Beyond Data Storage -

**PUF**, a Must for New Semiconductor Industry Arena.

Charles Hsu
May, 2019
Outline

- Embedded Non-Volatile Memory in IoT
- Embedded Memory Beyond Storage - PUF
- Feature of PUF
- Usage of PUF
- Application of PUF
- Summary
eMemory's embedded Memory for IoT

- eMemory's embedded memory IP includes NeoBit, NeoEE, NeoMTP, NeoFuse, NeoPUF.
- eMemory's IP works under low power, small size with high reliability.
- eMemory's IP portfolio covers many functions such as parameter setting, trimming, function selection, data storage, identification.
- With the advantages of eMemory's IP, we can cover most of the usage in IoT.
Beyond Data Storage: From Memory to PUF

From uniform to non-uniform

Memory

- The quality of the Memory lies in the uniform memory cells’ threshold voltage ($V_{th}$).
- The design of the peripheral circuit aims to minify the $V_{th}$ mismatch to get better memory quality.

PUF

- The quality of the PUF lies in the non-uniform memory cells’ threshold voltage ($V_{th}$).
- The design of the peripheral circuit aims to amplify the $V_{th}$ mismatch to get better PUF quality.
What is PUF?

A physical unclonable function (PUF) is a physically-defined "fingerprint" that serves as a unique identity for a semiconductor device.

PUF depends on the uniqueness of the physical microstructure variation. These factors are unpredictable and uncontrollable.

The Feature of PUF

- **Random**: PUF depends on randomness of microstructure variation.
- **Unique**: PUF depends on the uniqueness of their physical microstructure.
- **Robust**: PUF provides much higher security level with strong robustness.
### The Properties of Ideal PUF

<table>
<thead>
<tr>
<th></th>
<th>Ideal PUF</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Randomness</strong></td>
<td></td>
</tr>
<tr>
<td>Hamming Weight</td>
<td>50%</td>
</tr>
<tr>
<td><strong>Uniqueness</strong></td>
<td></td>
</tr>
<tr>
<td>Hamming Distance</td>
<td>0.5</td>
</tr>
<tr>
<td><strong>Robustness</strong></td>
<td></td>
</tr>
<tr>
<td>Intra- Distance</td>
<td>100%</td>
</tr>
<tr>
<td>Correction Methods</td>
<td>None</td>
</tr>
<tr>
<td>Bit Error Rate</td>
<td>0%</td>
</tr>
</tbody>
</table>

**Hamming Weight:**
the number of the values that are different from the zero-symbol.
In PUF, 50% indicates the perfect randomness.

**Hamming Distance:**
a parameter to measure the number of different elements of two strings with the same length.
In PUF, 0.5 indicates the perfect uniqueness.

Resource:
Advantages of PUF-based Security Solutions

The Inborn & Unique Secret Inside the Chips for

1. Securing from Inside
   PUF can be the invisible key inside the chip for protecting the injected secrets as secure storage.

2. Inborn Root of Trust
   PUF as the inborn root of trust that can be used as the unique key for different kinds of key usages for security functions.

3. Making tRNG Easily
   PUF provides the randomness source for the true random number generator, reducing the cost for high quality entropies.
What are PUF Used For?

**Key Generations**
Each device can generate its own key from PUF.

**Secure Storage**
PUF is an invisible embedded key to protect the store memory.

**On Chip Unique ID**
PUF generates a unique code similar to a fingerprint ID for each chip.

**True Random Number Generator**
PUF based true random number generator (tRNG) with the best randomness.

**Authentication**
Authentication process can be applied by using PUF key.

**Firmware Protection**
PUF can protect firmware using local secure key, which is from inborn NeoPUF secret.
PUF-based Secure Storage

- PUF can be the inborn root of trust for secure storage.
- Data can be protected by entangling with the PUF secret. Without security algorithms, it provides a faster and lower power consumption solution for IoT security.
- Secure storage is essential for IoT devices. Because it doesn’t involve complex cryptographic algorithms, which require higher power consumption.
- Secure storage can prevent the data from being stolen, tampered, and accessed while unauthorized.
PUF-based random number generator

- PUFtrng’s randomness pass all NIST 800-22 test
  - **Easy Design** (High Quality Seeding Entropies are Unnecessary)
  - **Fast Latency** (Post Processing like AES or HASH is Unnecessary)
  - **True Random Bits** (Post Processing or HW tuning is Unnecessary)
  - **Unique tRNG sampling space chip-to-chip**
Applications Markets for Security Functions

**IoT**

With the growth of the IoT, PUF-based security can provide low power security functions to protect users’ privacy.

