Counterfeit Mitigation with PUF-Embedded Readout

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*— An anticounterfeit strategy based upon PUF-embedded authentication circuits is proposed that will eliminate financial incentives for counterfeiters and reduce the insertion barrier for COTS manufactures. In many applications, the authentication circuit will not require additional die area, pins, or a power overhead and will not adversely affect the performance of the original circuitry. The performance of an implementation of the authentication circuit which has a large number of challenge/response pairs has been designed in a UMC 65 nm process will be discussed.**

Keywords—counterfeit, anticounterfeiting, PUF, hardware security, challenge/response pairs (CRPs)

I. INTRODUCTION

The perceived high cost associated with authentication of integrated chips has created a financial barrier to the development of an effective strategy for purging counterfeit ICs from the semiconductor supply chain that most of the major Commercial Off The Shelf (COTS) manufacturers have not overcome. The recognized ongoing presence of a significant number of counterfeit ICs in the supply chain presents a significant challenge to design and manufacture electronic systems with high lifetime reliability as is expected in many medical, transportation, and financial systems. The counterfeit IC problem is probably even of more concern to defense contractors where the impact of preventable failures of military systems can be catastrophic.

Unauthentic ICs in the supply chain can be decomposed into two major classes. One class of unauthentic integrated circuits has arisen strictly because of existing financial incentives to perpetuators to compete with legitimate manufacturers with sales in an ongoing commodity market. The other class is associated with circuits that contain hardware Trojans and can be termed the Trojan-bearing IC class. Perpetuators that contribute Trojan-bearing components have a more nefarious goal of compromising the performance of systems in which the parts are utilized. Though both classes involve counterfeit parts, in this work we will refer to those unauthentic ICs created for financial incentives as counterfeit ICs. There are numerous examples of counterfeit ICs with various estimates of the size of the annual counterfeit market being in the $5 billion to $15 billion range. Though only a single-digit percentage of the total semiconductor market, it is still large. Often counterfeiting can be traced to parts that can be illicitly manufactured at a lower cost than the authentic component[1] but often with reduced reliability. Other counterfeit approaches include reinserting used ICs into the supply chain and remarking inferior or alternative parts as premium parts. Several cryptographic or fingerprinting techniques have been proposed that can be very effective at screening counterfeit parts from the supply chain if the appropriate cryptographic circuitry is included on the IC. Unfortunately the authentication circuitry is often quite complex and expensive (i.e. requires additional die area, pins, or more power) thus there is minimal utilization by COTs manufacturers of authentication circuitry because these approaches are not thought to be cost effective.

One of the most practical strategies for generating unique fingerprints on an IC is based upon Physically Unclonable Functions (PUFs) which can provide unique identity for each IC. The inherent random variations in a semiconductor process can be used to produce unique digital codes. Many PUFs have a large number of challenge-response pairs (CRP) making it difficult for a counterfeiter or adversary to spoof a PUF. Although PUFs can be used for counterfeit mitigation, a more common use of PUFs is for establishing secure communications or transactions and in these latter cases, a large number of CRPs is even more important. In this work, emphasis will be placed entirely on counterfeit protection. When used for counterfeit protection to reduce or eliminate financial incentives, rewards to the counterfeiter for an occasionally successful spoof will be dramatically reduced and thus the number of challenge/response pairs can be relaxed as can the strength of a cryptographic key that the PUF must provide.

In earlier work on counterfeit mitigation [2], the authors focused on a single random Boolean sequence (i.e. fingerprint) generated with a PUF that could be generated on demand and that would be close, in the Hamming distance sense, to a sequence that was extracted and archived during the manufacturing process. Because of weak bits and noise, a few of the bits in the random PUF-derived Boolean sequence may vary with temperature, with aging, and from one reading to the next thus closeness in the Hamming distance sense rather than identical Boolean sequences are used to characterize a specific fingerprint. Though technically each IC would be required to have a unique neighborhood in an n-dimensional space, in this work we will simply say that each IC will have a unique code or fingerprint. In the earlier work, the fingerprint circuit reused existing pins thus eliminating the need for additional pins and was placed under the bonding pads (and termed an "under-circuit") thus reducing or eliminating die area overhead. And the under-circuit was operated in deep weak inversion and turned off during normal operation thus eliminating its effect on the desired circuit. Continued technology scaling leads to shrinking in MOSFET channel geometries which causes increased threshold voltage variation between ideally matched devices on a die. Thus

minimum sized devices were used maximize mismatch variations which reduced the size of the n-dimensional neighborhoods corresponding to the individual fingerprints. But some questions were raised with the earlier work about having a single bit sequence for the PUF code which is essentially a single challenge-response pair for the authentication circuit.

