

Synthesizable PUF Design with Library Characterization for Secure Storage in Edge Devices

Yuseong Lee¹, Donghyun Park², Jang Hyun Kim^{1,3}, Jongmin Lee^{1,3}

¹Dept. of Intelligence Semiconductor Engineering, Ajou University, Suwon, Republic of Korea

²Dept. of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea

³Dept. of Electrical and Computer Engineering, Ajou University, Suwon, Republic of Korea

{janghyun, jongmin}@ajou.ac.kr

Abstract—This work presents a synthesizable physically unclonable function (PUF) with library characterization that enables stable and secure key generation (KG) for edge-device storage. By combining sample-and-hold inverter-chain with digital tilting, masking, and optional temporal majority voting (TMV), the proposed design achieves low bit flip rate (BFR) under environmental variations and integrates with advanced encryption standard (AES) with only 5.72% area overhead. The results verify robust stability, uniqueness, and randomness, demonstrating its practicality for hardware-based secure storage.

I. INTRODUCTION

As the proliferation of the Internet of Things (IoT) and Artificial Intelligence (AI) increases the demand for personalized functionalities on edge devices, generating reliable secret keys for securely storing sensitive user data has become essential. As shown in Fig. 1(a), conventional approaches generate keys through a random number generator (RNG) and store them in non-volatile memory (NVM), but this creates security vulnerabilities because the stored keys may be extracted through physical attacks [1]-[3]. To address this issue, PUF technology, which exploits inherent semiconductor process variations to produce unique responses, has gained significant attention [4]. In particular, weak PUFs—whose responses disappear when power is off—are well suited for key generation [5]-[26].

However, existing PUF architectures face two major limitations. Array-based PUFs suffer from peripheral circuit overhead and bit-error problems [5]-[21], while synthesizable PUFs, despite their ability to integrate seamlessly with digital blocks as illustrated in Fig. 1(b), exhibit degraded randomness or insufficient stability due to distortions introduced during automatic place-and-route [25], [26]. Some approaches also require additional fabrication steps, such as ReRAM, which increases manufacturing cost [22], [23].

To overcome these limitations, this work proposes a new PUF architecture that is fully synthesizable using a standard-cell library and achieves stable responses through digital tilting and masking. This approach leverages device-level variations without relying on peripheral circuits, enabling secure KG while maintaining CMOS compatibility and high integration efficiency.

II. PROPOSED SYNTHESIZABLE PUF CELL DESIGN

A. Inverter Chain PUF Cell with Sample-and-hold operation

Previous studies have proposed architectures that utilize the switching-threshold mismatch between the first and second

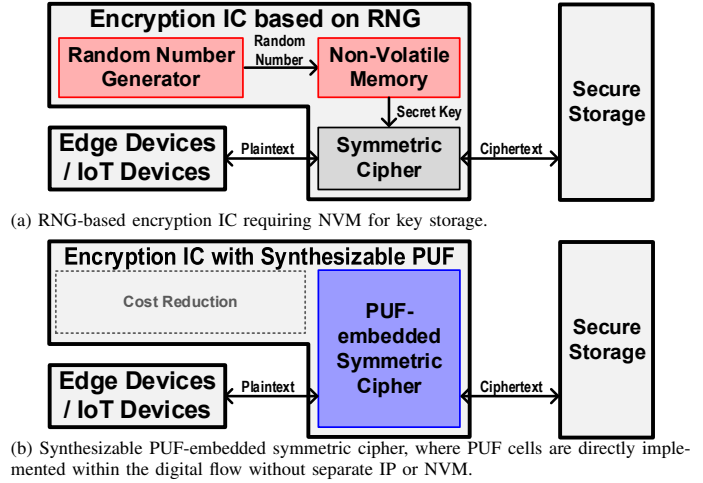


Fig. 1. Conventional data encryption IC architectures for secure storage.

