eMemory 1Q23 Earnings Call Q&A Transcript

May 10th, 2023, 16:00-17:00 Taiwan Time

Q&A Transcript

1. **Compared to Q1, there was still no improvement in fabs in Q2, and the inventory level of design houses remained high. Since the company's royalty revenue is a quarter behind that of the fabs, what is the outlook on royalty in the second half of the year?**

   >> We have seen that the earliest customers who adjusted their inventories started wafer production in February. In addition, the new tape outs over the last two years were for new product applications and will begin mass production in the latter part of the year and drive the royalty growth. We expect royalty to grow sequentially in the second half of the year.

2. **eMemory has been very successful in the development of DDI, PMIC and analog applications. May I ask which new applications will drive the company's royalty momentum in the future? When do you expect to start seeing noticeable contributions?**

   >> Besides DDI and PMIC, we also have applied to other applications, such as various sensors. Because die size of the sensors is relatively small, the amount of wafer used is much less than that of DDI and PMIC, so it is not as obvious.

   As we develop into more new advanced process nodes, for sure we will be adopted by even more applications on new process nodes once qualified. For example, when 28nm was ready, customers like ISP, WiFi, Tcon and other high-speed IOs started to adopt our solutions from one customer to many, all followed the pattern of DDI and PMIC, and will eventually become industry standards. Regarding which application will be the next driving force for royalty revenue, we believe ISP-related will be next, followed by WiFi and Networking-related. As we accumulate production records for 7nm and progress to 5nm and 3nm, we are confident that other processor-related applications will be the next following areas.

3. **Since the largest portion of the company's royalties come from DDI, have we seen a recovery in DDI customers?**

   >> This type of customer started wafer productions at the end of Q1.

4. **Are there any royalty contributions that reflect the company's progress in automotive and AI customers?**

   >> Yes, automotive customers from 7nm ADAS, and 28nm Networking-related to mature processes such as DDI, Sensor and PMIC-related are all in mass production. Most AI customers are still in the tape-out stage, only minimal volume production.

5. **You mentioned before that most companies are your customers. Why is the market share for 8-inch capped at 20% if that is the case?**

   >> There is another 8-inch embedded memory technology (eNVM) called embedded flash, developed by SST in the 1990s and mainly used in MCUs. Its market share is also around 20%, with the remaining others using the foundry eFuse solution.

   We believe that the penetration rate of mature processes has room to grow because we still see customers switching from eFuse to our OTP due to density and performance requirement. In addition, our MTP-related technologies provide better cost performance than embedded flash. For example, compared to Embedded Flash, NeoFlash does not require additional investment in equipment and uses fewer mask layers with much lower wafer cost. It is also suitable for special processes (embedded flash is not available) and is currently being developed with many foundries customers. NeoEE has been adopted for PMIC in DDR5 modules and will start big volume production at the end of year. The above reasons will continue to increase our penetration rate in mature processes.

6. **Are Amazon/Google pushing CPU/GPU partners to adopt PUF-based confidential computing?**

   >> These two customers are currently collaborating with us for security related applications.

7. **Modern processors are often attacked, can PUF protect them?**

   >> The process of protecting information is divided into:
   1. Protect data in storage
   2. Protect data in transit
   3. Protect data in use

   To attack the processor is to attack data in use. In order to accelerate the speed of information processing, current high performance computing uses multi-core architecture and shared virtual memory to facilitate the application of multi-tasking by multiple users.

   Because of the shared virtual memory, the attacker will have the opportunity to manipulate other programs through the virtual memory.

   The solution is to ensure that each program only uses its designated virtual memory during operation, and not access other virtual memories. PUF protects data in use in CPU by providing a key tag to computing programs and their corresponding virtual memory. Each computing program can only use its own key tag to access their own virtual memory. This prevents the attacker from gaining access to other program operations through virtual memory.

8. **This year, licensing fee is the focus of eMemory's growth. What are the main process and applications that are adopting your technology?**

   >> It will be mainly driven by PUF-based security solutions and 5/6/7nm CPU, DPU, AI and Automotive-related applications.

9. **What is used to protect the hardware security of AP in mobile phone factories? What is the benefit of switching to eMemory solutions?**

   >> Currently, the hardware security mobile phone manufacturers use is eFuse to store public and private keys. It does not use chip fingerprints to protect the entire hardware root of trust. Our solutions can obtain the best hardware root of trust, while the PUF chip fingerprint protects the whole security system. At the same time, the public and private keys from the chip can significantly reduce security concerns and costs when injecting keys.

