Hardware Intrinsic Security, from theory to practice

Vincent van der Leest
Intrinsic-ID, Eindhoven, The Netherlands
vincent.van.der.leest@intrinsic-id.com
Table of Contents

- Introduction
- PUF type analysis
- Use case for PUF technology
- Testing of PUF behavior
  - PUF Reliability
  - PUF Uniqueness
- Additional PUF research examples at Intrinsic-ID
Introduction

PUF = Function embodied in a physical structure that consists of many random characteristics originating from uncontrollable process variations during manufacturing.

In other words: “Fingerprint” based on hardware intrinsic properties that vary due to manufacturing process variations.

Should be:

- Easy to evaluate / measure
- Inseparably bound to the object
- Not reproducible by manufacturer
Introduction

Timeline

- …… : Preliminary work on PUF-like technologies
- 2001: First publication of PUFs by Pappu
- 2001: Start of PUF research Philips Research
- 2002: Introduction of silicon based PUFs
- 2006: PUF technology promising enough for Philips to start “business unit”
- 2008: Successful spin-out Intrinsic-ID from Philips
Table of Contents

• Introduction
• PUF type analysis
• Use case for PUF technology
• Testing of PUF behavior
  • PUF Reliability
  • PUF Uniqueness
• Additional PUF research examples at Intrinsic-ID
Optical PUF

Pro’s
Huge set of C/R-pairs

Con’s
Difficult to integrate in IC
Coating PUF

<table>
<thead>
<tr>
<th>Pro’s</th>
<th>Con’s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part of IC</td>
<td>Expensive to produce</td>
</tr>
<tr>
<td></td>
<td>Limited set of C/R-pairs</td>
</tr>
</tbody>
</table>
Delay based PUFs

- **Pro’s**
  - Part of IC
  - Relatively large set of C/R-pairs

- **Con’s**
  - Place and Route constraints due to non-standard components
  - Susceptible to modeling attacks
Memory based PUFs

**Pro’s**
- Constructed from standard CMOS components

**Con’s**
- Limited set of C/R-pairs
Example: SRAM memory cell (6T)
SRAM startup behavior
SRAM Uniqueness

Device 1

Device 2

~ 50% difference
SRAM Noise

~ 10% errors
Table of Contents

• Introduction
• PUF type analysis
• Use case for PUF technology
• Testing of PUF behavior
  • PUF Reliability
  • PUF Uniqueness
• Additional PUF research examples at Intrinsic-ID
Application: Secure Key Storage

Known key storage options:

- Fuses, E(E)PROM, Flash, Battery backed RAM, ROM, etc.

Problems of these methods:

- Security
- Costs
- Availability
- Time to Market
Hardware Intrinsic Security (HIS)

Due to deep sub-micron process variations ICs are intrinsically unique.

Start-up SRAM values establish a unique and robust fingerprint.

The electronic fingerprint is turned into a secure secret key, which is the foundation of enhanced security.
Security advantages of HIS

In order to protect keys against physical attacks:

1. Do **not** permanently store a key in non-volatile memory

2. Generate the key **only when needed** from a Physical Unclonable Function (PUF) in the IC

3. **Delete** the key
Key Storage With PUFs

Enrollment

C → PUF → R → Helper Data Algorithm → W → Key

One-Time Process

Reconstruction

C → PUF → R' → Helper Data Algorithm → Key

In the field

I(W, Key) < ε

P[Key not Correct] < δ
Quiddikey™ Product, Key Programming

- **Functionality**
  - Storage of unique device keys
  - Storage of user keys
  - Key storage for AES, RSA, ECC

- **Requirements**
  - Uninitialized SRAM
  - Storage for device-unique activation code
Quiddikey™ Product, Key Reconstruction

- **Functionality**
  - Storage of unique device keys
  - Storage of user keys
  - Key storage for AES, RSA, ECC

- **Requirements**
  - Uninitialized SRAM
  - Storage for device-unique activation code
Anti-cloning property
Confidentio™-SC

- Integrated security processing unit:
  - Secure key storage
  - Content / data encryption
  - Randomness generation
- Root of trust for mobile apps
- Targets SIM/SmartCard, Secure Digital (SD-) card or embedded Secure Element
- Complementary to
  - ARM TrustZone
  - GlobalPlatform Trusted Execution Environment (TEE)
Table of Contents

- Introduction
- PUF type analysis
- Use case for PUF technology
- Testing of PUF behavior
  - PUF Reliability
  - PUF Uniqueness
- Additional PUF research examples at Intrinsic-ID
SRAM PUF test results

