Why should your next secure design be PUF based?

Christophe TREMLET, Marketing & Sales Director
Vincent TELANDRO, Sales Manager

Design & Re-Use Bay Virtual Event Apr 20
Why Should Your Next Design be PUF Based: Outline

- Introduction to Embedded Security And Cryptography
- Keys Protection Challenge
- PUF Fundamentals
- INVIA’s PUF Solution And Its Benefits
Hierarchy in Security Measures

- Human Based
- Software Cryptography
- HW Based
Cryptography Supports The 3 Security Pillars

- **Confidentiality**: Only the intended recipient of a message can decrypt its contents.
- **Integrity**: The recipient can verify that the message has not been altered.
- **Authenticity**: The recipient can verify that the sender is who he/she claims to be.
Modern Cryptography

**Secret algorithm**

1919

Enigma

**Public algorithm / Secret key**

- 1971
- 1975
- 1977

Lucifer

DES

RSA

- 1991
- 1992
- 1999
- 2000

DSA

ECDSA

TDES

AES

- Requires highly protected keys
- Approved by a community
- Public Algos
- Requires highly protected keys
- Approved by a community
- Public Algos
Secret Key – Attacks

Non-invasive attacks

Passive (observation)
- On-board probing
- Side-channel attacks

Active (perturbation)
- Over/under V, T° or clock
- Voltage, laser, clock or EM glitches

Invasive attacks

- Chemical & laser etching
- On-chip microprobing
- Layout reconstruction
- Memory content recovery
- Electron Beam Tester (EBT)
- FIB-SEM nanofabrication
Secret Keys Protection

- **Sensors**
  - Voltage
  - Temperature
  - Clock
  - Laser & EM pulses

- **Cryptography**
  - Key diversification
  - Memory encryption

- **Obfuscation**
  - Bus scrambling
  - Random P&R
  - Shield: metal mesh
  - Power randomisation

Protect keys
Physical Unclonable Function (PUF)

**Principle**
- Acts as a device fingerprint
- Generates a per-chip unique identifier
- Exploits the random variations of the devices’ parameters

**Benefits**
- Much stronger protection than obfuscation
- Key generation without storage
- Accessible without security knowledge as an IP block
- Ground for full security of an ASIC / SoC
Physical Unclonable Function (PUF)

Challenges

- Unclonable: robust against counterfeiting
- Uncontrollable: robust against invasive attacks
- Unpredictable: robust against reverse engineering
- Invariant: stable across voltage, temperature and aging
PUF Use Cases

**Key Vault**

- PUF
- Encryption (e.g. AES)
- User Key 1
- User Key 2
- Encrypted vault
- NVM
- ASIC / SoC

**Software IP Protection**

- CPU Cache
- System bus
- Encryption (e.g. AES)
- NVM
- ASIC / SoC

- PUF

- **Keys are the most valuable assets**
- **Physical key protection available to non security experts**
- **Stronger than obfuscation**

- **Software IP is gaining value**
- **PUF with encryption**
  - provides the strongest protection
  - enables revenue protection
PUF – Examples

Delay based
- Arbiter
- Ring oscillator
- Glitch

Memory based
- SRAM
- Latch

Process based
- $V_{GS}$ or $V_{DS}$
- Via

![PUF Examples Diagram]
Invia’s PUF – Principle (patented)

Digital controller

Digital post processing

PUF cell array

Comparator

Selection and «P» parameter measurement

Biasing

Digital post-processing

Comparator

PUF cell 1,1

PUF cell 8,16

Selection

Biasing

Parameter measurement

Comparator

Comparison: $P_B > P_A \rightarrow out = 1$

Comparison: $P_B \leq P_A \rightarrow out = 0$

Digital post-processing

Selection and «P» parameter measurement

Biasing

Comparator

PUF cell 1,1

PUF cell 8,16

Selection

Biasing

Parameter measurement

Comparator

Comparison: $P_B > P_A \rightarrow out = 1$

Comparison: $P_B \leq P_A \rightarrow out = 0$
Invia’s PUF – Reliability

Weak cells are discarded

Naturally reliable

➢ 100 million PUF deployed
➢ 1.7 B bits tested
➢ 5 ppm before error correction
Invia’s PUF – Digital post-processing

Enables multiple keys generation to support « one key for one usage »
# Invia’s PUF – Facts And Benefits

## Benefits

- **Low-power**: consumption significantly smaller than most alternatives
- **Modelled**: means robust and certifiable
- **Stable and reliable**: sigma optimized by design
- **Secure**: active monitoring of the sub-blocks’ integrity
- **Scalable**: the smaller the node, the better the gaussian distribution

## Performances

<table>
<thead>
<tr>
<th><strong>Perfomances</strong> (f&lt;sub&gt;clk&lt;/sub&gt;=50 MHz)</th>
<th><strong>Size</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ Active current &lt; 10 µA</td>
<td>➢ Digital &lt; 15 kgates</td>
</tr>
<tr>
<td>➢ Stby current &lt; 10 nA</td>
<td>➢ Analog &lt; 0.02 mm²</td>
</tr>
<tr>
<td>➢ First key &lt; 210 µs</td>
<td></td>
</tr>
<tr>
<td>➢ Next keys &lt; 20 µs</td>
<td></td>
</tr>
</tbody>
</table>

- **Active** current < 10 µA
- **Stby** current < 10 nA
- **First key** < 210 µs
- **Next keys** < 20 µs

## Performances (f<sub>clk</sub>=50 MHz)

- **Active** current < 10 µA
- **Stby** current < 10 nA
- **First key** < 210 µs
- **Next keys** < 20 µs

**Performances** with **f<sub>clk</sub>=50 MHz**:

- **Active current** < 10 µA
- **Stby current** < 10 nA
- **First key** < 210 µs
- **Next keys** < 20 µs

---

*This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or distributed to a third party without the prior written consent of Thales © Thales 2018 All rights reserved.*
Takeaways

INVIA, a Thales company

- Conducts exhaustive security audits
- Assists companies in securing their systems
- Delivers silicon-proven IPs part of EAL5+ ASICs
- Protects more than 2.0 billion deployed devices

Thank you for your attention