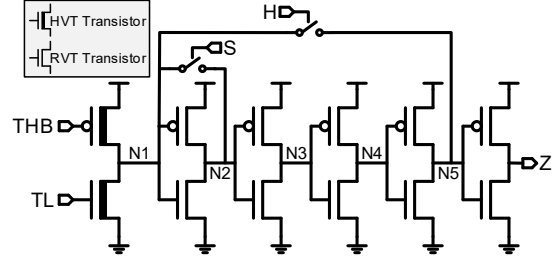


Fig. 2. Proposed synthesizable PUF cell.

inverter stages as an entropy source [6], [12]. Early approaches, including a 2-transistor amplification structure [6] and series-connected inverter designs [12], amplified this mismatch to generate PUF responses, but still exhibited limitations such as the absence of stabilization techniques. Building upon these works, this paper proposes an enhanced cell structure with sample and hold mode shown in Fig. 2.

B. Digital Tilting for Unstable Cell Identification and Masking

For PUF-based keys to be practically used for secure storage, the generated responses must remain stable even under environmental variations such as supply-voltage and temperature fluctuations. In addition, for a synthesizable PUF to be smoothly integrated into EDA-tool-based digital circuit design, all input and output signals must operate in the digital domain. However, conventional analog-driven tilting techniques [26] have a limitation in that they are vulnerable to coupling noise when signals are delivered deep inside digital circuits.

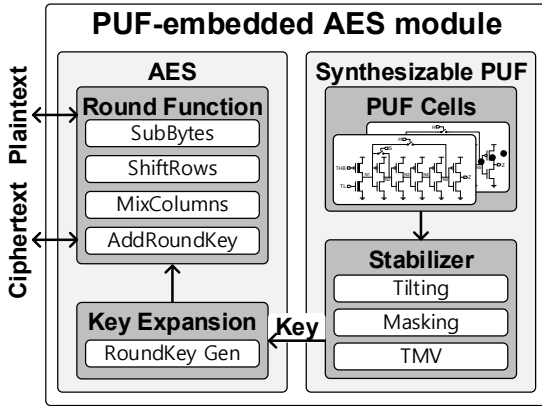


Fig. 3. Top-level architecture of synthesizable PUF-embedded AES module.

To address this issue, the proposed structure introduces THB (tilt-high bar) and TL (tilt-low) transistors controlled by digital signals, as shown in Fig. 2, to intentionally shift the switching threshold of the first-stage inverter upward or downward. Cells that exhibit different responses under the two tilting conditions are regarded as unstable and are classified as targets for masking.

C. Library Characterization and Standard Cell Implementation

To enable EDA-based automatic design, the proposed PUF cell undergoes a standard library characterization process. The transistor-level schematic is processed through Synopsys PrimeLib to generate library files that cover various corner conditions, and CEL and FRAM files for backend design are created using Synopsys Milkyway based on the 65-nm CMOS layout of the PUF cell (1.8 μm height, 9-track cell). Through this characterization flow, the PUF cell is defined as a standard-cell element, allowing multiple instances to be used within structural HDL and supporting seamless integration with RTL-based modules in a fully automated EDA design flow.

III. INTEGRATION WITH AES FOR SECURE STORAGE

To validate its applicability to secure storage, the synthesizable PUF-based cryptographic module shown in Fig. 1(b) was implemented as illustrated in Fig. 3, consisting of an AES block and a PUF block. The AES block, based on an open-source design [27], performs encryption, decryption, and round-key generation, while the PUF block generates the secret keys required for AES key expansion. Since even a single unstable bit in the PUF response can lead to critical errors in cryptographic operations, a stabilizer block is incorporated.

The stabilizer block consists of three functions: (i) identifying unstable cells through tilting, (ii) masking the outputs of those unstable cells, and (iii) optionally applying TMV to enhance noise immunity.

During evaluation, unstable cells are detected by comparing the responses under tilt-high and tilt-low conditions, and the corresponding masking information is stored without exposing any raw responses. The secret key is then constructed only from the stable cell outputs, while TMV can be selectively enabled to improve reliability at the cost of additional latency.

