IDEC Chip Design Contest

# A Reconfigurable SRAM-based Challenge-Response Generating PUF in 65nm CMOS

Seungbum Baek, Ju-Hyeok Ahn, and Jong-Phil Hong

School of Electrical Engineering, Chungbuk National University, Republic of Korea

## Motivation

- **Advantage of CMOS based Physical Unclonable Function (PUF) for IoT Technology**
  - **Truly physically unclonable: Random process variation**
  - **Low cost, high yield, small area & low power**
  - **Main feature of IoT PUF: Area, uniqueness, reproducibility & number of available CRPs (I/O pairs)**

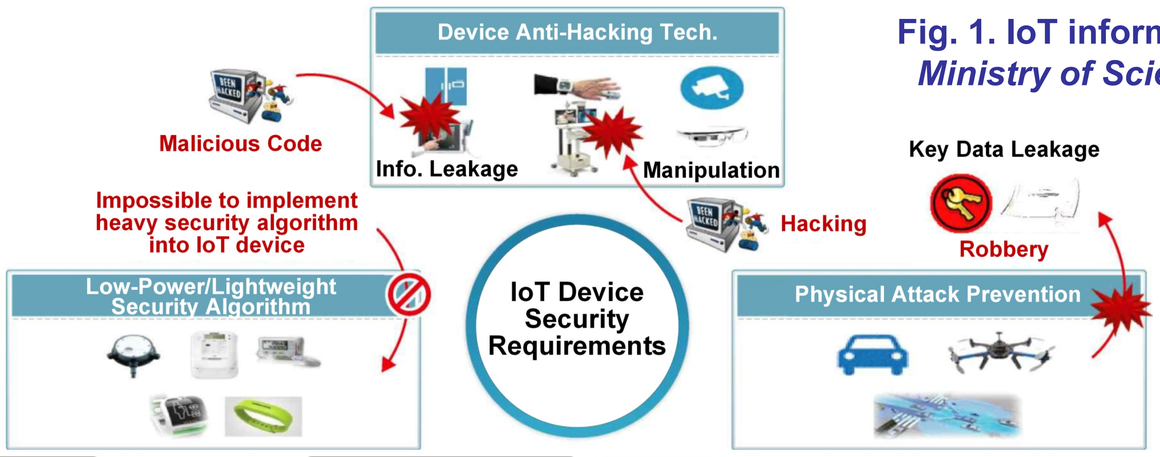



Fig. 1. IoT information security road map, *Ministry of Science and ICT*, RoK, 2014

