25.2 A Reconfigurable RRAM Physically Unclonable Function Utilizing Post-Process Randomness Source with <6×10^{-6} Native Bit Error Rate

Yachuan Pang[1], Bin Gao[1], Dong Wu[1], Shengyu Yi[1], Qi Liu[1], Wei-Hao Chen[2], Ting-Wei Chang[2], Wei-En Lin[2], Xiaoyu Sun[3], Shimeng Yu[3], He Qian[1], Meng-Fan Chang[2], Huaqiang Wu[1]

[1]Tsinghua University, Beijing, China
[2]National Tsing Hua University, Hsinchu, Taiwan
[3]Georgia Institute of Technology, Atlanta, GA

Physically unclonable functions (PUFs) are promising primitives for hardware security with wide applications in the Internet of Things (IoT), e.g., authentication and encryption key generation [1, 2]. Most silicon PUFs utilize process variability of semiconductor manufacturing [1, 3, 4]. These implementations are sensitive to variations in operating conditions (e.g., supply voltage and temperature variations) and undergo significant native bit-error-rates (N-BERs). Thus, additional stabilizing strategies, such as ECC, majority voting, and masking, are necessary. Furthermore, the PUF key after enrollment cannot be changed in prior implementations [1–5]. This could be unsafe if the PUFs are repeatedly used in insecure environments, as PUFs suffer from the challenges of ownership change and overuse (Fig. 25.2.1).

To achieve low N-BER, high reconfigurability, a compact area, and true randomness, we present a reconfigurable resistive random access memory (RRAM)-based PUF by using: 1) an intrinsic (or post-process randomness) physical randomness source instead of a process randomness source for the generation of a key; 2) a resistance-differential comparison between two RRAM arrays for the exact PUF key; and, 3) a split-resistance technique to achieve a low N-BER. The table in Fig. 25.2.1 compares the performance of different PUF implementations. In this study, a 130nm, 8Kb, RRAM PUF macro was implemented to realize a reconfigurable nonvolatile PUF with post-process randomness. This RRAM PUF achieves a low <6E^{-6} N-BER, with a bit-cell area of 2.86μm^2 and 47.29% reconfigure-Hamming Distance (reconfigure-HD) at runtime.

The PUF can obtain a true random encryption key by converting the random analog resistance distribution to a random digital distribution. Two 1-transistor-1-RRAM (1T1R) units are used as a PUF bit cell (PUF cell: RRAM1, differential cell: RRAM2). The RRAM has two resistance states when it is used for memory applications. These two states are called the high and low resistance states (HRS and LRS, respectively). A normal distribution of resistance is formed when programming an RRAM to one of the aforementioned states with a single programming pulse. The random distribution is attributed to the RRAM's device-to-device (D2D) variation, which is the entropy source for the RRAM PUF. Moreover, the distribution of different switching cycles differs considerably owing to the Write cycle-to-cycle (C2C) variation, which is the basis for the PUF reconfigurability (Fig. 25.2.2). To generate one stable PUF bit, we developed a split-resistance technique. A RESET pulse (as HRS has wider resistance distribution) was applied to RRAM1 and RRAM2, the resistances of which were then differentially compared through a small offset sense amplifier (SA). The cell with the smaller/larger resistance is SET/RESET to LRS (<100kΩ)/HRS (>1.5MΩ) with verification. As such, the sensing window is enlarged.

Figure 25.2.3 shows the architecture of the reconfigurable RRAM PUF macro. It includes two 8Kb 1T1R RRAM arrays as PUF and differential arrays. This macro also includes peripheral circuits, such as an X/Y decoder, a program control circuit, a driver, and a small offset SA. The PUF states are defined in this figure as follows: state 1, $R_{\text{PUF cell}} < R_{\text{differential\_cell}}$; state 0, $R_{\text{PUF cell}} > R_{\text{differential\_cell}}$. For the basic PUF bit, a 1×0.5μm^2 *n*-type transistor serves as the selector to provide enough drive capability for RRAM, and a 0.5×0.5μm^2 RRAM cell is integrated between M5 to M6. To extract the PUF key based on the resistance distribution of HRS, a small offset SA is required for small cell current (~500nA). The differential SA is shown in Fig. 25.2.3. A current-sampling-based SA (CSB-SA) technology [6] is used to distinguish the two resistances of RRAM1 and RRAM2. In addition, owing to the V_t-independent current sampling scheme using C1/C2, the SA can be implemented for differential current input. This approach uses the same device (P1/P2) to sample cell currents (Icell/Iref) and amplifies the current difference; this suppresses the input current offset due to device mismatch and small cell current.

