A Lifetime-Robust PUF With Inherently Secure Supply Chain

Carl Riehm[1], Florin Burcea[1], Vartika Verma[1], Tobias Chlan[1], Szabolcs Molnar[1],
Matthias Hiller[2], Michael Pehl[1], Ralf Brederlow[1]
[1]*Technical University of Munich*, Munich, Germany
[2]*Fraunhofer AISEC*, Garching, Germany
Email: carl.riehm@tum.de

***Abstract*—This paper presents a fully CMOS-compatible Physical Unclonable Function (PUF) primitive robust against process, supply voltage, temperature (PVT) variations, electrical aging, and mechanical stress. It is based on resistive bit cells implementing compensation on circuit level. Random statistical variations are separated from systematic PVT variations in the analog design flow of this PUF to achieve high entropy and robustness over the entire temperature and supply range. Additionally, the piezoresistive effect of the resistive bit cells shifts trusted environment needs to final packaging. Since entropy arises from both device mismatch and mechanical stress induced by packaging, the final PUF response is determined only after soldering. This enables device authentication and prevents third-party readout during shipping between production steps.**

I. Introduction

Secure embedded devices require stable cryptographic keys under all operating conditions and the complete product lifecycle. Therefore, circuit drifts are particularly challenging in the design of Physical Unclonable Functions (PUFs). To keep the overhead of silicon area and digital post-processing low, the PUF bit cells have to be robust against process, voltage, and temperature (PVT) variations, noise, electrical aging, and mechanical stress. High native bit stability during operation, i.e., a very low number of bit flips, enables Error Correction Codes (ECCs) based solely on BCH codes, avoiding concatenation with repetition codes, which increases the number of required bit cells (and the silicon area) by multiples [1]. Temperature- and aging-related drifts have a significant impact on established PUF concepts, such as SRAM, arbiter, or ring-oscillator PUFs [2]. A digital design flow (independent of the PUF concept) summarizes the effect of PVT variations in worst-case corners. Flipping bits in the PUF, however, typically occur at random temperatures and supply voltages and require accounting for electrical aging over the IC lifetime [3]. Additionally, digital design does not distinguish between local, purely random statistical variations and systematic process gradients, both of which can cause bit flips. The entropy and the bias of the PUF response can be simulated with PDKs for analog circuits, providing statistical parameters and aging models. Additionally, they enable the simulation of physical noise. In particular, low-frequency 1/f-noise impairs the robustness of the PUF response and can only be experimentally distinguished in long-term measurements of static offset, making the reliable determination of unstable bits costly. Package-related mechanical stress, which is caused by different material properties of the mold compound, the lead frame, and the silicon die during packaging, significantly depends on humidity [4] and has been proven to impact the frequency of, e.g., oscillators [5], [6]. Mechanical stress can be included in analog circuit simulations as demonstrated in [7]. Furthermore, package stress, which is essentially a parasitic effect, splits the source of entropy of the proposed PUF across the manufacturing chain, which allows the use of a simple cryptography-based challenge-response protocol enabling chip authentication along the supply chain and preventing chip manipulation and replacement by counterfeits. Systematic process drifts, which can be predicted only statistically in simulations, result in a bias in the PUF response on silicon and have to be addressed either by calibration on circuit level or by adding additional bits and digital countermeasures. In summary, the proposed PUF considers the combination of PVT variations, electrical aging, physical noise, and package stress to provide high-quality randomness throughout the product lifetime.

This work is funded by the DFG project STAMPS and STAMPS-PLUS (BR 6306/1-1, HI 2230/1-1, and PE3242/2-2). We thank Anika Kwiatkowski for the microscope views.