Finally, the stabilized PUF responses are collected to match the AES key length and used as the secret key, enabling the

TABLE I
SUMMARY OF AES IMPLEMENTATION RESULTS WITH AND WITHOUT SYNTHESIZABLE PUF INTEGRATION

		Gate Count	Area
AES-128	Without PUF	98,985	0.328mm ²
	With PUF Integration	101,972	0.343mm ²
	Overhead	+3.02%	+4.63%
AES-192	Without PUF	115,033	0.389mm ²
	With PUF Integration	117,387	0.409mm ²
	Overhead	+2.05%	+5.30%
AES-256	Without PUF	142,215	0.493mm ²
	With PUF Integration	146,151	0.521mm ²
	Overhead	+2.77%	+5.72%

The overall core utilization was 70%.

proposed PUF-embedded AES module to support reliable KG and secure encryption for storage applications.

IV. EXPERIMENTAL RESULTS

The proposed synthesizable PUF cell exhibits a stability–cost tradeoff depending on the tilting-transistor length, and simulation results indicate that a 60-nm length provides the most balanced performance. At this length, the discarded-cell ratio remains below 30%, and the BFR is stabilized to several tens of ppm under voltage and temperature variations. Based on this configuration, the integrated AES architecture—incorporating tilting-based cell identification, masking, and optional TMV—successfully generates stable keys across all environmental conditions and noise levels, achieving a bit error rate (BER) of zero.

The generated PUF keys also satisfy inter-key Hamming-distance and NIST SP800-22 test [28] randomness requirements. When integrated into AES-128/192/256, the maximum area overhead is only 5.72% (Table I). This demonstrates that, compared to prior synthesizable PUF designs, the proposed approach achieves both design efficiency and security, enabling direct AES KG from stabilized PUF outputs while maintaining a smaller area footprint. Consequently, the proposed PUF cell provides the stability, uniqueness, and randomness required for secure-storage applications, while preserving CMOS compatibility and supporting full EDA-based automated design.

V. CONCLUSION

The proposed synthesizable PUF is integrated into a single digital block without a peripheral reading circuit through library characterization, and it directly generates a stable secret key for AES with low BFR and high uniqueness through tilting, masking, and TMV-based stabilization. In addition, the area efficiency was increased by using only the small cell structure and the required cells, and the AES-128/192/256 integration proved reliability and practicality suitable for safe storage with only 5.72% overhead.

ACKNOWLEDGMENT

This research was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government (MSIT) (RS-2023-00249784, RS-2024-00408040), BK21 FOUR (Department of Intelligence Semiconductor Engineering, Ajou University) and Ajou University research fund. The EDA tool was supported by the IC Design Education Center (IDEC), Korea.