Figure 25.2.4 shows the measured randomness test results among 20 PUF test chips (each PUF chip has 64 PUF keys, and each key is 128b) fabricated in the 130nm 1.8V/5V CMOS process. The tested spatial data mapping of 80 keys showed random and uniform (0/1 bias) distributions, and no apparent spatial correlations. For the Hamming weight (HW) of each key, the probability of 1 in a 128b key among 1000 PUF keys is very close to the ideal value (50%) with a tight normal distribution (μ/σ = 50.013%/2.866%). The embedded table shows the NIST randomness test results. The developed PUF passes all test indices with average P-value >> 0.01 (criteria value).

Figure 25.2.5 demonstrates the PUF's uniqueness and reproducibility among 20 test chips in normal conditions (25°C). For uniqueness, the data show an almost ideal value (50%) of inter-chip HD (μ/σ = 49.99%/4.35%) across 600 PUF keys. As for reproducibility, no error was detected in 10^{10} reproduction cycles, implying that the intra-chip HD is very close to the ideal value of 0 (BER < 1/160Kb ≈ 6.1E^{-6}). As mentioned above, almost all prior PUF implementations are vulnerable to environmental changes. Owing to the split-resistance technique, our PUF is robust under voltage and temperature changes (temperature: 25-150°C, voltage: 1.4-2.2V/2.5-5.5 V). No errors were found after long-term baking for 6000 minutes at 125°C. Furthermore, the spatial autocorrelation function (ACF) test shows no correlation among 30Kb PUF keys (confidence intervals: ±0.0075). This result implies PUF keys are independent, whether from the same or different chips.

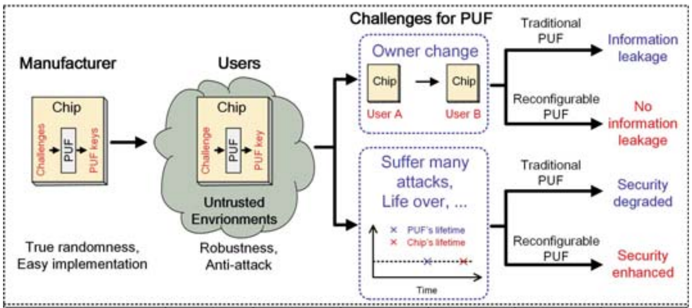
The most unique advantage of the developed RRAM-based PUF is its reconfigurability, indicating that the PUF's security can be enhanced. Fig. 25.2.6 shows the reconfiguration flow chart. The reconfiguration operation is easy to implement without a complex stabilizing method (e.g., masking, baking, and ECC). Regarding the uniqueness of the reconfigured PUF keys, 60 continuous reconfiguration cycles for the same PUF show values close to the ideal value of the reconfigure-HD (μ/σ = 47.29%/6.07%). In addition, the correlation matrix of 60 continuous reconfigured PUF keys demonstrates little correlation between the different reconfigured keys.

Figure 25.2.7 shows the top view of the PUF micrograph with a summary table and 2T2R PUF bit-cell layout. The micrograph also shows the details of the test chip, including an 8Kb PUF array, an 8Kb differential array, a program control circuit, an X/Y decoder, a driver, an SA, timing control, and other peripheral circuits. The area of the PUF array is smaller than peripheral circuits. This is because the PUF array only has 8Kb PUF bit cells, and the X/Y decoder and driver are designed to support a future 16M PUF bit array . In particular, the developed RRAM-based PUF shows the advantages of reconfigurability, easy implementation, high reliability, and good randomness.

Acknowledgements:
This work is supported in part by the NSFC (61674092), MOST of China (2016YFA0201803), Beijing Innovation Center for Future Chip (ICFC), Beijing Municipal Science and Technology Project (Z181100003218001), NSF-CNS-1615774 and SRC-2016-TS-2691, and Tsinghua and National Tsinghua joint project.

References:
[1] Y. Su, et al., "A 1.6pJ/bit 96% Stable Chip-ID Generating Circuit Using Process Variations,", *ISSCC*, pp. 406-407, Feb. 2007.
[2] N. Liu, et al., "OxID: On-chip One-Time Random ID Generation Using Oxide Breakdown," *IEEE Symp. VLSI Circuits*, pp. 231-232, 2010.
[3] S.K Mathew, et al., "A 0.19pJ/b PVT-Variation-Tolerant Hybrid Physically Unclonable Function Circuit for 100% Stable Secure Key Generation in 22nm CMOS," *ISSCC*, pp. 278–280, 2014.
[4] B. Karpinskyy, et al., "Physically Unclonable Function for Secure Key Generation with a Key Error Rate of 2E-38 in 45nm smart-card chips," *ISSCC*, pp. 158-159, 2016.
[5] M. Wu, et al., "A PUF Scheme Using Competing Oxide Rupture with Bit Error Rate Approaching Zero," *ISSCC*, pp. 130-131, 2018.
[6] M. Chang, et al., "An Offset-Tolerant Current-Sampling-Based Sense Amplifier for Sub-100nA-Cell-Current Nonvolatile Memory," *ISSCC*, pp. 206-207, 2011.