II. Circuit Implementation and Trimming

The proposed PUF (Fig. 1) is based on a theoretical concept described in [8]. The entropy in the proposed PUF is obtained from p-diffusion resistors with minimal sizing to achieve high mismatch. They have low 1/f noise, which is crucial for achieving long-term stability [9]. Furthermore, they are highly sensitive to in-plane mechanical stress, which increases the PUF entropy, and are only slightly impacted by out-of-plane stress (Fig. 2), which makes them robust against humidity drifts [4]. Their high doping prevents cross-coupling between mechanical stress sensitivity and temperature [10]. The system consists of a PUF array of 256 resistors. To cancel out systematic temperature drifts, a reference resistor R_{ref} is included (one for the entire array): R_{ref} (almost stress-independent) adjusts the temperature drift of the current, which is mirrored into the PUF array. The OTA (folded cascode) regulates variations in the supply voltage, stress-, and aging effects in the feedback loop. The Differential Difference Amplifier (DDA) amplifies the difference of V_{sense} (selected bit cell) and V_{ref} (reference

voltage). V_{BG} and V_{ref} are derived from an internal bandgap reference designed for minimal stress drift as in [7]. Since R_{ref} and the bit cell resistors are different resistor types with different piezoresistive sensitivity, the voltage difference $V_{sense} - V_{ref}$ is stable over temperature, supply variations, and insensitive to aging. V_{sense} intentionally changes with mechanical stress (Fig. 3) as discussed later. Although a comparator is sufficient to derive one bit from the sign of $V_{sense} - V_{ref}$, a dual-slope-ADC is implemented to fully understand the entropy, and, e.g., to gain more bits per resistor. During calibration (Fig. 4), the DDA offset is removed by trimming its input differential pair. R_{ref} is selected from the best of 32 instances with different temperature coefficients (TCs) implemented as varying portion of different resistor types. Systematic manufacturing variations determine the TC of the resistor combination. Thus, R_{ref} can be selected from characterization values, but is always the same on one wafer. The average of the bit cells is trimmed per chip after PCB assembly to prevent a PUF bias. All trim values provide information on the average of the PUF array only. Hence, they do not leak the distribution of the bit cells.

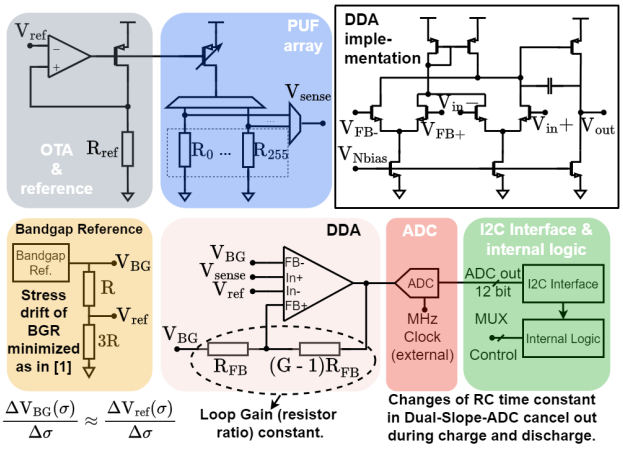

Fig. 1. System-level schematic view of proposed PUF and transistor-level implementation of selected analog blocks. The colors correspond to those in the chip view. The stress drifts of the readout circuit blocks are minimized on circuit level.

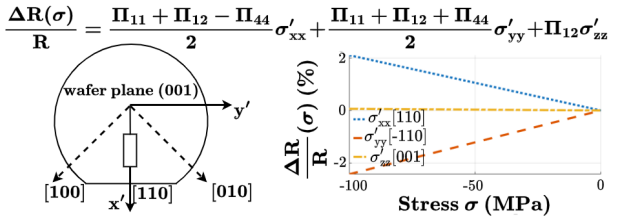

Fig. 2. Sensitivity of bit cell resistors (layout orientation in [110] direction) to in-plane stresses σ'_{xx} and σ'_{yy}, and low sensitivity to out-of-plane stress σ'_{zz}. The experimental characterization is described in [4].

III. PUF DURING MANUFACTURING

While PVT variations remain constant after the wafer is manufactured, mechanical stress caused by packaging, soldering, and humidity absorption changes over the lifetime

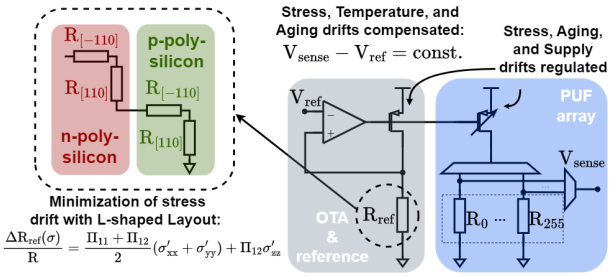

Fig. 3. Compensation of PVT variations, electrical aging, and mechanical stress drifts of the PUF array. Drifts of V_{ref} are suppressed, stress effects on R_{ref} minimized with L-shaped layout.

