MeLPUF: Memory in Logic PUF

Christopher Vega, Patanjali SLPSK, Shubhra Deb Paul, Swarup Bhunia
{c.vega, patanjali.sri@illinois.edu, shubhra.paul}@uiuc.edu
University of Illinois at Urbana-Champaign

ABSTRACT

Physical Unclonable Functions (PUFs) are used for securing electronic designs across the implementation spectrum ranging from lightweight FPGA to server-class ASIC designs. However, current PUF implementations are vulnerable to model-building attacks; they often incur significant design overheads and are challenging to configure based on application-specific requirements. These factors limit their application, primarily in the case of the system on chip (SoC) designs used in diverse applications. In this work, we propose MeL-PUF—Memory-in-Logic PUF, a low-overhead, distributed, and synthesizable PUF that takes advantage of existing logic gates in a design and transforms them to create cross-coupled inverters (i.e. memory cells) controlled by a PUF control signal. The power-up states of these memory cells are used as the source of entropy in the proposed PUF architecture. These on-demand memory cells can be distributed across the combinational logic of various intellectual property (IP) blocks in a system on chip (SoC) design. They can also be synthesized with a standard logic synthesis tool to meet the area/power/performance constraints of a design. By aggregating the power-up states from multiple such memory cells, we can create a PUF signature or digital fingerprint of varying size. We evaluate the MeL-PUF signature quality with both circuit-level simulations as well as with measurements in FPGA devices. We show that MeL-PUF provides high-quality signatures with both circuit-level simulations as well as with measurements in FPGA devices. We also suggest additional optimizations that can be leveraged to improve the performance of MeL-PUF.

Table 1: Table listing the properties of various PUFs

| Property                | [9] | [13] | [8] | [7] | [22] | [3] | MeL-PUF |
|-------------------------|-----|------|-----|-----|------|-----|--------|
| Uniqueness              | ✓   | ✓    | ✓   | ✓   | ✓    | ✓   | ✓      |
| Randomness              | ✗   | ✗    | ✗   | ✗   | ✓    | ✗   | ✓      |
| Unclonability           | ✗   | ✗    | ✗   | ✗   | ✗    | ✗   | ✓      |
| Reliability             | ✓   | ✓    | ✓   | ✓   | ✓    | ✓   | ✓      |
| Robustness              | ✓   | ✓    | ✓   | ✓   | ✓    | ✓   | ✓      |
| Synthesizability        | ✗   | ✗    | ✗   | ✗   | ✓    | ✗   | ✓      |
| Resistance to           |     |      |    |    |      |    | ✓      |
| Model building attacks  |     |      |    |    |      |    | ✓      |
| Fully digital           | ✓   | ✓    | ✓   | ✓   | ✓    | ✓   | ✓      |

While strong PUF may appear to be the more suitable candidate the ability to input challenges and readout responses makes them vulnerable to model-building attacks [6]. Weak PUFs have shown resistance to model-building attacks making them more desirable for commercial applications [19]. Delay PUFs like Arbiter PUFs, and ROPUFs are examples of Strong PUFs, while Memory PUFs are examples of Weak PUFs.

An interesting observation here is that a majority of the PUF structures require dedicated structures leading to increased area and performance overheads. This makes them especially unsuitable for resource-constrained environments such as the Internet of Things applications. Strong PUFs are vulnerable towards model-building attacks while weak PUFs require specialized structures for implementation. Additionally, these structures are vulnerable to tampering attacks where the attacker could remove the PUF structure and thus bypass the authentication mechanism. Table 1 summarizes the capabilities of the existing PUFs reported in the literature.

In this paper, we present MeL-PUF, a novel fully synthesizable PUF structure obtained by integrating memory elements into the digital logic of a combinational circuit. Figure 1(a) illustrates the MeL-PUF structure. MeL-PUF consists of two cross-coupled inverters connected to form a bistable memory cell. Upon powering on, the values at the two inverter inputs are randomly initialized due to which they enter a meta-stable state. The value at the output stabilizes to either a 1 or a 0 at random. MeL-PUF consists of a control logic comprising of a multiplexer and control signal. The control signal can be used to read the value of the bi-stable element. Figure 1(b) shows the proposed MeL-PUF structure integrated into a digital design. To the best of our knowledge MeL-PUFs is the first fully synthesizable PUF structure. We show that our proposed MeL-PUF structure incurs low overhead, and can be incorporated into a wide variety of designs. We demonstrate the utility of MeL-PUF using both simulation and hardware implementation.