978-1-5386-8531-0/19/$31.00 ©2019 IEEE



Entropy Source	SRAM	INV	SA	Photodetectors	Anti- Fuse	RRAM (This work)
Reliability	Low	Low	Low	Medium	High	High
Uniqueness	Low	Medium	Medium	Medium	High	High
Bit cell area	Large	Large	Large	Medium	Small	Small
Power consumption	Small	Small	Small	Large	Large	Medium
ECC, Masking, TMV ?	YES	YES	YES	YES	NO	NO
Re-configurability ?	NO	NO	NO	NO	NO	YES

Figure 25.2.1: Key features and challenges of PUFs in practical applications, showing the advantage of reconfigurable PUF and a brief comparison table of previous works and our implementation.

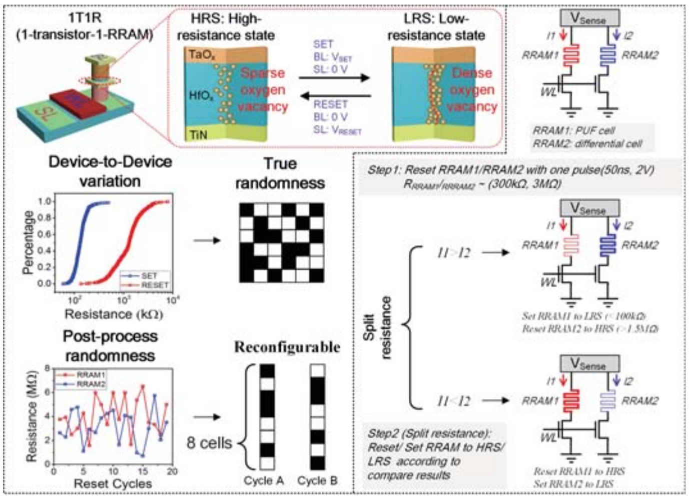


Figure 25.2.2: 1T1R RRAM structure with two typical states and two features of RRAM for PUF application; functional diagram of the split resistance technique to enhance the PUF's reliability.

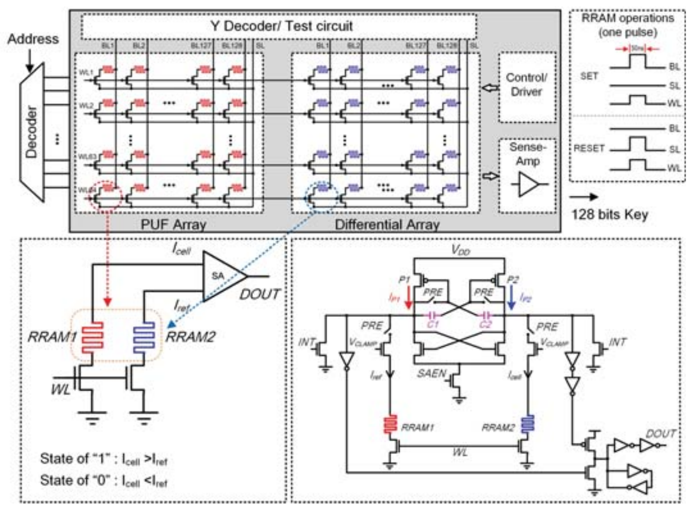
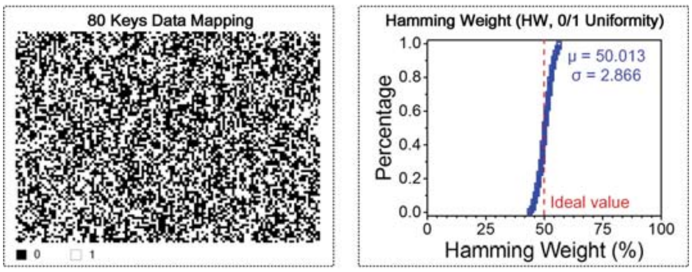


Figure 25.2.3: Architecture of RRAM PUF test chip with a PUF bitcell and a detailed schematic of differential sense amplifier. Each PUF key includes 128b.