In this work, a PUF-based fingerprint approach is still used which requires no additional pins, little or no additional die area, and that does not adversely affect the operation of the original circuit but that overcomes limitations associated with a single CRP. Specifically, in this work, a large number of challenge-response pairs are provided. In addition, the random bit generators themselves will be used to form a dynamic shift register that continuously streams the PUF codes to the output thus providing the readout function without requiring an additional readout circuit.

II. Prior Work

Extensive research has been done in the field of hardware security especially with PUFs [3], [4]. Related works include PUF designs that depend on the random variations in electrical characteristics of simple circuits such as the delay of gates[3], the threshold voltage of transistors[5], the resistance in segments of the power grid of a chip[2], [6], the relative delay of two nominally identical paths in a circuit, the oscillation frequency of a ring oscillator, and the inherent binary output of memory elements, such as SRAMs[7], latches, and flip-flops. Whereas much of the prior work on PUFs has focused on creating strong PUFs, in this work the emphasis is on a PUF along with the readout circuit that can be used for fingerprint-based authentication that is adequate to reduce or eliminate financial incentives of potential counterfeiters yet simple, noninvasive, and small enough to be viewed as cost effective by the COTS manufacturers.

III. PUF Architecture

The PUF used in this work is quite similar to the SRAM PUFs as two back to back connected inverter unit cells will be used to generate the individual random codes during power up but is distinct in that the inverter cells are also used to help create the readout circuit. The fingerprint generator will be comprised of a number of dynamic shift-register based rings though only two rings will be depicted in this paper. At power-up, a predetermined number of bits in each ring will assume a Boolean value that defines a unique fingerprint for the ring. The remaining bits will be deterministic and can be viewed as a frame header used for synchronization during readout. Pairs of adjacent inverters in the shift registers will be connected in a plurality of local feedback loops to generate random bits. When paired together, the two inverters form a standard four transistor (4T) PUF bit cell. Two additional transistors or transmission gates are used to close the loop and eventually to provide the shift and transfer operations required in the dynamic shift register. A brief description of these cells follows.

A. PUF Cell

The PUF cell is built using four transistors configured as two inverters connected back to back is shown in Figure 1. This circuit generates a Boolean code when power is applied. The two transistors (or transmission gates) designated as S and H complete the feedback loop which is necessary to generate the bit code at power up. To maximize the randomness of the bits generated and minimize the number of weak bits, near minimum-sized transistors are used in the two inverters. Each PUF cell can randomly generate two outputs either '1' or '0' due to random parameter variation in the four transistors that comprise the two inverters. This discrete random variable is characterized by the uniform Bernoulli distribution. For an n-bit PUF array, there are 2^n possible output codes. The probability that an n-bit PUF code is unique, that is not the same as that of another n-bit PUF code in a sample of N randomly generated n-bit PUF codes, is given by Equation (1). Though the probability of a duplicate code increases with the number of integrated circuits in the population, n can be practically selected, even when there are a large number of parts, so that the probability of a duplicate code is very small. Although the probability of a duplicate code can practically be made to be very small, the financial incentive for a counterfeiter will still be removed if an occasional duplicate code occurs.

