2021 IEEE Asian Solid-State Circuits Conference (A-SSCC) | 978-1-6654-4350-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/A-SSCC53895.2021.9634795

A 0.46pJ/bit Ultralow-Power Entropy-Preselection-Based Strong PUF with Worst-Case BER<6.7×10^{-6}

Jiahao Liu[1], Yan Zhu[1], Chi-Hang Chan[1], Rui Paulo Martins[1,2]

[1]University of Macau, Macao, China

[2]Universidade de Lisboa, Portugal

Internet of things (IoT) devices become ubiquitous, interconnected platforms for everyday tasks, which dictate a growing demand for low-cost security primitives. Physically Unclonable Functions (PUFs) are one of the promising solutions for low-cost key storage and device authentication, where strong PUFs [1-5] are suitable for authentication due to the exponentially large challenge-response pairs (CRPs) space. Early strong PUFs were vulnerable to machine learning (ML) attacks [3], [4], while [1], [2], [5] introduce various nonlinear entropy cells to enhance resilience. However, they all suffer from low energy efficiency because many trivial entropy cells need to be activated for sufficient nonlinearity. Besides, with many enabled cells, a small number of challenge bits flipping only imposes a very small probability for the change on the final response, resulting in a poor standard deviation on their Hamming Weight (HW).

Unlike conventional strong PUFs where their nonlinearity of CRPs space relies on the number of enabled entropy cells, the nonlinearity of the presented EP-based PUF derives from two parts: 1) the nonlinear challenges-controlled selection front-end and 2) subthreshold-biased latch-based sub PUFs back-end, which in combination show a high resilience to ML attacks. The selection front-end simultaneously serves as the power-down indicator for trivial sub PUFs, enabling an outstanding energy efficiency of 0.46pJ/bit. Further incorporation with the unstable CRPs filtering scheme, the bit error rate (BER) in the worst-case is suppressed to less than 6.7×10^{-6}. Besides, the presented structure with a randomness enhancement technique, allows the strong PUF to attain an excellent uniformity with a variance of the HW of 0.0051 which is 21.4-fold lower than [5].

The proposed strong PUF structure is shown in Fig. 1. The front-end selection network, realized based on an XOR tree, originates high nonlinearity when converting the challenge word (C_0-C_{63}) into sub-PUFs selection signals (S_0, S_1). They enable one out of four subthreshold-biased latch-based entropy sources (Source A-D) by the decoder. Each source is configured by a quarter of the challenge bits and gives a one-bit response (R_o) after the decoder selection, while the remaining three-quarter work as the 'fake feature vector' to dramatically increase the nonlinearity. Profiting from this selection scheme, only a few PUF cells need activation while still maintaining a high nonlinearity, eventually fulfilling both low power and high resilience of ML attacks. To further enhance the randomness, R_o is XORed with $S_0\oplus S_1$ to give the final response R_F.

The block diagram and circuit schematic of the entropy source is displayed in Fig. 2. Each source consists of four set minimum-sized subthreshold-biased inverter arrays (SIA). Four challenge bits select 1 inverter out of 16 in each SIA. A quarter of the total challenge bits (C_0-C_{15} for source A) configures the connection of the inverter array to form a latch for the response. When Reset=1, nodes V_p and V_n discharge to the Gnd to clean out their memory. When Reset = 0, depending on the random mismatches between the selected inverters, the formed latch regenerates a raw response. We utilize diode-connected transistors M_0, M_1 to bias the inverters into the subthreshold region for better nonlinearity regarding the threshold voltage. Two voltage-controlled current sources are used to introduce current difference between nodes V_p and V_n, helping to identify unstable CRPs. The CRPs filtering is accomplished based on detecting the commonness of the response in three different modes. A normal response R_N is obtained when the signal Cal = 0. Under Cal = 1 and the same challenges, two extra responses R_+ and R_- are attained with a reversed polarity on the bias ($V_+ - V_- = \Delta V_{bias}$; $V_- - V_+ = \Delta V_{bias}$). If three responses are equal, implying that the CRP owns a large mismatch, then the CRP is enrolled, otherwise discarded.

