Design of SRAM PUF with Improved Uniformity and Reliability Utilizing Device Aging Effect

presented by

Achiranshu Garg and Tony T. Kim
VIRTUS, IC Design Centre of Excellence
School of EEE, Nanyang Technological University, Singapore

June 5th, 2014
Counterfeiting

Fake Apple Store in China: It's a Wrap *

Staff believe they are working in a real Apple store

Electronics Resellers Association International (ERAI) tracks the counterfeit electronics over the period of 5 years reports

Super-power military was even not spared by counterfeits **

---


** http://spectrum.ieee.org/computing/hardware/counterfeit-chips-on-the-rise
Memories based Security System

- Battery Backed
- Physical Unclonable Function (PUF)
- Non-Volatile Memory (NVM)

Electronic Device*

Sends a random number

Sign the number with a secret key
Only the IC’s key can generate a valid signature

Needs a security key to access

NVM based

PUF

Battery backed
Classification of PUF

- Extrinsic
  - Optical
  - Coating
- Intrinsic
  - Delay
  - SRAM
  - Butterfly
Our Selection: SRAM PUF

Criteria for ideal security systems*

- **Easy to fabricate**: produced in large quantities, highly cost efficient
- **Easy to probe**: easy internal probing, extensive development in read/write circuitry.
- **Hard to clone**: due to random device variations
- **Structurally stable**: numerous research and development works have been done in making 6T SRAM a very stable structure

Start-up Value & Cell Skew

- **SRAM Operations**
  - Read Operation
  - Write Operation
  - Start-up Value

- **Partially skewed cells**
  - 2, 6, 7, 8

- **Fully skewed cells**
  - 1, 3, 4, 5, 9, 10
Ideal Requirements in PUF

• **Uniformity**: Equal distribution of 1’s & 0’s

• **Reliability**: Hamming distance between power-ups should ideally be zero, minimum number of partially skewed cells. Bit-pattern shouldn’t change in subsequent power-up(s).
More about Reliability

• **Hamming Distance** gives the parity between two bit-strings

<table>
<thead>
<tr>
<th>String1</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>String2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Hamming distance between String1 & String2 is 2

• **Conventional approach** uses ECC (Error Correction Code), complexity of which depends on the number of error bits
Monte Carlo Simulations: 8kb SRAM

- Standard PVT for all simulations
  - Process = TT
  - Voltage = 600mV
  - Temperature = 25°C

- As the output is random, it is difficult to clone
Monte Carlo Simulations: 8kb SRAM

- For same input variations, output variation is different.

- For different devices, hamming distance is nearly 50%
Negative Bias Temperature Instability (NBTI)

- Mismatches at Si-SiO₂ leads to interface traps
- Minority Si atoms form weak bond with H
- Disassociation of weak Si-H bonds due to inverse biasing of PMOS
- Broken bonds leads to electrically active traps
- Active traps leads to increase in $V_{TH}$

Impact of NBTI on SRAM SNM

- **Before NBTI stress**
  - Prob. of ‘1’ = Prob. of ‘0’

- **After NBTI stress**
  - Prob. of ‘1’ > Prob. of ‘0’ or
  - Prob. of ‘1’ < Prob. of ‘0’

Uniformity Improvement

• **NBTI (Ageing)**
  Ageing results in flipping of start-up for majority-cells

• **Uniformity**
  Equal Probability of 0’s or 1’s in output string, makes it difficult to guess.
Cell Flip under NBTI

- Due to the action of NBTI, the stronger PMOS P1 becomes weaker in subsequent power-up 2.
- Power-up value at node OUTB flips from ‘1’ to ‘0’ in subsequent power-up.
Reliability Improvement

- **Check Variations**
  Power-up multiple times and check the variations.

- **Flip the Values**
  If variations are there, flip the internal values of SRAM

- **NBTI Ageing**
  Ageing results in increase the skew between the cells
Reliability Improvement

Power-up 1

\[ |V_{tp1}| \geq |V_{tp2}| \]

Small mismatch not reliable

Flip

Power-up 2

\[ |V''_{tp1}| >> |V_{tp2}| \]

Increased mismatch more reliable

Ageing
SRAM Cell Flipping Setup

- Built-in Flip mechanism.
- For every address location, a bit is read in first cycle and flipped bit is written in next cycle.
SRAM-PUF Improvement Methodology

- Uniformity Improvement
  Ageing and power-up

- Reliability Improvement
  Flip and Ageing
  Power-up
SRAM Cell Flipping Setup

# of ‘1’s >> # of ‘0’s

# of ‘1’s >> # of ‘0’s
### SRAM Cell Flipping Setup

#### # of ‘1’s > # of ‘0’s

<table>
<thead>
<tr>
<th>Ageing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Strong ‘1’**

**Matched cell**

**Strong ‘0’**
### SRAM Cell Flipping Setup

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

- **Ageing**: Moving from left to right (holding top row fixed), the number of '1's increases down the left side of the cell, and the number of '0's increases down the right side of the cell. This results in more '1's compared to '0's.
- **Uniformity achieved**!

**Note**: The grid represents the states of a SRAM cell under different ageing conditions. The uniformity achieved is indicated by the equality of the number of '1's and '0's in the column.

**Strong ‘1’**

**Strong ‘0’**

# of ‘1’\'s ≈ # of ‘0’\'s

---

**Ageing**

**Uniformity achieved!**

---

**Strong ‘1’**

**Strong ‘0’**

---

**Matched cell**

---

**NANYANG TECHNOLOGICAL UNIVERSITY**
### SRAM Cell Flipping Setup

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

- **Flip** + **Ageing** → **Uniformity** + **Reliability achieved!**

- # of ‘1’s ≈ # of ‘0’s

- Strong ‘1’
- Matched cell
- Strong ‘0’
Uniformity Output in an 8KB SRAM

- Increasing ageing results in flipping of majority cells.
- SRAM-PUF was powering up to ‘1’ as majority cells initially.
- After NBTI, ‘1’ and ‘0’s are more balanced.
Reliability Output in an 8KB SRAM

- For a particular cell, powering-up probabilities were same due to external fluctuations initially.

- Flipping + Increasing ageing results in increase in skew in a particular cell.
Summary

• A post-fabrication methodology (Device ageing) is described to improve reliability and uniformity of SRAM-PUF
  – Uniformity improved by action of ageing
  – Reliability improved by action of flipping and ageing

• ECC (Error Correction Code) complexity can be removed, hence overall cost can be reduced