High performance bistable weak physical unclonable function for IoT security

Gang Li, Pengjun Wang^{a)}, and Huihong Zhang

*Faculty of Electrical Engineering and Computer Science, Ningbo University,
Ningbo, 315211, China*

a) wangpengjun@nbu.edu.cn

Abstract: This paper proposes a high performance physical unclonable function (PUF) implemented in a standard 65 nm CMOS process. The PUF cell is derived from SRAM-PUF cell, but it only use the NMOS or PMOS cross coupling structure with two additional access transistors. Random process variations between two cross coupling transistors are digitized to produce one bit output. Post-layout simulation results show that the 2k-bit PUF has high randomness and uniqueness, and it has some excellent features: (1) small PUF cell with a minimum feature size of 240F²; (2) high energy efficiency of 17.3 fJ/b at nominal 1.2 V; (3) excellent stability: only 2.6% bit-error-rate (BER) across a wide temperature range (−40–100 °C) and 10% V_{DD} variations.

Keywords: physical unclonable function (PUF), high performance, IoT security, circuit design

Classification: Integrated circuits

References

- [1] C. Herder, *et al.*: “Physical unclonable functions and applications: a tutorial,” *Proc. IEEE* **102** (2014) 1126 (DOI: [10.1109/JPROC.2014.2320516](https://doi.org/10.1109/JPROC.2014.2320516)).
- [2] S. K. Mathew, *et al.*: “A 0.19 pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22 nm CMOS,” *ISSCC Dig. Tech. Papers* (2014) 278 (DOI: [10.1109/ISSCC.2014.6757433](https://doi.org/10.1109/ISSCC.2014.6757433)).
- [3] B. Karpinsky, *et al.*: “Physically unclonable function for secure key generation with a key error rate of 2E-38 in 45 nm smart-card chips,” *ISSCC Dig. Tech. Papers* (2016) 158 (DOI: [10.1109/ISSCC.2016.7417955](https://doi.org/10.1109/ISSCC.2016.7417955)).
- [4] D. E. Holcomb, *et al.*: “Power-up SRAM state as an identifying fingerprint and source of true random numbers,” *IEEE Trans. Comput.* **58** (2009) 1198 (DOI: [10.1109/TC.2008.212](https://doi.org/10.1109/TC.2008.212)).
- [5] F. Tehranipoor, *et al.*: “DRAM-based intrinsic physically unclonable functions for system-level security and authentication,” *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **25** (2017) 1085 (DOI: [10.1109/TVLSI.2016.2606658](https://doi.org/10.1109/TVLSI.2016.2606658)).
- [6] A. Pan, *et al.*: “A comprehensive metering scheme for intellectual property protection during both after-scale and evaluation periods of IC design,” *IEICE Electron. Express* **10** (2013) 20130649 (DOI: [10.1587/elex.10.20130649](https://doi.org/10.1587/elex.10.20130649)).
- [7] U. Rührmair, *et al.*: “PUF modeling attacks on simulated and silicon data,” *IEEE Trans. Inf. Forensics Security* **8** (2013) 1876 (DOI: [10.1109/TIFS.2013](https://doi.org/10.1109/TIFS.2013)).

- 2279798).
- [8] D. P. Sahoo, *et al.*: “A case of lightweight PUF constructions: Cryptanalysis and machine learning attacks,” *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **34** (2015) 1334 (DOI: [10.1109/TCAD.2015.2448677](https://doi.org/10.1109/TCAD.2015.2448677)).
 - [9] Y. Su, *et al.*: “A digital 1.6 pJ/bit chip identification circuit using process variations,” *IEEE J. Solid-State Circuits* **43** (2008) 69 (DOI: [10.1109/JSSC.2007.910961](https://doi.org/10.1109/JSSC.2007.910961)).
 - [10] J. Li, *et al.*: “Ultra-compact and robust physically unclonable function based on voltage compensated proportional to absolute-temperature voltage generators,” *IEEE J. Solid-State Circuits* **51** (2016) 2192 (DOI: [10.1109/JSSC.2016.2586498](https://doi.org/10.1109/JSSC.2016.2586498)).
 - [11] S. Tao and E. Dubrova: “Ultra-energy-efficient temperature-stable physical unclonable function in 65 nm CMOS,” *Electron. Lett.* **52** (2016) 805 (DOI: [10.1049/el.2016.0292](https://doi.org/10.1049/el.2016.0292)).
 - [12] J. Lee, *et al.*: “A $445F^2$ leakage-based physically unclonable function with lossless stabilization through remapping for IoT security,” *ISSCC Dig. Tech. Papers* (2018) 132 (DOI: [10.1109/ISSCC.2018.8310219](https://doi.org/10.1109/ISSCC.2018.8310219)).

