Hybrid PUF for Counterfeit Mitigation

Authors: Pallavi Ebenezer, Degang Chen, and Randall Geiger
Authors Affiliation: Iowa State University
Authors Contact Information: Randall Geiger rlgeiger@iastate.edu 515-294-7745

***Abstract*— A subthreshold hybrid PUF-embedded authentication circuit is proposed to mitigate the financial incentives that drive the counterfeit community and to encourage the COTS manufacturers to use authentication for system identification in their parts. The proposed hybrid PUF with cross-coupled inverters and a delay-based PUF strategy has sufficient entropy for authentication and a reduced number of transistors per bit. The area efficient fingerprint circuit does not require additional die area, pins, or power overhead. The performance of the primary circuit is unaffected by the fingerprint circuit. The hybrid circuit designed in a 65 nm CMOS process is discussed.**

Keywords— subthreshold fingerprint circuit, hybrid PUF, cross-coupled inverters, PUF, counterfeit countermeasure, authentication

I. Introduction

With the growth of the semiconductor industry and the corresponding supply chain, the internet and online markets have become a great channel for the expansion of more than $100 billion a year in counterfeit electronics [1]. Though much smaller, the counterfeit semiconductor business is also large. Demand for obsolete and cheap parts has created significant financial incentives for counterfeiters. International agreements and anticounterfeit initiatives have failed to thwart the counterfeiters. Though counterfeiters compromise the reputation and profitability of semiconductor manufacturers, the greater threat is to reliability concerned consumers, particularly those in the military and the medical and transportation industries. A simple, cost-effective, and reliable authentication solution is needed for semiconductor manufacturers to combat the counterfeiters. Physically unclonable functions (PUFs) are recognized as a key component of authentication [2] solution. PUFs utilize the inherent entropy of the random process and mismatch variations of devices and interconnects in a circuit to generate unique fingerprints for system authentication. Ongoing research on the design of reliable and spoof proof PUF does not often address the need for producing the cost-effective strategies needed to motivate COTs manufacturers to incorporate authentication circuits in their parts. The work focuses on the challenge of designing area, pin, and power efficient fingerprint circuits that can be practically used for authentication.

II. Subthreshold Hybrid Puf Architecture

A. Block Diagram

A simple high entropy cross-coupled inverter pair (sometimes called a SRAM PUF cell [2]) and a delay based arbiter PUF [2],[4] with a large number of challenge response pairs are combined to form a cost effective fingerprint PUF. The circuit is designed to operate in subthreshold at around half of the nominal supply voltage ($V_{DD,nom}$) and self-disconnects as the supply voltage approaches $V_{DD,nom}$. This ensures that the performance of the main COT circuits is unaffected during normal operation at $V_{DD,nom}$. The V_{DD}, ground and the I/O pins are shared between the main circuit and the PUF circuit, thereby eliminating the need for additional pins. Minimum sized transistors are used to increase the randomness of the response generated from the PUF cell and to reduce die area. The fingerprint circuit is small enough to be placed under a bonding pad. The block diagram of the proposed hybrid PUF is shown in Figure 1.

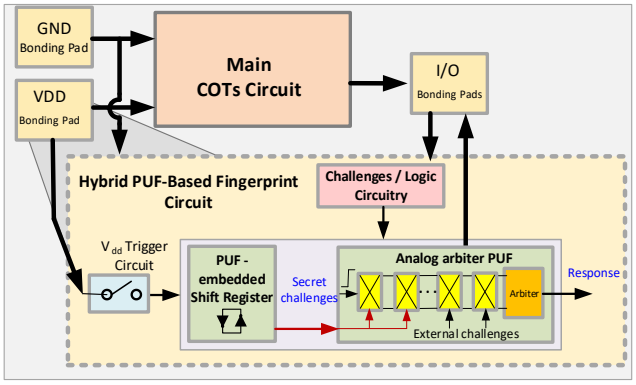

Fig. 1. Block diagram of the authentication circuit

B. Delay Based Analog Arbiter PUF

The delay-based silicon PUF uses cross-coupled or butterfly switches and an analog arbiter (voltage sense amplifier) as shown in Figure 2. The circuit has multiple input challenges to generate a 1-bit output based on the differences in the random path delays through the butterfly switches. The input challenge selects the state of the butterfly switches (straight or cross). A latched voltage sense amplifier determines whether the upper or lower path delay is faster, thereby generating the corresponding 1-bit response. The arbiter PUF is classified as a strong PUF due to its exponentially increasing Challenge-Response pairs (CRPs). For N butterfly bit-cells, there are 2^N possible responses. The number of transistors used to build an analog arbiter PUF is N*4 (transistors in switch blocks) + X (transistors in voltage sense amplifier). The number of transistors per bit is $\frac{4N+X}{2^N}$ which is small compared to many other approaches.

