A Must in IOT
PUF-based Hardware Security

Speaker: Evans Yang
PUFsecurity

PUF-based Security IP Solutions

NeoPUF Technology & Platform

PUFtrng
PUFkeygen
PUFkeygen
PUFenc
PUFauth
- eMemory’s security IP blocks enables a wide range of different security functions.
- Integrate security IPs to cover all security functions with higher flexibility.

**Benefits**
- Lower Cost
- Better Fit
- Reduce Time to Market
- Higher Processing Efficiency
Outline

I. New IOT Security Challenges
II. The Rise of Hardware Security
III. The Holy Grail of HW Security
IV. PUF-based Security for IOT
V. Conclusion
New IOT Security Challenges
Believe in Autonomous Driving Functions?

- Electronic system of autonomous vehicles become more and more complicated.

How to make sure system integrity and function safety?

2018.09.04  Hackers control auto electronics through wireless connectivity

2019.02.14  Automatic scooter can be controlled by hackers, causing sudden breaks or acceleration

(ref. News form iThome, Yahoo)
Privacy Leak through IoT Devices?

- Simple IoT devices are inadequate to afford high-end security algorithms. (computing, power issue)
- IoT might reveal your personal information and secrets without noticing.

2018.07.31 Hackers demonstrate hacking into WiFi PLC (power line communication)
2019.03.19 New type of Mirai botnet virus aims to industrial IoT devices

(ref. News form iThome, Yahoo)
Trusted Mobile Payment?

The insecure payment system may expose your financial information, privacy, and money loss.

2018.09.18 Mobile payment reveal user data
2018.10.12 Online shops’ user ID being stolen
2018.11.07 Online bank users’ data are revealed

(ref. News form iThome, Yahoo)
Attacks and Purposes

**Theft of Service** (business loss of service provider):
- Service pirate bypasses security check and use service illegally

**Cloning and Overbuilding** (dishonest competition without investment in R&D):
- Product pirate gets products by illegal cloning or over-production

**IP Piracy** (theft of know-how):
- Sensitive information of product or trade secret is extracted and be used for better product design with lower investment

**Denial of Service** (business loss or denial of service):
- Malicious attack is performed and leads to malfunction of genuine product
The Rise of Hardware Security
4 Security Levels: PDRR

Level 4: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Level 3: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Level 2: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Level 1: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

• Recovery Planning; Improvements; and Communications.
• Response Planning; Communications; Analysis; Mitigation; Improvements
• Anomalies and Events
• Continuous Monitoring
• Detection Processes
• Access Control
• Awareness and Training
• Data Security

Ref. https://www.nist.gov/cyberframework/online-learning/five-functions
H/W Security in IoT World

- **Edge to Cloud**
  - Authentication
  - Communicate Data Encryption

- **Edge to Edge**
  - Authentication
  - Communicate Data Encryption

- **Edge to Local Memory**
  - Local Data Encryption

![Diagram showing H/W Security in IoT World with concepts like Edge to Cloud, Edge to Edge, Edge to Local Memory, Authentication, and Key Management.](image-url)
Attacks on Chip Security

Fault Generation Attack
using abnormal conditions to generate malfunctions that provide additional access.

Software Attack
exploiting security vulnerabilities in protocols, cryptographic algorithms, or implementation. (through normal communication I/F)

Side Channel Attack
monitoring the analog characteristics of supply, I/F connection, EM radiation during normal operation

Microprobing Attack
access chip surface directly to observe, manipulate, interfere device.

Reverse Engineering Attack
understanding the inner structure and learn or emulate functionality.

(refer Physical Attacks and Tamper Resistance by Sergei Skorobogatov)
### Advantage of On-chip Hardware Security

<table>
<thead>
<tr>
<th>Hardware Root of Trust</th>
<th>Accelerated Crypto Engine</th>
<th>Binding Software &amp; Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of a standalone security element or embedded with hardware security</td>
<td>Hardware crypto engine provide high-efficient, real-time cryptography</td>
<td>Software binding with hardware provides a robust and anti-tampering security</td>
</tr>
</tbody>
</table>
ARM Trust Zone Secure CPU Architecture

- ARM trust zone create an isolated secure world which can be used to provide confidentiality and integrity to the system.

- The partitioning of two worlds is physical isolation and controlled by secure monitor instruction.

- Isolated environment, trusted boot, trusted OS make up the trusted execution environment (TEE).

Source:
PUF Can Enhance Trust Zone Security Level

- NeoPUF can protect the OTP by entangling with PUF, enhancing the security level for ARM trust zone.
- NeoPUF can provide the device unique fingerprint to authenticate the external memory.
- NeoPUF can be the unique secret for crypto engine and the TRNG generation.
- The partitioning of TEE can be bundled with NeoPUF to create unique feature for the ARM trust zone.

