IDEC Chip Design Contest

Adjustable Majority Voting Algorithm for Stability Improvement in SRAM-based CMOS PUFs

Kwangmin Yu, Woojin Jeong, Jimin Yoo, Hyunyoung Yoo, Su-Hyeon Kim,
Yeonsu Kim, Myung Hyun Jeon, Eunji Yoo, and Jae-Won Nam
Department of Electronic Engineering, Seoul National University of Science and Technology

Abstract

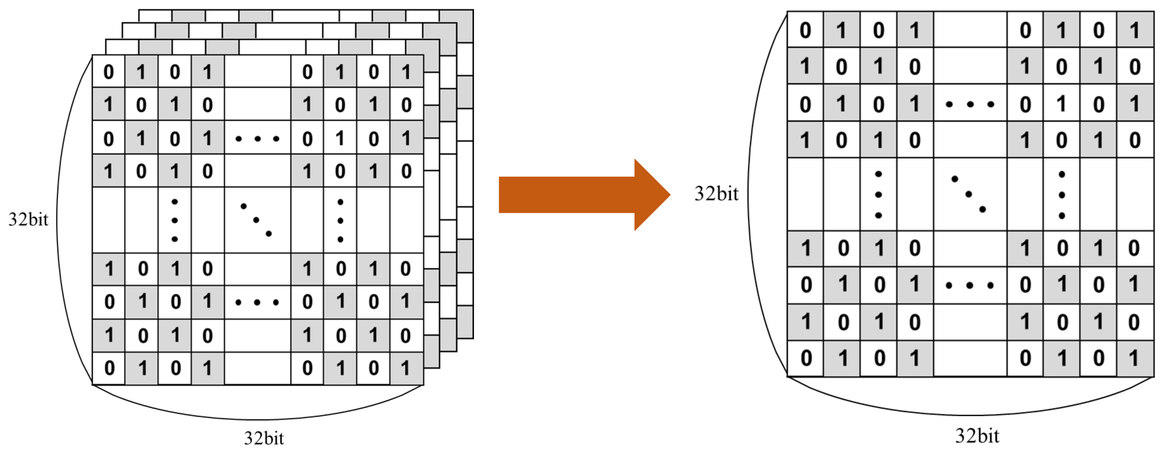
The SRAM-based CMOS physically unclonable function (PUF) employing the adjustable majority voting algorithm is presented. In memory-based PUFs with limited challenge-response pairs (CRPs), output stability is critical. To achieve a target bit error rate (BER), an error-correction algorithm using a user-configurable majority voting scheme is implemented using a data accumulator and majority selector. Fabricated in 28nm CMOS, the 1024-bit SRAM PUF core achieves 24.12 μm²/bit area and 0.09 pJ/bit energy efficiency. With 2^{10}+1 repetitions, unstable bits reduce from 31.54% to 8.40%, and BER improves from 6.28% to 0.93%. Utilizing all SRAM bitcells, unstable bits and BER improve by 73.37% and 85.19%, respectively, at 1.0 V and 25°C. Consequently, masking only about 1% of the error cells leads to a zero BER. Furthermore, the inter-die and intra-die Hamming distances are 49.84% and 1.37% (1,000 evaluations), respectively.

Concept of technique

◆ **Conventional error-correction algorithm**

- Discard unstable SRAM bit-stream ➡ “Reduction of active bits”

◆ **Majority Voting algorithm**

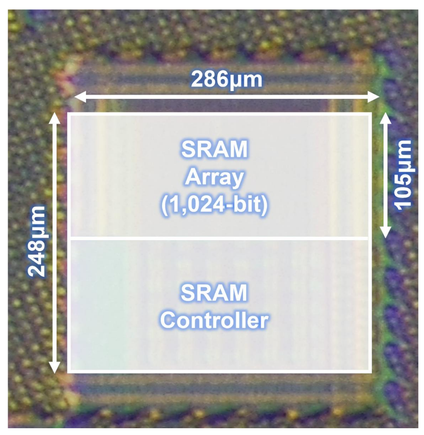


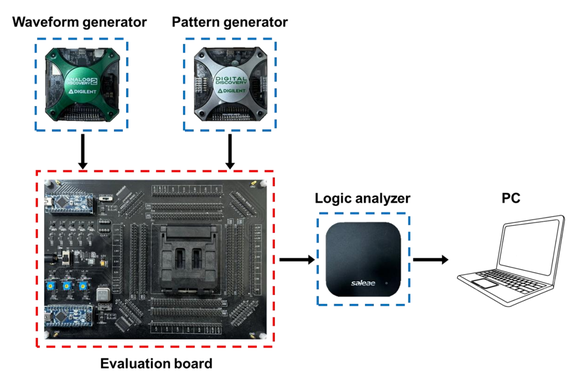
- Set the number of iteration cycles using the ‘user-configurable option’.