REFERENCES

- [1] X. Pan, A. Bacha, S. Rudolph, L. Zhou, Y. Zhang and R. Teodorescu, "NVCool: When Non-Volatile Caches Meet Cold Boot Attacks," *IEEE International Conference on Computer Design (ICCD)*, pp. 439–448, Oct. 2018.
- [2] A. schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J-P Seifert, "Simple Photonic Emission Analysis of AES," *Cryptographic Hardware and Embedded Systems (CHES)*, pp. 41–57, Sep. 2012.
- [3] T. Unterluggauer, and S. Mangard, "Exploiting the Physical Disparity: Side-Channel Attacks on Memory Encryption," *International Workshop on Constructive Side-Channel Analysis and Secure Design*, pp. 3–18, Jul. 2016.
- [4] Y. Lee, B. Karpinskyy, Y. Choi, K-M Ahn, Y. Kim, J. Park, S. Noh, J. Kang, J. Shin, J. Park, Y. Chung, and J. Shin, "Samsung Physically Unclonable Function (SAMPUFTM) and its integration with Samsung Security System," *IEEE Custom Integrated Circuits Conference (CICC)*, pp. 1–4, Apr. 2021.
- [5] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh, and S. Lee, "Physically Unclonable Function for Secure Key Generation with a Key Error Rate of $2E-38$ in 45nm Smart-Card Chips," *IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 158–159, Feb. 2016.
- [6] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "A $553F^2$ 2-Transistor Amplifier-Based Physically Unclonable Function (PUF) with 1.67% Native Instability," *IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 146–147, Feb. 2017.
- [7] S. Satpathy, S. K. Mathew, V. Suresh, M. A. Anders, H. Kaul, A. Agarwal, S. K. Hsu, G. Chen, R. K. Krishnamurthy, and V. K. De, "A 4-fJ/b Delay-Hardened Physically Unclonable Function Circuit With Selective Bit Destabilization in 14-nm Trigate CMOS," *IEEE Journal of Solid-State Circuits (JSSC)*, vol. 52, no. 4, pp. 940–949 Apr. 2017.
- [8] T. Bryant, S. Chowdhury, D. Forte, M. Tehranipoor, and N. Maghari, "A Stochastic All-Digital Weak Physically Unclonable Function for Analog/Mixed-Signal Applications," *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 140–145, May. 2017.
- [9] J. Lee, D. Lee, Y. Lee, and Y. Lee "A $445F^2$ Leakage-Based Physically Unclonable Function with Lossless Stabilization through Remapping for IoT Security," *IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 132–133, Feb. 2018.
- [10] J. Lee, M. Kim, G. Shin, and Y. Lee, "A $20F^2$ Area-Efficient Differential NAND-Structured Physically Unclonable Function for Low-Cost IoT Security," *IEEE European Solid-State Circuits Conference (ESSCIRC)*, pp. 1–4, Sep. 2019.
- [11] Y. Choi, B. Karpinskyy, K-M. Ahn, Y. Kim, S. Kwon, J. Park, Y. Lee and M. Noh, "Physically Unclonable Function in 28nm FDSOI Technology Achieving High Reliability for AEC-Q100 Grade 1 and ISO26262 ASIL-B," *IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 426–427, Feb. 2020.
- [12] D. Li, and K. Yang, "A Self-Regulated and Reconfigurable CMOS Physically Unclonable Function Featuring Zero-Overhead Stabilization," *IEEE Journal of Solid-State Circuits (JSSC)*, vol. 55, no. 1, pp. 98–107 Jan. 2020.
- [13] Y. Shifman, A. Miller, O. Keren, Y. Weizman, and Joseph Shor, "An SRAM-Based PUF With a Capacitive Digital Preselection for a $1E-9$ Key Error Probability," *IEEE Transactions on Circuits and Systems-I: Regular Papers (TCAS-I)*, pp. 4855–4868, Dec. 2020.
- [14] J. Lee, D. Lee, Y. Lee, and Y. Lee, "A $354F^2$ Leakage-Based Physically Unclonable Function With Lossless Stabilization Through Remapping for Low-Cost IoT Security," *IEEE Journal of Solid-State Circuits (JSSC)*, vol. 56, no. 2, pp. 648–657 Feb. 2021.