The EP-PUF, fabricated in 65nm CMOS, occupies a core area of 0.0122mm^2. The measured inter-die and intra-die Hamming Distance, which presents the uniqueness and reproducibility, are 0.4996 and 0.0091, respectively, with 54.9× separation (Fig. 3a). The HW of R_F is measured to be μ=0.5010 and σ=0.0051 (Fig. 3b). The σ is 21.4-fold lower than [5], thus providing excellent uniformity across dies. We combine the variations of the temperature and supply voltage to measure the BER, with golden CRPs collected at 25℃ and 1.2V supply voltage. The worst-case BER is 5.83% at -20℃ and 1.08V (Fig. 3c). The increase of the biasing force (ΔV_{bias}) suppresses the worst-case BER of measured 150K CRPs to less than 6.7×10^{-6}, proving outstanding stability (Fig. 3d).

We adopt the NIST SP800-22 suite to test the randomness of the raw response R_0 and enhanced R_F. The randomness-enhanced scheme imposes P-values of R_F dramatically larger than R_o (Fig. 4) Further, it improves the percentage of fabricated dies that pass the NIST Frequency Test from around 48% to 99% for 10K bitstream length. We utilize, three popular ML algorithms, including Support Vector Machine (SVM), Artificial Neuron Network (ANN), and Logistic Regression (LR), to attack the EP-PUF. The selection signals (S_0, S_1) are combined with challenges to be the feature vector (S_0, S_1, C_0, C_1, …, C_{63}), assuming the hacker somehow knows (S_0, S_1) from the selection network. After training 1M CRPs (for SVM maximum CRPs are 100K due to the unacceptable time complexity), the prediction accuracy is still near 50%, verifying the EP-PUF has high resilience to ML attacks (Fig. 4).

The entire 2^{64} CRP space of EP-PUF is constructed by the four entropy sources, each of which contains 2^{16} independent CRPs. To avoid these root CRPs (2^{18} in total) being read out directly (assumed somehow the hackers have access to the design database), a simple obfuscation-based protection mechanism can be adopted as illustrated in Fig.5 (a). In Phase 1, the initial challenges (C_0, C_1, …, C_{63}) are input to the EP-PUF, and responses (R_1, $\overline{R}_1$) are generated. Then in Phase 2, R_1 and $\overline{R}_1$ feedback to the original EP-PUF and bitwise XOR challenge bit C_0 and C_{32}, respectively, that ensures one of the entropy source selection bits S_0 and S_1 (Fig. 1) flips to increase obfuscation. Meanwhile, a new response R_2 is generated. Finally, in Phase 3, R_1 and R_2 feedback to the original EP-PUF and bitwise XOR C_{16}, C_{48} again to ensure that the initial selection bits in Phase 1 have equal probability to become any one of the cases, so as to maximize obfuscation. The final response R is based on XORing R_1, R_2, and R_3. Through this obfuscation scheme, even if the hackers can read the CRPs from the chip, they can only obtain the obfuscated CRPs but not those root ones.

Since the final response R is a function of the root CRPs, the remote server can reconstruct the whole CRPs space only by storing the 2^{18} root CRPs enrolled in the safe environment, which greatly reduces the storage overhead compared with conventional strong PUF. The stability-aware-based challenge selection scheme is illustrated in Fig. 5 (b). This obfuscation scheme only introduces a mild effect on the final bit error rate since a random challenge is only adopted if all computed sub-responses (R_1, R_2, R_3) in the server are stable. The worst-case BER' of final response R can be calculated as BER'=1-(1-BER)^3, which is only tripled because the smaller the BER, the smaller the effect of this scheme. For the proposed EP-PUF, after CRPs filtering, the BER is already suppressed to a low level, therefore this obfuscation scheme fits the EP-PUF very well.

The summary of measurement results of EP-PUF and comparison with state-of-the-art strong PUFs are presented in Fig. 6. The proposed EP-PUF has superior randomness and resilience to ML attacks. It obtains 0.46pJ/bit energy efficiency at 520K bit rate, which is 17×, 206×, 39×, 24× lower than [1-3], [5], respectively. With the obfuscated-based protection mechanism, the root CRPs of EP-PUF are well-protected at a low cost. The chip micrograph is exhibited in Fig. 7.