1 Introduction

Physical unclonable function (PUF) [1, 2, 3] is a promising hardware primitive for generating embedded secret that is easy to verify but extremely difficult to predict. PUF has drawn increasing attention, since it can preserve information security down to the chip level. By capturing manufacturing process variations of sensitive element, i.e. PUF cell, PUF can generate a large number of identifications (IDs). These IDs have features of randomness, uniqueness and unclonability, which render PUF to have potential applications, such as key generation [2, 3], device identification and authentication [4, 5] and IP protection [6].

PUF can be mainly classified into two main categories: weak PUF and strong PUF [1]. For weak PUF, one PUF cell usually produce one bit ID, and the PUF IDs can be considered as independent to each other. As for strong PUF, the IDs have certain correlations among each other, as a result of cell configuration. Thus, the weak PUF is more robust to model attacks [7] and machine-learning attacks [8] than strong PUF. Unfortunately, to generate exponential IDs, chip area of the weak PUF will be very considerable compared to the strong PUF. SRAM-PUF [4] is one of the most typical weak PUFs that uses the power-up states as the unique IDs. The SRAM-PUF cell [4] and the modified SRAM-PUF cell [9] are shown in Fig. 1. Their core structure is a pair of cross coupled inverters which are used to capture

Fig. 1. (a) SRAM-PUF cell; (b) SRAM-PUF cell with reset function

the random process variations. Although those weak PUFs have good randomness and uniqueness, they still have some limitations such as poor area or energy efficiency, as well as low cell-stability. Therefore, in this letter we dedicate to propose a high area and energy efficiency weak PUF with excellent reliability.

2 PUF implementation

Fig. 2 illustrates two PUF designs, namely, n-type PUF and p-type PUF. The n-type PUF is composed of n-cell array and a shared head, and the p-type PUF consist of p-cell array and a shared foot. Here, we only give an introduction to the n-type PUF, and the p-type PUF has the similar operating principle. In the n-type PUF (see Fig. 2(a)), excepting transistors, P2-P3 and N2-N3, the rest ones, P0-P1 and N0-N1 form a pair of across-coupled inverters. When PRE and WL_j are low (the precharge-stage), P2 and P3 are turned on, and N2 and N3 are turned off, then nodes Q and QB are pulled up to V_{DD} . When PRE and WL_j are high (the evaluation-stage), P2 and P3 are turned off, and N2 and N3 are turned on, then the metastable state ‘11’ of nodes Q/QB change over to a bistable state ‘01’ or ‘10’, which mainly depends on the process variations of n-cell and the shared head. As the head uses large transistor size and the n-cell adopts the minimum process size ($W/L = 120\text{ nm}/60\text{ nm}$), the mismatch between P0 and P1 compared to N0 and N1 can be neglected. Therefore, the PUF unique IDs are almost completely determined by the n-cell mismatch.

Fig. 2. (a) N-type PUF; (b) P-type PUF; (c) Monte-Carlo simulations of the N-type PUF; (d) Monte Carlo simulations of the P-type PUF

The PUF overall structure is shown in Fig. 3, it is composed of four modules including PUF cell array ($N \times M$), decoder (with word-line drivers), head arrays and

timing controller (TC). It is designed in a scheme of parallel M -port that enables to extract M -bit IDs in one clock cycle. The address sequence is defined as a challenge, and the M -bit IDs are considered as a response. Under the control of decoder, there are M cells enabled in the cell array in each clock cycle. The PUF IDs are captured by the RS-latch array. As the p-cell is directly connected to the supply, it is more sensitive to voltage variation than n-cell. Besides, the p-cell charging rate is slower than the n-cell discharging rate (see Fig. 2(c) and Fig. 2(d)). Thus, the n-cell has better performance than p-cell in term of stability and speed. Therefore, we choose n-cell to construct PUF, and the detailed PUF column and the cell layout are also shown in Fig. 3. The cell layout area is $0.75\ \mu\text{m} \times 1.35\ \mu\text{m}$ in 65 nm CMOS process which corresponding to a feature size of $240F^2$. The small PUF cell area is benefited from the fewer transistors (only 4 T) and the all NMOS structure.