Source:
The Holy Grail of Hardware Security
What is PUF?

● PUF (Physical Unclonable Function) Definition
  • Unique physical characteristics derived from manufacturing variations of the integrated circuit

● PUF Requirements
  • Randomness, Uniqueness: No relation between elements
  • Unclonability, Unpredictability: Extremely hard to obtain and reproduce
  • Robustness, Reliability: Reliable over the whole product lifecycle
• PUF is a physically-defined "fingerprint" that serves as a unique identity for a semiconductor device.
  • Inborn secrets of PUF are resilient to reverse engineering.

Usage of PUF ranges from ID to keys

Small variation during manufacturing

Unique FP as inborn randomness

From randomness to security keys
Easy Security Design with PUF

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

Invisible Key Storage
NeoFuse is an invisible one-time key storage memory.

Key Generations
Each device can generate its own key from embedded NeoPUF.

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

Authentication
Authentication process can be applied by using PUF key.

Firmware Protection
NeoPUF can protect firmware using local secure key, which is from inborn NeoPUF secret.
Integrated Security IP Solution

**PUFrt : Root of Trust**
A hardware-based root of trust inside the SoC with basic security functions, including:
1. Unique identity (UID), True random number generator (TRNG), Secure key storage
2. Built-in OTP capacity and inborn OTP protection

**PUFiot : Light Engine for IoT**
An engine-based solution for IoT applications with
1. Crypto algorithms: SM2, SM3, ECC, Hash, ECDH, ECDSA……
2. System bus interface, direct memory access (DMA)
3. Secure boot, side channel resistant

**PUFse : Embedded Secure Element**
An engine-based solution for higher level customers with
1. Advanced algorithms: (optional) high-speed AES/SM4- XTS, GCM
2. OTA firmware protection, key management
3. Crypto-processor inside to off load the CPU computing power
**PUFsecurity SE IP Engine**

- unique identity
- secure key storage
- tRNG
- secure boot
- integrity check
- authentication
- encryption

Protect the data inside eFlash

Protect the data in transmission

**PUFse**

**PUFrt**

- PUF Macro
- PUFfluid
- PUFtrng
- PUFkeygen

- Secure OTP

**Peripheral**

- RTC
- GPIOs
- SPIs
- PWM
- I2C

I/F

Processor

Engine

- AES
- ECC
- Hash
PUF-based Security for IoT
Secure OTP Storage

- NeoFuse is totally protected by unique NeoPUF inborn secrets

Secure NeoFuse with embedded NeoPUF Secrets
eNVM storage can be also further protected using robust NeoPUF inborn secrets; Key length can be adjusted by encryption demand.

**Secure e-Flash Storage**

- **Data**
  - Physical Storage in Chip A or external flash A
  - Physical Storage in Chip B or external flash B

**NeoPUF**

Ex: AES256
No need for post-processing, PUFrt solution can offers Unique ID, tRNG and Secure OTP after power-on for building robust hardware root of trust.
Edge Protection with Inborn Feature

Data Communication

- Connectivity
- Sensor
- Processor Core
- Flash

- Authentication and encryption by software-based cryptography
- Additional processor load and power consumption
- Potential key exposure

Secure Data Communication

- Connectivity
- Sensor
- Processor Core
- Flash
- PUF based hardware root of trust for protecting chip unique secret and know-how
- Unload processor computing
- High-efficient crypto operation without key exposure
Product know-how and biz are protected by inborn unique secret & identity from PUFrt

Module 1

Reconfigurable Processing Unit

PUFrt

Unique Secret

Secure Programing Tool

RAM

NVM (Flash)

Write ciphertext to NVM

Protecting configuration file with chip unique secret
Real-Time Function Protection

- Performance limited by crypto operation
- Potential key exposure

- Real-time access with protection thru PUF based masking & hiding
- High-efficient operation without key exposure
Securing Service Ecosystem

- Biz and application services are securely binding with hardware inborn security

  Software integrity is guaranteed. Biz data and user privacy are protected.

  Hardware integrity is guaranteed. Physical design know-how and property are protected.

Built-in with PUF-based secure core
Conclusions
The deployment of AIOT will increase the attack vectors of the intruders.

Security in AIOT is still in its infancy, but definitely a big concern for the growth of AIOT industry.

PUF can reliably generate unique and unpredictable secret for highly secure and inexpensive hardware security solutions in IC’s.

To use PUF-based hardware security solutions to protect AIOT’s trust-worthy sustainable operation through life cycle has become the most urgent and important mission in IOT era.
Thank You

For More Information : www.pufsecurity.com