10. **In the past, the encryption protocol, RSA, played an important role; how will NeoPUF replace it? In addition, the BIOS can also be put into the security authentication (secure boot). Is this mutually exclusive from NeoPUF?**

    >> RSA is the algorithm which can generate public key from private key. The key (private and public keys) pairs are mainly used for authentication and signing of security functions.

    NeoPUF is the Chip fingerprint which can provide the unique private key. This private key is input to RSA and the output is the corresponding public key.

    In summary, RSA is an algorithm to create public key, NeoPUF is the source of private key.

11. **Can NeoPUF be applied to PFR (Platform Firmware Resilience)? If so, how?**

    >> Yes, our PUFcc (PUF coprocessor) can act as the digital signature and certificate for secure boot. It can also encrypt and authenticate the data stored in Flash.

12. **As Charles described, Confidential Computing is a huge opportunity. What are the competing Root of Trust solutions for this application? Follow up: if hyperscalers adopt your solution will we see press releases to that effect?**

    >> Using PUF-based solution to encrypt and protect computing data is much faster. Doing so will achieve the safest and fastest performance confidential computing.

    As I answered previously, the purpose of confidential computing is to protect Data in Use, so that hackers will not have the opportunity to modify the contents of programs or data through shared virtual memory during computing.

Because the computing speed of CPUs need to be fast, it cannot be slowed down by the encryption function. Therefore, if the encryption can be generated very quickly, it can be used as the key tag of each program to access its corresponding computing virtual memory. This can prevent hackers from entering the area to steal or modify the programs or data.
PUF-based solution is much faster than other competitors' solutions in terms of true randomness, speed and density requirements.

13. **Is the development of chiplets good or bad for the company's IP? Follow up: Is it true that as long as the company's IP is used in chips with cheaper processes and packaged together in a chiplet, then a more advanced processor is not needed?**

    >> The purpose of Chiplet is more than moore. Chiplets divide the SoC into small chips and package them. Therefore, the function of the SoC remains the same, and security functions are still needed.

    However, after being separated into smaller chips, the communication between each separated chips whether it is a original chip, will lead to many security problems and other challenges, including yield loss during packaging, IO connection and confidentiality, and certification of original chips. All of these require OTP for yield repair, PUF for original chip certification, and PUF-based solutions for encryption protection. Therefore, in the chiplet architecture, OTP and security become even more important.

14. **As the utilization rate of fabs are very low, have you seen a sharp decrease in foundry prices, and will they affect the company's royalty income?**

    >> Currently, the pricing strategies of foundries are different. The big foundries maintain pricing, and only relatively small-scale foundries have discounts. Overall, ASP has little impact to royalties.

15. **What is the progress of your collaboration with Arm? When will we start seeing contributions?**

    >> Our collaboration is going very well. We'll see contributions soon**.**

16. **How is your PUF-based IP licensed to customers? Do you work with fab or customize for chip designers?**

    >> Because our NeoPUF is made up of NeoFuse transistors, developed on foundry process and is licensed directly to foundries. The Roof of Trust function and our PUFcc Co-Processor is digital design Soft IP, directly licensed to chip companies.

17. **Has ChatGPT led to more interest in eMemory? More specifically, have you started to see interest in the data center and AI-related areas?**

    >> We've always had AI and Data center customers engaging with us. Whether it is AI-related requirements driven by ChatGPT, or self-driving, IoT, and all connected devices, the level of security requirement is getting higher and higher. The trend for security requirement on chip level is very obvious.

18. **Have recent chip customers inquire more about self-driving (ADAS) applications? In addition, are eMemory IPs being adopted in automotive MCUs? Thank you!**

    >> Yes, in addition to the mass production of 7nm ADAS by Japanese customers, we expect US customer to tape out 5nm in Q2.

19. **Can you talk a little about the effect of PMIC and DDIC pricing on your royalty income?**

    >> Our ASP is based on the foundry wafer price, which has nothing to do with the chip price. The price fluctuation of foundry wafers is much lower than chip prices. We know that the wafer price fluctuation in major foundries is not much.

20. **eMemory has a very unique business model based on licensing and royalty. What is the time lag between licensing and royalties?**

    >> It typically takes 2-3 years from licensing to royalty.