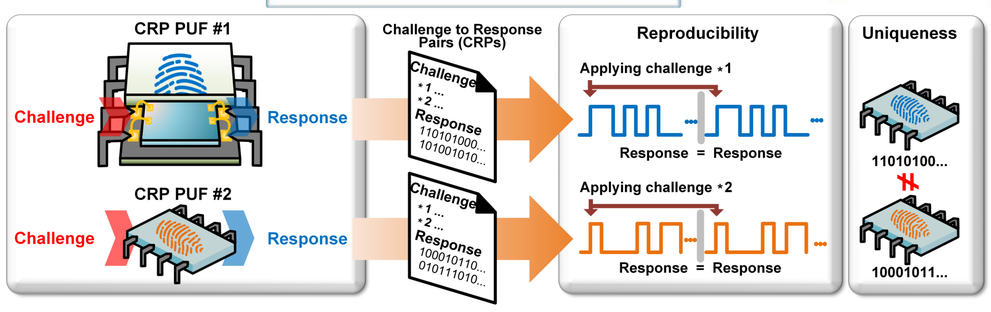



Fig. 2. CRP PUF characteristics

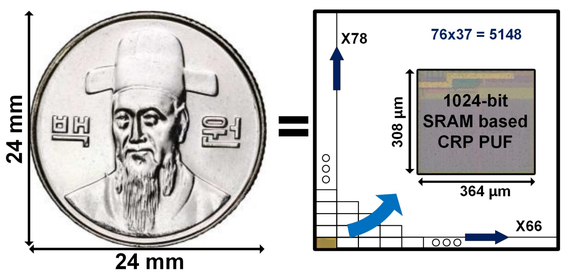



Fig. 3. Ultra-small PUF RNG IC

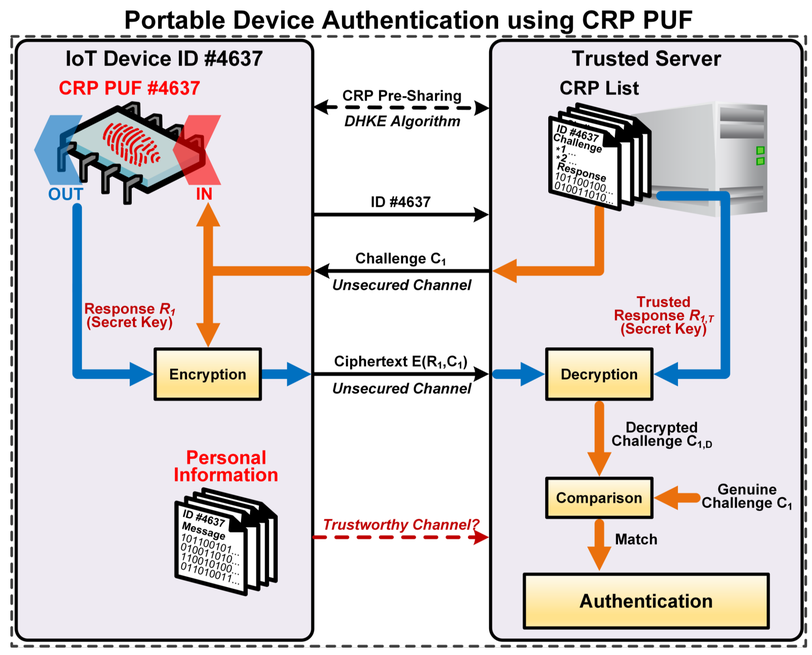



Fig. 4. Authentication using CRP PUF

## Reconfigurable SRAM Strong PUF

- **Conventional SRAM based Weak PUF**
  - **Utilizing settling state of SRAM → Randomly storing a zero, a one, or no preference → Unique ID (1 CRP)**
- **Proposed Reconfigurable SRAM Strong PUF**
  - **Exhibiting advantages of weak PUF (speed and power) & activating large number of CRPs**

