eMemory – Company Overview

eMemory was established in 2000 by Dr. Charles Hsu and his students from National Tsing Hua University (NTHU). Our president, Dr. Rick Shen, is one of Charles' first Ph.D. student, as are some our management team. From the beginning, working in a laboratory for eight years, to running the company for 20 years, they have spent a total of 28 years together. This loyalty is characteristic of eMemory employees and, notably, our executive team have stayed with us since they joined the company. We have published a textbook "Logic Non-Volatile Memory: The NVM Solutions from eMemory", and another one about hardware security is underway. eMemory is offering two formal courses on our eNVM and hardware security technology at Tsing-Hua University.

Regarding our shareholder structure, at the time of establishment, the Powerchip Group held 30% of eMemory. By 2016, the Powerchip Group divested their stake and withdrew from the board of directors. Our top three shareholders are the Government of Singapore, Swedbank, and the Capital Group.

eMemory is a silicon intellectual property (IP) company. Silicon denotes semiconductors. If we use the comparison of a human body, the body is made up of many organs. The "organs" inside a chip are silicon IP. For example, the well-known IP provider Arm supplies processors that can be used as the "heart" of a chip. We provide embedded non-volatile memory (eNVM). Like a small brain, non-volatile memory stores data even when electrical power to a system is turned off. In the chip-design process, many types of IP are combined like building blocks. Some may have been created in house, and others may be provided by a chip foundry, while still others may be licensed from a third-party supplier. We are a third-party licenser just like Arm.

Today, we hold more than 700 patents that we have licensed to 24 foundries worldwide as well as 10 integrated device manufacturers (IDMs) and more than 1800 chip-design houses. Every year, more than 5 billion chips are made with our technology. Every handset made has our IP. Starting in 2013, among the world's top-ten semiconductor IP suppliers, we dominate in our technology field. Our financial indicators such as return on equity and operating margin, rank us as the world's highest profitable IP company.

In early 2000, we invented our first technology, NeoBit, which is mainly used in 8-inch wafers. Our first customer was Renesas Semiconductor. The first wave of our growth was attributable to smartphones. We captured a very high market share in chips for display drivers, power management and fingerprint identification. Our penetration rate for 8-inch wafers was about 20%. In 2010, we started to develop NeoFuse technology for 12-inch wafers and won patents in 2013. We began technology development for foundries and won our first customer, Realtek, in 2015. After years of technology development, NeoFuse was designed into chips for set-top boxes, TVs, networking and other applications. Last year, our IP was also adopted by the world's largest semiconductor companies. As our customers' products enter the mass production stage, this drives future royalty growth. Therefore, we are confident that the company has entered a multi-year growth phase.

Our confidence derives from our business model based on future revenue streams that have already been secured. Currently, 25-30% of our revenue comes from one-time licensing fees and more than 70% comes from royalties that are recurring. Our royalties as a percentage of revenue are the highest of all the semiconductor IP companies in the world. We can earn royalties because the technology we invented is the most fundamental part of a semiconductor structure.

Our business starts when we license technology to a foundry. The foundry will first pay us a licensing fee. Afterwards, we design dedicated IP for the process technology of that foundry, followed by 2-3 years of effort to pass different verifications. Once verification is completed, we will engage with chip companies such as Qualcomm and license our technology to them, for which we receive a design licensing fee. After a product design is finalized and taped out at a foundry, the chip companies will spend 1-2 years finding customers such as smartphone makers to buy their chips. After end-product makers decide on production volumes, they place wafer orders with the foundries using our technology. After such a foundry receives payment from their customer, we receive royalties from the foundry in the following quarter based on our negotiated percentage of a wafer price.

Based on this business model, 70 percent of our revenue comes from our efforts during the past two to four years or even longer. Out of total revenue, our operating expense is about 50 percent and our total licensing fees are somewhat less than 30 percent. This indicates that we need to help our customers succeed in order to earn substantial income from royalties.