• Evaluation properties:
  • Reliability: when PUF responses are measured, the reference measurement should be recognized which was taken at enrollment
  • Uniqueness: PUF responses of a specific device are random and unpredictable, even given all PUF responses of other devices

• Studied SRAM instances from different technology nodes and vendors. Each SRAM memory was evaluated using the following tests:
  • Temperature Test (reliability)
  • Voltage Variation Test (reliability)
  • Hamming Weight Test (uniqueness)
  • Between-Class Uniqueness Test (uniqueness)
  • Secrecy Rate & Compression Test (reliability + uniqueness)

• Publication: “Comparative analysis of SRAM memories used as PUF primitives”, published at DATE 2012 (March 2012)
Temperature Test

- Study stability of start-up values at different temperatures
- ICs measured under varying ambient temperature
- Measurement at 20°C has been used as reference
Voltage Variation Test

- Study stability of start-up values under variations of power supply voltage level
- Measurement at Vdd has been used as reference
- Hamming Distance during test very low and constant

<table>
<thead>
<tr>
<th>SRAM</th>
<th>Technology</th>
<th>Devices</th>
<th>90% of Vdd</th>
<th>Vdd</th>
<th>110% of Vdd</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Min</td>
<td>Avg</td>
<td>Max</td>
</tr>
<tr>
<td>Cypress CY7C15632KV18</td>
<td>65nm</td>
<td>10</td>
<td>3.3%</td>
<td>3.9%</td>
<td>4.4%</td>
</tr>
<tr>
<td>Virage HP ASAP SP ULP 32-bit</td>
<td>90nm</td>
<td>8</td>
<td>5.0%</td>
<td>5.5%</td>
<td>6.0%</td>
</tr>
<tr>
<td>Virage HP ASAP SP ULP 64-bit</td>
<td>90nm</td>
<td>8</td>
<td>4.9%</td>
<td>5.5%</td>
<td>6.2%</td>
</tr>
<tr>
<td>Faraday SHGD130-1760X8X1BM1</td>
<td>130nm</td>
<td>10</td>
<td>4.0%</td>
<td>4.6%</td>
<td>5.2%</td>
</tr>
<tr>
<td>Virage asdsvsnfs1p1750x8cm16sw0</td>
<td>130nm</td>
<td>10</td>
<td>4.0%</td>
<td>5.4%</td>
<td>6.3%</td>
</tr>
<tr>
<td>Cypress CY7C1041CV33-20ZSX</td>
<td>150nm</td>
<td>8</td>
<td>3.2%</td>
<td>3.5%</td>
<td>3.8%</td>
</tr>
<tr>
<td>IDT 71V416S15PHI</td>
<td>180nm</td>
<td>8</td>
<td>1.6%</td>
<td>1.8%</td>
<td>2.0%</td>
</tr>
</tbody>
</table>
Hamming Weight Test

- Study uniqueness based on Hamming weight as well as stability at different temperatures
- ICs measured under varying ambient temperature
- Hamming weight during test around 50% and constant over temperature for most devices
Between-class Uniqueness Test

- Study uniqueness based on between-class HD distributions
- Hamming Distances should be Gaussian distribution with mean at 0.5 and small standard deviation
- Results very good for devices that also had good results in Hamming Weight Test, less for devices with bias
Secrecy Rate & Compression Test

- Direct CTW compression test indicates that worst-case there is only small amount of non-randomness in PUF responses (compression to 98.2%)

- Context-Tree Weighting (CTW) algorithm was used to estimate the mutual information between PUF responses: \( I(X) = H(X) - H(X | X') \)

- Mutual information provides maximum achievable secrecy rate, which determines amount of compression needed for privacy amplification

- Worst-case mutual information found is 0.38 (Virage HP SRAM)

- Worst-case required compression factor is therefore \( 1/0.38 = 2.6 \)