$$P = \left(\frac{2^n - 1}{2^n}\right)^{N-1} \qquad (1)$$

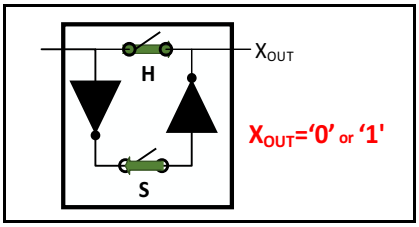

Fig. 1. 4T PUF cell

B. Dynamic Shift registers

A dynamic shift register can be built by combining a string of 4T PUF cells together along with additional transfer switches designates as S1,S3,S5, … as shown in Figure 2. The readout of the codes that were acquired during power up is quite simple in this architecture and uses a two-phase non-overlapping clock. After power up when in the readout mode, the H switches are opened. In clock Phase 1, odd-numbered switches S1, S3, S5, … are closed. This moves the PUF code from one PUF cell to the next. During Phase 2, the even-numbered switches S2, S4,… are closed. This shifts the PUF code from one inverter to another within the PUF cell. Thus the PUF code is both generated in and transferred by the inverters in the PUF cells. This forms a PUF-embedded shift register and when connected in a recirculating manner a ring is formed. The fingerprint codes are always present in the shift register while it is being clocked. By embedding the rings formed with the PUF generators in the readout circuit, the need for additional readout circuity to read the response for a

given challenge is eliminated. To identify the beginning of a PUF code sequence, a frame header circuit comprised of additional inverter pairs is inserted into the ring. The inverters in the frame header circuit are sized to provide a deterministic rather than a random output when power is applied.

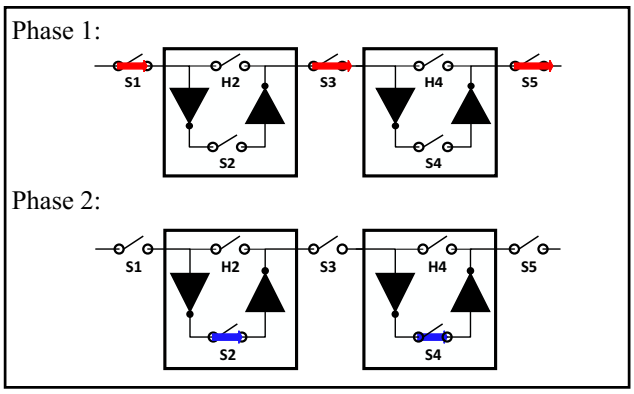

Fig. 2. PUF-Embedded Dynamic Shift Register

C. *Generating additional CRPs*

In previous work [3], the 4T PUF cells were re-partitioned by using left-adjacent and right-adjacent inverters to generate two PUF sequences thereby doubling the number of random bits generated with a minimal increase in transistor count. This alternate pairing of the inverters along with bi-directional shifting in the ring is depicted in Figure 3. In addition to the alternate inverter pairing, the switch transistors H3, H5… were added to provide for the bi-directional circulation in the dynamic shift registers. The alternate adjacent pairing of the inverters in the PUF cells will be used in this work as well to double the number of random bits available per equivalent PUF cell.

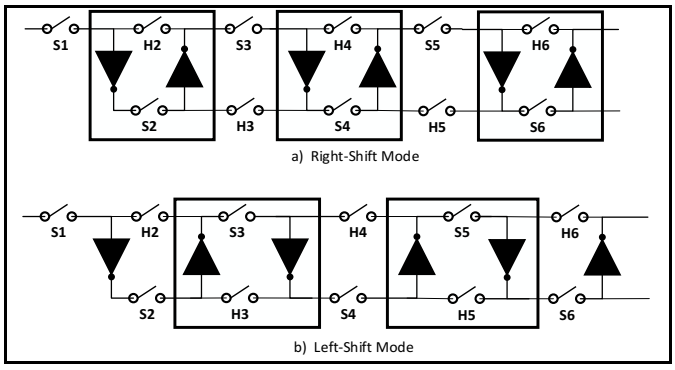

Fig. 3. Bi-directional Shifting to Double Random Bits

A new authentication circuit that has a large number of challenge-response pairs is shown in Figure 4. It is comprised of two circular PUF-embedded dynamic shift registers, each of which can be shifted left or right. After power-up and after frame synchronization for the two rings, one of the rings is advanced by k clock cycles. The index k and the direction of clocking of the two rings (right or left) serve as external inputs to the authentication circuit and represent the challenges. After data in one of the rings is advanced by k clock cycles, the two rings are clocked synchronously. The readout sequence is obtained by alternately selecting the output from the two rings as shown by the sampling clocks φ3 and φ4 in the figure. By increasing the number of rings(R), the number of inputs on the mux, by changing the mux sequence, by setting the index(k) on each ring, and by changing the number of inverters included in each of the rings, a very large number of challenge-response pairs can be obtained with little circuit overhead.

