Leveraging Circuit Reliability Effects for Designing Robust and Secure Physical Unclonable Functions

M. Kim, G. Park, P. Chiu and C. H. Kim
University of Minnesota

chriskim@umn.edu
chriskim.umn.edu
Outline

• Background

• Case Study: Hybrid SRAM + Metal Fuse PUF Design

• 65nm Test Chip Results

• Conclusions
Physical Unclonable Function (PUF)

- **Unique and random:** Based on physical entropy source
- **Secure:** Large # of challenge-response pairs (CRPs), resilient to machine learning based attacks
- **Stable and reliable:** Output should be consistent under temperature, voltage variation and aging
Entropy Sources Available On-Chip

- Process variation: threshold voltage, mobility, W, L, dielectric thickness, metal RC, etc → delay or voltage difference
- Reliability variation: activation energy, defect density, acceleration factor, dielectric thickness, etc → lifetime difference

http://viennashe.sourceforge.net/viennashe-finfet.html

S. Natarajan, IEDM 2014

C. Zhou, VLSI 2015
• Parallel or crossed signal paths configured by challenge bits
• Delay difference polarity detected by arbiter circuit
• “Strong PUF” but susceptible to machine learning attacks → must incorporate nonlinearity (e.g. XOR)
PUF Circuit Example: Voltage Type

- SRAM power up state is unique to each chip
- “Weak PUF” where challenge = address, response = stored bit
PUF Circuit Example: Voltage Type

- Trip point of first NAND compared with next trip point, and next trip point, ...
- Static PUF: Based on DC voltage comparison, utilizes standard NAND gate

Samsung, ISSCC 2016
PUF Circuit Example: Oxide Breakdown Type

KU Leuven, IMEC, ASSCC 2018, JSSC 2019

eMemory, ISSCC 2018
PUF Stability Problem (SRAM PUF Data)

Unstable cells

Data 0

Data 1

\[ T = 80^\circ C \]

\[ T = 25^\circ C \]

\[ T = -10^\circ C \]

Power up ramp time = 0.78V/\mu s

Power up ramp time = 1.25V/\mu s

Power up ramp time = 8.33V/\mu s

Avg. Intra-chip Hamming distance = 7.12%

M. Liu, et al., ISLPED 2017
Existing Solutions for Hardening PUF Responses

- Temporal majority voting
- Spatial majority voting
- Select strong bits (e.g. data remanence)
- Error correction codes (requires NVM)

→ Significant area, performance, resource overhead
Alternative Method for Hardening PUF Responses

Time dependent dielectric breakdown (TDDB)

Electromigration (EM)

- TDDB, EM: Non-volatile, irreversible, abrupt
- Advantages of metal fuse (as per Intel’s JSSC 2016 paper): Compatible with IO voltage, metal cross section scales, transistor drive current increases

A.S. Oates, et al., TDMR, 2009
Outline

• Background

• Case Study: Hybrid SRAM + Metal Fuse PUF Design

• 65nm Test Chip Results

• Conclusions
Split vs. Hybrid Architecture

• Simpler design but security may be compromised

• Extra design effort but security is improved
Entropy Source Design

Standard 6T SRAM Cell

Modified SRAM Cell

• All IO devices, no write path, high drive current, perfect symmetry

Not a typo
Hybrid PUF Cell with Symmetric Layout

- Symmetric layout in x, y, z directions ensures an unbiased PUF response

(1) SRAM power gating PMOS, (2-3) Tri-state buffers, (4) Split NMOS program device, (5) SRAM cell, (6) Split discharge NMOS, (7) Split read NMOS

• Symmetric layout in x, y, z directions ensures an unbiased PUF response
Post-layout Simulation Results of PUF Cell

- Initial Q and QB voltages are 1.25V + offset and 1.25V, respectively
- Q and QB nodes switch at <0.1mV offset condition which confirms a perfectly symmetric layout
• Metal fuse layouts with different M3 and M2 lengths implemented in the same chip
Fuse Program and Read Operations

- Key parameters: (1) Metal fuse program time, (2) Bitline charging time
• 4 X 32 Hybrid SRAM + metal fuse PUF cells and array
• PWS and WL for each row and IN_LOW for each column
Header PMOS, Metal Fuse and 4 Unit Cells

- Header PMOS, metal fuse and 4 unit cell layout structure
  - (a) Header PMOS, (b) Unit Cell, (c) Metal Fuse
65nm Die Photo and Feature Summary

**Technology Core Size**

65nm GP CMOS

**Size**

300 X 60 μm²

**Logic / I/O Supplies**

1.0V / 2.5V

**Unit Cell Size**

7.7 X 5.6 μm²

**# of Cells**

128 Cells

**Fuse PGM Current**

30mA (per Fuse)

**Fuse PGM Time**

Mean 5525ms (M3/M2 (2/3μm))

- **90° Rotation**
- **300μm**
- **60μm**

**Control and Test**

- BL Control Circuit & Buffer
- 32 Column Scan In/Out Register

**M3/M2**

- (2/2μ) 64Cells
- (1.5/2μ) 16Cells
- (1/2μ) 16Cells
- (2/3μ) 16Cells
- (2+1/2μ) 16Cells
Outline

• Background

• Case Study: Hybrid SRAM + Metal Fuse PUF Design

• 65nm Test Chip Results

• Conclusions
Fuse Program Results (25°C and 90°C)

![Graphs showing Fuse PGM Time for 25°C and 90°C conditions.]
128 bit PUF Output Response

- Average ratio between the number of ‘1’s and number of ‘0’s measured from 10 chips is 49.8%
Intra-chip and Inter-chip Hamming Distance

- Intra-chip Hamming distance measured from 5 chips over 20 power up trials.
Reliability of PUF Response

- Excellent metal fuse reliability
  - No changes in the PUF response after baking at 150°C for 192 hours

Baking test
(192 hours, 150°C)
Conclusions

• Oxide breakdown or electromigration can be utilized as entropy source or hardening mechanism for PUF

• Case study: Hybrid SRAM + metal fuse PUF
  – Stable 128 bit key generation demonstrated in 65nm CMOS
  – Perfectly symmetric PUF cell schematic and layout
  – Hamming distance distributions show excellent margin
  – Program time of various fuse layouts studied