Acknowledgement:

This work funded by The Science and Technology Development Fund, Macao SAR (File no. 0004/2020/AKP&SKL-AMSV(UM)-2020-2022) and University of Macau Grant (MYRG2019-00049-AMSV)

References:

[1] Y. Cao, et al., "A Low Power Diode-Clamped Inverter-Based Strong Physical Unclonable Function for Robust and Lightweight Authentication," *IEEE TCAS I: Reg. Papers*, vol. 65, no. 11, pp. 3864-3873, Nov. 2018.

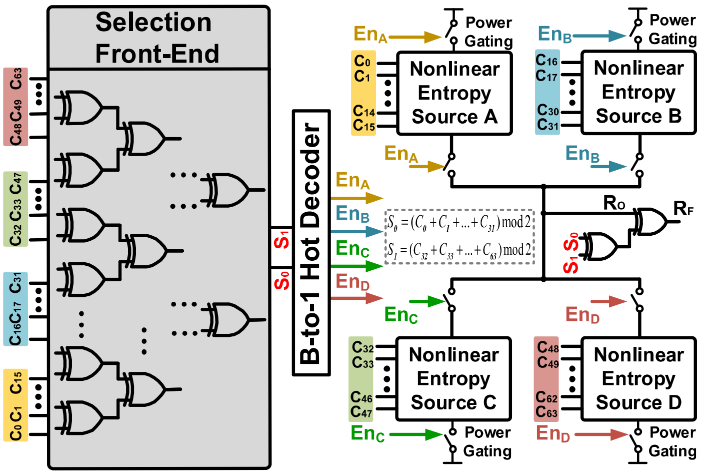
Selection Front-End
C48 C49 C63
C32 C33 C47
C16C17 C31
C0 C1 C15
B-to-1 Hot Decoder
S0
S1
EnA
EnB
EnC
EnD
Power Gating
C0 C1 C14 C15
Nonlinear Entropy Source A
C16 C17 C30 C31
Nonlinear Entropy Source B
C32 C33 C46 C47
Nonlinear Entropy Source C
C48 C49 C62 C63
Nonlinear Entropy Source D
$S_0 = (C_0 + C_1 + ... + C_{31}) \bmod 2$
$S_1 = (C_{32} + C_{33} + ... + C_{63}) \bmod 2$
S1 S0
RO
RF

Fig. 1. System diagram of the proposed EP-based strong PUF.

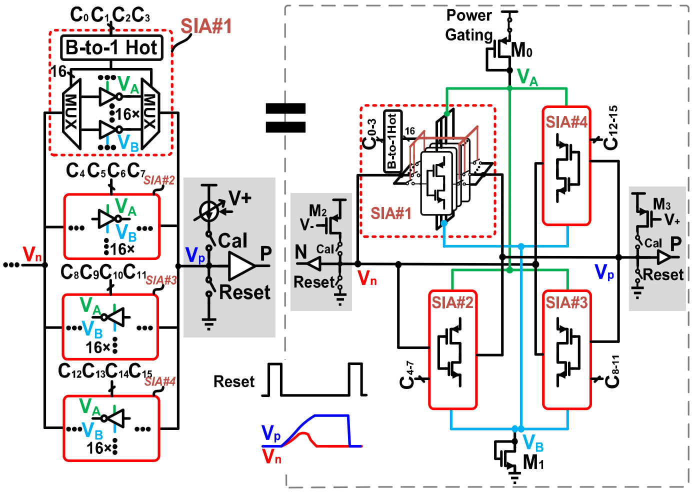

Fig. 2. Simplified block diagram and circuit schematic of the nonlinear entropy source.