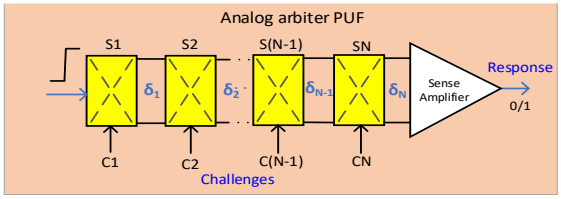

Fig. 2. Analog Arbiter PUF

A drawback of the arbiter PUF is its predictable linear delay model and can be easily broken by machine learning algorithms. However, strategies such as feed-forward loops and the inclusion of nonlinear delay elements provide immunity to machine learning attacks. But when used as a fingerprint generator for integrated circuit authentication, the predictability of the delay is of little concern.

C. *Cross-coupled inverter based PUF*

A bistable cross-coupled inverter pair circuit is also used to generate a 1-bit response. The circuit stabilizes at its favored state based on the relative strength of the 4 transistors. The random mismatch in threshold voltages (V_{th}) of the transistors as well as the mismatch in parasitic capacitances at the input nodes of the inverters provide high entropy in these PUF cells. These PUF cells [5],[6] have been used to generate a standalone fingerprint circuit embedded in a recirculating shift register readout circuit. The inverters can be practically paired with physically adjacent inverters in two ways (right and left) to effectively produce two unique responses. For a circular shift register with n 4-transistor PUF cells, the number of transistors per bit, including the interstage shift register coupling transistors, is $\frac{4n}{n}$. Here, the area increases linearly with the number of random bits. The entire PUF code generated in these cells remains in the circular shift register and hence subsets of the total number of bit cells in the ring can be sent to the output in response to a challenge. However, this structure is prone to a larger number of unstable (weak) bits. Reliability enhancement techniques [7] can be used to deal with the unstable bits.

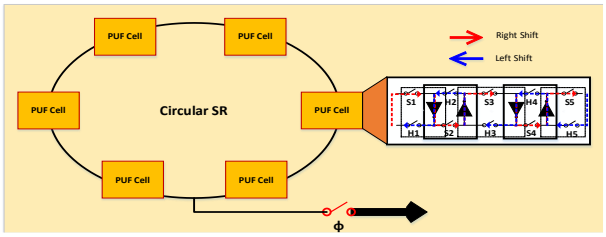

Fig. 3. PUF embedded shift register

D. *Operation of the Hybrid PUF*

The fingerprint circuit is activated at half the $V_{DD,nom}$ using the V_{DD} trigger circuit. Challenges to the PUF include the shift direction (left or right), the index position in the rings (the circular shift register can be clocked K times to choose the starting location to read the output), and the external challenges to the right half of the switch blocks in the analog arbiter. In this design, the first half of the switch blocks (S_1 to $S_{\frac{N}{2}}$) receive a secret challenge from a subset $\frac{N}{2}$ of the responses from the PUF embedded in the circular shift register. The input to the analog arbiter is an N cycle input signal. Therefore, for every set of challenges applied to the system, a $\frac{N}{2}$ bit response is generated at the output of the sense amplifier. Hence, the hybrid structure forms a reliable, unique, reproducible, low die area authentication circuit.

III. Simulation Result

The hybrid PUF is implemented in a 65nm CMOS process. Monte Carlo simulations were used to predict the performance due to process and mismatch variations. For proof of concept, a 16-bit 4T PUF embedded shift register circuit generating a 4-bit secret challenge first 4 switches of the 8-bit arbiter PUF is implemented. Hence for a given challenge sequence, a 4-bit sequence is generated. Detailed simulation results would be provided in the final document.

IV. Conclusions

A strategy for designing a subthreshold hybrid PUF-based circuit for counterfeit intervention that can support many challenge-response pairs and a small number of transistors per bit in the fingerprint has been introduced. The minimum sized transistors provide high entropy for an area efficient design that requires a very small die area, no additional pins, and that does not interfere with the operation of the main circuit.

Acknowledgment

This work was supported, in part, by the Semiconductor Research Corporation (SRC) and by the National Science Foundation (NSF).

References

[1] M. Pecht and S. Tiku, "Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics," *IEEE Spectr.*, vol. 43, no. 5, pp. 37–46, May 2006.

[2] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in *2007 44th ACM/IEEE Design Automation Conference*, Jun. 2007, pp. 9–14.

[3] Y. Su, J. Holleman, and B. Otis, "A 1.6pJ/bit 96% Stable Chip-ID Generating Circuit using Process Variations," in *2007 IEEE International Solid-State Circuits Conference. Digest of Technical Papers*, Feb. 2007, pp. 406–611.

[4] A. Vijayakumar, V. C. Patil, C. B. Prado, and S. Kundu, "Machine learning resistant strong PUF: Possible or a pipe dream?," in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2016, pp. 19–24.

[5] P. Ebenezer, D. Chen, and R. Geiger, "Authentication Circuit with Low Incorporation Barrier for COTs Manufacturers," in *2019 IEEE National Aerospace and Electronics Conference (NAECON)*, Jul. 2019, pp. 269–272.

[6] P. Ebenezer, D. Chen, and R. Geiger, "Counterfeit IC Countermeasure with 4T Cell Based Authentication Circuit," Iowa State University Ames United States, 2019.

[7] S. K. Mathew *et al.*, "16.2 A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," in *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, Feb. 2014, pp. 278–279.