The paper is organized as follows: we describe the MeL-PUF structure in section 2. We discuss the evaluation of our proposed PUF structure along with its overheads in section 3. We highlight the utility of MeL-PUF in section 4.
2 MEL-PUF: MEMORY IN LOGIC PUF

2.1 MeL-PUF Structure

Figure 1(a) illustrates the proposed MeL-PUF structure. MeL-PUF consists of two cross-coupled inverter structures and a control element, thus constituting the structure of a memory element, such as an SRAM cell. Upon startup, the output of the bistable element is unknown and is random, which is then used as our PUF response. The structure of the PUF allows us to distribute and place the PUF in the data-path of a combinational circuit as shown in Figure 1(b). This is accomplished through the control MUX. A two-input MUX allows us to switch between the PUF response and logic data.

Figure 1(b) depicts MeL-PUF implementation where we incorporate bi-stable memory element in a circuit to create a PUF. The additional MeL-PUF circuitry is highlighted in red, with original paths in black. During power-up, the output of the memory cell results in an unknown state, which we use as our source of entropy. The output of one inverter is connected to a MUX which acts as the control element. When the control signal is low, the MUX allows the PUF signature to be captured at startup. When the control signal is high, then the circuit functions normally.

2.2 MeL-PUF Signature Generation

The data-paths for generating a response from the PUF are outlined in Figure 1(c). The PUF structure can be inserted and distributed throughout a circuit as shown in figure 1(b). On startup, the bistable element enters a metastable state, similar to an SRAM cell. As such the state in which the bistable element stabilizes is unknown and random. In the example shown in figure 1(c), the value of inverter 1 stabilizes to 1 and is sampled by the control element. This is shown as the blue data-path. When the control signal, highlighted in red, is low the output of inverter 1 is sampled as the PUF output. Sampling multiple PUF elements and combining their response allows you to create a cross-coupled inverter with special emphasis on making it symmetric.

2.3 MeL-PUF Integration

In our proposed approach, we incorporate the PUF elements into the datapath or control logic of a combinational design. We accomplish this as described in the following steps:

1. Judiciously selecting the gates where the feedback loop can be created and adding the feedback loop there such that we create a cross-coupled inverter with special emphasis on making it symmetric.
2. Controlling the feedback loop by incorporating MUXes or other control logic in the feedback path and control signals.
3. By connecting the output of the cross-coupled inverter to the scan chain (or to primary outputs using muxes).

3 EXPERIMENTAL SETUP AND RESULTS

PUFs demonstrate the following four properties [14]: uniqueness, reliability, unclonability, and randomness. Uniqueness is the ability of the PUF to produce distinct signatures for different challenges. Reliability is defined as the ability to produce the same response for the same input challenge every time. Unclonability is the property of a PUF that withstands against any replication, and randomness means that the corresponding PUF can generate random signatures for a wide variety of input challenges. We evaluate our proposed PUF structure based on these metrics using both transistor-level simulations and implementation on an FPGA.

3.1 MeL-PUF Simulation and Analysis

We create a transistor-level model of the MeL-PUF circuit in HSPICE using the 45 nm high-performance CMOS process node from Predictive Technology Model (PTM) [1]. We use an input clock frequency of 100 MHz signal to this circuit along with the nominal supply voltage, \( V_{DD} = 1.0 \text{ V} \). We initialize all the circuit nodes as ‘0’ at the beginning of the simulation. We consider the manufacturing process variations by combining the effects of physical specifications such as \( t_{ox} \), \( W \), \( L \), etc. into a single parameter - the threshold voltage, \( V_{th} \) [16]. We model these process variations as variations of \( V_{th} \) by using a Gaussian distribution for 10000 MeL-PUF circuit models/instances with \( \sigma_{inter-die} = 25\% \). We apply the in-built parameter distribution function of HSPICE, AGAUSS, to shift/skew the transistor threshold values to generate this distribution as depicted in Fig. 2(a). To characterize the effect of manufacturing process variations, we perform Monte-Carlo simulation on power-up values at nominal temperature, \( T_{NOM} = 25^\circ \text{C} \) on the generated model. Each Monte-Carlo simulation run results in a 1-bit power-up value for that specific MeL-PUF circuit instance, and we use that as a corresponding binary signature. Fig. 2(b) illustrates the gray colormap of collected power-up values for 10000 MeL-PUF instances.
Comparison of MeL-PUF robustness

We observe that the simulation design of MeL-PUF demonstrates intra-HD for evaluating the robustness of MeL-PUF.