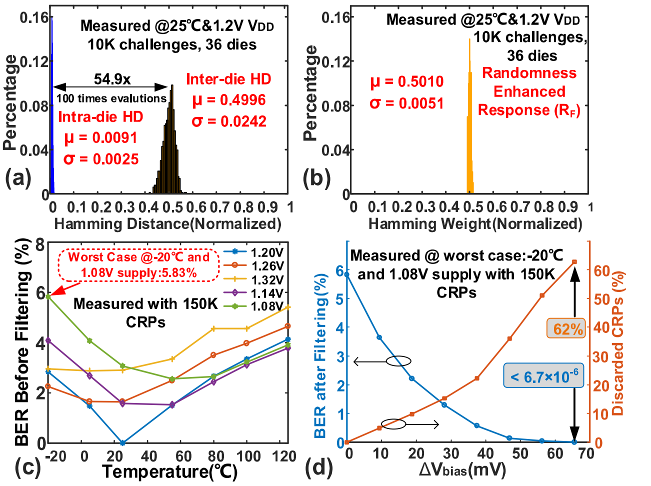

Fig. 3. (a) Measurement results of inter-die and intra-die Hamming Distance, (b) Hamming Weight of the response RF, (c) BER across variations of temperature and supply voltage and (d) BER after CRPs filtering.

NIST SP800-22 Test Suite Results

Test	P-value (R_o)	P-value (R_F)	Result
Frequency	0.213	0.739*	Pass
Block Frequency	0.439	0.819*	Pass
Cumulative Sum (forward)	0.035	0.739*	Pass
Cumulative Sum (reverse)	0.340	0.213	Pass
Runs	0.354	0.534*	Pass
Longest Runs	0.162	0.739*	Pass
Rank	0.069	0.069	Pass
FFT	0.018	0.122*	Pass
Overlap Template	0.312	0.434*	Pass
Approximate Entropy	0.350	0.740*	Pass
Serial(forward)	0.630	0.739*	Pass
Serial(reverse)	0.022	0.350*	Pass
Linear Complexity	0.122	0.067	Pass

* The P-value of randomness enhanced response R_F is larger than P-value of raw response Ro.

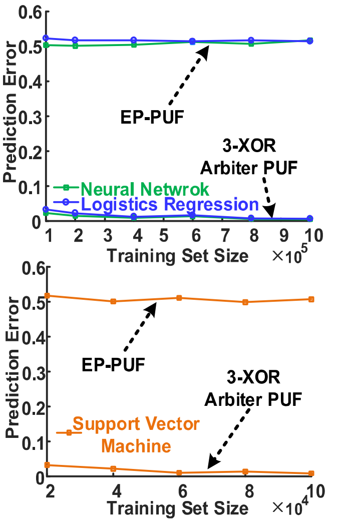

Fig. 4. NIST randomness test and machine learning attacks results.

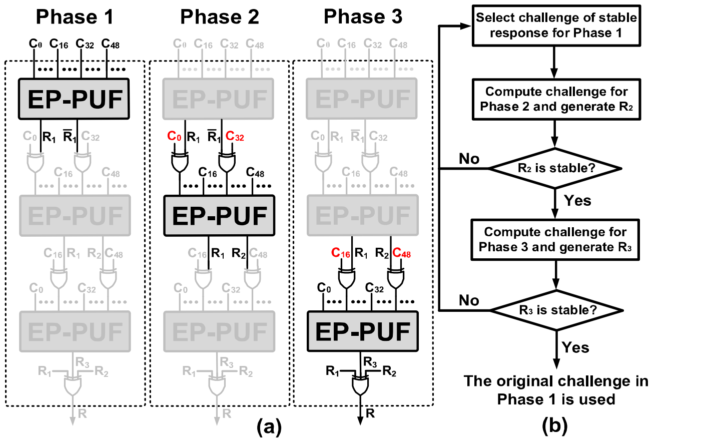
Phase 1
Phase 2
Phase 3
C0 C16 C32 C48
EP-PUF
R1
R2
R3
R
(a)
Select challenge of stable response for Phase 1
Compute challenge for Phase 2 and generate R2
R2 is stable?
No
Yes
Compute challenge for Phase 3 and generate R3
R3 is stable?
The original challenge in Phase 1 is used
(b)

Fig. 5. (a) System diagram of the proposed obfuscation-based protection mechanism for EP-PUF and (b) stability-aware-based challenge selection scheme.