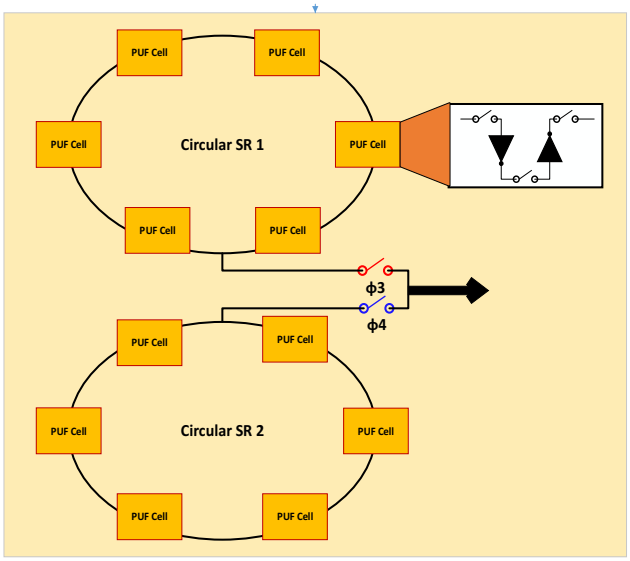

Fig. 4. Increasing CRPs

D. *Operation and Implementation of the fingerprint circuit*

The proposed fingerprint circuit, even with multiple rings, is simple and will occupy a very small area and may be small enough to be placed 'under' a bonding pad in some processes. It is designed to be operate at supply voltages that are at levels well 'under' the supply voltage to the main circuit, and to disconnect itself from the pins at normal operating voltages and will be referred to as an 'undercircuit'. Devices in the undercircuit will be operating in the weak inversion mode because of the low supply voltage. The supply pin, as shown in Figure 5, is shared between the main circuit and the undercircuit. At nominal supply voltages the main circuit is functional and the undercircuit is cut off from the supply with a level-sensing trigger circuit. When the supply voltgae is at approximately 50% of the nominal supply, the PUF circuit is functional and will overpower the impact the main circuit has on the relevant pins. Hence the undercircuit does not interfere with the main circuit's operation. Other pins for the main IC are shared with the undercircuit for inputting the challenge and reading the response.

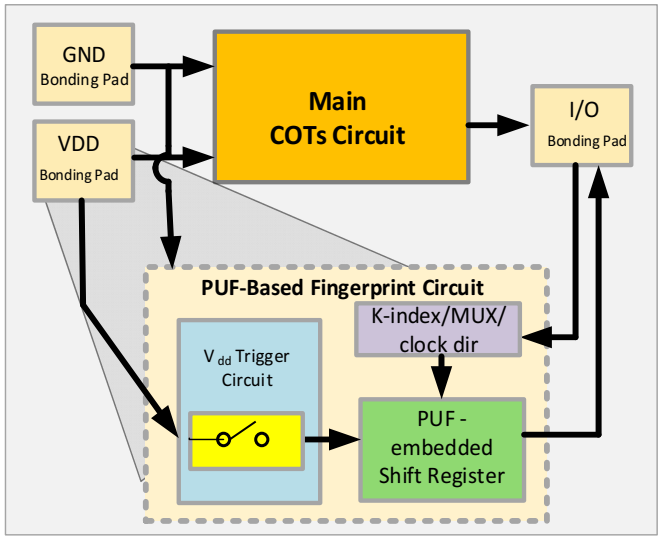

Fig. 5. Block diagram of the authentication circuit

IV. Simulation Results and Discussions

As a proof of concept, two PUF-embedded circular shift registers were designed in a UMC 65nm process. Each was comprised of five 4T PUF cells using minimum-sized transistors. Spectre transient simulation results for a supply voltage of V_{DD}=1.3V for one instantiation of the PUF cells with random variations in the model parameters and a single phase relationships (i.e. a single value for index k), a single rotational direction for each shift register, and for fixed ring lengths are shown in Figure 6. In this figure, the output for one complete cycle of the recirculating shift registers is shown. This corresponds to a single challenge. The plots show that the final output sequence is a 10-bit sequence obtained by alternating the codes from the two PUF-embedded shift registers SR_1 and SR_2. Though simulations here are at a supply voltage of 1.3V, the same performance can be obtained if operated in deep weak inversion. Though shown here only for a single challenge, simulation results are as expected for other challenges as well.