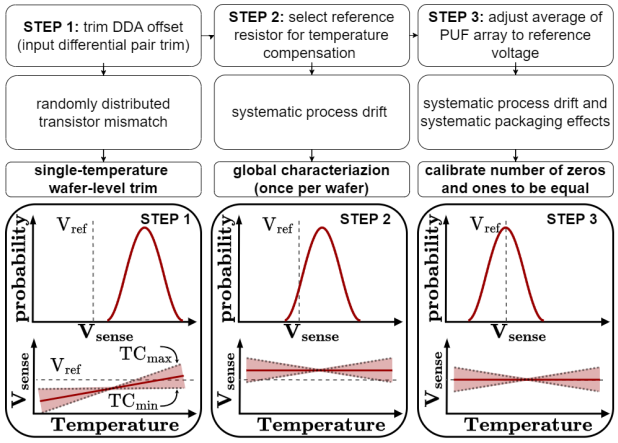

Fig. 4. Concept of single-temperature calibration of the amplifier offset, the TC of the reference resistor, and the average of the PUF array: The individual steps illustrate the compensation of the temperature drift and mean value bias of the PUF array.

of the IC. Measurements in [4] show package-to-package variations in average in-plane normal stresses σ'_{xx} and σ'_{yy}, superimposed by statistical effects from the granularity of the mold compound. Fig. 5 summarizes the effects on the statistical distribution of the PUF array: The mean value is shifted and the standard deviation increased. Measurements with a 3D-Laserscanning microscope (Fig. 6) indicate a grain size of 10 μm, which is nearly equal to the edge length of a PUF bit cell and explains the increased entropy after packaging and soldering. The large piezoresistive coefficient Π_{44} of the p-diffusion resistors (Fig. 2) causes high sensitivity to random variations in in-plane stress and hence increases the simulated bit cell mismatch $\sigma_{sim} \approx 9$ mV to $\sigma_{meas} \approx 27$ mV in measurements after packaging. Changes of mechanical stress during the manufacturing chain can be exploited for chip authentication (Fig. 7): The IC manufacturer creates helper data W_M and sends challenge C_M and response R_M via secure channel to the packager. After shipping of the ICs, which is considered as potentially insecure, the packager checks at the beginning if the chip is authentic ($R_M = R'_M$). After IC packaging, the PUF response changes due to additional mechanical stress, and the previous steps can be repeated

between packaging and PCB assembly. An attacker who gains access to the chip during the different production steps cannot read the key because either the package is still missing or the clamps of the IC test socket, ensuring electrical connection, add additional stress, which overwrites the entire key (Fig. 8).

IV. Experimental Results

The proposed circuit has been manufactured in a 180 nm CMOS process (Fig. 9) and packaged in plastic QFN packages.

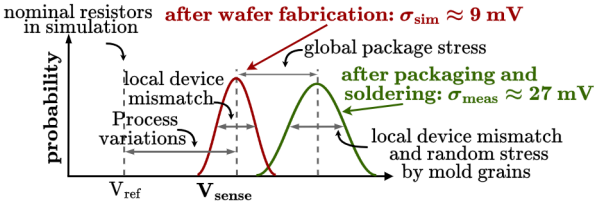

Fig. 5. Overview on systematic deviation versus local randomness in the resistors of the PUF array.

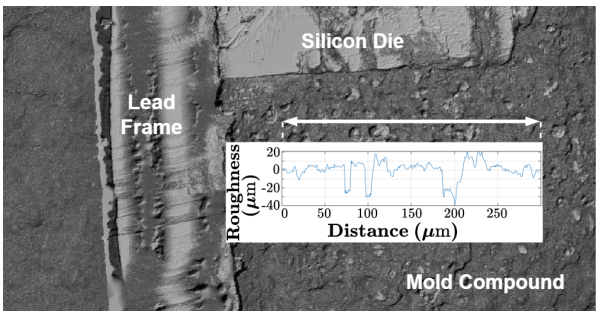

Fig. 6. 3D-Laserscanning microscope view of the cross-section of the package with leadframe, silicon die, and plastic mold compound. The surface roughness profile indicates a grain size in the range of 10 μm, which is close to the dimensions of the piezoresistive bit cells and adds additional package-related entropy to the PUF response.

