

eMemory Q2 2020 Results – Earnings Call Q&A

August 12th, 2020

PUFsecurity/PUF-based Solutions

1. Please provide some examples of new NeoPUF customers, and which specific type of NeoPUF products is driving the development?

One of our customers uses NeoPUF in NB-IoT, which is the interconnection application, while another uses NeoPUF in FPGA application. As mentioned earlier, our PUFrt, is based on NeoPUF to generate the unique ID and key storage related usage. Now, we are also developing PUFiot, so that we can embed it in CPU, and customers can use PUF to encrypt and decrypt the design. Therefore, there are various applications which will drive NeoPUF usage in the near future. We also have customers who uses NeoPUF solely, and we can add additional functions to create PUFrt. Inside PUFrt is NeoFuse, NeoPUF, and true random number generator. Basically, customers are interested in using PUFrt as their solution because it provides the root of trust function. Currently, many customers are requesting PUFrt and we also provide a promotion platform called IP Go, which customers can download PUFrt freely to do simulation. The other IP is the PUFiot, which is PUFrt plus all the cryptographic functions. We have recently completed this IP and there are customers who are interested in it. Next, we have PUFse (PUF Secure Element), which is still under development. The requirement from customers are basically their interest in our PUFs to provide security solutions. In the future, we are not only an IP provider, but also a security solution provider.

2. How will the revenue model work for NeoPUF related new IPs?

Basically it is just an additional revenue stream. For example, if a customer licensed our PUFrt, we will have two royalties: one royalty through the end-chip company, another is royalty from the foundry during production. Hence, this creates an additional royalty stream for eMemory.

- 3. eMemory's two main royalty streams are currently NeoBit and NeoFuse, with PUF-based being very small at just 1.5% of licensing and 0.0% of royalties. On the call Charles mentioned that eMemory has several PUF solutions such as PUFrt, PUFiot and PUFse. Are PUFrt + PUFiot + PUFse included in NeoPUF or are they separate IP streams? That is, could eMemory get 3 additional revenue streams?**

We already have many NeoPUF taped outs. The reason why we did not show it in NeoPUF license revenue is because when customers use NeoFuse and NeoPUF (which are most of the cases), we will charge the same royalty rate (1.5% of wafer price) collected through foundries, and reported as NeoFuse revenue. The purpose of doing this is to increase the adoption rate of our IPs in leading edge process node.

- 4. On the call there was the question (copied below) about the royalty streams for PUF. The answer here seems to suggest that eMemory will get a royalty from the chip company and another one collected from the foundry. Currently, I think that you only collect royalties from the foundry (approx. 1.5% of the wafer price). So, is the chip company royalty new? And is that royalty still based on the wafer price or more like ARM's royalty model?**

The reason we set up the subsidiary – PUFsecurity is to develop security solution IP (soft IP) based on NeoPUF and increase our revenue stream to charge additional license and royalty collected from end customers (chip companies, not foundries). It is like ARM charging CPU (soft IP) license and royalty to chip companies and physical IP or hard IP (Artisans) license and royalty collected from foundries. This difference is ARM's CPU royalty is based on the percentage of end chip ASP and our solution IP is based on percentage of wafer price (easy for us to audit). The royalty rate will be similar to our foundry royalty rate, but negotiable as on promotion stage. Customers will choose only one solution: PUFrt, PUFiot or PUFse. For this case, there is only one additional revenue stream. We are

developing software to pave the road to provide security solutions, such as IoT or cloud key management services. We will be sharing more with you once we have further progress.

Additional: Quantum Tunneling Effect of eMemory's Security IP Solution

In figure 1, I will explain the mechanism of our NeoFuse. We invented the NeoFuse transistor. The programming mechanism is to apply voltage just high enough to generate a tunneling current path in the gate oxide. We call this current path quantum tunneling.

Programming Mechanism

- Apply one high voltage, V^{+++} , to form a Quantum Tunneling path.



Read Mechanism

- Apply a normal operation voltage, V_R , to read the current flow through the tunneling path.