Fig. 3. Proposed PUF block diagram, column structure and cell layout

The head transistor size (W_p/L_p) is directly related to the precharge-time (T_P) and the evaluation-time (T_E) as well as the randomness of IDs. Therefore, the head transistor size should be properly selected. The recommend W_p/L_p in this letter is not less than $2\ \mu\text{m}/60\ \text{nm}$ but not more than $16\ \mu\text{m}/60\ \text{nm}$. Through 500 Monte-Carlo simulations, the statistical results of T_P , T_E and the corresponding maximum operating frequency, $f_{\max}$, are shown in Table I. The bit-line (BL/BLB) parasitic

Table I. T_P , T_E and $f_{\max}$ with different W_p/L_p and load

Cell count	C_p (fF)	W_p/L_p											
		$2\ \mu\text{m}/60\ \text{nm}$			$4\ \mu\text{m}/60\ \text{nm}$			$8\ \mu\text{m}/60\ \text{nm}$			$16\ \mu\text{m}/60\ \text{nm}$		
		T_P (ns)	T_E (ns)	$f_{\max}$ (MHz)	T_P (ns)	T_E (ns)	$f_{\max}$ (MHz)	T_P (ns)	T_E (ns)	$f_{\max}$ (MHz)	T_P (ns)	T_E (ns)	$f_{\max}$ (MHz)
16	5	0.09	3.37	289.4	0.06	3.48	282.6	0.05	5.64	175.7	0.04	7.37	134.9
32	10	0.13	4.67	208.4	0.08	5.93	166.3	0.06	7.07	140.3	0.05	9.92	100.3
64	20	0.22	7.37	131.8	0.13	8.06	122.1	0.08	9.63	103.0	0.06	12.76	79.0
128	40	0.41	12.36	78.3	0.23	12.78	76.9	0.13	14.74	67.2	0.08	17.94	55.5
256	80	0.78	23.33	41.5	0.42	23.58	41.7	0.23	24.69	40.1	0.13	27.88	35.7

capacitance (C_p) is derived from post-layout parameter extraction, and the $f_{\max}$ is calculated as: $f_{\max} = 1/(T_P + T_E)$.

3 Simulation results

This section shows simulation results by using the extracted netlist with parasitic parameters. The proposed PUF is implemented in TSMC 65 nm CMOS process and simulated using Cadence/Spectre. As an embodiment, the 2k PUF-cells are arranged in a 16×128 array, and the head transistor size is $2 \mu\text{m}/60 \text{ nm}$. Monte Carlo simulations (100 times) with both local and global variations are performed to evaluate the performance. Since unclonability is an inherent characteristic of PUF, we therefore pay more attention to evaluate the randomness, uniqueness, reliability and energy efficiency.

Two-dimensional (2-D) map and the gray-scale map are commonly used to observe the randomness of weak PUF IDs [10]. Fig. 4(a) shows the 2-D map of the IDs derived from a randomly selected PUF instance. A black pixel is interpreted as a logic ‘1’ and a white one as a logic ‘0’. The probability of generating logic ‘1’ (49.7%) and logic ‘0’ (50.3%) is very close to the idea value (50%), indicating no obvious bias to logic ‘0’ or logic ‘1’. In addition, similar results are obtained from all the other PUF instances. Fig. 4(b) shows the gray-scale map (reshaped) of the IDs averaged across 100 PUF instances. The gray-values fluctuate around 0.5, and no apparent spatial correlation is observed, indicating a negligible systematic bias.