Another important feature of our business model is that the licensing contract we signed with foundries has no expiration date. A foundry using our technology to produce wafers must pay royalties beyond the typical 17-year patent protection period. Our first technology invented in 2000 is still earning royalties and still accounts for more than 60% of our royalty income. At present, more than half of our royalties come from Taiwan Semiconductor Manufacturing Co. (TSMC), our largest customer.

Next, I will explain our technology. As I just mentioned we invented a transistor structure for storage. Just imagine that something the size of a fingernail can contain billions of transistors. A normal transistor cannot store data without electrical power. Unlike a normal transistor, the

transistor we invented can store data without power. What is the data we store? Inside a chip, all information and signals are represented as zeros or ones. The transistors we have invented need to store these zeros and ones even when the power is off.

How do we do that? It is achieved through a quantum tunneling property of semiconductor physics. In simple terms, quantum tunneling is a way that particles can pass through solid wall, where there is no channel. We utilize the nature defect of the oxide layer inside the transistor. The more defect, the easier for an electron to pass through the oxide layer when applying the proper voltage. If a “one” passes through, that means there’s no “zero”.

It seems simple, but in fact, it’s quite difficult. Because it is so difficult to control, we have obtained hundreds of patents for the process. Since it involves quantum tunneling, none of the zeros and ones can be detected by external means. Moreover, these invisible channels cannot be changed by the ambient environment except by applying temperatures higher than 600 degrees Celsius. For this reason, the stored data can be kept very securely for more than 10 years.

Most chips used for non-volatile memory use an e-Fuse technology that requires the application of a strong electrical current to burn the fuse, which is quite similar to the fuse in a circuit breaker. A burned fuse represents “one” and an unburned fuse represents “zero”. Reverse engineering can easily compromise such an e-Fuse memory and expose its once-secret contents. In addition, an e-Fuse cannot shrink to keep up with new advances in chip technology. This means that an e-Fuse needs an increasing portion of chip space while the amount of storage becomes increasingly limited. Adding an e-fuse to a chip requires the use of an additional mask in the chip making process for leading edge technology, and that increases production costs. The strong current needed to burn an e-fuse needs a significant amount of electricity, and once the chip is

packaged, the memory cannot be re-written, all of which make e-Fuse technology inconvenient. As a result, over the past 20 years, our technology has been replacing e-fuse and has already managed to replace 20% of the eFuse demand for 8-inch wafers, with a similar trend for 12-inch wafers underway.

Next, I'd like to introduce what we consider our most important technology going forward – NeoPUF. We expect this to extend our growth beyond the next five to ten years. What is a PUF? It stands for physically unclonable function. In simple terms, the object itself is inherently unique, like unique biological characteristics used for identification, such as fingerprints, the iris, and facial features used for recognition in humans.

Research has been done on PUFs for chips for many years. Many companies have evaluated or tried to pursue this business without success. As a result, no other company has been able to develop large volume applications.

This type of technology started to gain increasing attention since 2015, when the US Department of Defense organization DARPA tried to promote PUF technology for commercial chips.

The reason for this push was that DARPA suspects that as many as 20 percent of chips used for military applications are counterfeited. Since many chips are used both for military and commercial purposes, there are several ways that such chips can be counterfeited. I mentioned reverse engineering. Because of the drawbacks of e-fuse technology, a circuit diagram can be copied and replicated by compromising an e-fuse. Most common way of doing this is to recycle chips from discarded electronic products, repackage them and resell them. Reports say that the first time a Russian rocket launch failed, it was because the electronic system contained counterfeit chips. When airplanes malfunction, very likely that their electronic systems also contain counterfeit chips.