3.1.2 Robustness Analysis. We use the intra-Hamming distance (intra-HD) for evaluating the robustness of MeL-PUF. The intra-HD is the difference in response offered when two different challenges are applied to the same PUF implementation. Intra-HD is estimated using equation 2. We assess the intra-HD by simulating the operation of MeL-PUF over five different temperature levels: 0, 20, 45, 65, and 85 °C (at nominal VDD = 1 V). Fig. 2(d) shows the percentage bit-errors in terms of average intra-HD at different temperature levels. We observed that the PUF exhibits 8.37%, 1.23%, 6.03%, 11.49%, and 15.89% bit-errors 0, 20, 45, 65, and 85 °C respectively.

3.1.3 Randomness Analysis. To evaluate the randomness, we perform simulation on our MeL-PUF model and collect one million response bits to facilitate in assessing some tests in the NIST (National Institute of Standards and Technology) randomness test suite [2]. We observed that generated sequences successfully pass all of the performed tests at a \( p-value \) higher than 0.001. Thus we conclude that the simulated MeL-PUF responses are random with a confidence level of 99.9%.

3.2 Hardware-level Evaluation of MeL-PUF

We also validate our MeL-PUF structure by implementing it on an FPGA platform. We used a Max 10 FPGA (10M50SAE144C8G) based platform [17]. Figure 3(a) presents the layout of the FPGA board. We used ISCAS85 benchmark circuits to insert the MeL-PUF structure while ensuring that the LUTs were not simplified or combined with any other logic. Internal observation points are also added to the circuit observing the output of the control MUXes. These points are routed to RAM (Random Access Memory) and used to extract the signature through the in-system memory content editor of Quartus software. To test different regions of the board, LUT placements for the PUF are set using the assignment editor.

To evaluate the signatures generated by our design, we insert a set of PUFs into an ISCAS85 benchmark circuit for signature generation. This design is programmed to a Max 10 FPGA and we sample 1024-bit signatures from the circuit for ten boards. For each board, we sample five different LUT regions and collect four signatures per-region. These regions were used to calculate the uniqueness, reliability, and randomness of our PUF. Signatures are collected under nominal conditions (3.3 V at 25 °C). Additionally, we also sampled the signatures under a range of voltages between 3 V - 1.97 V to quantify the robustness of our designed PUF.

3.2.1 Uniqueness. Figure 4(a) shows the histogram plotting the uniqueness between all boards. The X-axis shows the percentage of...
V - 1.97 V and compare the signature to those of 3.3 V. The average (c) and (d) show the improvement in uniqueness and reliability using the optimizations described in section 4

4 ANALYSIS

4.0.2 PUF Distribution and Randomness. The reliability of MeL-PUF is calculated by comparing signatures from the same LUT region over multiple measurements. Certain LUTs may exhibit different levels of stability due to manufacturing variations. Figure 4(b) shows a histogram of reliability, giving our solution an average inter-hamming distance is 3.07%.

3.3.2 Reliability. The reliability of MeL-PUF is calculated by comparing signatures from the same LUT region over multiple measurements. Certain LUTs may exhibit different levels of stability due to manufacturing variations. Figure 4(b) shows a histogram of reliability, giving our solution an average inter-hamming distance is 3.07%.

3.2.4 Robustness. As a measure of PUF robustness, voltage variations are also taken into account. In this case, the typical voltage supplied to the board is 3.3 V. We collect data for voltages between 3 V - 1.97 V and compare the signature to those of 3.3 V. The average Hamming distances are shown in the table 3. The average inter-HD between voltages is recorded as 7% and the intra-HD as 2%. Significant changes only begin occurring at 2.2 V when the inter-HD rose to 4%, with the highest being 13% at 1.97 V, the lowest the board could function. Above 2.2V, the variations were around 2.5% which is a reasonable variation. We observe that the reliability of the PUF is not significantly affected at different voltages.

4 CONCLUSION

The emergence of the internet of things (IoT) era has necessitated low-cost, robust, and highly secure hardware-based authentication primitives. We have presented a novel PUF implementation paradigm that can be integrated into combinational logic and is distributed, synthesizable, easily configurable, and lightweight (in terms of area, power, performance overhead). Such a PUF implementation can serve as an attractive authentication primitive in diverse applications, including IoT. While the proposed PUF is a weak PUF and provides one-bit entropy per cell, it is capable of generating a high-quality signature in terms of uniqueness, randomness, and robustness. The PUF signatures can be easily read out through the scan chain. We have evaluated MeL-PUF implementations using simulation and FPGA platform with promising results. Our future work will include further optimization of the PUF design, analysis of the effectiveness of MeL-PUF further through measurements, and evaluation on large scale designs.

6 ACKNOWLEDGEMENT

The work is funded in part by Defense Advanced Research Project Agency (DARPA) as part of the Automatic Implementation of Secure Silicon (AISS) program in collaboration with Northrop Grumman Corporation (NGC).