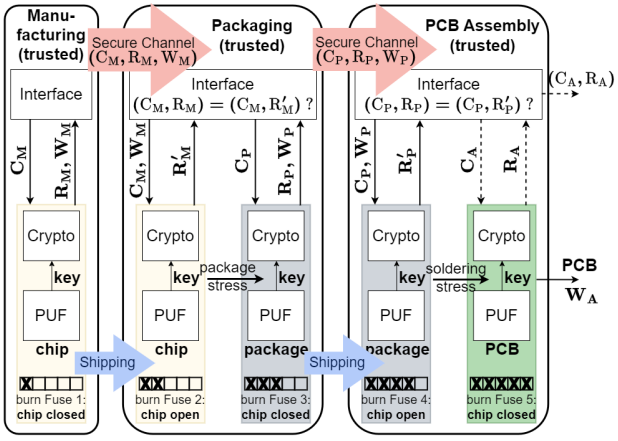

Fig. 7. IC Manufacturer creates helper data W_M and sends challenge C_M and response R_M via secure channel. After shipping (potentially insecure) the packager checks if $R_M = R'_M$ (chip authentic). Fuses open or close access to the cryptographic implementation during the production steps. (C_A, R_A) are optional for future authentication.

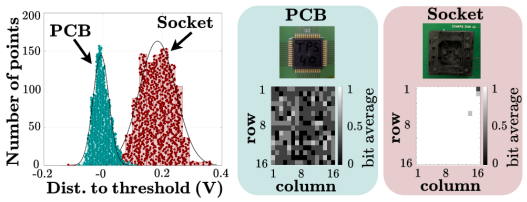

Fig. 8. Comparison of the statistical distribution of 1024 bits from 4 chips read with IC test socket and after soldering on a PCB (with identical calibration values), and the average spatial distribution of the bit cell values.

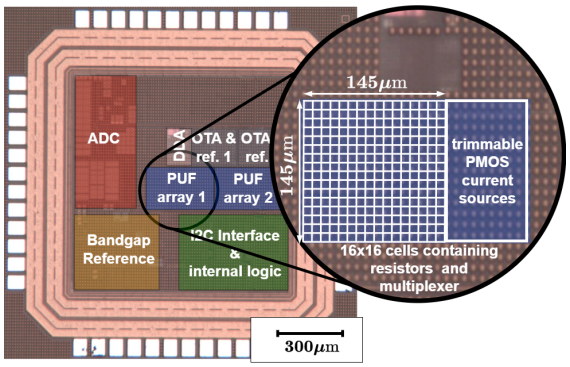

Fig. 9. Chip view of the PUF with circuit components highlighted. Zoom in: PUF array with 256 resistor cells and adjustable PMOS current source. The colors correspond to those in the system-level schematic view.

NIST randomness tests and autocorrelation (Fig. 10) indicate high randomness. Fig. 11 shows the measured statistical distribution with mean and standard deviation remaining stable over temperature. The bit error rate (BER) is determined by 1/f-noise, requiring extensive long-term measurements to detect almost stable bits flipping very rarely. Therefore, all bits within ± 300 μV (6σ-value of the measured noise) to the threshold are potentially unstable, leading to 0.9% native unstable bit cells. The remaining bits show high stability over humidity, temperature, and supply voltage. The bit errors over temperature and supply voltage in Tab. I are too small to be compared with statistical significance for such a low number of measured bits and depend on the individual IC samples. Aging simulations (long-term reliability cannot be measured within a reasonable timeframe) indicate negligible effects lower than the noise floor in measurements. Since PUFs are typically only read out rarely, power consumption and key

Test name	No. of runs	Pass %	Average p-value	Pass ?
Frequency	16	100	0.12232	YES
Block Freq.	16	100	0.21330	YES
Runs	16	100	0.21330	YES
Longest run	16	100	0.08879	YES
Cumulative sum	16	100	0.03517	YES
Cumulative sum 2	16	100	0.35048	YES

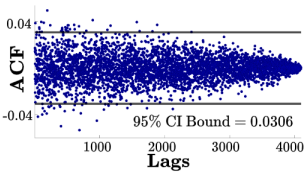

Fig. 10. NIST SP 800-22 Randomness Test Results and Auto Correlation (from 16 PUF arrays on 8 chips after soldering).