<table>
<thead>
<tr>
<th>SRAM</th>
<th>Technology</th>
<th>Devices</th>
<th>Compressed size (bits)</th>
<th>Original size (bits)</th>
<th>Compression ratio</th>
<th>Minimum I(R,R(^*))</th>
<th>Average I(R,R(^*))</th>
<th>Maximum I(R,R(^*))</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cypress CY7C15632KV18</td>
<td>65nm</td>
<td>10</td>
<td>16392</td>
<td>16384</td>
<td>100.0 %</td>
<td>0.62</td>
<td>0.64</td>
<td>0.65</td>
</tr>
<tr>
<td>Virage HP ASAP SP ULP 32-bit</td>
<td>90nm</td>
<td>34</td>
<td>16385</td>
<td>16384</td>
<td>100.0 %</td>
<td>0.38</td>
<td>0.59</td>
<td>0.69</td>
</tr>
<tr>
<td>Virage HP ASAP SP ULP 64-bit</td>
<td>90nm</td>
<td>34</td>
<td>16389</td>
<td>16384</td>
<td>100.0 %</td>
<td>0.49</td>
<td>0.63</td>
<td>0.73</td>
</tr>
<tr>
<td>Faraday SHGD130-1760X8X1BM1</td>
<td>130nm</td>
<td>40</td>
<td>13896</td>
<td>14000</td>
<td>99.3%</td>
<td>0.52</td>
<td>0.61</td>
<td>0.69</td>
</tr>
<tr>
<td>Virage asdssnsf1p1750x8cm16sw0</td>
<td>130nm</td>
<td>40</td>
<td>13903</td>
<td>14000</td>
<td>99.3%</td>
<td>0.47</td>
<td>0.57</td>
<td>0.67</td>
</tr>
<tr>
<td>Cypress CY7C1041CV33-20ZSX</td>
<td>150nm</td>
<td>8</td>
<td>16392</td>
<td>16384</td>
<td>100.0 %</td>
<td>0.60</td>
<td>0.70</td>
<td>0.76</td>
</tr>
<tr>
<td>IDT 71V416S15PHI</td>
<td>180nm</td>
<td>8</td>
<td>16091</td>
<td>16384</td>
<td>98.2%</td>
<td>0.57</td>
<td>0.70</td>
<td>0.79</td>
</tr>
</tbody>
</table>
Fuzzy Extractor Design

- Design goal: derive 128-bit cryptographic key with failure rate $< 10^{-9}$, using worst-case secrecy rate (0.38) and noise (21%) assumptions
- Amount of secret bits required $= 128/0.38 = 337$
- Concatenated error-correcting code design that achieves failure rate $< 10^{-9}$ assuming 21% noise:
  - Inner code: $3 \times$ BCH-code $[n,k,d]=[255,115,43]$
  - Outer code: $765 \times$ Repetition-11 code
- This design requires 1.03KB of SRAM memory
Reliability tests performed at Intrinsic-ID

- Tested: 180, 150, 130, 90, 65 nm
- Temperature cycle / temperature ramp
- Endurance low temperature: IEC 60068-2-1
- Endurance high temperature: IEC 60068-2-2
- Radio frequency electromagnetic field: IEC 61000-4-3
- Ambient electromagnetic fields immunity: EMC: EN55020
- Electromagnetic compatibility
- Humidity
- Voltage ramp-up
- Data retention voltage
- Accelerated lifetime
- Extensive End customer validation
- Millions of measurements performed

Photo: Philips Innovation Services
Table of Contents

• Introduction
• PUF type analysis
• Use case for PUF technology
• Testing of PUF behavior
  • PUF Reliability
  • PUF Uniqueness
• Additional PUF research examples at Intrinsic-ID
European research projects

- **PUFFIN**
  - Providing intrinsic and long-wanted basis for security in everyone's most common computing platforms: PCs and mobile devices

- **RELY**
  - Targeting reliability as parameter throughout chip development

- **UNIQUE (finalized in 2012)**
  - Tackling counterfeiting of and tampering with Integrated Circuits

- **RATE**
  - Dutch project focused on modeling impact of process variations, environmental parameters and ageing on SRAM PUFs
Some selected papers from Intrinsic-ID

- **Using PUF noise for random number generation**
  - “Efficient Implementation of True Random Number Generator based on SRAM PUFs” in Cryptography & Security: From Theory to Applications, 2012

- **Soft decision error correction (decreasing required SRAM)**
  - “Soft Decision Error Correction for Compact Memory-Based PUFs using a Single Enrollment” at CHES 2012 conference

- **New type of memory based PUF: Buskeepers**
  - “Buskeeper PUFs, a Promising Alternative to D Flip-Flop PUFs” at HOST 2012 workshop

- **Re-usable PUF: Logically Reconfigurable PUF**
  - “Recyclable PUFs: Logically Reconfigurable PUFs” in Journal of Cryptographic Engineering, November 2011 and at CHES 2011 conference
  - “Logically Reconfigurable PUFs: Memory-Based Secure Key Storage” at ACM STC 2011 workshop