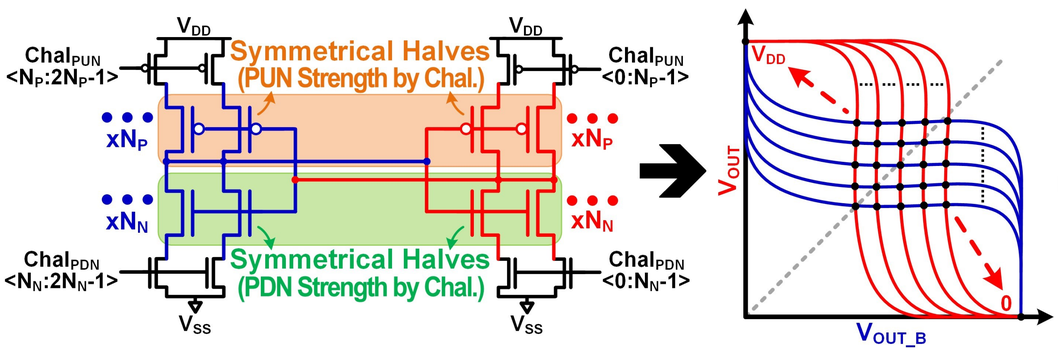



Fig. 5. Conceptual structure of the proposed reconfigurable SRAM PUF

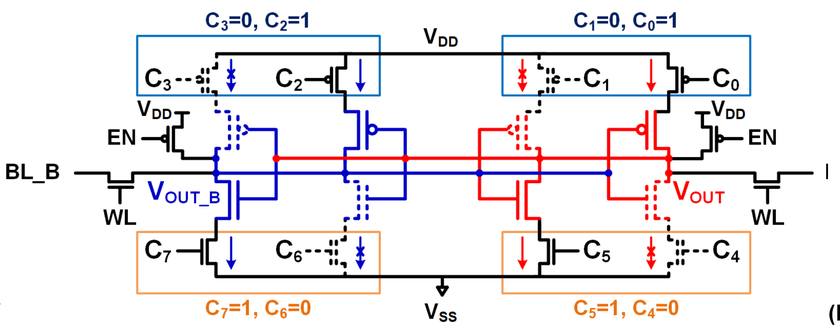



Fig. 6. Operation principle by challenge input in which $N_N = N_P = 2$

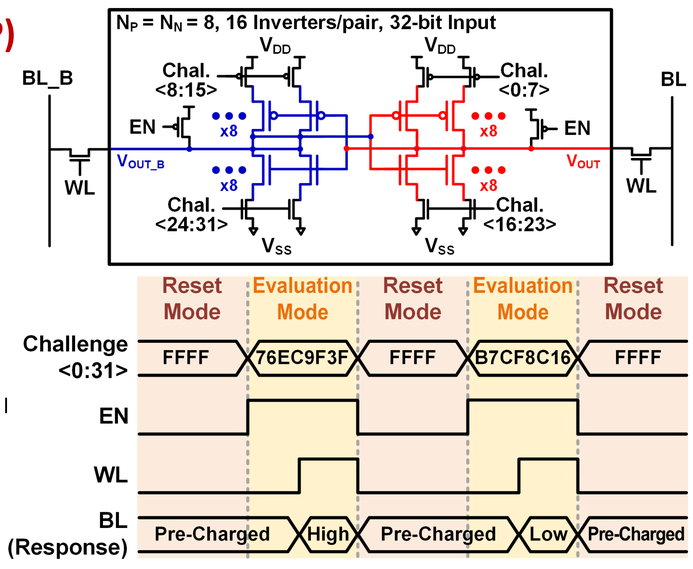



Fig. 7. Schematic and timing diagram in which $N_N = N_P = 8$

## Implementation Result and Performance Comparison

**Table I. Performance comparison with state-of-the-art CRP PUF designs**

| | This Work | VLSI'17 Jeloka *et al.* | ISSCC'15 Yang *et al.* | VLSI'17 Xi *et al.* | JSSC'11 Stanzione *et al.* |
|---|---|---|---|---|---|
| CMOS Technology | 65nm | 28nm | 40nm | 130nm | 90nm |
| PUF Topology | Bi-Stable (SRAM) | Bi-Stable (SRAM) | Delay (RO) | Analog | Analog |
| Bit-Width of Challenge [bit] | 32 | 256 | 96 | 65 | 256 |
| Bit-Width of Response [bit] | 1024 | 64 | 1 | 1 | 31 |
| BER (Stabilized) [%] | 0.81 (17% discarded) | 3.17 | 0 (34% discarded) | 0.4 (42% discarded) | 0.1 |
| Uniqueness [%] | 48.93 | 48.3 | 50.07 | 49.9 | - |
| Core Area [um²/bit] | 88.867 | 0.7605 | 845 | 44700 | 1129 |
| Throughput [Mb/sec] | 1600 | 1100 | 1.6 | 0.006 | 0.00625 |
| Energy Efficiency [pJ/bit] | 0.082 | 0.097 | 17.75 | 11 | 6080 |

- **65nm bulk CMOS, 68T/cell, 32b input, 1024b output**
- **$1.6 \times 10^8$ CRPs/die**
- **Throughput up to 1.6Gbps & Efficiency 82fJ/bit**
- **Uniqueness 48.93% & BER ~0.81%**

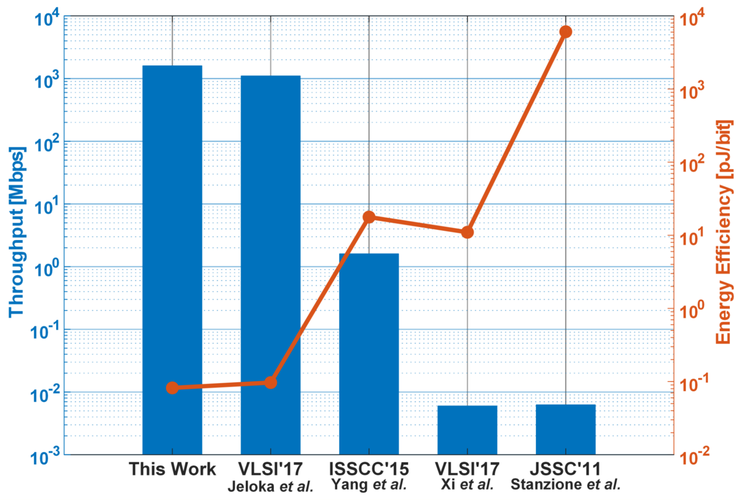
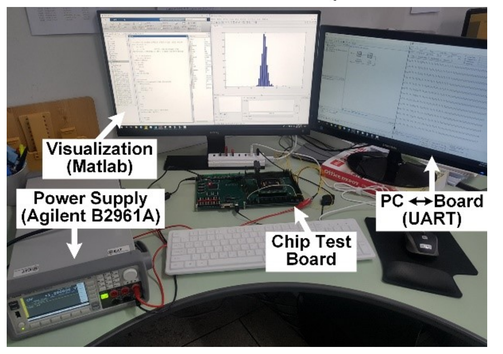






Fig. 8. Chip micrograph and measurement environment




### Acknowledgments

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1B07042607).
The chip fabrication and EDA tool were supported by the IC Design Education Center(IDEC), Korea.

반도체설계교육센터 IC DESIGN EDUCATION CENTER