- [15] K. Liu, H. Pu, and H. Shinohara, "A 0.5-V 2.07-fJ/b $497-F^2$ EE/CMOS Hybrid SRAM Physically Unclonable Function with $< 1E-7$ Bit Error Rate Achieved through Hot Carrier Injection Burn-in," *IEEE Custom Integrated Circuits Conference (CICC)*, pp. 1–4, Apr. 2020.
- [16] J. Lee, M. Kim, M. Jeong, G. Shin, and Y. Lee, "A $20F^2$ /Bit Current-Integration-Based Differential NAND-Structured PUF for Stable and V/T Variation-Tolerant Low-Cost IoT Security," *IEEE Journal of Solid-State Circuits (JSSC)*, vol. 57, no. 10, pp. 2957–2968 Oct. 2022.
- [17] N. Li, J. Zhang, "S2RAM PUF: An Ultra-low Power Subthreshold SRAM PUF with Zero Bit Error Rate," *ACM/IEEE Design Automation Conference (DAC)*, pp. 1–6, Jun. 2024.
- [18] E. Hunt-Schroeder, P. Lin-Bulter, A. Degada, and T. Xia, "3nm Physical Unclonable Function with Multi-Mode Self-Destruction and 3.48×10^{-5} Bit Error rate," *IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 300–301, Feb. 2024.
- [19] S. S. Kudva, M. E. Sinangil, S. Tell, N. Nedovic, S. Song, B. Zimmer, and C. T. Gray, "High-Density and Low-Power PUF Designs in 5nm Achieving $23 \times$ and $39 \times$ BER Reduction After Unstable Bit Detection and Masking," *IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 302–303, Feb. 2024.
- [20] B. Karpinskyy, Y. K. Lee, S. Noh, Y. Choi, J. Park, J. Kang, T. Park, E. Oh, G. Kim, S. Lee, H. Ko, J. Shin, H-G, Rhew, and J. Shin, "An Efficient V_{th} -Tilting PUF Design in 3nm GAA and 3nm FinFET Technologies," *IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 298–299, Feb. 2025.
- [21] B. Driemeyer, H. Mandry, D-P. Wiens, J. Becker, J. G. Kauffman, and M. Ortmanns, "An Eye-Opening Arbiter PUF for Fingerprint Generation Using Auto-Error Detection for PVT-Robust Masking and Bit Stabilization Achieving a BER of $2e-8$ in 28nm CMOS," *IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 300–301, Feb. 2025.
- [22] Y. Yoshimoto, Y. Katoh, S. Ogasahara, Z. Wei, and K. Kouno, "A ReRAM-based Physically Unclonable Function with Bit Error Rate $< 0.5\%$ after 10 years at 125°C for 40nm embedded application," *IEEE Symposium on VLSI Technology (SOVT)*, pp. 1–2, Jun. 2016.
- [23] Y. Pang, B. Gao, D. Wu, S. Yi, Q. Liu, W-H. Chen, T-W. Chang, W-E. Lin, X. Sun, S. Yu, H. Qian, M-F. Chang, and H. Wu, "A Reconfigurable RRAM Physically Unclonable Function Utilizing Post-Process Randomness Source with $< 6 \times 10^{-6}$ Native Bit Error Rate," *IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 402–403, Feb. 2019.
- [24] D. Jeon, J. H. Baek, Y-D. Kim, J. Lee, D. K. Kim, B-D. Choi, "A Physical Unclonable Function With Bit Error Rate $< 2.3 \times 10^{-8}$ Based on Contact Formation Probability Without Error Correction Code," *IEEE Journal of Solid-State Circuits (JSSC)*, vol. 55, no. 3, pp. 805–816 Mar. 2020.
- [25] S. Taneja, A. B. Alvarez, and M. Alioto, "Fully Synthesizable PUF Featuring Hysteresis and Temperature Compensation for 3.2% Native BER and 1.02 fJ/b in 40nm," *IEEE Journal of Solid-State Circuits (JSSC)*, vol. 53, no. 10, pp. 2828–2839, Oct. 2018.
- [26] S. Kim, C. Im, J. Lee, S. Jeong, J. Kim, and Y. Lee, "Logic-embedded Physically Unclonable Functions for Synthesizable and Periphery-free Implementation for Low Area and Design Cost IoT Security," *IEEE European Solid-State Circuits Conference (ESSCIRC)*, pp. 521–524, Sep. 2022.
- [27] "AES," OpenCores, [Online]. Available: https://opencores.org/projects/tiny_aes
- [28] NIST. NIST SP 800-22: Documentation and Software—Random Bit Generation. Accessed: Apr. 14, 2019. [Online]. Available: <https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software>