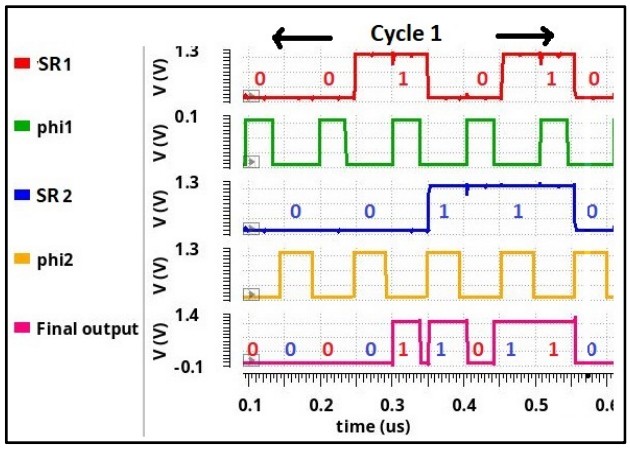

Fig. 6. Simulation results of two circular shift registers

Figure 7 shows Spectre simulation results, again with a single challenge, in the same process for an implementation of two PUF-embedded circular shift registers operated in deep weak inversion with a 4 bit comma code (4-bit frame header) and a 5-bit PUF code in each of the circular shift registers. The final output thus has an 8-bit comma code and a 10 bit PUF code. The first shift register SR_1 has 4 comma bits <0101> followed by 5 PUF codes represented by 'X' and the second shift register SR_2 has 4 comma bits <1101> followed by 5 PUF codes as well. The challenge here is aligned with the comma bits for the two shift registers though different challenges corresponding to different k indexes would not align the comma bits in the two shift registers. The final output is read alternatively from SR_1 and SR_2 (in this example the phase of SR_2 leads the phase of SR_1) as <10110011X X X X X X X X X X>, where 'X' represents the PUF code bits obtained due to random variations of the process parameters of the transistors. In these simulations, noise was not included so if any of the random bits were weak, it would not be apparent in these simulation results. However, for this process, and with the minimum sizing of the inverters in the PUF cells, the probability of a weak bit is very low.

The robustness of the proposed circuit was partially validated by using 200 Monte Carlo simulations to generate 200 implementations of the authentication circuit in the same 65nm process. Each shift register contained 4 deterministic comma bits and 5 random PUF codes. Simulation results randomly selected from the 200 simulations for 4 out of the 200 iterations, each with a single challenge, are shown in Figure 8. These are representative of what was obtained from the remaining 196 simulations. The corresponding 8 comma-bits, highlighted in the interleaved outputs, are all <10110011> whereas the random PUF bits appear to be varying randomly.