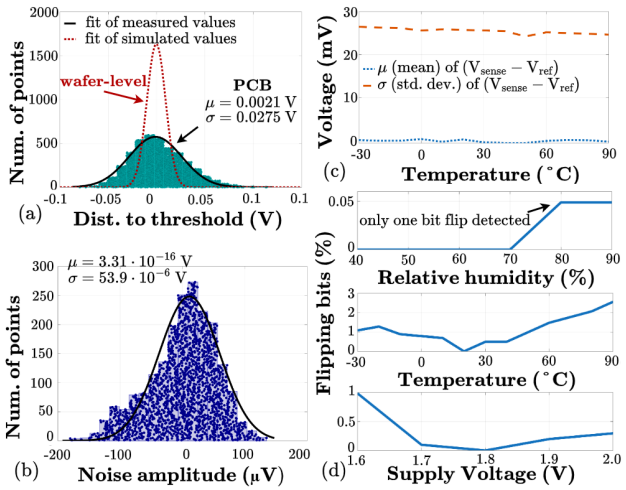

Fig. 11. (a) Statistical distribution of 4096 resistor cells (16 PUF arrays on 8 chips) after calibration with and without random package stress, (b) measured noise distribution of a single bit cell (2000 readings), (c) mean μ and standard deviation σ of distance to threshold ($V_{sense} - V_{ref}$) over temperature, and (d) number of bit flips over temperature, supply voltage and humidity. Humidity effects are measured at T = 90 °C after 30 min. at the respective humidity.

TABLE I
COMPARISON WITH STATE-OF-THE-ART PUF CIRCUITS.

	This work	**TCAS 2021 [11]**	**JSSC 2016 [12]**	**JSSC 2022 [13]**	**TCAS 2023 [14]**
Process (nm)	180	65	65	180	40
PUF type	Res.	Res.	PTAT	Volt.	RO
Stabilization	Trim	None	TMV	None[1]	Config.
Pre-Selection	None	None	Mask	None	Mask
Native Unst. bits (# of eval.)	0.93%[2] (≡5e8)	-	-	-	-
	0.39% (≡15k)	1.42% (5000)	6.54% (-)	0.61% (500)	11% (10k)
BER[3] (# of eval.)	0.14% (2000)	0.11% (5000)	-	0.13% (500)	1.3% (10k)
Bit Err. / 10 °C	0.32%	0.52%	0.44%	0.16%[4]	-
Bit Err. / 0.1 V	0.27%	0.54%	0.13%	0.06%	-
Bit Err. / 10% rel. humidity	0.01%	–	–	–	–
Temperature range (°C)	-30 – +90	0 – +85	0 – +80	10 – +80	-40 – +125
Supply Voltage (V)	1.6 - 2.0	0.9 - 1.4	0.8 - 1.0	0.4 - 1.8	0.9 - 1.4
Area / bit (F^2)	2500	1187	726	7200	-
# of meas. bits	4096	17280	5120	1792	2048
# of chips	8	6	10	7[5]	16
Electr. Aging Compensation	YES	-	-	-	-
Mechan. Stress Compensation	YES	-	-	-	-
Inherent Supply Chain Security	YES	-	-	-	-

[1]Shift of PMOS to NMOS threshold voltage shifts the inv. threshold.
[2]all bits in the range of 6σ-noise to the comparator threshold.
[3]given as numErrors * 100 / (numEvaluations * numBits).
[4]Temperature drift typically correlates with inverter offset.
[5]from the same manufacturing lot (process variations unclear).

read-out time are of little practical relevance. The low PUF bias and the high standard deviation, providing high entropy, prevent information leakage via the helper data [1].