NIST Test Results (Native data)

Test name	Stream length	No. of runs	Pass rate %	Avg. P-value	Pass?
Approximate entropy	1024	60	100	0.9973	YES
Block frequency	1024	60	100	0.9951	YES
FFT	1024	60	98.33	0.4983	YES
Frequency	1024	60	100	0.7338	YES
Longest runs	1024	60	98.33	0.5818	YES
Rank	1024	60	100	0.5059	YES
Runs	1024	60	100	0.5127	YES
Serial-1	1024	60	98.33	0.5102	YES
Serial-2	1024	60	100	0.5261	YES

Figure 25.2.4: Spatial data mapping of 80 keys from 20 PUF chips at typical conditions; bias of 1000 PUF keys from 20 test chips; summary table of NIST test results.

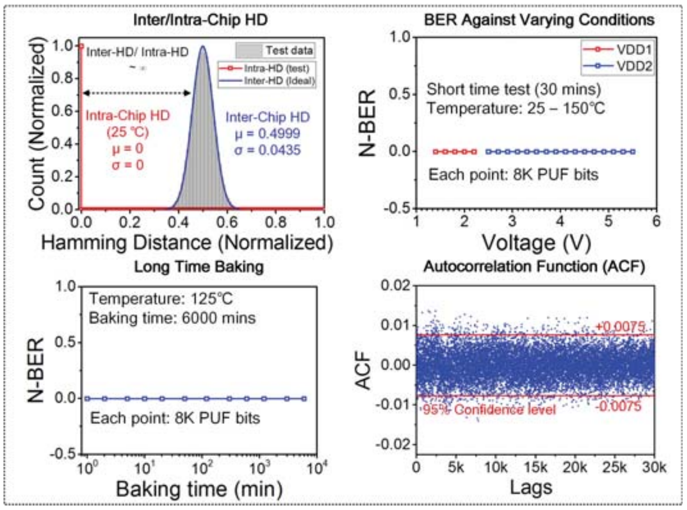


Figure 25.2.5: Measured inter- and intra- Hamming distance; N-BER vs. varying supplying voltage and temperature; N-BER under long-term baking; spatial autocorrelation function.

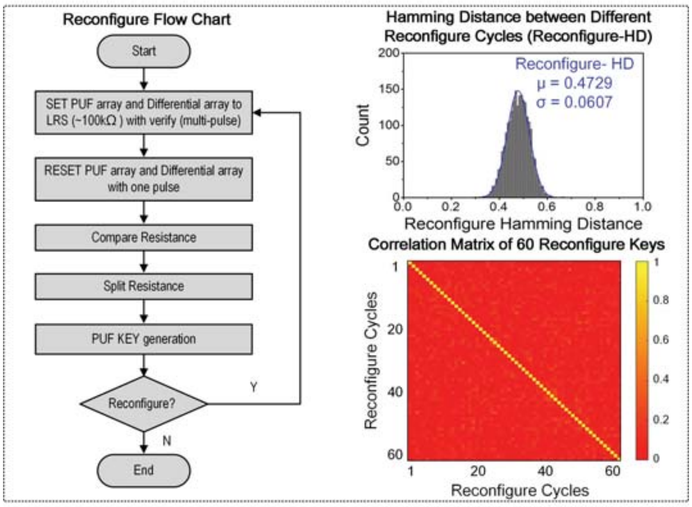
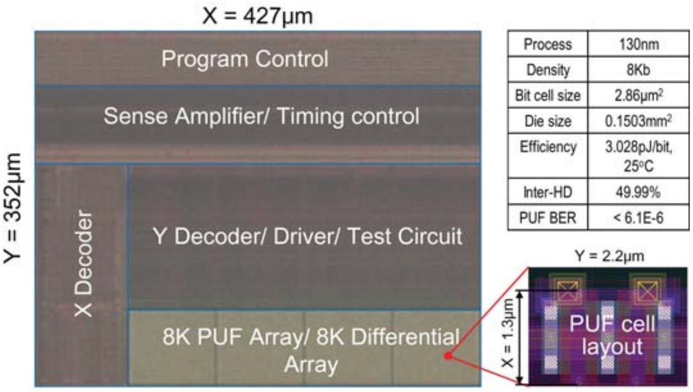


Figure 25.2.6: Flow chart of PUF key reconfiguration process; reconfigure-Hamming distance distribution between 60 reconfigured keys; correlation matrix of 60 reconfigured keys.


X = 427µm
Y = 352µm
Program Control
Sense Amplifier/ Timing control
X Decoder
Y Decoder/ Driver/ Test Circuit
8K PUF Array/ 8K Differential Array
Y = 2.2µm
X = 1.3µm
PUF cell layout

Process	130nm
Density	8Kb
Bit cell size	$2.86\mu m^2$
Die size	$0.1503mm^2$
Efficiency	3.028pJ/bit, 25°C
Inter-HD	49.99%
PUF BER	< 6.1E-6

Figure 25.2.7: Top view of chip micrograph with a measurement summary and two PUF-cell layout.