REFERENCES

[1] 2009. Predictive Technology Model. http://ptm.asu.edu/
[2] 2010. SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Gaithersburg, MD, United States. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf
Table 2: NIST Test Suite Results for MeLPUF signatures. Signatures from ten different boards (i.e., 10 different chips) are measured for each region. The results indicate the number of signatures are above the threshold for the passing p-value (0.001) and the uniformity of the p-value. Cumulative sums test is run on two different subsets of the signature, indicated by \( S_1 \) and \( S_2 \).

| Test | D1 | D2 | D3 | D4 |
|------|----|----|----|----|
|      | No. of Passing Inputs | P-value | No. of Passing Inputs | P-value | No. of Passing Inputs | P-value | No. of Passing Inputs | P-value |
| Frequency | 6/10 | 0.00000 | 7/10 | 0.00000 | 7/10 | 0.00000 | 10/10 | 0.53415 |
| Block Frequency | 10/10 | 0.35049 | 10/10 | 0.00204 | 10/10 | 0.00200 | 10/10 | 0.00200 |
| Cumulative Sums \( S_1 \) | 8/10 | 0.00000 | 7/10 | 0.00000 | 8/10 | 0.00000 | 10/10 | 0.53415 |
| Cumulative Sums \( S_2 \) | 6/10 | 0.00000 | 7/10 | 0.00000 | 8/10 | 0.00000 | 10/10 | 0.35049 |
| Runs | 8/10 | 0.00000 | 6/10 | 0.00000 | 6/10 | 0.00000 | 5/10 | 0.00000 |
| Longest Run | 9/10 | 0.01791 | 0/10 | 0.00000 | 10/10 | 0.21331 | 10/10 | 0.53415 |
| Range | 10/10 | 0.00000 | 10/10 | 0.00000 | 10/10 | 0.00000 | 10/10 | 0.00000 |
| FFT | 10/10 | 0.00000 | 10/10 | 0.00000 | 10/10 | 0.00000 | 9/10 | 0.00000 |

Figure 5: FPGA floor-plans with both clustered and distributed MeLPUF layouts. We performed experimental measurements with four different levels of spatial distribution of the PUF elements to analyze the effect of PUF cell placements.

Table 3: Average hamming distance between chip instances for a range of voltages.

| Voltage | 1.8V | 2.0V | 2.2V | 2.4V | 2.6V | 2.8V |
|---------|------|------|------|------|------|------|
| Intra-TFF | 2.2±2 | 2.7±4 | 2.3±3 | 2.5±4 | 2.1±3 | 1.8±3 |
| Inter-TFF | 2.6±2 | 2.6±4 | 2.4±3 | 2.4±3 | 2.2±3 | 1.8±3 |

[3] X. Wang A. R. Krishna, S. Narasimhan and S. Bhuina. 2011. MECCA: arboost low-overhead PUF using embedded memory array. In CHES 407–420.
[4] M. van Dijk B. Gassend, D. Clarke and S. Devadas. 2002. Silicon physical random functions. In Proceedings of the 9th ACM conference on Computer and communications security. New York, NY, USA, 148–160.
[5] A. Babaei and G. Schiele. 2019. Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges. Sensors (Basel) 19, 14 (July 2019).
[6] L. Santiago et al. 2017. Realizing strong PUF from weak PUF via neural computing. In IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 1–6.
[7] W. Liu et al. 2019. XOR-Based Low-Cost Reconfigurable PUFs for IoT Security. ACM Trans. Embed. Comput. Syst. 18, 3 (June 2019), 1–21.
[8] A. Dawoud M. Niamat F. Amsaad, A. Sherif and S. Kose. 2018. A Novel FPGA-implmentation of a PUF implemented as 32 × 32-bit clusters.
[9] J. Zhou J. Gan and N. Wang. 2018. A FPGA-based RO PUF with LUT-Based PUF for FPGA. In Proceedings of the 2018 IEEE International Symposium on Circuits and Systems (ISCAS). 77–80.
[10] T. M. Bauer J. R. Hamlet and L. G. Perison. 2014. Deterrence of Device Counterfeiting, Cloning, and Subversion by Substitution Using Hardware Fingerprinting. In MIT CSAIL CSG Technical Memo 481 (2004).
[11] B. Gassend G. E. Suh M. van Dijk J. W. Lee. Daihyun Lim and S. Devadas. 2004. A technique to build a secret key in integrated circuits for identification and authentication applications. In Symposium on VLSI Circuits. Digest of Technical Papers. 176–179.
[12] J. Jang and S. Ghosh. 2015. Design and analysis of novel SRAM PUFs with embedded latch for robustness. In Sixteenth International Symposium on Quality Electronic Design. 298–302.