	This Work	TCAS I'18 [1]	VLSI'20 [2]	ISSCC'15 [3]	VLSI'17 [5]	VLSI'17 [4]
Technology	65nm	40nm	14nm	40nm	130nm	28nm
Number of CRPs	$\sim 1.8\times10^{19}$	$\sim 1.8\times10^{19}$	$\sim 3.4\times10^{38}$	$\sim 5.5\times10^{28}$	$\sim 3.7\times10^{19}$	$\sim 1.17\times10^{11}$
Bit Rate	520 Kb/s	500 Kb/s	106.7 Mb/s	1.6 Mb/s	6 Kb/s	1.1 Gb/s
BER in Worst Case	5.83%	6.1%	14.5%	9%	9%	10.5%
Worst-Case BER after Filtering	$< 6.7\times10^{-6}$	0.82%	0.26%	$< 1\times10^{-8}$	0.4%	-
Power	240nW	3.85uW	10.1mW	28.4uW	68nW	-
Energy Efficiency(pJ/bit)	0.46	7.7	94.7	17.75	11	0.097
Uniqueness(μ / σ)	0.4996/0.0242	0.4989/0.0576	0.498/-	0.5007/0.0627	0.499/0.043	0.483/-
Uniformity(μ / σ)	0.5010/0.0051	-	0.5/-	-	0.528/0.109	-
VDD Range(V)	1.08~1.32	0.9~1.3	0.65~0.85	0.7~1.2	1.08~1.32	0.5~0.9
Temperature Range(℃)	-20~125	-40~90	0~100	-20~125	-20~80	0~80
ML Prediction Accuracy (Maximum Number of Training Samples)	50% (1M)	50% (10K)	50% (6M)	-	60% (10K)	89% (10K)
Enrollment CRPs (for 10^n CPRs)	2^{18}	10^n	2^{11}	10^n	10^n	10^n

Fig. 6. Measurement results and comparison with state-of-the-art strong PUFs.

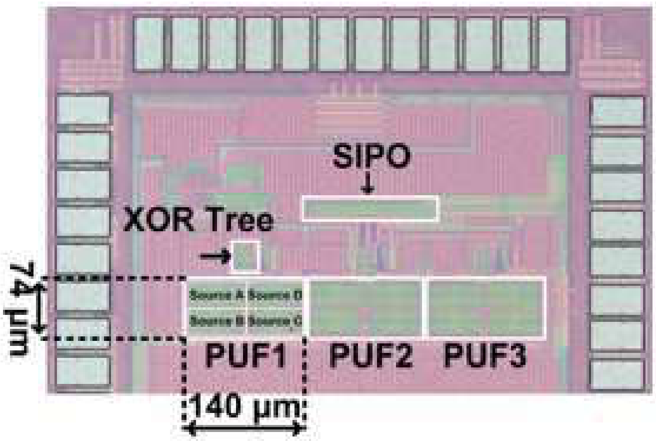

Fig. 7. Chip micrograpy of EP-PUF.

Additional References:

[2] V. Suresh, et al., "A 0.26% BER, 10^{28} Challenge-Response Machine-Learning Resistant Strong-PUF in 14nm CMOS Featuring Stability-Aware Adversarial Challenge Selection,'' *IEEE Symp. VLSI Circuits*, pp. 1-2, 2020.

[3] K. Yang, et al., "A Physically Unclonable Function with BER<10^{-8} for Robust Chip Authentication Using Oscillator Collapse in 40nm CMOS," *ISSCC,* pp. 254-255, 2015.

[4] S. Jeloka, et al., "A sequence dependent challenge-response PUF using 28nm SRAM 6T bit cell," *IEEE Symp. VLSI Circuits*, pp. C270-C271, 2017.

[5] X. Xi, et al., "Strong subthreshold current array PUF with 2^{65} challenge-response pairs resilient to machine learning attacks in 130nm CMOS," *IEEE Symp. VLSI Circuits*, pp. C268-C269, 2017.