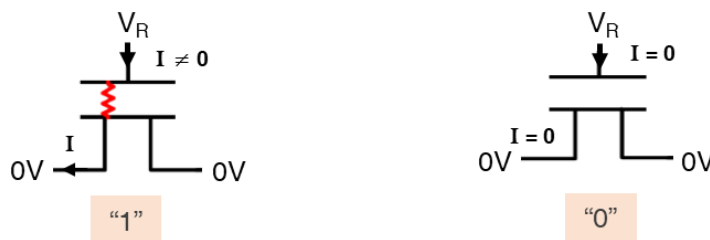


Figure 1: NeoFuse Mechanism

Figure 2 tells how quantum tunneling works. On the left side of the figure, it is the physical structure of the oxide with many defects (upper) and without defects (lower) respectively. The figure on the right is the corresponding energy band diagram. From semiconductor physics, we know that the defect in the oxide is a trap, and in the corresponding band diagram is the quantum well. So, if you have many quantum wells in the oxide, it will facilitate the electron to tunnel from one well to another such that the electron can tunnel from the substrate to the gate and contribute to the tunneling current. For the lower figure, in the oxide without defects, it is very difficult for the electron to tunnel from the substrate to the gate and consequently generate very little tunneling current. And once the defect is generated, it is very difficult to recover. From the literature, it shows that the broken bond (Si-O) needs at least more than 600 degree Celsius to recover. Therefore, the program numbers created by this mechanism is very stable. It is resilient to voltage variation, temperature variation, noise, and aging effects.

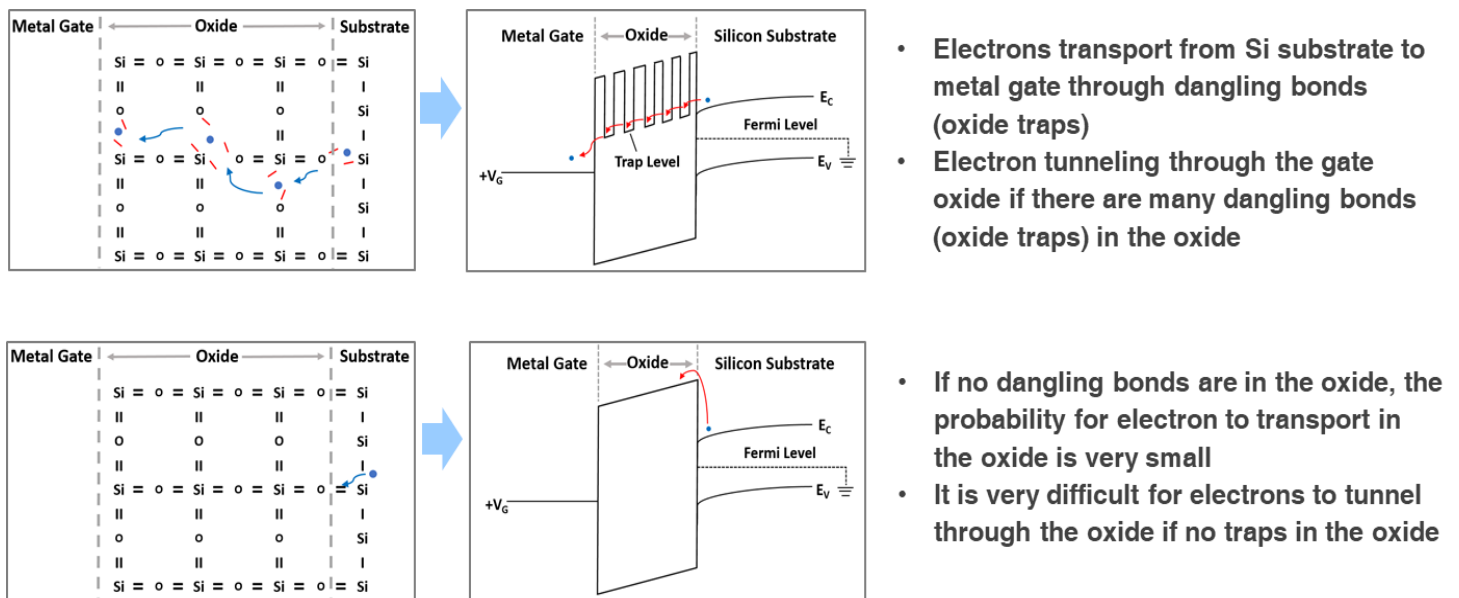
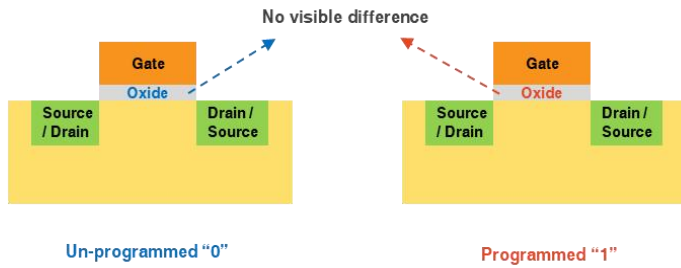


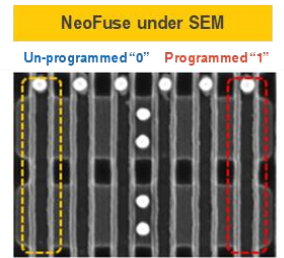
Figure 2: Quantum Tunneling Mechanism

As shown in figure 3, our NeoFuse is known for its reliability (data retention much more than 10 years), and for being invisible and untraceable, perfect for secure storage. This is in contrast to eFuse, the most commonly used process that uses fuse burn-out to establish “1” or “0” in the circuit, and is highly vulnerable to reverse engineering and data leakage.