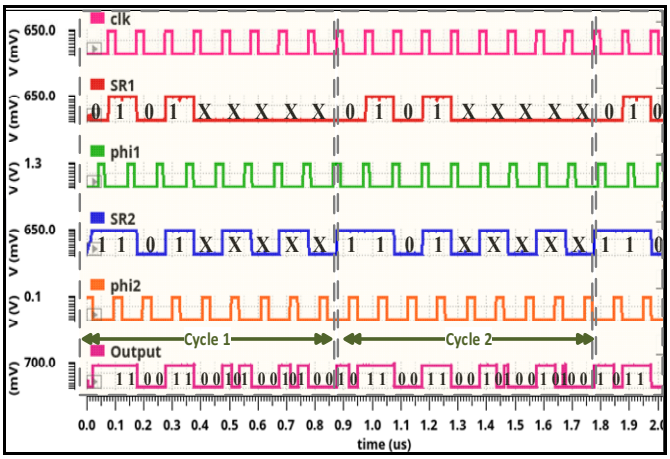

Fig. 7. Simulation results of two PUF-embedded shift registers

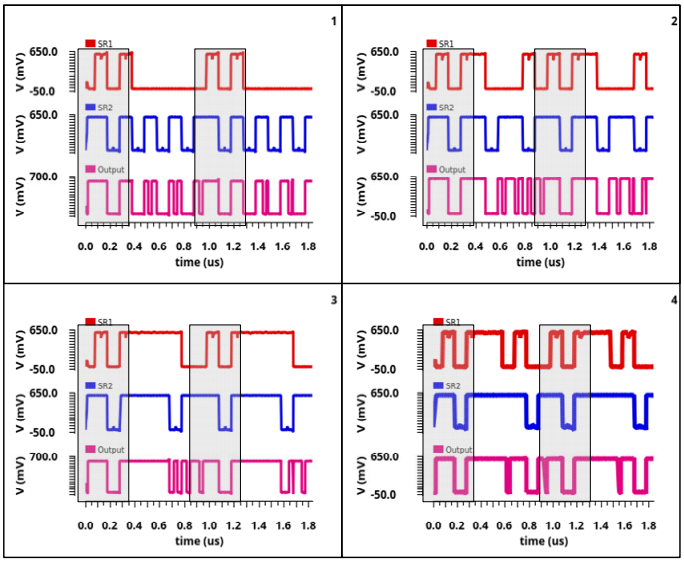

Fig. 8. Monte carlo simualtions to show robustness of the PUF circuit

Though the Spectre simulation results were for only two shift registers with 4 deterministic comma bits and 10 random PUF bits, a more realistic implementation would have a much larger number of PUF bits, maybe 64 or more, and modestly more frame-header bits, maybe 8 or 10. In addition to increasing the size of the PUF code, larger numbers of bits in the shift register would provide for larger numbers of challenge-response pairs. The only reason a larger number of bits was not included in these simulations was to reduce the simulation time required for the random circuit generation. The random nature of the PUF bits, the deterministic nature of the frame-header bits, and the performance of the recirculating shift register should be independent of the number of comma bits and the number of PUF codes in the shift registers.

The estimated area of the authentication circuit with two shift registers for a total of 8 comma bits and 10 bit PUF code bits when designed in a 65nm process is 0.005mm^2. Since the PUF codes and the frame headers are embedded in the readout circuit, no additional circuitry is required for the readout circuit itself. In this circuit, the PUF codes occupy 6% of the area, the header bits take up 10% of the area, and rest of the area is used for clock generation, trigger and other logic circuitry. Hence, even if the number of random bits is much larger, the area required for the authentication circuit will be very small.

V. Conclusions

An approach for designing a PUF-based authentication circuit that can support a large number of challenge-response pairs has been introduced. This approach requires no pin overhead, a very small area, draws no power during operation of the main circuit, and does not alter the operation of the main circuit. The low area is obtained, in part, by using minimum-sized devices to intentionally reduce the number of weak bits in the PUF cells and by embedding the inverters in the PUF cells directly in the readout circuit.

Acknowledgment

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

References

[1] [1] M. Pecht, “The Counterfeit Electronics Problem,” Open J. Soc. Sci., vol. 01, no. 07, pp. 12–16, 2013.

[2] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, “Design and Implementation of PUF-Based ‘Unclonable’ RFID ICs for Anti-Counterfeiting and Security Applications,” in 2008 IEEE International Conference on RFID, 2008, pp. 58–64.

[3] P. Ebenezer, D. Chen, and R. Geiger, “Unauthentic IC Countermeasures for Future Integrity of the Semiconductor Supply Chain,” in NAECON 2018 - IEEE National Aerospace and Electronics Conference, 2018, pp. 158–164.

[4] P. Ebenezer, D. Chen, and R. Geiger, “Counterfeit IC Countermeasure with 4T Cell Based Authentication Circuit,” Iowa State University, 2019.

[5] R. Maes and I. Verbauwhede, “Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions,” in Towards Hardware-Intrinsic Security: Foundations and Practice, A.-R. Sadeghi and D. Naccache, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 3–37.

[6] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial,” Proc. IEEE, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

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

[8] K. Lofstrom, W. R. Daasch, and D. Taylor, “IC identification circuit using device mismatch,” in 2000 IEEE International Solid-State Circuits Conference. Digest of Technical Papers (Cat. No.00CH37056), 2000, pp. 372–373.

[9] D. E. Holcomb, W. P. Burleson, and K. Fu, “Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers,” IEEE Trans. Comput., vol. 58, no. 9, pp. 1198–1210, Sep. 2009.