In 2015, we received this kind of information and started thinking of ways to use our transistor technology to perform PUF functions. Soon after, we designed a pair of connected NeoFuse transistors, which became our NeoPUF IP. Based on the quantum tunneling mechanics mentioned before, when voltage is applied to them, the defects in the oxide layers in the two transistors will not be the same, so electrons will first pass through the structure with more defects. The structure that first passes electrons is labeled as “one” and the structure that does not it is “zero”. If we design 256 pairs of such transistors and apply voltage, this will generate a random set of 256 ones and zeros. It is like a virtual coin toss. The chance of getting identical heads up and heads down results for one set of 256 tosses and another set of 256 tosses is one out of 2 to the 256th power.

This is the same as collecting all the grains of sand in the world and not being able to find any identical grains. In other words, this is perfect random naturalness! We have done many experiments and discovered that NeoPUF meets the quality of perfect natural randomness. We therefore applied for patents, which soon were granted. We also received the highest honor in the semiconductor field from the International Solid State Circuits Conference (ISSCC), the annual disruptive technology award. Our PUF is the only one that meets DARPA’s 16 requirements for perfect natural randomness.

For example, one silicon wafer of chips designed with our technology might have tens of thousands of individual chips. Each of those chips has its own unique array of zeros and ones, just as if each chip naturally had its own QR code or barcode.

Of course, where there is perfection, there’s also imperfection. What about an inferior PUF? The combinations of ones and zeros generated might not be sufficiently random, and out of 10,000 chips, some will have identical combinations, failing to meet the requirement for uniqueness.

In addition to its function as a chip ID, a PUF has many other applications such as a random number generator. What is a random number generator? When we go online, we often need to create a password. Frequently, a webpage may suggest a strong password and warn that the password we have created isn't secure enough. The suggested password, which probably looks like gibberish, has been created by a software random number generator. If you want to buy Bitcoin, the exchange will give you a jumbled string of data to use as your wallet. This also comes from a software random number generator. Because software is created by an algorithm based on certain rules, the security world is worried about the emergence of quantum computers which Google claimed its quantum computer can break all of the world's military passwords in 300 seconds. Hence, the most secure solution is to use hardware to generate random numbers.

Hardware random number generators exist in the marketplace, but they are very expensive and complicated because they have to meet the test of perfect randomness. To do so, they may use different chips or materials to derive randomness from the natural world in a module or complex IP. IBM, for example, created a hardware security module and sold it to Visa for US$40,000 so that when we do money transfers, we will receive an OTP (one-time password) which we will have to enter in a few seconds before it expires and a new password is created. Because money is as stake, these random numbers are generated by expensive hardware random number generators.

Therefore, natural randomness is the holy grail that the entire security industry is looking for, and our NeoPUF is this holy grail. The chip itself can store secret keys that are invisible, unpredictable and undetectable, providing the most fundamental security to protect data.

Because of this core technology, we established our 100% owned subsidiary, PUFsecurity, in May last year. PUFsecurity invented a series

of security IPs with different functions based on eMemory's NeoPUF. This means that we can use the IP to implement what once were very expensive hardware random number generators and other security functions directly onto a chip. This is equivalent to simplifying what once cost tens of thousands of dollars into just one IP, making it very cheap, convenient to use, and secure.

Making a solution that's secure, easy to adopt, and cost effective is the only way hardware security can become ubiquitous. For our company, this means more technologies that can be licensed and collect royalties.

Currently, there are many customers who have adopted our technology in their chip designs and are preparing for mass production. After COVID-19, the demand for our NeoPUF has increased significantly because distance working and communication have become the new norm. In addition, for 5G, AI, IoT and autonomous vehicles, security is a must. We are engaging with many leading international companies now on implementations of our technology to enhance their chip security.

We are also developing software to pave the way for security as a service business. Because of our core technology, NeoPUF, we have a lot of business opportunities, such as cloud and IoT key management, blockchain digital signatures, security certification for financial transactions, and much more!

To conclude, I want to cite what our chairman Dr. Hsu told our employees when he founded the company. He believes that every chip in the future will use our technology, and this belief will be realized through our NeoBit/ NeoFuse/NeoPUF technologies.