extract Random Numbers. A true Random Number is something that a physical device produces, and we cannot know its value until it has been generated.

Another way is by…

Hardware Random Number Generator

Hardware random numbers do not require a seed because they are not computed values and not derived through a repeatable algorithm.

So the next question is, what are the processes or behaviors of the device we can measure that are really unpredictable?

Let me give two examples:

We can find a Random Number by counting the number of passengers in an intersection every 10 seconds. If the number is odd, we can set it as *one*. If the number is even, we set it to *zero*. After 2560 seconds we can derive a 256-bits random numbers.

For 256-bits random number, the probability of guessing it correctly is

1 over $2^{256} = 2^6 \times 2^{250} = 64 \times (10^3)^{25} = 64 \times 10^{75} \approx 10^{77}$; $\frac{1}{10^{77}}$

10^{77} is 77 zero after 1, (1 trillion is 10^{12}.) Which is almost to zero!

Another example is, we can measure the widths of every two transistors placed aside. Even if the drawn width is the same, after fabrication, they may still have slightly different widths. Based on their widths, we can set a "*1*" if the one on the left is longer and set "*0*" if it is shorter. By measuring 256 pairs of transistors we can get 256-bits of random numbers.

(Page 18: On-Chip Randomness from PUF)

However, in the above examples it is important to note that:

1. This cannot be done electronically on a chip.
2. The randomness is not likely enough; for example, for the passenger case mentioned above, we may get a long stream of *1* or *0* depending on if the intersection is busy or not, and for the transistor width example, the patterning may be biased such that the transistor width on one side is always longer than the other side. Thus, the problems we really need to solve are:

   1) The Random Numbers need to be electronically measurable on the chip. AND

2) The randomness of the Random Numbers need to be high enough such that it cannot be predictable or repeatable.

In our invention, NeoPUF, we extract the quantum tunneling behavior of the electrons tunneling through the thin insulators of the transistor's gate dielectrics.

The tunneling behavior is strongly dependent on the quality of the thin dielectric film. A slight difference in the film quality will result in a significant difference in tunneling probability. We measured the electron tunneling behavior of two adjacent transistors gate dielectrics. If the one on the right hand side has a larger tunneling current, we define it as a digit "*0*", smaller as a digit "*1*". We can generate 256-bits random number if we have 256 pairs of adjacent transistors.

This results in true randomness since 1) the film is uniformly grown on the silicon substrate, the difference in tunneling behavior of these two transistors are unpredictable. 2) The tunneling current is electronically measurable. 3) The difference in quality is randomly distributed so that high randomness can be achieved.

By performing quantum tunneling behavior extraction, we are able to create the Random Number for each chip to act as unique hardware key which governs the security of the chip.

(Page 19: Building upon PUF-based Security)

We have taken this PUF random number to build basic security functions such as Root of Trust (PUFrt), security co-processors (PUFcc), and secure element (PUFse) to provide a new architecture for achieving high level security.

Both of our recent releases, in cooperation with Arm and with Intel Foundry Service respectively, focus on security solutions based on our quantum-tunneling PUF, NeoPUF, including hardware root-of-trust trust and a secure co-processor.

With the proliferated cloud applications that require confidential computing, PUF-based hardware root of trust is extremely important in next-generation CPUs. Arm selects PUFrt, the flagship product of PUFsecurity Corporation, to be the secure subsystem in Armv9 confidential computing architecture reference design. PUFrt fully integrates key generation and secure storage, as well as a true random number generator that is indispensable for all secure operations. This collaboration help customers seamlessly apply security designs at the beginning of the design when selecting computing cores.

Looking ahead at the growing demand and importance of security in the future for various applications such as AI, DPU, FPGA, IoT, automotive, etc., the cooperation with IFS is an important step forward, allowing customers who utilize IFS's (Intel Foundry Service) advanced process platform to directly import our security IP to meet the desire of secure supply chain and zero-trust applications, which is emphasized especially in the US market. Our shared vision is to provide global customers with the best chip security while enjoying the performance enhanced by advanced process nodes.

Closing comment by Chairman, Dr. Charles Hsu

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!