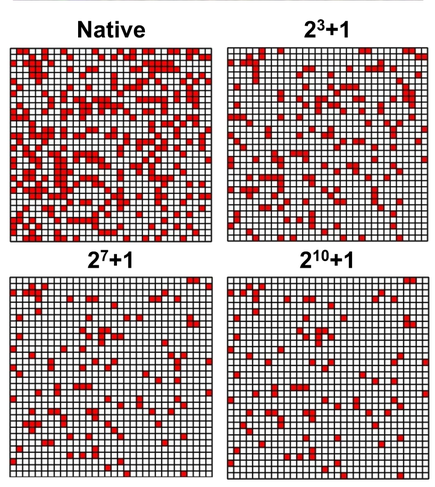
- The chip internally averages multiple SRAM cell trials and outputs a single 32x32 bit array.

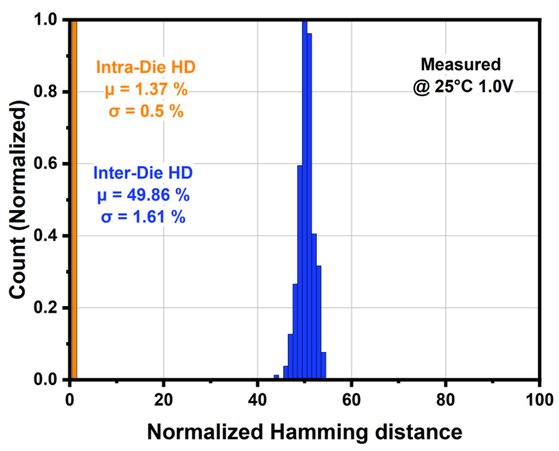
- Increasing the number of trials mitigates noise, yielding a more stable SRAM cell output and utilizing a more active bits.

Measurement Setup & Results

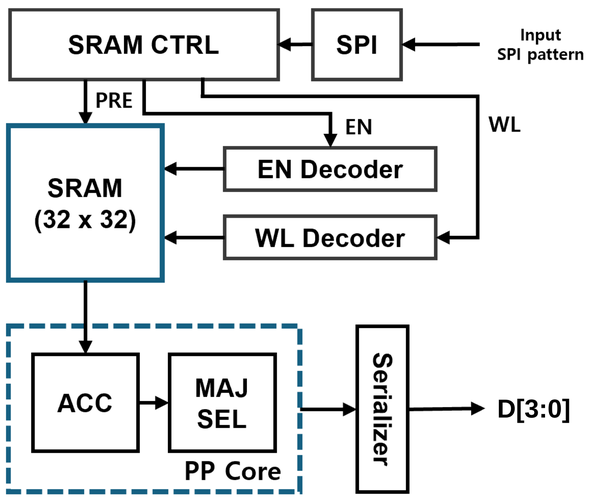


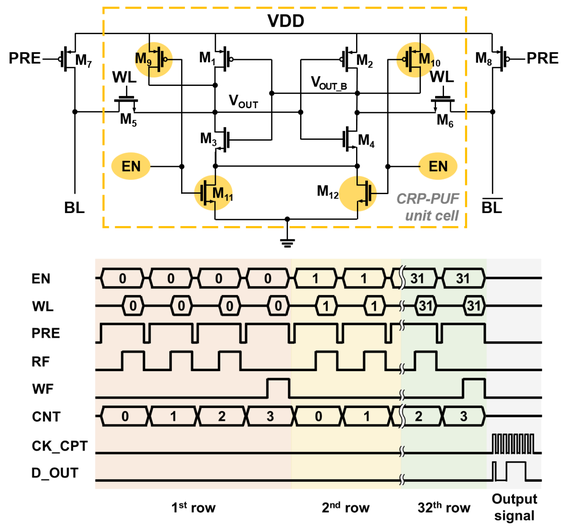






Overall Architecture





◆ **32 x 32 SRAM PUF with multiple CRPs (1.6E+8).**

◆ **An adjustable majority voting scheme is implemented using an accumulator and majority selector.**

◆ **The prototype is fabricated in 28nm technology.**

Comparison

	This work	TCAS’2022	VLSI’2023
CMOS Technology	28nm	40nm	28nm
Pre-Stabilization BER (%)	6.28	5.27	-
After-Stabilization BER (%)	0.93	0.8	0.42 / 2.25
Active bit ratio (%)	100	70.24	87.5 / 39.9
Intra-HD (%)	1.37	-	1.87 / 2.95
Inter-HD (%)	49.84	49.84	50.11 / 50.09

Acknowledgement

The chip fabrication and EDA tool were supported by the IC Design Education Center (IDEC), Korea.

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant under 2022R1A4A3029433 and 2021R1A2C2005258), and in part by the Ministry of Science and ICT (MSIT), South Korea, through the Information Technology Research Center (ITRC) Support Program supervised by the Institute for Information and Communications Technology Planning and Evaluation (IITP) under Grant IITP-2024-RS-2022-00156295.

반도체설계교육센터 IC DESIGN EDUCATION CENTER