A Physical Unclonable Function Chip Exploiting Load Transistors’ Variation in SRAM Bitcells

Shunsuke Okumura¹, Shusuke Yoshimoto¹, Hiroshi Kawaguchi¹, and Masahiko Yoshimoto¹,².

¹Kobe University
²JST, CREST

Jan. 23th, 2013, ASP-DAC
Background

Anti-counterfeiting
Supply-chain-management

To prevent illegal replication of chip ID

Physical Unclonable Function (PUF) is applied to chip ID.

“Challenge” data

Vth variation

“Response” data

0 1 1 0 1 – – – 1

PUF needs
• **Repeatability**
• **Randomness**
• **Low power**
Proposed ID generation Scheme

I. Add bitline driver

II. Add VBC switch

- Small area O.H
- Low power
- Higher repeatability

Stop continuous current

Ground both bitline simultaneously
Simulation waveforms

Bitcells store unique values depending on the variation.

Old data is overwritten by “0”
Test chip

1-Mb ID generating SRAM (16 kb x 64 blocks)

Technology
- 65-nm CMOS
- 12 metal layers

Area
- 4.82 mm²
  (1260 um x 3240 um)

SRAM organization
- 16-kb block x 64 (= 1 Mb)

Block configuration
- 128 rows x 8 columns x 16 bits/word

16-kb SRAM Block

X decoder & Y decoder & I/O circuits

Generated chip ID
(128 b x 128 rows)
Experimental results

- **12,288** sample ID
- **Voltage fluctuation test**
- **Temperature fluctuation test**
- **Aging test**

Repeatability and Identification fail rate are estimated.

**Identification fail rate test**

Identification fail rate: $2.1 \times 10^{-12}$