NeoFuse



- Invisible
- Untraceable
- Reliable



e-Fuse



- Visible
- Insecure

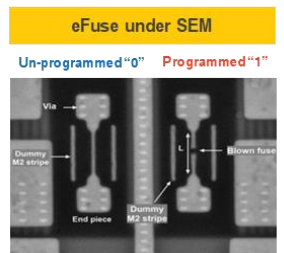


Figure 3: NeoFuse vs. eFuse

In figure 4, based on our NeoFuse, we design a pair of NeoFuse transistors and apply the voltage on their gate in parallel. When the voltage is high enough, we will see the oxide with more defects generated begins to have higher tunneling current; whereas the oxide with fewer defects generated has less. Thus, every time when we choose a pair of NeoFuse transistor to compare the tunneling current during high voltage stress, we will always see one of them, either the left one or the right one, having high tunneling current. Like tossing a coin, you never know which side will turn up. By doing this repeatedly, we will generate a group of random numbers which are dependent on the variation of the gate oxides. As shown in the second figure below, the probability of high tunneling current occurring first on the right or left is 50%. When high tunneling current happens on the left hand side, we will define it as “1” and as “0” when it happens on the right hand side. As our NeoPUF was based on the nature randomness of oxide quality, we amplify the variation of gate oxide and transform them into digital signals, which become unique fingerprint for chip itself.

- A path of oxide quantum tunneling would be located at either left or right one after high voltage is applied to a pair of NeoFuse in parallel, which depends on the micro-difference in oxide quality variations.
- Awarded 2018 ISSCC outstanding paper

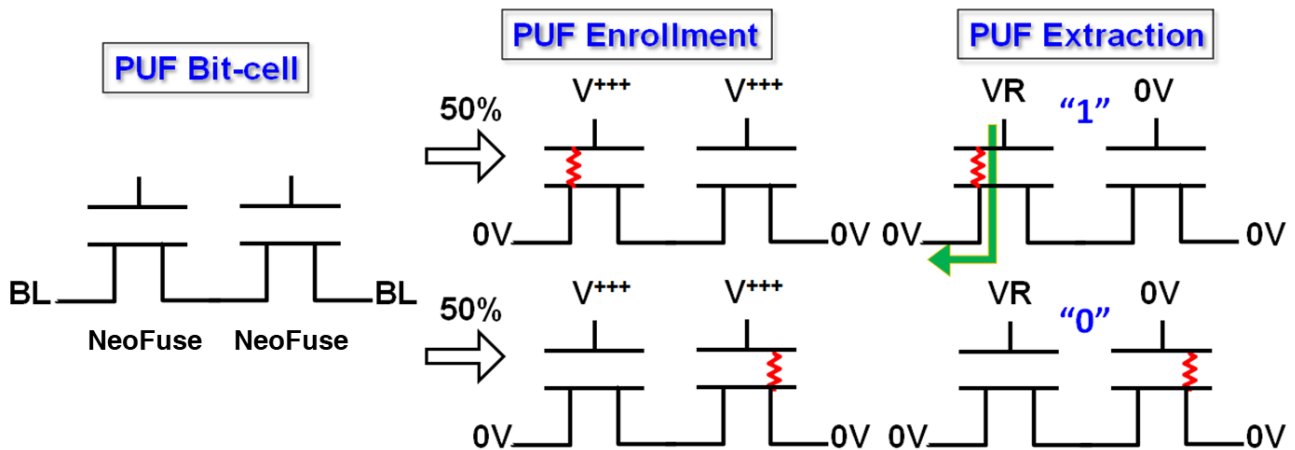


Figure 4: NeoPUF Mechanism

In summary, our NeoPUF is built on the foundations of our NeoFuse technology and shares the same qualities of reliability, invisibility and non-traceability. Since we have many NeoFuse platforms, so there are also many NeoPUF platforms that are available and ready to be used. NeoPUF is the one and only one produced using Quantum tunneling mechanism. This is something no other competitors or new comers can do and catch up with. I think our NeoPUF technology will dominate the world's PUF technology.

In figure 5 and 6, I will explain what hardware root of trust is and how our NeoPUF and NeoFuse work as a root of trust. A root of trust must ensure that the secret key is stored in a manner that cannot be detected and is not susceptible to reverse engineering, guaranteeing the safety of the data. The root of trust is therefore the key component that protects the storage of system data and maintains its integrity.