V. CONCLUSION

In contrast to prior work, the proposed PUF includes the compensation of aging and mechanical stress. This PUF concept uses an industrial-grade analog design flow to predict statistical errors over product lifetime with high confidence for a larger number of devices. It demonstrates similar error rates at a lower number of native unstable bits as well as simplified logistics during manufacturing compared to state-of-the-art PUFs.

REFERENCES

[1] C. Frisch, F. Wilde, T. Holzner and M. Pehl, "A Practical Approach to Estimate the Min-Entropy in PUFs", Journal of Hardware and Systems Security, vol. 7, pp. 138-146, 2023.

[2] R. Maes, *et al.*, "Experimental evaluation of Physically Unclonable Functions in 65 nm CMOS," 2012 Proceedings of the ESSCIRC (ESSCIRC), Bordeaux, France, 2012, pp. 486-489.

[3] R. Maes and V. van der Leest, "Countering the effects of silicon aging on SRAM PUFs," 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Arlington, USA, 2014.

[4] C. Riehm, T. Chlan, S. Molnar, V. Verma and R. Brederlow, "Measurement of Thermal, Humidity, Solder, and Aging Effects of Mechanical Stress and Silicon Circuit Electrical Performance in Quad Flat Packages," 2025 IEEE 75th Electronic Components and Technology Conference (ECTC), Dallas, TX, USA, 2025, pp. 2325-2330.

[5] X. An, S. Pan, H. Jiang and K. A. A. Makinwa, "A 0.01 mm^2 10MHz RC Frequency Reference with a 1-Point On-Chip-Trimmed Inaccuracy of ±0.28% from 45°C to 125°C in 0.18m CMOS," 2023 IEEE International Solid-State Circuits Conference (ISSCC), USA, 2023, pp. 60-62.

[6] S. Parvin, *et al.*, "Special Session: Hardware Security at the Circuit and Layout Levels," 2026 IEEE European Test Symposium (ETS), Chania, Greece, 2026, in press.

[7] C. Riehm, T. Chlan, V. Verma, P. Xu and R. Brederlow, "Including Package-Induced Mechanical Stress in Bandgap Reference Circuit Design," 2025 IEEE European Solid-State Electronics Research Conference (ESSERC), Munich, Germany, 2025, pp. 189-192.

[8] C. Riehm, *et al.*, "Structured Design and Evaluation of a Resistor-Based PUF Robust Against PVT-Variations," 2023 26th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS), Tallinn, Estonia, 2023, pp. 93-98.

[9] R. Brederlow, *et al.*, "Low Frequency Noise Considerations for CMOS Analog Circuit Design", International Conference on Noise and Fluctuations (ICNF), Salamanca, Spain, 2005, pp. 703-708.

[10] Y. Kanda, "A graphical representation of the piezoresistance coefficients in silicon," in IEEE Transactions on Electron Devices, vol. 29, no. 1, pp. 64-70, Jan. 1982.

[11] B. Park, D. Forte, M. M. Tehranipoor and N. Maghari, "A Metal-Via Resistance Based Physically Unclonable Function With Backend Incremental ADC," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 68, no. 11, pp. 4700-4709, Nov. 2021.

[12] J. Li and M. Seok, "Ultra-Compact and Robust Physically Unclonable Function Based on Voltage-Compensated Proportional-to-Absolute-Temperature Voltage Generators," in IEEE Journal of Solid-State Circuits, vol. 51, no. 9, pp. 2192-2202, Sept. 2016.

[13] M. Vatalaro, R. De Rose, M. Lanuzza and F. Crupi, "Static CMOS Physically Unclonable Function Based on 4T Voltage Divider With 0.6%–1.5% Bit Instability at 0.4–1.8 V Operation in 180 nm," in IEEE Journal of Solid-State Circuits, vol. 57, no. 8, pp. 2509-2520, Aug. 2022.

[14] J. Park and J. -Y. Sim, "A Reconfigurable LDO-Assisted Physically Unclonable Function Achieving a Zero-BER With 14% Masking," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 70, no. 8, pp. 3244-3253, Aug. 2023.