Fig. 4. (a) 2-D map of PUF IDs; (b) Spatial distribution of PUF IDs

Uniqueness is another important metric that refers to produce different IDs for the duplicated PUF instances. In general, PUF uniqueness is estimated by inter Hamming Distance (HD) of different PUF instances. For 100 PUF instances, there are totally 1279200 ($1600 \times 1599/2$) comparisons (each with 128-bit wide) that can be used to evaluate the inter-PUF HD. As shown in Fig. 5, the inter-PUF HD is 63.99 which corresponding to a uniqueness of 49.99%.

Fig. 5. Statistical distribution of inter-PUF HD

Reliability is the ability to produce the same PUF IDs under different operating conditions. We evaluate the reliability through calculating the bit-error-rate (BER) across a wide range of temperature and supply variations. To be more specific, the reference IDs are obtained from 100 PUF instances at the nominal operating condition (1.2 V, 25°C), and the comparison IDs are extracted from the same PUF instances at different working conditions. Fig. 6 shows the BER versus temperature and voltage. The average BER over the commercial range (0–85°C) and the industrial range (–40–100°C) with 10% V_{DD} changes from 1.2 V are 0.9% and 1.1%, respectively. And their corresponding worst-case BERs are 2.2% (@1.32 V, 85°C) and 2.6% (@1.32 V, 100°C), respectively.

Fig. 6. BER over the industrial and commercial temperature ranges

The energy efficiency is calculated as $E_{\text{bit}} = P_{\text{total}} / (w * f_{\text{clk}})$, where w denotes the bit-wide of a PUF response. Table II shows the total power dissipation (@50 MHz), P_{total} , and the corresponding energy efficiency, E_{bit} , averaged from 100 PUF instances. The proposed PUF delivers 6.4 Gb/s (@50 MHz, 1.2 V) while consuming 17.3 fJ/b for the PUF core, which includes PUF cell static power, bit-

Table II. P_{total} and E_{bit} of the PUF over $\pm 20\%$ supply variation

V_{DD} (V)	0.96	1.02	1.08	1.14	1.2	1.26	1.32	1.38	1.44
P_{total} (μW)	68.6	77.9	89.0	99.1	111.0	123.6	137.6	152.6	168.4
E_{bit} (fJ/b)	10.71	12.18	13.91	15.48	17.34	19.31	21.50	23.84	26.32

Table III. Performance and comparison with the state-of-art weak-PUFs

	Proposed	JSSC'16 [10]	EL'16 [11]	JSSC'08 [9]	ISSCC'18 [12]
Technology (nm)	65	65	65	130	180
Cell transistor num.	4	6	25	10	3/5
PUF cell area (F^2)	240	726.6	-	2991/6089	445/890
Number of IDs	2048	128	128	128	512
Temp. range (°C)	–40~100	0~80	–40~100	0~80	0~80
Voltage range (V)	1.08~1.32	0.6~1.2	0.8~1.8	0.9~1.2	1.2~1.8
Inter-PUF HD	49.99	50.01	50.04	50.54/50.12	49.2/50
BER (%)	2.6	6.54	3.2*	3.89/4.83	6.65/5.62
Bit rate (Mb/s)	6400	10.2	1	1	-
Energy/bit (pJ/b)	0.0173 @1.2 V	0.548 @1.2 V	0.0103 @0.6 V	0.93/1.6 @1 V	9.8/3.6 @1.8 V

*only temperature or voltage variation

line driver dynamic power and the peripheral circuits consumed power. The presented PUF performance summary and comparison with other related works are shown in Table III. From Table III, we get that the proposed PUF has excellent area and energy efficiency, and superior reliability.

4 Conclusions

This letter presents a bistable weak PUF with ultra-small PUF cell (i.e., $240F^2$) and high energy efficiency (i.e., 17.3 fJ/b). It can parallelly generate 128-bit IDs in one clock cycle with a throughput of 6.4 Gb/s. Post-layout simulation results show that the proposed PUF has best-in-class randomness and uniqueness. Moreover, strong resilience to environmental variations is achieved, with BER less than 2.6% under voltage varying within 1.08–1.32 V and temperature within -40 – 100 °C, without applying any stability-enhancement techniques. The proposed PUF has potential applications in the field of IoT security.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61474068) and the K.C. Wong Magna Fund in Ningbo University, China.