**Artificial Intelligence**

AI applications include training and inference. Both are expensive and valuable intellectual property to protect by PUF-based security.

**Automotive**

In smart cars, PUF-based security can provide a robust root of trust to protect drivers from the malicious attacks.

**Fintech**

PUF-based inborn secret unique ID provide the trustworthy devices for fintech services, e.g. block chain, transaction, etc.
Examples of Memory-based PUFs

Commercially Available PUF

OTP PUF、SRAM PUF are the two memory-based PUFs are commercially available PUF in the market.

• OTP PUF: eMemory (NeoPUF)
• SRAM PUF: Intrinsic ID (QuiddiKey)

Research Proposed PUF

There are also different type of PUFs are under research, such as ReRAM PUF, MRAM PUF, DRAM PUF, Flash PUF.

• ReRAM PUF: Y. Yoshimoto et.al, 2016.
• MRAM PUF: Jayita Das et.al, 2015.
• DRAM PUF: F. Tehranipoor et. al, 2017.
• Flash PUF: Moon-Seok Kim et. al, 2015.
## NeoPUF vs Other PUFs

<table>
<thead>
<tr>
<th></th>
<th>Ideal PUF</th>
<th>NeoPUF(eMemory)</th>
<th>SRAM PUF(Intrinsic ID)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unit Cell</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Method</strong></td>
<td>Oxide rupture</td>
<td></td>
<td>SRAM startup behavior</td>
</tr>
<tr>
<td><strong>Hamming Distance</strong></td>
<td>50%</td>
<td>50%</td>
<td>47%</td>
</tr>
<tr>
<td><strong>Hamming Weight</strong></td>
<td>0.5</td>
<td>0.5</td>
<td>0.62</td>
</tr>
<tr>
<td><strong>Bit Error Rate</strong></td>
<td>0%</td>
<td>0%</td>
<td>5.5%</td>
</tr>
<tr>
<td><strong>Correction Methods</strong></td>
<td>None</td>
<td>None</td>
<td>Voting, Masking, ECC</td>
</tr>
<tr>
<td><strong>Operation Temperature</strong></td>
<td>Any Temp</td>
<td>-40~175 °C</td>
<td>&lt;85°C</td>
</tr>
</tbody>
</table>

Resource:  
Introduction to NeoPUF

Singular random ruptured spot is generated unpredictably at either left or right MOSFET.

Steps for NeoPUF Enrollment:

1. NeoPUF unit cell contains two MOSFETs.
2. With the WL turned on, the process is activated by applying a high voltage.
3. When enrolled, the stress will result in different levels of rupturing due to inherent differences of oxide thickness or uniformity.
4. The stress will result in different levels of rupturing with perfect randomness.
Memory Application in IoT Beyond Data Storage: PUF - A must for IoT Security

**Features**
- **Random**: Random physical factors via manufacturing
- **Robust**: Hardware root of trust for higher security level
- **Unique**: Uniqueness of physical microstructure

**Usage**
- **Key Generations**
- **Secure Storage**
- **TRNG**
- **Authentication**
- **On Chip Unique ID**
- **Firmware Protection**

**Application**
- **IoT**
- **AI**
- **Automotive**
- **Fintech**

Memory Application in IoT Beyond Data Storage: PUF - A must for IoT Security
Reference

- **OTP PUF**: eMemory’s NeoPUF  

- **SRAM PUF**: Intrinsic ID’s QuiddiKey  

- **ReRAM PUF**  

- **MRAM PUF**  

- **DRAM PUF**  

- **Flash PUF**  

- **Samsung PUF**  
Thank you

Embedded wisely, Embedded widely.