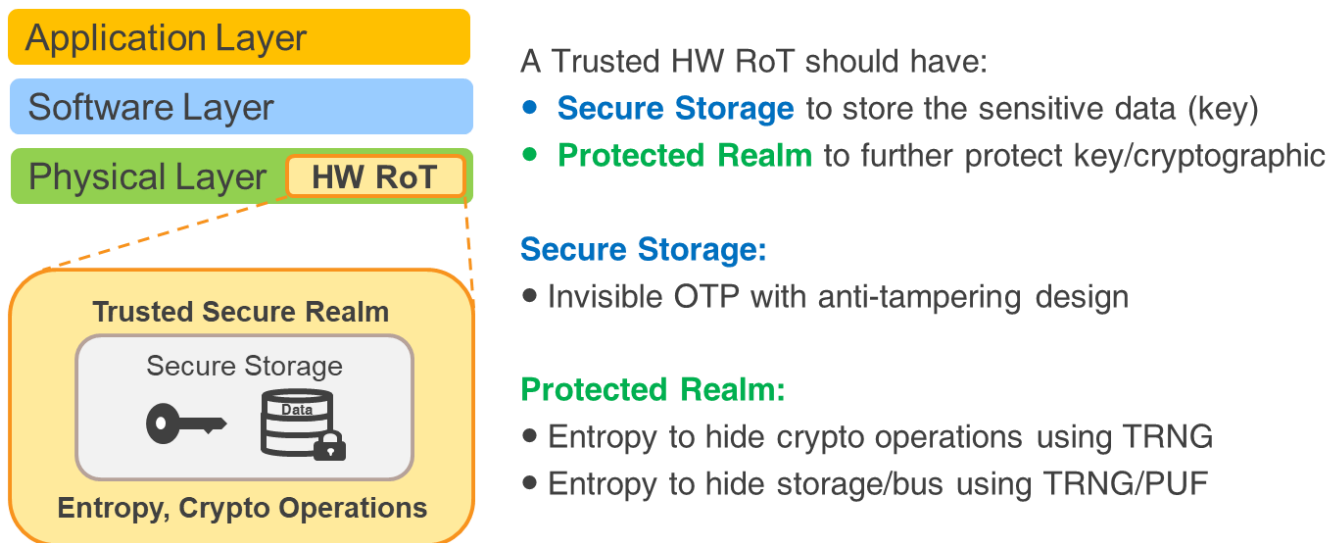
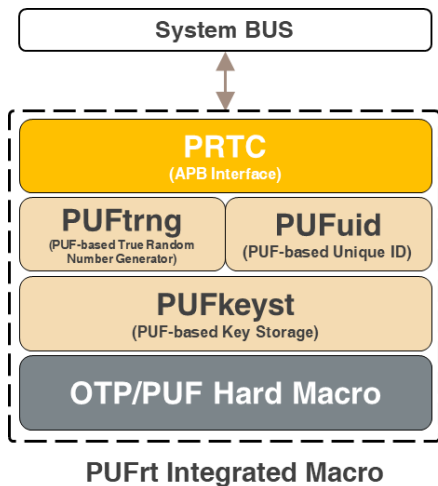


Figure 5: Hardware Root-of-Trust (HROt)

Our PUFrt solution leverages our NeoPUF and NeoFuse technologies to establish a robust root of trust. First, our NeoPUF allows us to extract a unique ID (UID) for the chip, essentially a digital fingerprint. This UID is then stored within our NeoFuse, where it remains securely, free from detection and the threat of reverse engineering.



A Highly Integrated PUF-based HRoT




- PRTC: **R/W Access Authority** Control Interface
- PUFuid: **Instant Ready** On-chip UIDs 
- PUFtrng: **Instant Ready** PUF-based TRNG 
- PUFkeyst: **Trusted Self-encrypted** Storage 
- Complete **Anti-Tampering** Design

Figure 6: PUFrt

Key generation, which is crucial for coding and decoding sensitive data, can be executed through the combination of the unique ID and true random number generator. And the keys are securely protected from physical tampering in the embedded secure NeoFuse OTP. This helps solve the major security problems that chip designers face.

The root of trust based on NeoFuse and NeoPUF has many outstanding features: in particular, ease of use, high speed, low power utilization, and low cost. Before the availability of our root of trust solution, customers need to incorporate at least three IP vendors' IP (OTP, PUF, and TRNG) into their designs or use very expensive external hardware random number generator. Consequently, we have strong conviction that our PUFrt will become the future market leader due to its overwhelming competitive advantages.